ACADEMIA MILITAR

DIREÇÃO DE ENSINO

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

CYBER INTELLIGENCE
A OBTENÇÃO DE INFORMAÇÕES A PARTIR DE FONTES ABERTAS NO CIBERESPAÇO

Óscar Luís Soeiro Frias

Dissertação/Trabalho de Projeto para a obtenção do grau de

Mestre em Guerra de Informação

Lisboa

2013

ACADEMIA MILITAR

DIREÇÃO DE ENSINO

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

CYBER INTELLIGENCE
A OBTENÇÃO DE INFORMAÇÕES A PARTIR DE FONTES ABERTAS NO CIBERESPAÇO

Óscar Luís Soeiro Frias

Dissertação de Mestrado em Guerra de Informação

Trabalho realizado sob a supervisão:

Doutor Paulo Fernando Viegas Nunes

Lisboa

2013

DEDICATÓRIA

Aos meus pais, Luís e Natália. Sempre presentes!

À minha esposa e à minha filha.

AGRADECIMENTOS

A realização desta Dissertação de Mestrado é mais uma etapa na minha formação pessoal e profissional e só foi possível graças à colaboração e ao contributo de várias pessoas. Gostaria de exprimir algumas palavras de agradecimento, na expectativa de não os ter desiludido de forma alguma. Agradeço em particular:

ao Senhor Professor Doutor Tenente Coronel Paulo Fernando Viegas Nunes, por ter aceite, desde o início, orientar a minha tese. Agradeço-lhe, sobretudo, por toda a amabilidade e acompanhamento ao longo não só da realização desta tese, bem como do meu percurso académico. Espero que a minha prestação tenha correspondido às suas expectativas.

ao Senhor Tenente Coronel Gonçalves e ao Tenente Coronel Lima Alves, que me permitiram o acesso a informação bastante útil e me transmitiram valiosos conhecimentos. Agradeço o contributo, assim como, a amabilidade e disponibilidade dedicadas.

ao Senhor Professor Doutor Pedro Borges Graça pela agradável conversa, de onde surgiram novas perspetivas de abordar o tema e que contribuíram, de forma indiscutível, para a valorização do mesmo. Um forte agradecimento pela disponibilidade e atenção.

à Senhora Major Fátima Nunes Bento e ao Senhor Major Pedro Pimentel pela pronta disponibilidade e sugestões que me fizeram, as quais contribuíram para a introdução de consideráveis melhorias.

ao Exército Português e militares presentes no exercício do Exército "Ciber Perseu 2013", pela oportunidade de participar no evento e que muito contribuiu para a realização deste estudo. Foi sem dúvida um marco importante na consecução desta prova.

a todos os meus professores e aos meus camaradas da 2.ª Edição do Curso de Mestrado em Guerra de Informação, com quem tive a oportunidade de partilhar conhecimentos e por quem tenho enorme estima e consideração.

ao meu amigo, de longa data, Rui Amorim e à sua família, pela amizade, incentivo e contributo imensurável na minha formação pessoal e profissional.

à minha família e amigos pelo apoio incondicional, em especial ao meu irmão e à minha irmã, pelo constante encorajamento, à minha tia Alegria e ao meu tio José Manuel, aos meus sogros pelo apoio e compreensão inestimáveis.

à minha esposa, Sandra Gonçalves, pelos diversos sacrifícios suportados, pelas muitas ausências e pelas revisões incansáveis. Obrigado por tudo.

RESUMO

Na sequência do desenvolvimento de estratégias de segurança e defesa no ciberespaço, surgiu a necessidade de Portugal desenvolver a sua própria Estrutura Nacional de Cibersegurança, de modo a fazer face às exigências internacionais, ao nível económico, político e militar.

Desta forma, o Conceito Estratégico de Defesa Nacional**,** aprovado a 21 de março de 2013, em Conselho de Ministros, confirma a relevância da obtenção de informações no ciberespaço pelo caráter imprevisível, multifacetado e transnacional das novas ameaças e preconiza a edificação, ao nível das Forças Armadas, de uma capacidade de Ciberdefesa.

Tendo em consideração o binómio Segurança e Defesa, a condução de operações de gestão de crises no ciberespaço é fortemente influenciada pela forma como é realizada a gestão de informação aberta e como é efetuada a sua utilização (des)cuidada, neste novo domínio de interação de natureza virtual. Assim, é fundamental que exista uma cooperação interinstitucional civil-militar, baseada num ciberespaço livre, aberto e seguro, de forma a garantir uma decisão mais informada e eficaz.

O presente trabalho aborda a obtenção de informações através de fontes abertas no ciberespaço, inserindo-se o tratamento deste tema na mudança do paradigma da aplicação/ adaptação dos conceitos de Segurança e de Defesa, à Era da Informação. Neste âmbito, procura-se equacionar a recolha de informações e produção do conhecimento situacional sobre as ciberameaças, no contexto da tomada de decisão em situações de gestão de crises, melhorando a resiliência nacional no ciberespaço.

Face aos desafios e ameaças emergentes neste novo ambiente de interação global, a Ciberdefesa representa um novo desafio para a Segurança Nacional dos Estados e para a condução eficaz das operações de gestão de crises, reunindo para esse efeito capacidades civis e militares, que devem trabalhar em conjunto para atingir um objetivo comum.

O objetivo do presente trabalho está centrado no desenvolvimento de um modelo proactivo e preventivo de informações, capaz de reforçar a capacidade de recolha e análise de informações no ciberespaço e de integrar, em tempo oportuno, a informação obtida na condução das operações de Ciberdefesa. Esta atividade deve, ainda, intercetar e negar as atividades de informações conduzidas por terceiros.

Palavras-chave: Ciberespaço, Ciberdefesa, Cibersegurança, Defesa, Segurança, Informações de Fontes Abertas, Gestão de Crises.

ABSTRACT

Along with the development of national cyber security and cyber defence strategies, Portugal felt the urgency to develop it's own National Cyber Security Structure in order to face international demands on economic, political and military levels.

The National Strategic Defence Concept, approved on March 21st 2013 by the cabinet council, emphasizes the Cyber Intelligence relevance regarding the new threats, as they are unpredictable and transnational, advocating the creation of cyber defence capabilities by the Armed Forces.

Considering Security and Defence binomial, the cyber crisis management operations are strongly influenced by the way open source information is processed and how is (un)carefully used in this new domain of interaction of virtual nature. So it is of the upmost importance that civil-military inter-institutional cooperation thrives based on an open, free and safe cyberspace, in order to insure an informed and effective decision-making.

This paper addresses the open source intelligence gathering through cyberspace, by inserting the treatment of this theme in the changing paradigm of the security and defence concepts application/adaptation, to the Information Age. In this perspective, consider collecting information and situational awareness production about the cyber threats in the context of decision making in crisis management situations, improving the national resilience in cyberspace.

Facing the challenges and emerging threats in this new environment of global interaction, Cyber defence represents a new challenge for homeland security and for the effective crisis management operations, gathering civil and military skills that should work together to attain a common goal.

This paper is focused on the development of a proactive and preventive Cyber Intelligence Model, capable of reinforcing the Cyber Intelligence collect and analysis capabilities and integrate them, on time, in the Cyber defence operations. This activity should also be able to intercept and deny the information conducted by others.

Key-words: Cyberspace, Cyber defence, Cyber Security, Defence, Security, Cyber Intelligence, Crisis Management.

LISTA DE ABREVIATURAS E ACRÓNIMOS

ADNI	*Deputy Director of National Intelligence*
ADNI-OS	*Deputy Director of National Intelligence for Open Source*
AED	Agência Europeia de Defesa
AFCEA	Associação para as Comunicações, Eletrónica, Informações, e Sistemas de Informação para Profissionais
AJP	*Allied Joint Publication*
AM	Academia Militar
APDSI	Associação para a Promoção e Desenvolvimento da Sociedade da Informação
C2	*Command and Control* (Comando e Controlo)
CCDP	*Compreensive Capability Development Plan*
CCIR	Requisitos de Informações Críticas do Comandante
CDP	*Capability Development Plan*
CDS	*Content Delivery System*
CE	Comissão Europeia
CEDN	Conceito Estratégico de Defesa Nacional
CEGER	Centro de Gestão Informática do Governo
CEMGFA	Chefe de Estado-Maior General das Forças Armadas
CEO	*Chief Executive Officer*
CERT	*Computer Emergency Response Team* (conhecido por Serviço de Resposta a Incidentes de Segurança Informática)
CFT	Comando das Forças Terrestres
CIIP	*Critical Information Infrastructure Protection*
CIIWA	*Competitive Intelligence & Information Warfare Association*
CINAMIL	Centro de Investigação da Academia Militar
CIRT	*Cyber Intelligence & Response Technology*
CIS	*Communications and Information Systems* (Sistemas de Comunicação e Informação)
CISMIL	Centro de Informações e Segurança Militares
CMO	*Crisis Management Operations* (Operações de Gestão de Crises)

CNA	*Computer Network Attack*
CND	*Computer Network Defense*
CNE	*Computer Network Exploitation*
CNO	*Computer Network Operations*
CRIT	Serviço de Resposta a Incidentes de Segurança Informática na área de Investigação
CRP	Constituição da República Portuguesa
CRS	*Congressional Research Service*
CSDP	*Common Security and Defense Policy*
CSI	Comunicações e Sistemas de Informação
CSIRT	Rede nacional de serviços de resposta a incidentes de segurança informática
CSO	*Chief Security Officer*
CYBER INTEL	*Cyber Intelligence* (Obtenção de informações a partir de fontes abertas no ciberespaço)
DLP	*Data Loss Prevention*
DHS	*Department of Homeland Security* (Departamento de Segurança Interna)
DI2E	*Defense Intelligence Information Enterprise*
DNI	*Director of National Intelligence* (Departamento de Informações Nacionais)
DOA	*Department of Army* (Exército norte-americano)
DOD	*Department of Defense* (Departamento de Defesa)
DR	Diário da República
EEAS	*European External Action Service*
EIN	Estratégia da Informação Nacional (Seminário Anual da Academia Militar)
ELINT	*Electronics Intelligence*
ENC	Estratégia Nacional de Cibersegurança
ENISA	*European Network and Information Security Agency*
ENSI	Estratégia Nacional de Segurança da Informação
EUA	Estados Unidos da América
EXCON	*Exercise Control*

EXPLAN	*Exercise Plan*
EW	*Electronic Warfare* (Guerra Eletrónica)
FA	Forças Armadas
FBSI	*Foreign Broadcast Service Information*
FGI	Fórum sobre a Governação da *Internet*
FPOBE	Ferramenta de Planeamento Operacional Baseada em Efeitos
GEOINT	*Geospatial Intelliegence*
GNS	Gabinete Nacional de Segurança
HUMINT	*Human Intelligence*
IA	*Information Assurance*
IC	*Intelligence Community* (Comunidade de Inteligência)
IDN	Instituto de Defesa Nacional
IDS	*Intrusion Detection System*
INFOSEC	*Information Security* (Segurança da Informação)
INSA	*Information Network Security Agency*
IP	*Internet Protocol*
ISCSP	Instituto Superior de Ciências Sociais e Públicas
ISE	*Information Sharing Environment*
JAPCC	*Joint Air Power Competence Centre*
JP	*Joint Publication*
M4IS	*Multinational, Multiagency, Multidisciplinary, Multidomain Information-Sharing*
MASINT	*Measurements and Signatures Intelligence*
MGI	Curso de Mestrado em Guerra de Informação
MNIOE	*Multinational Information Operations Experiment*
NAC	*North Atlantic Council* (Conselho do Atlântico Norte)
NATO	*North Atlantic Treaty Organization*
NBD	*Network Block Device*
NOSC	*National Open Source Center* **(**Centro Nacional de Fontes Abertas)
OCS	Órgãos de Comunicação Social
ODNI	*Office of the Director of National Intelligence* (Gabinete do Departamento de Informações Nacionais)
OI	Operações de Informação (*Infornation Operations*)

ONG	Organização Não-Governamental
ONU	Organização das Nações Unidas
OPSEC	*Operations Security*
OSINT	*Open Source Intelligence* (Informações de Fontes Abertas)
OSINT-V	*Validated Open Source Intelligence*
OSC	*Open Source Center* **(**Centro de Fontes Abertas)
OSD	*Open Source Data*
OSI	*Open Source Information*
OSS	*Open Source Solutions*
OVL	Organizações, Valores e Liderança (Seminário Anual da Academia Militar)
OTAN	Organização do Tratado do Atlântico Norte
PALOP	Países Africanos de Língua Oficial Portuguesa
PCSD	Política Comum de Segurança e Defesa
PDC	Plano de Desenvolvimento de Capacidades
PESD	Política Europeia de Segurança e Defesa
PESC	Política Externa e de Segurança Comum
PfP	*Partners for Peace* (países parceiros não-OTAN)
PSYOPS	*Psychological Operations*
PIR	*Priority Intelligence Requirements*
RCM	Resolução de Conselho de Ministros
RFI	*Requirement For Information* **(**Pedidos de informação)
SIGINT	*Signals Intelligence*
SIRP	Sistema de Informações da Republica Portuguesa
SIS	Serviços de Informações de Segurança
SRC	*Syracuse Research Corporation*
UC	Unidade Curricular
UE	União Europeia
TI	Tecnologias de Informação
TIC	Tecnologias de Informação e Comunicação
VPN	*Virtual Private Network* **(**Rede Privada Virtual)
WWW	*World Wide Web*
XML	*eXtensible Markup Language*

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABELAS

Introdução

1.1. Enquadramento do Tema

> *"Se conheces o inimigo e te conheces a ti próprio, não precisas temer o resultado de cem batalhas. Se te conheces a ti próprio, mas não conheces o inimigo, a cada vitória ganha sofrerás também uma derrota. Se não conheces nem o inimigo nem a ti próprio, vais sucumbir em cada batalha."* (Sun Tzu)

Os novos sistemas de comunicações e a *Internet* tornaram-se multiplicadores de forças, na terra, no mar, no ar e no ciberespaço (Radabaugh, 2012:62). A globalização e a *Internet* permitem o acesso público à informação e ao conhecimento, algo que os serviços de segurança e os governos antes viam como um acesso a informações secretas (INSA, 2011).

A génese deste estudo recai, em particular, sobre as operações destinadas a obter Informações de Fontes Abertas (OSINT), refletindo sobre a forma como estas operações evoluíram no tempo, influenciadas pelo crescente desenvolvimento tecnológico, registado no domínio do ciberespaço.

Neste domínio, falamos da *Internet* e de como a necessidade exponencial de troca e partilha de informação deu origem a serviços, agora segregados na denominada "computação em nuvem"[1], que potenciam a vantagem competitiva das empresas, desenvolvendo áreas como o: *eCommerce*, *eGovernment*, *eBusiness* e *eStrategy*.

Face ao exposto, este estudo pode servir de alavanca para estimular o enfoque nacional neste domínio e reunir condições para o desenvolvimento de uma Estrutura Nacional de Cibersegurança (ENC), melhorando a resiliência das infraestruturas de informação, através da salvaguarda da sua Cibersegurança/ Ciberdefesa e garantindo assim uma gestão de crises mais eficaz.

Daí o particular interesse em contribuir com este estudo para, através da obtenção de informações, tornar mais eficaz o processo de decisão, associado à defesa e proteção das infraestruturas de informação crítica nacionais e, por outro lado, contribuir para a utilização livre, segura e eficiente do ciberespaço.

[1] Esta denominação, também conhecida em inglês por *Cloud Computing*, refere-se à ideia de se utilizar, em qualquer lugar e independente da plataforma, as mais variadas aplicações, através da *Internet*, com a mesma facilidade de estarem instaladas em qualquer computador (ver também, definição no Apêndice I - Glossário).

Qualquer agência do governo que tenha necessidade de pesquisar, através de fontes abertas, por exemplo na *Internet*, deve implementar um programa seguro e global "não-atributivo"[2], para minimizar as vulnerabilidades cibernéticas e maximizar as oportunidades de pesquisa, através de fontes abertas (Radabaugh, 2012). Assim, pode ocorrer uma alteração da perspetiva e do entendimento dos conceitos de Segurança e Defesa, dando origem a transformações, não só, no domínio político estratégico como, também, na própria ENC.

Perante este fenómeno, julga-se útil e pertinente compreender de que forma a obtenção de informações a partir de fontes abertas no ciberespaço (*Cyber Intelligence*) poderá fortalecer a capacidade de Cibersegurança e Ciberdefesa nacional, tornando a nova estrutura mais eficiente em termos operacionais e favorecendo a participação em projetos multinacionais, facto que facilita a convergência e a satisfação das exigências europeias e internacionais.

Desta forma, a *Cyber Intelligence* será responsável pela análise e exploração da informação, dita de fontes abertas, e pelo seu posterior contributo para o conhecimento atempado das respetivas ciberameaças, colmatando, assim, uma falha na leitura e avaliação do espectro das ameaças, emergentes do ciberespaço. Por outras palavras, a *Cyber Intelligence*, deve garantir a gestão de informação aberta, a utilização das demais extensões do ciberespaço, de forma a assegurar uma decisão mais informada e eficaz.

De modo a desenvolver este tema, de forma clara, e responder às questões a ele subjacentes a seguir enunciadas, o trabalho encontra-se dividido em duas partes distintas. Numa primeira parte, é feita a descrição da metodologia adotada, o enquadramento teórico, a contextualização nacional e internacional, segundo várias perspetivas, e a apresentação resumida da revisão de literatura. Numa segunda parte, é elaborada uma proposta de modelo de *Cyber Intelligence*, aplicável à gestão de crises no ciberespaço, em cinco etapas distintas: breve revisão de alguns modelos de *Cyber Intelligence*, descrição geral do modelo proposto, análise das variáveis chave e das suas condições, validação e revisão do modelo apresentado, com auxílio a entrevistas e de um trabalho de campo, num exercício de Ciberdefesa. Por fim, conclui-se o estudo com algumas considerações finais, recomendações e proposta de trabalhos futuros.

[2]Adoção de uma abordagem "não-atribuível" do perfil cibernauta, para minimizar a pegada digital, isto é, quem tenta esconder-se no ciberespaço torna-se suspeito, por isso, o melhor é ser impercetível (Radabaugh, 2012).

1.2. Metodologia da Investigação

A metodologia utilizada neste trabalho baseia-se no método de investigação de Quivy e Campenhoudt (2008), composto por três etapas (rutura, construção e verificação), interligados e subdivididos em sete fases interativas, mas com carácter retroativo, conforme figura apresentada no Apêndice II.

Para definir a pergunta de partida, o estudo começa com uma fase de exploração, das principais envolventes do tema central do presente trabalho, as informações recolhidas no ciberespaço (*Cyber Intelligence*). A pesquisa inicia-se através da recolha de dados e de informação adicional consubstanciada, essencialmente, em três relatórios da Agência Europeia de Defesa (AED): "*A Stock Take of Capabilities for Cyber Defence in the military domain (milCyberCAP)*"(2011); *"Cyber Intelligence for EU-led Operations (CyTelOPS)"*(2012); e *"A Framework Contract on developing cyber defence capabilities for the military (frameCyberCAP)"*(2012).

Após esta exploração inicial do tema, surge a questão de partida e são enumeradas as questões derivadas e as hipóteses da problemática, que terão de ser verificadas e testadas posteriormente. Nesta fase o que se pretendeu essencialmente fazer foi enquadrar e relacionar metodologicamente a *Cyber Intelligence* com as áreas da Segurança, Defesa, Política, Tecnologia, Indústria e Economia, embora estas duas últimas áreas sejam abordadas de um modo menos profundo, designadamente através de relatórios e outras publicações elaboradas por entidades governamentais e organizações internacionais.

Através de várias perspetivas, nacionais e internacionais, governamentais e privadas, é possível obter uma investigação interdisciplinar. A revisão de literatura e a definição do estado da arte fica completo com uma pesquisa e análise comparativa dos modelos de *Cyber Intelligence* identificados.

Após esta primeira etapa (a rutura), foi construída e apresentada uma proposta de modelo de *Cyber Intelligence*, com base na pesquisa anterior e sujeita a validação e revisão. Na terceira etapa da investigação, a verificação, o processo divide-se em vários passos que culminam com a verificação e avaliação da proposta de modelo, através da observação no campo operacional. A recolha de dados e a validação é efetuada através da criação de uma célula de *Cyber Intelligence* no exercício anual de Ciberdefesa do Exército "Ciber Perseu 2013" e de entrevistas realizadas a alguns especialistas da matéria.

Depois da análise dos dados recolhidos e respetiva revisão do modelo, são apresentadas as conclusões, finalizando assim a última etapa da metodologia de Quivy e Campenhoudt.

1.2.1. Objetivos da Investigação

O objetivo do presente trabalho está centrado na criação de um modelo de *Cyber Intelligence*, isto é, na criação de um conjunto de passos que, de forma proactiva e preventiva, permite obter informações através de fontes abertas no ciberespaço. Conforme antes referido, esta investigação enquadra-se na problemática associada à mudança do paradigma referente aos conceitos tradicionais de Segurança e de Defesa, quando pespetivados no contexto da Era da Informação.

O estudo tem em conta as investigações já existentes, ou em curso, nomeadamente, as que decorrem no âmbito do processo de desenvolvimento de capacidades da União Europeia (UE), cuja coordenação compete à AED.

Assim, pretende-se não só reforçar e dar visibilidade ao tema, mas sobretudo demonstrar que esta matéria tem uma importância fulcral para a construção de um futuro projeto orientado para a Cibersegurança de Portugal, atendendo neste processo ao trabalho já desenvolvido pelo Gabinete Nacional de Segurança (GNS), nomeadamente, a definição da ENC.

O presente estudo, em particular, irá contribuir para a definição de orientações, de forma a melhorar o conhecimento situacional de Ciberdefesa[3] e fortalecer os mecanismos atuais e futuros de combate contra as ciberameaças.

Desta forma, uma vez que Portugal é membro da UE e terá que participar num esforço cooperativo na área da Cibersegurança e Ciberdefesa, esta investigação têm também como propósito desenvolver uma abordagem das operações de *Cyber Intelligence,* estruturada com base em normas e procedimentos comuns, tanto no âmbito nacional, como da UE, no âmbito da *Cyber Threat Intelligence*.

Assim, respeitando os princípios adotados pela arquitetura e modelo da UE, este estudo pretende contribuir para ampliar o conhecimento sobre as ciberameaças e melhorar a resiliência nacional, no domínio do ciberespaço (AED, 2012)[4].

Em suma, a Ciberdefesa representa um novo desafio para a Segurança Nacional dos Estados e para a condução eficaz e segura das Operações de Gestão de Crises (CMO), reunindo para esse efeito capacidades civis e militares que, de forma sinérgica, devem trabalhar em conjunto para atingir um objetivo comum.

[3] Tradução do autor de "*Cyber Defence Situational Awareness".*
[4] Projeto da AED, intitulado de *"Cyber Intelligence for EU-led Operations (CyTelOPS)"*.

A informação que circula na *Internet*, relativa a redes sociais, "partilha de vídeos" e "blogosfera", necessita de controlo e regulação, defesa preventiva e resiliência. A complexidade associada tanto ao assunto como aos processos de interação, muito influenciados por fatores internos e externos, impõe que seja adotada uma abordagem integrada[5], a fim de harmonizar as ações militares, com qualquer outra atividade desenvolvida no âmbito civil e institucional.

1.2.2. Formulação do Problema

A obtenção de informações a partir de fontes abertas foi muitas vezes negligenciada e até remetida para segundo plano durante muitos anos. Contudo, a emergência da *Internet* colocou esta área de estudo no primeiro patamar no que respeita à recolha e armazenamento de informação (Best e Cumming, 2007).

A escolha do presente tema prende-se, essencialmente, com duas importantes iniciativas em curso. A primeira está ligada à necessidade de dotar Portugal de uma ENC, contribuindo para uma Política Comum de Segurança e Defesa (PCSD) do ciberespaço, atendendo aos compromissos internacionais assumidos. A segunda diz respeito à iniciativa da construção de uma "Agenda Digital" europeia[6], que diz ser imprescindível o empenho e contribuição de cada Estado-membro, face aos desafios da Ciberdefesa e da Cibersegurança.

A relevância do tema *Cyber Intelligence*, decorre das atuais questões relacionadas com os conceitos de Segurança e de Defesa quando equacionados nas relações internacionais no ciberespaço e, simultaneamente, com a necessidade de Portugal dotar os seus decisores políticos com mecanismos mais capazes de responder aos requisitos internos e externos, da Ciberdefesa e da Cibersegurança. Este é um tema indispensável para o Estado mas, também para o setor privado, uma vez que é função do Estado preservar a Segurança Interna e preparar as suas Forças Armadas (FA), para responder às necessidades emergentes de Defesa e de Segurança no ciberespaço, e é o setor privado quem disponibiliza as Tecnologias de Informação e Comunicação (TIC) utilizadas.

O interesse neste trabalho é utilizar o conceito tradicional de informações e aplicá-lo, especificamente, ao serviço da *Cyber Intelligence*. As organizações são, constantemente, confrontadas com a necessidade de atualização deste contexto de aplicações. Com um

[5] Tradução do autor de "*comprehensive approach*".

[6] Enquadrada na estratégia "Europa 2020", que afirma como objetivo o estímulo da economia digital e a resposta aos desafios sociais, através das Tecnologias de Informação e Comunicação.

pouco de imaginação é possível traçar um cenário para este efeito: um jornalista teve acesso a informação privilegiada, obtida a partir de fontes abertas no ciberespaço, como por exemplo, na "Blogosfera", de carácter político, comercial, financeiro e resolve publicá-la. Quais são as consequências desse ato? Como proteger as fontes? Como validar a informação? E o que fazer para esclarecer a opinião pública?

Tendo em consideração o ciberespaço e o binómio Segurança/Defesa, a condução de operações de gestão de crises é fortemente influenciada pela forma como é realizada a gestão de informação aberta e como é efetuada a sua utilização no ciberespaço. Por essa razão, é fundamental que exista uma cooperação, de carácter interinstitucional civil-militar, ou de carácter público-privada, de forma a garantir uma decisão mais informada e segura. Deste modo, julga-se que a *Cyber Intelligence* é uma ferramenta fundamental para uma gestão de crises mais eficiente e eficaz.

Tendo em vista os objetivos a atingir com este trabalho, o método utilizado na investigação foi o método dedutivo, isto é, partiu-se de uma abordagem geral para o particular, onde a questão central do presente trabalho é: "Como poderão as informações de fontes abertas no ciberespaço melhorar a Cibersegurança/ Ciberdefesa nacional, garantindo assim que, através de uma adequada gestão de informação, a cooperação interinstitucional contribua para uma gestão de crises mais eficaz?"

Desta questão central derivam outras questões, às quais se pretende responder ao longo do presente trabalho:

- Como pode a *Cyber Intelligence* minimizar os riscos e potenciar as oportunidades que a *Internet* oferece?
- Como tornar a *Cyber Intelligence* uma ferramenta indispensável para assegurar os serviços providenciados pela *Internet* e garantir a confiança dos seus utilizadores?
- De que forma a cooperação interinstitucional garante uma decisão mais informada e segura, permitindo a gestão de crises mais eficaz?
- Será possível definir um modelo de gestão de informação interinstitucional integrado (órgãos do Estado e setor privado) no ciberespaço, capaz de melhorar a resiliência nacional, face à ocorrência de ciberataques?

1.2.3. Limitações e Dificuldades

A primeira dificuldade identificada, que se traduziu numa importante limitação na fase do projeto de investigação, foi a frequência de cursos de índole profissional (militar), nomeadamente o Curso Básico de Comando, na Academia da Força Aérea.

Na sequência desta, outra das grandes limitações sentidas foi a vasta literatura, nacional e internacional, relativa ao ciberespaço e à Cibersegurança/ Ciberdefesa. Estes temas encontram-se em permanente evolução, surgindo notícias, artigos e publicações, quase todos os dias, um pouco por todo o mundo. Tratando-se de um tema contemporâneo exigiu um esforço de acompanhamento contínuo, quase permanente.

Outra das dificuldades prendeu-se com a revisão dos modelos de *Cyber Intelligence.* Quando falamos de *Open Source Intelligence* (OSINT), ainda que se reconheça existirem dificuldades na sua operacionalização, não é difícil encontrar alguém ou mesmo instituições com conhecimentos na área. Contudo, importa também referir que quando se fala de ciberespaço, existe ainda alguns preconceitos relacionados com esta temática, encarando-a com uma realidade ligada à "ficção científica". Este facto acabou por se revelar um verdadeiro desafio na escolha de modelos e empresas que praticam *Cyber Intelligence*, de forma estruturada e credível, nomeadamente na realização de entrevistas.

As dificuldades sentidas com a revisão de literatura prenderam-se também com a escassa produção científica no âmbito da *Cyber Intelligence* e em particular no nosso país. Por essa razão, a escolha dos modelos a analizar limitou-se a empresas reconhecidas internacionalmente (como por exemplo a *Deloitte*) e a metodologias seguidas no âmbito de operações militares, como é o caso dos manuais OSINT da Organização do Tratado do Atlântico Norte (OTAN).

1.2.4. Cronograma

No âmbito da estruturação da investigação, foram definidas as seguintes fases do trabalho:

- Fase 0 – Análise exploratória de dados e recolha de informação.

Esta fase envolve a elaboração do projeto de investigação propriamente dito. Nesta fase, teve lugar a recolha de informação relativa à temática a investigar e a sua posterior análise exploratória.

- Fase 1 – Revisão de Literatura e definição do Estado da Arte.

Neste âmbito, teve lugar a análise de outras possíveis abordagens ao tema consubstanciado, em estudos anteriores, assim como a análise contextualizada dos resultados entretanto

obtidos. As abordagens enunciadas foram sistematizadas segundo o seu autor, ideia principal e resultado obtido.

- Fase 2 – Análise das variáveis-chave e contextualização do tema.

Nesta fase, foi realizada a identificação e caracterização mais detalhada do contexto da investigação e identificadas e delimitadas as respetivas variáveis-chave.

- Fase 3 – Criação do Modelo.

Com base nas variáveis-chave identificadas, foi construído um modelo operacional para a condução de *Cyber Intelligence*, promovendo-se a articulação entre fontes, ferramentas e efeitos a obter no processo da sua condução.

- Fase 4 – Validação do Modelo (aplicação/ casos práticos).

Nesta fase, teve lugar a aplicação do modelo, através de um caso prático aplicado no exercício anual de Ciberdefesa do Exército.

- Fase 5 – Revisão do Modelo.

Com base nos resultados obtidos na fase 4, promoveram-se os ajustes considerados necessários ao modelo inicial.

- Fase 6 – Conclusões, recomendações e trabalhos futuros.

Nesta fase procura-se sistematizar os resultados da investigação e referir alguns trabalhos futuros.

- Fase 7 – Redação da dissertação.

Na última fase, é elaborado o texto da dissertação, o resumo e realizada a revisão geral do trabalho.

1.2.5. Corpo de Conceitos

Em primeiro lugar, é necessário definir informação e *Intelligence* e, desta forma, distinguir estes dois conceitos que formam um binómio paradigmático, no seio da língua portuguesa.
Conforme a doutrina OTAN, "os dados, quando recolhidos, aleatoriamente, têm pouca utilidade operacional, no entanto, quando recolhidos oportunamente, o seu formato é alterado e transformado, para que estes deixem se ser meros dados e passem a ser uma informação ou notícia" (DOA, 2012).
Por sua vez, da relação entre a informação recolhida e as experiências passadas, ou seja, "uma série de acontecimentos que, quando analisados e relacionados com outros eventos conhecidos de experiências passadas, permitem obter o que se pode denominar por *Intelligence"* ou Informações (DOA, 2012).

O termo *Intelligence* em Portugal é traduzido e, geralmente, é aplicado sob a designação de Informações. Já os brasileiros, por exemplo, traduzem o mesmo termo para "Inteligência". No entender da OTAN, *Intelligence* significa *"*O produto resultante do processamento de informações, relativas a Nações estrangeiras hostis, ou forças ou elementos ou áreas de operações potencialmente hostis. O termo também é aplicado na atividade que dá nome à *Intelligence* e a título genérico, naqueles que realizam o processo que conduz à sua produção*"* (DOA, 2012).

Concluindo, os dados, quando recolhidos, dão origem à informação. Esta informação quando processada transforma-se em informações. As informações são o resultado de uma previsão dos acontecimentos prováveis, na base da análise de situações idênticas no passado.

Quando se fala em informações é necessário distinguir quais são as suas fontes. As fontes são a principal "matéria-prima" das informações, e podem ser abertas, cobertas ou serviços congéneres, quanto à sua tipologia (Graça, 2012). "Em particular, as fontes abertas, perfazem 80-90% das informações obtidas", salienta Pedro Borges Graça (2012). No entanto, são várias as áreas responsáveis pela produção de informações, das quais se salientam a *Human Intelligence* (HUMINT), *Signals Intelligence* (SIGINT), *Electronics Intelligence* (ELINT), *Measurements and Signatures Intelligence* (MASINT), *Geospatial Intelliegence* (GEOINT) e a OSINT.

Sendo assim, a obtenção de informações a partir de fontes abertas (OSINT) define-se como a "produção de informações a partir da recolha de notícias e dados em fontes abertas ao público, excluindo-se formalmente a atividade ilegal da espionagem" (Graça, 2010).

Contudo, este é um conceito muito recente, visto que a OSINT tem vindo a reformular-se, ao longo da última década[7]. Atualmente, encontra-se em expansão e é um assunto de elevado interesse para os serviços de informações, civis e militares e para as revistas académicas da área dos *Intelligence Studies* (Graça, 2010).

No âmbito militar, a OTAN tem, inclusivamente, desenvolvido desde os finais de 2001, doutrina em torno deste conceito. Neste âmbito, a Aliança Atlântica tem já definido os conceitos subsidiários de *Open Source Data* (OSD) e *Open Source Information* (OSI), referindo-se ambos à informação em bruto antes de ser objeto de recolha e tratamento.

[7] Em Portugal não existe ainda uma Universidade investigação e ensino no campo dos *Intelligence Studies*. Esta é uma vulnerabilidade importante da nossa Defesa Nacional, entendida não como conceito institucional, mas como sociocultural, abrangendo a elite governante e não-governante, a opinião pública e sobretudo publicada (Graça, 2003).

A OTAN define, pois, a OSINT como "a informação que foi deliberadamente descoberta, identificada, destilada e disseminada por uma audiência selecionada, de modo a responder a uma questão específica" (OTAN, 2001:V).

Já o governo estadunidense, define OSINT como "*Intelligence* produzida a partir de informação publicamente disponível que é coletada, explorada e disseminada de maneira oportuna para um público adequado, com a finalidade de abordar um requisito específico de inteligência" (IC, 2006).

A definição de OSINT é hoje consensual e é transportada para o campo da gestão, ou seja, assume uma posição preponderante no tradicional ciclo da produção de informações, diretamente dependente da primeira linha da tomada de decisão. A *Internet* é hoje a principal ferramenta utilizada pelos analistas no que respeita às "fontes abertas".

> "Os meios de comunicação social (impressos, áudio e audiovisuais) estão aí presentes, e neste momento assiste-se ao surgimento constante de «motores de busca» cada vez mais especializados e eficazes que, por exemplo, abrem a possibilidade de se proceder a pesquisas temáticas abrangendo milhares de jornais de praticamente todos os países do mundo, com uma atualidade na ordem dos minutos, o que permite inclusivamente em tempo real ultrapassar a barreira da diferença horária mais dilatada" (Graça, 2003).

Por sua vez, "a *Internet* é um elemento central neste contexto, e em Portugal parece não existir ainda sensibilidade, ao nível das empresas para o seu potencial, enquanto fator de vantagem competitiva, via OSINT", diz o autor Pedro Borges Graça (2010).

Contudo, a *Internet* não é o ciberespaço. No seu uso mais rigoroso, o termo ciberespaço[8] designa hoje a "rede global de infraestruturas de tecnologias de informação (TI) interligadas entre si, especialmente as redes de telecomunicações e os sistemas de processamento dos computadores" (Fernandes, 2012).

Hoje em dia, emprega-se erradamente o termo *Internet* quando se dirige ao ambiente digital que permite a fonte, processamento e troca de informações. Esse ambiente é o ciberespaço, ou seja todos os sistemas de informação e os serviços e redes de comunicações eletrónicas.

Todavia, a *Internet* constitui um novo *media* complexo que contribui para a comunicação e integração de vários canais de comunicação convencionais, incluindo a rádio e televisão, numa rede interativa e global. É um fator de transformação social e das relações de poder,

[8] O termo original surge pela primeira vez mencionado na obra de William Gibson - "*Neuromancer*", de 1984, escritor de ficção científica. Cit. por Fernandes, José P. T. – "Utopia, Liberdade e e Soberania no Ciberespaço",2012.

transformando e, simultaneamente, sendo ela própria transformada pelas sociedades modernas, pelas organizações e pelos indivíduos (Nunes e Martins, 2006).

O conceito de *Cyber Intelligence* (ou CYBER INTEL) surge, assim, da necessidade de aplicar a OSINT no ciberespaço, visto que, hoje em dia, praticamente toda a informação, disponível publicamente, se encontra neste domínio. Contudo, esta disciplina é praticamente inexistente no seio das empresas e, geralmente, a procura de dados e informações fica a "cargo dos habilidosos e amadores da navegação, ou de alguém designado para o efeito, acumulando melhor ou pior, casuisticamente, informação bruta em folhas de papel em dossiês" (Graça, 2010).

Deste modo, é imprescindível dotar as empresas, assim como os serviços públicos, desde os organismos do Estado às infraestruturas críticas nacionais, de resiliência no ciberespaço. Como se pode ver, o Exército norte-americano define mesmo o conceito de "*Cyberspace Internet Awareness*" como sendo "todo o pessoal que realiza pesquisa de informações a partir de fontes abertas, deve estar ciente do ambiente operacional digital, minimizando e reduzindo as "pegadas digitais", praticando eficazmente "*Cyber OPSEC*", utilizando técnicas e hábitos seguros de navegação em linha, e entender que "*metadata"* incorporada pode estar presente nos documentos" (DOA, 2012).

Desta forma, surge a necessidade de dotar as organizações de "*Cyber Threat Intelligence"*:

> "Informações que estão diretamente relacionadas com vulnerabilidades ou ameaças, de um sistema ou rede de governo ou entidade privada, incluindo informações referentes à proteção de um sistema ou rede. Estas ameaças visam degradar, perturbar ou destruir esse sistema ou rede; ou então roubar ou apropriar-se indevidamente de informações privadas ou governamentais, propriedade intelectual ou informações de identificação pessoal" (H.R. 3523, 2012).

Por último, mas não menos importante, é relevante definir Ciberdefesa e Cibersegurança. Segundo a Constituição Republica Portuguesa (CRP)[9], a Defesa Nacional fica responsável, apenas, por garantir a segurança do Estado contra ameaças externas, enquanto que a segurança interna se dedica a combater as ameaças internas, de carácter não militar.

Contudo, com a emergência das interações e capacidades do mundo digital surge, também, um novo conceito de segurança global, na medida em que não existe apenas a segurança individual e nacional, criando, assim, a necessidade de redefinir o papel das FA, dos Serviços de Informações de Segurança (SIS) e das forças de segurança.

[9] Artigo 272.º e Artigo 273.º da CRP.

No domínio do ciberespaço, a Ciberdefesa pode ser considerada como a "defesa contra um cibertaque e mitigação de suas consequências, enquanto que a Cibersegurança é um conjunto de meios legais, organizacionais, tecnológicos e educacionais que têm como fim proporcionar a proteção do ciberespaço" (OTAN CCD COE, 2011:12).

O primeiro conceito está mais ligado ao conceito de Ciberguerra, quando se trata do uso de Sistemas de Comunicação e Informação (CIS) para desenrolar/desenvolver uma guerra no ciberespaço. O segundo conceito está relacionado com a "capacidade de proteger adequadamente a confidencialidade, integridade e disponibilidade dos CIS e as informações processadas, armazenadas ou transmitidas" (OTAN CCD COE, 2011:12).

Contudo, as diferenças entre estes dois conceitos são irrelevantes face aos objetivos comuns que as duas áreas possuem: "proteger as informações do governo, permitindo a defesa nacional, além de proteger as infra-estruturas críticas que entrepõem e impulsionam a economia global do século XXI" (OTAN CCD COE, 2011:13).

Sendo o Estado responsável por assegurar o correto funcionamento e a proteção das principais infraestruturas críticas nacionais, é necessário dotar-se de forças armadas e de segurança, capacitadas e prontas, para fazer face a situações de crise ou guerra no ciberespaço, que ponham em causa a segurança individual ou coletiva dos cidadãos.

A Associação para as Comunicações, Eletrónica, Informações, e Sistemas de Informação para Profissionais (AFCEA) entende que a gestão de crises é "o conjunto das atividades de gestão dos organismos de gestão de crises, com a finalidade de analisar e avaliar riscos de segurança e planeamento, organização, implementação e verificação das atividades realizadas em conjunto com a preparação para situações de crise e sua solução ou a proteção da infraestrutura crítica".

Por seu lado, a OTAN defende que "a capacidade nacional de gestão de crises pode estar intimamente ligada à troca de informação com parcerias público-privadas, (…) sendo condição necessária que todas as relações, entre os diversos atores estatais e não-estatais, sejam construídas sob uma base de confiança" (OTAN CCD COE, 2011:126).

2. Revisão de Literatura

2.1. Enquadramento Teórico

> *"O carácter imprevisível, multifacetado e transnacional das novas ameaças confirma a relevância das informações (...) As informações são um instrumento estratégico do Estado, essencial para o apoio à decisão política (...)"* (RCM n.º19/ 2013)

A sociedade depende fortemente do funcionamento, sem restrições, de infraestruturas de informação críticas. Os avanços das TIC abrem novas potencialidades, mas trazem, também, novas vulnerabilidades. Os ataques contra redes e infraestruturas críticas, representam uma nova ameaça que está em constante transformação. As ciberatividades maliciosas, conduzidas por grupos terroristas, organizações criminosas, indivíduos ou mesmo Estados, materializam-se em ações, com um potencial altamente perturbador ou mesmo destrutivo.

Esta ameaça evoluiu, principalmente a partir de operações de espionagem e exploração dos recursos de informação, que envolvem a usurpação de propriedade intelectual comercial, para operações sofisticadas de larga escala (como por exemplo, o "DUQU"[10] e o "FLAME"[11]). Estas atividades de espionagem e exploração da informação são destinadas a negar serviços, tais como os ataques de "*botnets-for-hire*"[12] de grande escala, que degradam a capacidade de operar, embora não infligindo danos físicos (Constantin, 2012). A destruição representa, possivelmente, a consequência mais danosa que a ciberameaça pode causar no adversário.

[10] *Malware* sofisticado e totalmente customizado, sucessor do *Stuxnet*, responsável por sabotar o programa nuclear iraniano (Constantin,2012).

[11] *Malware* modular que ataca computadores que operam o *Windows* da *Microsoft*. Programa usado para espionagem cibernética, sobretudo em países do Médio Oriente. Segundo a *Kaspersky*, em maio de 2012, o "FLAME" tinha infetado cerca de 1000 máquinas, incluindo organizações não-governamentais (ONG's), instituições de ensino e particulares (Constantin, 2012).

[12] Rede de aplicativos (*bots*), capaz de se comunicar com os invasores que o colocaram. O *bot* pode ser um programa independente, propaga-se pelo computador, cria redes e espalha conteúdo perigoso através dela (Constantin, 2012).

No passado recente, assistiu-se a operações deste género, que têm como alvo a infraestrutura industrial e os seus sistemas de controlo, como por exemplo o "STUXNET"[13], que causaram danos físicos, constituindo um verdadeiro exemplo deste novo tipo de ameaça.

Neste momento, os ciberataques já possuem capacidade para ameaçar a prosperidade, a segurança e a estabilidade nacional. Exemplo disso, é o processo de desenvolvimento de capacidades de Ciberdefesa da UE. Esta organização defende a necessidade de criar mecanismos para enfrentar uma ampla gama de atividades maliciosas, de forma a incluir a intrusão, a espionagem, a destruição e a corrupção de dados, mas também as ameaças internas e vulnerabilidades.

O crescimento exponencial e a sofisticação da ciberatividade maliciosa, bem como a velocidade a que ocorrem os eventos no ciberespaço, acentuam a necessidade de criar medidas preventivas e reativas, postas em prática pelo Estado, para garantir a realização eficaz de qualquer atividade civil e militar.

Determinadas vulnerabilidades estão ligadas à computação móvel, cada vez mais omnipresente, e à partilha de informação (tais como programas, sistemas operativos e redes), mas, também, estão interligadas a plataformas e sistemas totalmente digitalizados (veículos terrestres, aéreos e marítimos; sistemas de armas; munições; navegação), assim como aos seus componentes eletrónicos.

As tecnologias e os processos ligados à Ciberdefesa terão que garantir uma maior proteção, bem como, em termos de recursos, uma proteção mais "inteligente", para que possam ser tomadas as medidas mais adequadas, na resposta a incidentes ou ciberataques.

Paralelamente, no atual contexto internacional, as modernas tecnologias de informação são imprescindíveis para o cumprimento de qualquer missão militar (o comando, o apoio logístico, o controlo global de forças, a disponibilização de serviços de informação e informações, em tempo real e operações remotas). Cada uma dessas operações apresenta uma forte dependência na capacidade de garantir as comunicações globais das FA.

Em menos de uma geração, as TIC, no meio militar, evoluíram de uma ferramenta de gestão, responsável por melhorar a produtividade administrativa, para um vetor estratégico, determinante na condução de toda a atividade operacional. O ataque às infraestruturas digitais governamentais, é hoje, também, cada vez mais provável. O controlo sobre estas

[13] É um *worm* (vírus) que controla e monitora processos industriais e projetado especificamente para atacar o sistema de controlo industrial SCADA. "Um protótipo funcional e temível de uma arma cibernética, que dará início a uma nova corrida ao armamento mundial" (Constantin, 2012).

infraestruturas oferece, neste momento, vantagens críticas a qualquer adversário que lance um ciberataque bem sucedido. Porém, a confiança total depositada nas redes computacionais, também, permite que os adversários possam obter informações valiosas, sobre as intenções, capacidades e operações nacionais; incapacitar os movimentos das forças militares convencionais e afetar o funcionamento da economia.

O domínio das missões militares mudou drasticamente. As operações conjuntas e combinadas[14] conduzidas no domínio do ciberespaço, nomeadamente designadas por *Crisis Management Operations* (CMO), associadas à crescente participação de atores não-militares, constituem bons exemplos desta alteração recentemente registada com o surgimento do ciberespaço.

Os novos sistemas de armas exigem interconectividade entre as redes militares e civis, o que gera grandes vulnerabilidades, algo que os adversários vão querer explorar. Portanto, é necessário que os Estados estejam preparados para conduzir operações, quando a rede estiver indisponível. A guerra não acaba quando o computador se desliga (JAPCC, 2012).

Ao mesmo tempo, existe um aumento de pedidos de partilha de informação e dados, obrigando à definição de requisitos de troca e partilha de informação[15], para as infraestruturas de Comunicações e Sistemas de Informação (CSI).

Por outro lado, a "re-perimeterização" e a degradação das relações de confiança, que já acontecem no universo empresarial, são ampliadas e aceleradas pela "computação em nuvem". Os requisitos para a troca de informações estão a crescer, a tornarem-se cada vez mais complexos e evidenciam que o "perímetro militar" também mudou. O maior desafio que se perspetiva é o de definir a forma como se prepara uma Força, uma empresa ou mesmo um Estado, para lidar com um ambiente tão volátil. Ou seja, como se garante a segurança da informação na "nuvem", nas redes sociais ou nos "Blogs"?

O processo de decisão é altamente influenciado pela credibilidade das fontes de informação, isto é, deve-se sempre questionar a origem e as propriedades da informação. As fontes de informação são o "coração" desta questão, sabendo que a informação disponibilizada para o decisor tem que ser atual, completa e assertiva e, consequentemente, validada e protegida.

[14] Entende-se por operações conjuntas todas as operações que envolvam forças militares de mais que um ramo. Entende-se por operações combinadas todas as operações que envolvam forças militares de mais de um que um país (JP3-0, 2011).

[15] Tradução pelo autor de *Information Exchange Requirements.*

Todos os processos de relacionamento, comunicação e conhecimento são, hoje, intermediados por sistemas informatizados, como o correio eletrónico, os bancos de dados e os *softwares* de interação (Kujawski, 2003).

Muitas vezes, o crescimento mal estruturado das aplicações informáticas nas empresas, gerou um excesso de dados e informação, que coloca em risco a capacidade dos executivos em analisá-los e tomar decisões (Kujawski, 2003).

Desta forma, os requisitos para a troca de informações no dito domínio público/privado suscitam uma análise aprofundada, não por esta problemática ser novidade, no seio dos serviços de informações, mas sobretudo devido ao seu domínio de partilha. O ciberespaço é, hoje, caracterizado pela constante mudança e volatilidade, devido à emergência de contínuas necessidades de partilha de informação. Os requisitos de mais segurança e privacidade, ligados ao acesso aberto e global à informação, colidem muitas vezes com interesses associados de troca de informação privilegiada.

O crescimento da informação obtida por fontes abertas, ou OSINT, agora conhecida como a "fonte de primeira instância" deve-se à explosão de recursos de recolha de informação digital (Hlosek , 2012).

Os utilizadores precisam de encontrar soluções "não-atribuíveis" de *Internet*, diversas e mais eficazes, que sejam, também, ágeis o suficiente, para acompanhar a evolução das ciberameaças. Ao contrário das abordagens mais atuais, o objetivo dos analistas de OSINT de, hoje, não deve passar por ter um perfil anónimo, mas sim um perfil impercetível. A "não-atribuição" eficaz pode ser alcançada, quando os utilizadores de *Internet* aplicam uma abordagem, em múltiplas vertentes, que os ajuda a misturar-se impercetivelmente à *Web*, ao invés de tentarem esconder-se (Hlosek , 2012).

É de salientar, ainda, que qualquer agência do governo, que tenha necessidade de pesquisar na *Internet*, através de fonte aberta, deve implementar um programa seguro e integrado "não-atributivo", para minimizar as vulnerabilidades cibernéticas e maximizar as oportunidades de pesquisa, através de fonte aberta (Hlosek , 2012).

A "computação em nuvem" proporciona uma maior flexibilidade, menos custos e uma grande capacidade de realocar recursos. Segundo a *Delloite Development LLC*[16], muitas empresas consideram que um dos principais objetivos é disponibilizar serviços na

[16] A *Deloitte* é uma empresa sob a qual, cerca de 200 000 profissionais em empresas independentes de todo o mundo, colaboram na prestação de serviços de consultoria, auditoria, assessoria financeira, gestão de riscos e serviços fiscais.

"nuvem". A "nuvem" é considerada como um instrumento que gera vantagem competitiva empresarial, a par de outras vantagens, como a eficiência financeira.

Segundo a *Delloite*, é fundamental cumprir com 10 passos, no sentido de garantir uma maior eficácia no combate às ciberameaças. O décimo passo sugere, mesmo, que se deve "reconhecer que a eficácia da gestão de risco da ciberameaça, pode dar mais confiança à sua empresa para tomar certos riscos "compensados" para obter mais valor*"*(Deloitte, 2010).

O que se constata é que o setor privado está a adotar diferentes tipos de "computação em nuvem", e nesta fase é difícil prever o futuro, pois não existe um quadro comparativo com o passado.

É neste contexto que surgem as operações de OSINT. Este conceito, aparentemente recente, é definido pelo *Department of Defense* (DOD), como sendo "matéria produzida a partir de informação disponível publicamente, que é coletada, explorada e divulgada, em tempo útil, a um audiência apropriada, com a finalidade de abordar um requisito específico de informações*"* (HR, 2006).

O binómio vulnerabilidade/oportunidade surge em grande destaque nesta esfera da informação dita aberta, na medida em que a exploração desta fonte de informação é descentralizada e altamente corruptível. A acessibilidade pode ser feita por diversas formas e o conteúdo pode ser manipulado por todos, sem restrição. É uma oportunidade, acima de tudo, de conhecimento, mas que necessita, obrigatoriamente, da colaboração na análise, classificação, divulgação e proteção das fontes. Para tal, deve existir um equilíbrio entre a importância do conteúdo da notícia e a possível vulnerabilidade da fonte.

Muitos executivos perdem-se no universo paralelo dos *softwares* de simulação e esquecem-se que tais sistemas constituem modelos, que apenas representam, com limitações, a realidade. Como resultado, as modernas organizações criam executivos mergulhados em jogos e simulações, distantes da vida real, e como consequência, tomam decisões apressadas, colocando em risco os seus negócios (Kujawski, 2003).

Com efeito, não há executivo que não reclame do excesso de informação: são os *e-mails*, as publicações e os relatórios. A dificuldade passou da identificação para a seleção e tratamento da informação. O sucesso de uma empresa depende, agora, da sua capacidade de localizar, analisar e usar a informação de maneira apropriada (Kujawski, 2003).

Concluindo, para fazer frente ao problema do excesso de informação, há necessidade de tratar a informação e as ferramentas de gestão de informação, estrategicamente (Kujawski, 2003).

2.2. Contextualização

> *"(...) nenhum país, por mais poderoso que seja, pode conceber uma política externa, de defesa, económica ou qualquer outra, sem dispor das informações que proporcionam o conhecimento essencial, sobre o qual tais políticas assentam (...)"* (General Pedro Cardoso)

Atualmente, o contexto nacional e internacional são caracterizados pela incerteza e imprevisibilidade, devido a um novo conjunto de novas ameaças. Essas ameaças estão identificadas, quer ao nível internacional, quer ao nível nacional.

Ao nível internacional, são diversas as organizações e os Estados que redigem vários tipos de documentos estratégicos, onde mencionam as ameaças a que estão sujeitos, designadamente a UE. Ao nível nacional, as ameaças emergentes são citadas no Conceito Estratégico de Defesa Nacional (CEDN).

Segundo o CEDN, as ameaças são de vária ordem, designadamente: o crime organizado, o terrorismo transnacional, o ciberterrorismo e a cibercriminalidade; que se impõem a toda a comunidade internacional e aos Estados Democráticos, regidos por normas livremente aceites.

> "O ambiente de segurança global confronta -se, nomeadamente, com os seguintes riscos e ameaças: o terrorismo transnacional e outras formas de extremismo violento, com impacto altamente desestabilizador; a pirataria, baseada sobretudo em Estados em colapso ou com fraco controlo do seu território e afetando rotas vitais do comércio internacional; a criminalidade transnacional organizada, que inclui tráficos de pessoas, armas e estupefacientes, (…); a proliferação de armas de destruição massiva (nucleares, biológicas, químicas e radiológicas), com a agravante de poderem ser apropriadas por grupos terroristas; a multiplicação de Estados frágeis e de guerras civis em áreas estratégicas vitais, (…); os conflitos regionais, como resultado, nomeadamente, da afirmação hegemónica de potências em zonas estratégicas de elevada conflitualidade ou de separatismos com potencial impacto nos equilíbrios regionais e globais; o ciberterrorismo e a cibercriminalidade, tendo por alvo redes indispensáveis ao funcionamento da economia e da sociedade da informação globalizada; A disputa por recursos naturais escassos, (…); os desastres naturais e a mudança climática, (…)." (RCM n.º 19/ 2013)

Paralelamente, o desenvolvimento de novas tecnologias militares e a disseminação de formas de combate assimétrico – guerrilha e terrorismo – mudaram o quadro da segurança mundial e regional, o que permitem aos Estados, grupos ou organizações, pobres em recursos, acederem mais facilmente a tecnologias letais (RCM n.º 19/ 2013).

A emergência da *Internet* e a livre circulação de bens e serviços originou uma profunda transformação das sociedades, ao nível Económico, Social, Político e Cultural. E atualmente, os efeitos que são provocados por um acontecimento ou uma ameaça que ocorra, de forma isolada, numa qualquer parte do mundo, tornam-se problemas globais, que nenhum país será capaz de solucionar sozinho.

Contudo, a flexibilidade das fronteiras não facilitou apenas a mobilidade de pessoas, mercadorias e capitais, permitiu, também, a mobilidade de grupos terroristas e do crime organizado transnacional (RCM n.º 19/ 2013).

> "Porquanto os ciberataques são uma ameaça crescente a infraestruturas críticas, em que potenciais agressores (terroristas, criminalidade organizada, Estados ou indivíduos isolados) podem fazer colapsar a estrutura tecnológica de uma organização social moderna." (RCM n.º 19/ 2013).

As múltiplas ameaças que os Estados têm de enfrentar, nos dias que correm, originaram uma transformação substancial na amplitude e no paradigma dos conceitos de Segurança e de Defesa. A segurança interna e a defesa externa apresentam, atualmente, uma fronteira muito ténue e os governos estão a deparar-se, cada vez mais, com a dificuldade de delimitar o que devem ser considerado ameaças internas ou externas ao Estado.

Perante isto, existe a necessidade e a premência de haver, por parte dos governos, uma maior preocupação com as matérias respeitantes à Segurança e Defesa, conduzindo à criação e implementação de estratégias e Políticas Públicas nesse sentido, não apenas a nível interno, mas também na esfera internacional e comunitária. (Afonso, 2011)

A Comissão Europeia (CE) considera que os desenvolvimentos tecnológicos permitem aos cidadãos, de todo o mundo, utilizarem as novas TIC e aceder à *Internet*, fomentando, assim, mudanças revolucionárias nas sociedades, nomeadamente, no funcionamento da democracia, na governação, na economia, nas atividades comerciais, na comunicação social, no desenvolvimento e no comércio.

A CE considera, ainda, que a *Internet* é um instrumento essencial para o acesso à informação, à liberdade de expressão, à liberdade de imprensa, à liberdade de reunião e para o desenvolvimento económico, social, político e cultural (Parlamento Europeu, 2012b).

Segundo o relatório da Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias, na apreciação que esta faz, afirma-se que "os direitos fundamentais, a democracia e o Estado de Direito devem ser protegidos no ciberespaço", devendo aplicar-se "no universo em linha as mesmas normas, princípios e valores que a UE defende para o mundo físico" (Comissão Europeia, 2013b).

Afirma-se, simultaneamente, que se trata de uma realidade essencial ao crescimento económico, reconhecendo-se mesmo como "a espinha dorsal do nosso crescimento económico" e "um recurso crítico de que todos os setores económicos dependem", com destaque para setores fundamentais como as finanças, saúde, energia ou transportes.

A UE e os seus Estados-membros dependem fundamentalmente: da segurança do ciberespaço; da utilização segura das tecnologias digitais e de informação; da resiliência; da fiabilidade dos serviços de informação e das infraestruturas conexas. O ciberespaço, com os seus quase dois mil milhões de utilizadores, interligados a nível mundial, tornou-se um dos meios mais poderosos e eficazes de difundir ideias democráticas e organizar pessoas (Parlamento Europeu, 2012c).

Atualmente, existe uma ausência de definições, padrões e medidas comuns no domínio delicado e vulnerável da Cibersegurança. Assim como também, a partilha e coordenação entre as instituições da UE com os Estados-membros é quase inexistente, inclusivé entre estes e os parceiros externos. Ao nível internacional e da UE, as definições dos conceitos de Cibersegurança e Ciberdefesa são pouco claras e pouco harmonizadas.

Associado a este fato, a UE, ainda, não desenvolveu políticas consistentes próprias, que requerem uma abordagem multidisciplinar. O reforço da confiança entre o setor privado, as forças, os serviços de segurança, as instituições de defesa e as outras autoridades competentes, é da máxima importância (Parlamento Europeu, 2012c).

A confiança mútua, entre os intervenientes estatais e não estatais, constitui uma condição prévia para a fiabilidade da Cibersegurança. A maioria dos ciberincidentes, seja no setor público seja no setor privado, não é comunicada, dada a natureza sensível da informação e os eventuais prejuízos causados à imagem das empresas envolvidas.

A AED organizou, no contexto do Plano de Desenvolvimento de Capacidades (PDC), uma equipa de projeto no domínio da Cibersegurança, com a participação da maioria dos Estados-membros. O trabalho consiste em recolher experiências e apresentar recomendações de natureza global que a caracteriza, isto é a *Internet* e a ausência de

fronteiras. Os governos dependem, cada vez mais, de agentes privados relativamente à segurança das suas infraestruturas críticas (Parlamento Europeu, 2012a).

Desta forma, a UE tem feito esforços para a criação de uma Política Comum de Ciberdefesa e Cibersegurança, no âmbito da Política Externa e de Segurança Comum (PESC) e da Política Europeia de Segurança e Defesa (PESD) e, mais concretamente da AED. Esta Agência visa uma abordagem cooperativa no desenvolvimento de capacidades, contribuindo para uma melhor definição das necessidades futuras, no campo da Cibersegurança e da Ciberdefesa[17].

Relativamente ao projeto da UE, importa salientar que a AED lançou, em novembro de 2012, um projeto[18] onde visa abordar, de forma simples e integrada, o papel das informações no desenvolvimento das capacidades que vão contribuir para uma melhor definição das necessidades futuras da UE, no campo da Cibersegurança (AED, 2012).

A AED e os Estados-membros da UE participam, assim, no desenvolvimento conjunto de capacidades no domínio da Ciberdefesa e, como primeiro passo, esta Agência encomendou um estudo prévio[19], para fazer o levantamento das atuais capacidades de Ciberdefesa, entre seus Estados-membros (AED, 2011). Deste modo, os resultados dos vários estudos já concluídos vão ser, num futuro próximo, aproveitados para traçar um quadro de análise do impacto das atuais e futuras ameaças virtuais, nas operações lideradas pela UE.

Surgiu, então, a necessidade de investigar de que forma esta temática tem sido desenvolvida noutros países e constatou-se que muitas nações, tanto do continente europeu como do americano (nomeadamente, Brasil e Estados Unidos da América - EUA) elaboram e aplicam a sua própria Estratégia de Cibersegurança.

Neste processo de investigação e seleção das fontes e da informação recolhida, com vista a descrever o estado de arte, houve o cuidado em verificar se as fontes eram credíveis e seguras. Assim, os critérios de seleção encontrados para definir e escolher os autores e as obras para análise foram: a relação do autor com o assunto descrito; a origem do documento; a credibilidade do documento; o significado e representatividade do documento; e a atualidade do mesmo.

[17] A Agência Europeia de Defesa foi criada em 2004 e promove, a nível da UE, a cooperação no domínio do armamento, reforça a base industrial e tecnológica da UE no domínio da defesa e cria um mercado europeu dos equipamentos de defesa competitivo, promovendo também a investigação com vista a reforçar as potencialidades industriais e tecnológicas europeias no domínio da defesa.

[18] AED, *"Cyber Intelligence for EU-led Operations (CyTelOPS)",* 2012.

[19] AED, *"Capabilities for Cyber Defence in the military domain (milCyberCAP)",* 2011.

Sendo assim, sem que existisse primazia entre critérios, a pesquisa exploratória iniciou-se na análise de documentos de instituições governamentais e de organizações internacionais, tais como relatórios da CE, documentos da AED e da *European Network and Information Security Agency* (ENISA); publicações da OTAN, do *Cooperative Cyber Defence Centre of Excellence* (COC DCE) e do *North Atlantic Council* (NAC); relatórios do *Congressional Research Service* (CRS) e da *Information Network Security Agency* (INSA), publicações do DOD e do *Director of National Intelligence* (DNI) norte-americanos; e documentos relacionados com a estratégia cibernética do Reino Unido, Rússia, China e Brasil.

A nível nacional, os documentos que foram consultados prendem-se com alguns artigos e informação obtida por fonte aberta, do sítio da *Internet* do GNS, do Centro de Gestão Informática do Governo (CEGER), do Serviço de Informações da Republica Portuguesa (SIRP), do Instituto de Defesa Nacional (IDN) e da Academia Militar (AM).

Dos autores selecionados destacam-se os estudos de Robert Steele, Richard Best Jr e Alfred Cumming, ao nível internacional, e os artigos de Paulo Viegas Nunes e Pedro Borges Graça, ao nível nacional. Os respetivos estudos, também disponíveis em fontes abertas, são a base e referência bibliográfica da presente dissertação.

Outros artigos científicos, relacionados com a temática, também, foram, igualmente, essenciais no entendimento e contextualização do tema, na medida em que acrescentam discussões e ideias pertinentes sobre Cibersegurança e Ciberdefesa (como por exemplo, são os contributos da *Heritage Foundation*, do *Joint Air Power Competence Centre* (JAPCC), do *C4ISR Journal*, das revistas científicas portuguesas *Nação e Defesa* e *Proelium*.

2.3. A Perspetiva da UE

> *"Os ciberataques tornaram-se uma realidade diária, nas grandes organizações internacionais e nos governos (…) Precisamos (os países) de acordar normas de comportamento no ciberespaço (…) Há uma necessidade em estabelecer linhas de comunicação de crise e aperfeiçoar diálogos sobre questões do ciberespaço."* (Catherine Ashton, Alto Representante da União Europeia)

Relativamente à UE, a metodologia defendida é orientada para o desenvolvimento de uma "capacidade"[20] e dos seus programas, projetos e outras atividades que contribuem para a melhoria das capacidades militares, necessárias para as operações futuras da PCSD. A AED auxilia os Estados-membros no seu plano de defesa nacional e respetivos programas.

O *Capability Development Plan* (CDP)[21], da AED, constitui um modelo de referência para o desenvolvimento de capacidades que se prevê explorar ao longo deste estudo. Este modelo proporciona uma visão para a necessidade de futuras capacidades, tendo em conta o impacto dos futuros desafios de segurança, de desenvolvimento tecnológico e de outras tendências, que poderão vir a condicionar o seu desenvolvimento.

Uma das prioridades do CDP é a Ciberdefesa, dedicada à defesa proactiva de infraestruturas críticas de informação contra ciberataques. Os requisitos militares para a Ciberdefesa da UE são: "preparar, proteger, prevenir, detetar, responder, recuperar e aprender lições dos ataques, malefícios ou acessos não autorizados, que afetam as infraestruturas de informação[22], e que suportam e permitem a condução das tarefas militares da UE e das operações da PCSD" (AED, 2012).

Há algum tempo que a UE defende "um ciberespaço aberto, seguro e protegido", através de um reforço na segurança e liberdades fundamentais na *Internet* (Comissão Europeia, 2013b), bem como, a criação e implementação de uma Estratégia de Cibersegurança, através do desenvolvimento de uma abordagem global e unificada, para a Ciberdefesa e para a Cibersegurança (Parlamento Europeu, 2009).

O Plano de Cibersegurança da UE pretende proteger a *Internet* aberta, a liberdade e as oportunidades em linha. Para isso, define objetivos, limita prioridades e refere alguns deveres dos Estados-membros. Assim sendo, "o plano deve promover os valores europeus de liberdade e democracia; garantir que a economia digital se desenvolve em condições de segurança; constituir e financiar uma rede de centros nacionais de excelência, para facilitar a formação; e o desenvolvimento de capacidades, contra a cibercriminalidade" (Comissão Europeia, 2013a).

As prioridades dividem-se em: (i) "alcançar a resiliência do ciberespaço, (ii) reduzir drasticamente a cibercriminalidade, (iii) desenvolver uma política e ferramentas no

[20] Tradução do autor de *Capability-driven.*

[21] O CDP foi desenvolvido em conjunto com os Estados-membros participantes, a Secretaria do Conselho e do Comité Militar da UE, apoiada pelo pessoal militar da UE. O Conselho Diretivo da AED é quem orienta o programa e aprovou o CDP em julho de 2008.

[22] Incluindo redes militares e civis, sistemas usados por sistemas de computadores, bem como programas e dados usados dentro desse mesmo sistema.

domínio da Ciberdefesa, no quadro da PCSD, (iv) desenvolver os recursos industriais e tecnológicos para a Cibersegurança e (v) estabelecer uma política internacional coerente para a UE" (Comissão Europeia, 2013a).

A UE defende que "os Estados-membros devem designar uma autoridade nacional competente para o setor, criar um mecanismo de cooperação entre Estados-membros e a Comissão, e as plataformas de comércio eletrónico devem adotar práticas de gestão de risco" (Parlamento Europeu, 2009).

Com o objetivo de reforçar a segurança e liberdades fundamentais na *Internet*, a UE defende o acesso pleno e seguro de todos à *Internet*, através do apelo à cidadania ativa, viabilizando uma maior transparência do processo decisório e ao assegurar os direitos legais dos menores.

A UE faz entender que a "identidade digital" é cada vez mais parte integrante do nosso "eu", e reconhece que existe um perigo inerente a formas de vigilância e controlo da *Internet*. Por outro lado, esta recomendação, do Parlamento Europeu ao Conselho, defende que se deve "limitar, definir e regular, rigorosamente, os casos em que se pode exigir a uma empresa privada de *Internet* que divulgue dados a autoridades governamentais" (Parlamento Europeu, 2009).

Adicionalmente, outras premissas constantes do mesmo documento, defendem que se deve chamar a atenção para o desenvolvimento da "*Internet* das coisas" (*Internet of things*), (i) incentivar à incorporação dos princípios fundamentais da "Carta dos Direitos na *Internet*" (*Internet Bill of Rights*) no processo de investigação e desenvolvimento de instrumentos e aplicações, (ii) promover o princípio da integração da proteção de dados na conceção das ferramentas técnicas (*privacy by design*), (iii) desenvolver um verdadeiro fórum digital na *Internet* (*Web E-Agora*), (iv) participar ativamente nos diferentes fóruns internacionais que tratem de aspetos mundiais e locais da *Internet*, designadamente o Fórum sobre a Governação da *Internet* (FGI) e (v) criar um FGI europeu (Parlamento Europeu, 2009).

Concluindo, uma *Internet* livre, aberta e segura é o cerne da nova Estratégia de Segurança para o ciberespaço. Esta estratégia é uma proposta legislativa, que visa incentivar o crescimento económico, reforçar a confiança das pessoas na compra de bens e serviços em linha.

A Estratégia oferece, ainda, prioridades claras para uma política internacional do ciberespaço, tais como: (i) a promoção de reformas democráticas *Word Wide Web (WWW)*; (ii) a partilha de responsabilidades por cidadãos e governança; (iii) o envolvimento de

parceiros e organizações internacionais, no setor privado e na sociedade civil, para apoiar, à escala global, (iv) a construção nos países de terceiro mundo, reforçando, por outro lado, o papel da ENISA.

Por seu lado, a ENISA está a desenvolver um guia de boas práticas para apresentar bons procedimentos e recomendações sobre como desenvolver, implementar e manter uma Estratégia Nacional de Cibersegurança (ENC), de forma a definir como direcionar os esforços nacionais, para reforçar a segurança no ciberespaço (ENISA, 2012).

Mas a UE, tendo em consideração a emergência desta temática, compôs a Resolução do Parlamento Europeu, de 22 de novembro de 2012, sobre Cibersegurança e Ciberdefesa, em que descreve (i) quais as medidas e a coordenação na UE; (ii) o que deve ser realizado ao nível da UE, em particular ao nível da AED; (iii) qual o papel dos Estados-membros a cooperação entre os setores público e privado; (iv) a cooperação internacional, nomeadamente, com a OTAN e os EUA (Parlamento Europeu, 2012c).

Os responsáveis da CE afirmam que "já começou uma nova era nas políticas globais da *Internet*". Coligações de economias emergentes estão a colaborar no sentido de apresentar um quadro regulamentar global para a *Internet*, incluindo um aumento do controlo estatal e a implementação de um órgão de regulamentação da Organização das Nações Unidas (ONU). Os países desenvolvidos estão a preparar legislação, à porta fechada, e apenas um número reduzido de empresas é ouvido durante este processo[23].

Embora, a UE seja o mercado mais significativo do mundo, a maioria das empresas de *Internet* está sediada nos EUA, obrigando os cidadãos europeus a aceitar condições de utilizador dos EUA.

Os decisores políticos devem compreender que num mundo "ligado" ao nível global, os parâmetros do processo de legislação estão em constante mutação e os conceitos tradicionais de jurisdições fixas não correspondem, frequentemente, ao nosso hemisfério digital global. A UE deve fazer com que a celebração de novos acordos de comércio livre dependa da preservação da *Internet* aberta, ou fornecer apoio político (público) *ad hoc* em situações de emergência (Parlamento Europeu, 2012b).

A *Internet* e, principalmente, os meios de comunicação social, permitem aos governos praticar diplomacia direta e possibilitam o aumento do contacto interpessoal, em todo o

[23] Relatório sobre uma Estratégia para a Liberdade Digital na Politica Externa da UE (2012/2094(INI)) Comissão dos Assuntos Externos do Parlamento Europeu, 2012.

mundo. Os debates públicos sobre ideias podem refutar o extremismo, melhorar a comunicação e o entendimento intercultural (Parlamento Europeu, 2012b).

A CE está, atualmente, a desenvolver um conjunto de orientações relativas aos direitos humanos (e também responsabilidade social das empresas mais vasta) para o setor das TIC, com base nos Princípios Orientadores das Nações Unidas sobre Empresas e Direitos Humanos - Princípios de Ruggie (Parlamento Europeu, 2012b).

Em junho de 2013, a Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias, comunicou ao Presidente da Comissão de Assuntos Europeus, através do Relatório - [JOIN(2013)1 final], quais as prioridades estratégicas e ações, no campo da Cibersegurança (Comissão Europeia, 2013). A estratégia apresentada pela Comissão é relativa à Estratégia da União Europeia para a Cibersegurança e estrutura-se em cinco prioridades, visando a resposta aos desafios identificados:

1. Garantir a resiliência do ciberespaço.
2. Reduzir drasticamente a cibercriminalidade.
3. Desenvolver a política e as capacidades no domínio da Ciberdefesa, no quadro da PCSD.
4. Desenvolver os recursos industriais e tecnológicos para a Cibersegurança.
5. Estabelecer uma política internacional coerente em matéria de ciberespaço para a UE e promover os valores fundamentais da UE.

Em suma, a Estratégia da UE, presente nestes princípios, é de promover soluções seguras e independentes, em matéria de programas e equipamentos informáticos, que promovam a participação democrática ativa de todos os cidadãos, em particular, dos utilizadores da *Internet*, que praticam o comércio em linha.

Decerto que um maior envolvimento e regulação governamental da *Internet* prejudicam a sua natureza aberta e sem restrições, limitando o potencial de crescimento do comércio eletrónico e a atividade das empresas da UE, que operam na economia digital (Parlamento Europeu, 2012b).

2.4. A Perspetiva da OTAN

> *"A ciberdefesa é uma responsabilidade nacional, mas todos concordamos que a OTAN pode e deve desempenhar um papel útil no sentido de facilitar o desenvolvimento de capacidades robustas de ciberdefesa nacional".* (Anders Rasmussen, Secretário Geral da OTAN)

No que respeita a normativos da OTAN, a Aliança encoraja os 27 membros a "alcançarem um patamar mínimo de Ciberdefesa, a fim de reduzir as vulnerabilidades das infraestruturas nacionais críticas, fortalecendo, desta maneira, a resistência a ataques e reduzindo os riscos para toda a Aliança". Para isso, acrescenta que é necessário "um compromisso de longo prazo" (Healey, 2011).

A doutrina da OTAN, por seu lado, refere que a OSINT é uma componente vital na visão de futuro da Aliança. A obtenção de informações a partir de fontes abertas sempre desempenhou um papel importante na produção de informações classificadas. Através de sua concentração em informações não classificadas, a OSINT fornece os meios, com os quais o desenvolvimento de informações válidas e confiáveis, que podem ser partilhadas com os países parceiros não-OTAN (PfP), em operações internacionais.

A experiência nos recentes teatros de operações, a crescente importância da "Parceria para a Paz"[24] e dos membros do "Diálogo Mediterrânico"[25] no diálogo para a segurança, ilustra a necessidade de desenvolver fontes de informação, que permitem maior envolvimento com esses parceiros vitais (OTAN, 2001).

A OTAN defende, ainda, que apesar de a *Internet* ser uma fonte de muito conhecimento, toda a informação recolhida, a partir dela, deve ser avaliada quanto à sua origem, preconceito e confiabilidade. Por outras palavras, a *Internet* deve ser abordada com muita cautela.

Por outro lado, a *Internet* é imbatível como um meio de acesso a fontes de informação comerciais de qualidade e válidas. Porém, como as necessidades de informação da OTAN variam de acordo com os requisitos da missão, é praticamente impossível manter um conjunto exequível de material de fonte aberta, que seja precisa instantaneamente. De facto, a atenção deve estar na recolha de fontes de informações, não na recolha de informação.

Com o conhecimento de fontes relevantes e confiáveis de informação de fonte aberta, uma célula de informações pode dedicar, rapidamente, a energia na recolha e analise, para desenvolver produtos OSINT, em conformidade com as necessidades da missão.

[24] A Parceria para a Paz (PfP) é um programa de cooperação prática bilateral entre os países parceiros euro-atlânticos e a OTAN, permitindo aos parceiros construir uma relação individual com a OTAN, escolhendo suas próprias prioridades para a cooperação.

[25] É um fórum de cooperação entre a OTAN e sete países do Mediterrâneo com o objetivo de criar boas relações e uma melhor compreensão e confiança mútua em toda a região, promovendo a segurança e a estabilidade regionais, explicando as políticas e os objetivos da OTAN.

Assim, a OSINT é distinta das informações de fontes abertas produzida nas escolas, no meio empresarial ou na investigação jornalística, na medida em que representa a aplicação de um processo comprovado pelas entidades nacionais competentes (OTAN, 2001).

No seu guia prático para a exploração de uma fonte de informação (OTAN, 2002b), a OTAN define à partida, o Ciclo de Produção de Informações, que se inicia com a definição dos requisitos da missão. Para esta definição de requisitos devem ser respondidas três questões: "Esta informação é relevante para a missão?" "Qual o impacto desta informação para o decorrer das operações?" "Esta informação irá provocar alterações no ambiente operacional?" (OTAN, 2002b)

O passo seguinte é reunir a recolha de informação, proveniente da *Internet*, pelo que se deve elaborar um plano de recolha de dados da *Internet*. Assim sendo, antes de se iniciar qualquer pesquisa na *Internet*, deve ser definida a metodologia de pesquisa de dados da *Internet*. De novo, esta procura pode ter em conta dois ângulos: por "assunto" ou por "palavras-chave".

Pelas mesmas razões, os motores de busca devem ser criteriosamente selecionados e deve-se ter em conta os benefícios e os inconvenientes. A doutrina defende, ainda, que se deve procurar de forma anónima, ou, então, passar despercebido, devendo o autor esconder as suas intenções de pesquisa, sem deixar rasto (OTAN, 2002b).

Durante a fase de processamento da informação, tem lugar a avaliação criteriosa da fonte. Para tal, devem ser considerados diferentes "listas de tarefas"[26] para diferentes áreas. Na fase de disseminação é preciso ter em conta como fazer e como classificar, pois a classificação serve para proteger fontes, métodos e intenções.

O método defendido neste processo de classificação é o *Bottom Up*, começando por fontes não classificadas, como por exemplo um reporte, que permite construir informações, de forma rápida e eficaz, para diversos setores de segurança, sem necessitar de recorrer à divulgação do processo. Posteriormente, outras informações, de caráter classificado, podem ser acrescentadas para aumentar o valor dessas informações, sem que estas sejam comprometidas (OTAN, 2002b).

Recentemente, o Conceito Estratégico da OTAN, acordado em Lisboa, em novembro de 2010, veio reforçar o papel, único e essencial, de garantir a defesa e a segurança comum, para que a Aliança continue a ser eficaz, num mundo em mudança, contra novas ameaças, com novas capacidades e novos parceiros (OTAN, 2010).

[26] Tradução do autor de *Checklists.*

A estratégia da Aliança sublinha, ainda, que os ciberataques são cada vez mais frequentes, mais organizados e com consequências financeiras mais gravosas, pelos danos que provocam nas administrações governamentais, empresas, economias. Potencialmente, também podem provocar efeitos indesejados nos transportes e redes de abastecimento e outras infraestruturas críticas, ao ponto de ameaçar a prosperidade nacional e a segurança e estabilidade Euro-Atlântica (OTAN, 2010).

Com base no novo conceito estratégico, foi estabelecida uma Agenda para a Colaboração. Resumidamente, a ideia principal é: a OTAN, a UE e o setor privado adotarem uma Agenda que inclua a coordenação de recursos de monitorização e deteção, a partilha de informações e a investigação ligada à resposta e escalada. Esta cooperação deve ser sustentada por um acordo sobre um único conjunto de normas, melhores práticas comuns e atividades coordenadas (Parkhouse, 2012).

A Agenda visa desenvolver legislação sobre questões cibernéticas, envolvendo o setor privado, como protetores de muitas infraestruturas nacionais críticas e, especificamente, as empresas de TI, que desenvolvem o *hardware* e *software* utilizado pela maioria dos usuários de *Internet*.

As seis questões principais que constam da Agenda são (Parkhouse, 2012):

a. Melhorar a coordenação entre a UE-OTAN e a Indústria;
b. Combinar as informações do Setor Privado e do Governo;
c. Estabelecer um protocolo entre UE-OTAN, para a investigação de ataques em ativos de Segurança Nacional;
d. Acordo UE-OTAN, num protocolo em Resposta e Escalada a incidentes cibernéticos;
e. Coordenação UE-OTAN de Melhores Práticas e Alcance no Ciberespaço;
f. Demonstração dos líderes UE/ OTAN de coerência na segurança na Era Digital.

Presentemente, o desígnio da OTAN é desenvolver, ainda mais, a capacidade de prevenir, detetar, defender e recuperar de ciberataques. Para isso, pretende utilizar o processo de planeamento da OTAN, para melhorar e coordenar as capacidades de Ciberdefesa nacional, colocar todos os órgãos da organização sob a proteção cibernética centralizada e melhorar a integração do conhecimento situacional cibernético, alertando e respondendo com os países membros.

2.5. A Perspetiva dos EUA

> *"Noventa por cento das informações vem de fontes abertas. Apenas os outros dez por cento é que são o mais dramático, ou seja o trabalho clandestino. O herói das informações de hoje é o Sherlock Holmes, não é o James Bond."* (TGen Samuel V. Wilson, ex-diretor da *Defence Intelligence Agency)*

Segundo a INSA, a evolução sentida no campo das fontes de informação fornece aos analistas ideias sobre questões que, há duas décadas atrás, só os métodos classificados (relatórios diplomáticos, fontes clandestinas e os satélites) poderiam responder.

A recolha de informações a partir de fontes abertas foi remetida para segundo plano, durante muitos anos, contudo, a emergência da *Internet* colocou esta área de estudo no primeiro patamar, no que respeita à recolha e processamento de informação (INSA, 2011).

O conhecimento das áreas HUMINT, SIGINT e ELINT foi útil em tempos, mas não era primário nem facilmente acessível. Estes novos meios de comunicação e informação (fontes abertas no ciberespaço) podem reduzir a necessidade de uma gama de ferramentas de recolha de informação dispendiosa, que as agências outrora tinham como vantagem (INSA, 2011).

Tendo enm consideração o exposto e respondendo a uma exigência legislativa, a *Intelligence Community* (IC)[27] criou os cargos de *Deputy Director of Nacional Intelligence* (ADNI) e de *Deputy Director of Nacional Intelligence for Open Source* (ADNI-OS) , para assuntos relacionados com as fontes abertas, e o Centro Nacional de Fontes Abertas (NOSC). O objetivo deste centro é realizar funções de aquisição especializadas e análise OSINT, criando um núcleo de excelência que apoia e incentiva todas as agências de informações (INSA, 2011).

O processo de recolha de informações a partir de fontes abertas no ciberespaço, apresenta como vantagens o facto de ser um processo menos dispendioso e menos arriscado que as demais áreas de informações, ditas classificadas. O uso de OSINT pode resultar não apenas em poupanças monetárias, mas também num menor risco na sua utilização, quando comparado com outras fontes técnicas e humanas sensíveis (INSA, 2011).

Por outro lado, a OSINT, também pode fornecer indícios sobre que tipos de empreendimentos podem estar, ou não, na lista de prioridades para outros sistemas.

[27] A *Intelligence Community* é uma comunidade de 16 agências estadunidenses com o objetivo de realizar atividades de informações no âmbito das relações externas e de segurança nacional dos Estados Unidos. Os membros da organização incluem serviços de informações, informações militares e civis, como por exemplo o Departamento da Justiça, da Energia, da Defesa e da Segurança Interna.

Todavia, a sua recolha pode não ser suscetível através de outras abordagens de disciplinas de informações, tais com aplicações inovadoras de novas tecnologias, mudanças nas atitudes sociais, emergência de novos movimentos políticos e religiosos, crescente descontentamento popular e desilusão com a liderança (INSA, 2011).

A primeira necessidade e a mais importante, na elaboração de legislação relacionada com a *Cyber Intelligence* (ou qualquer tipo de legislação para essa matéria) é de assegurar a consistência com os princípios fundadores da nação (Rosenzweig, 2011). Esses princípios incumbem o governo federal de garantir a defesa comum, enquanto ao mesmo tempo, garante a proteção das liberdades civis e a manutenção dos mercados económicos livres (Rosenzweig, 2011).

O princípio fundamental e único, para o qual os americanos devem seguir, é a noção de humildade sobre algo do ciberespaço. Presentemente, as pessoas usam a *Internet* de uma forma que não imaginavam há cinco anos atrás. Testemunho disso é o crescimento das redes sociais e o desenvolvimento de protocolos de comunicações de *Internet* como o *Skype*, ou seja, a viragem para a *Web 3.0* (Rosenzweig, 2011).

A *Heritage Foundation,* num dos seus artigos dedicados à Cibersegurança, elaborou um quadro com sete medidas essenciais, para proteger os seus bens e interesses, no domínio do ciberespaço. Esta instituição defende que a regulação, especialmente regulação federal, é pesada, lenta e estática. Uma vez implementada, os regulamentos são muito difíceis de remover, ou até mesmo de alterar. Esta regulação é exatamente a abordagem errada para lidar com o desenvolvimento rápido e incrivelmente dinâmico, no campo da Cibersegurança (Bucci at al., 2013).

Uma vez mais, deve ser reconhecido a natureza dinâmica do ciberespaço e este deve ser orientado por políticas que sejam igualmente dinâmicas. Qualquer legislação deve fornecer uma proteção robusta, na privacidade e liberdades individuais. Sendo que, o primeiro propósito de qualquer legislação deve ser permitir e promover a partilha de informação, entre os setores público e privado, e entre entidades dentro do setor privado (Bucci at al., 2013).

Portanto, segundo esta organização, existem sete componentes chave, que devem ser incluídas numa verdadeira legislação cibernética eficaz:

1. Permitir a partilha de informação, em vez de impor informação;
2. Incentivar o desenvolvimento de uma responsabilidade de Cibersegurança viável e um sistema de segurança;

3. Criar uma estrutura no setor privado que promova classificações de segurança "*cyber-supply-chain*";
4. Definir padrões limitados de auto-defesa cibernética para a indústria;
5. Advogar para mais esforços do setor privado na promoção de uma conscientização geral, educação e formação em toda a América;
6. Reformar a ciência, tecnologia, engenharia e educação matemática, para criar um forte grupo de trabalho no campo do ciberespaço, dentro da indústria e do governo;
7. Liderar um comprometimento internacional responsável, relativo ao ciberespaço.

Numa conferência recente em Arlington, Virgínia, alguns especialistas defenderam que a melhor forma de corrigir as discrepâncias em questões de Ciberdefesa é a aplicação de técnicas utilizadas em outros assuntos militares e de segurança, deixando de se ver o ciberespaço como único e isolado (C4ISR Journal, 2013).

No entanto, quanto à proteção do ciberespaço, esta vai para além da visão de segurança física, pois a presente abordagem de Cibersegurança é deficiente, principalmente quando se pretende trazer às barras dos tribunais suspeitos de terem cometido crimes relacionados com Cibersegurança. Por isso, defende-se a criação de um centro integrado de Comunicações e Cibersegurança, que será o primeiro eixo para a recolha, processamento, disseminação e partilha de informação, relacionada com ciberameaças, com o setor privado (C4ISR Journal, 2013).

Este projeto deve incluir os chamados "portos seguros" e a proteção de responsabilidade civil, para as empresas que partilhem informações sobre ciberameaças. Porém, da conferência entre especialistas de informações ficou por determinar qual a função do Estado: "Vigilância ou proteção dos direitos e liberdades do cidadão?" (C4ISR Journal, 2013).

No que diz respeito à "computação em nuvem", ficou expressa que esta não é a resposta para todos os problemas relacionados com grandes bases de dados. As agências devem investir em ferramentas automatizadas e técnicas, que permitam que os dados sejam analisados. Contudo, o foco deve permanecer na partilha de informação no ciberespaço e não em outras questões, como por exemplo a pirataria na *Internet* (C4ISR Journal, 2013).

Segundo um artigo do jornal C4ISR, de Ben Iannotta (2011), o autor defende a necessidade de mais divulgação e menos custos com a *Cyber Intelligence*, na "computação em nuvem", isto é, o objetivo é descobrir como conseguir obter informações classificadas de Departamentos do Estado e "esterilizá-las" a um nível que seja proveitoso, para a

infraestrutura crítica no setor privado. Adianta ainda que, não é benéfico para ninguém ter informações classificadas, que porventura podem ser uma ameaça ou uma vulnerabilidade, e que não possam ser divulgadas ao setor privado (Iannotta, 2011).

James Clapper, *Director of National Intelligence* (DNI) dos Estados Unidos, disse acreditar que a "computação em nuvem irá reduzir os custos nos serviços de informações e evitar grandes cortes orçamentais nos seus programas. Para tal, é necessário investir numa *framework* comum, apelidada de *Defense Intelligence Information Enterprise* (DI2E)" (C4ISR Journal, 2013).

Paralelamente, num estudo de Harris Minas (2008), o autor tenta responder como a OSINT pode emergir como uma disciplina indispensável para as informações, no século XXI. Segundo este autor, a OSINT não pode surgir de repente, como a disciplina dominante no campo das informações.

As fontes OSINT, no ciberespaço, como a *Internet*, os *Media* "em linha" e as imagens de satélite têm surgido como principais fornecedores de informação. Porém, a desvantagem mais relevante é a sobrecarga de informação que veicula nestas fontes e, também, não esquecendo que atores, como terroristas ou grupos extremistas, também navegam neste ambiente (Minas, 2008).

Segundo Minas, a propensão cultural relativamente às fontes confidenciais deve deixar de existir, pois vive-se num mundo aberto, em que os governantes devem ser capazes de se adaptar a este ambiente, colocar em ação as suas agências, de acordo com as necessidades e os desafios emergentes (Minas, 2008).

Este autor conclui que a OSINT pode adquirir um papel dinâmico, no processo de informações do século XXI, pode completar o trabalho de outras áreas das informações e preencher as lacunas que existem (Minas, 2008).

Num artigo da INSA (2011), a *Cyber Intelligence* surge como uma disciplina emergente, que pode ser rapidamente partilhada com parceiros privados e estrangeiros apropriados. A disciplina de *Cyber Intelligence* é defendida como sendo um "conjunto de abordagens e esforços em toda a indústria, escolas e organizações governamentais, sem fins lucrativos, que fornecem conhecimento situacional não classificado, indicações, alertas, análise ininterrupta não classificada e classificada (conforme o caso), relatórios para agências do governo, da indústria e parceiros internacionais de confiança" (INSA, 2011).

Para a INSA, o objetivo é construir uma parceria virtual, entre todos os órgãos competentes e o setor privado, para assegurar uma partilha contínua de informações sobre ameaças,

juízos analíticos em tempo útil e respostas, fundamentadas e padronizadas, para eliminar ameaças (INSA, 2011).

Segundo Dan Butler, Vice-Diretor do ADNI/OS, o futuro da OSINT reside na convergência de esforços e multidisciplinaridade com outras fontes de informação. Butler adianta dizendo que se pode chegar a comunidades muito diversificadas, trabalhar com parceiros internacionais, que compreendem os mesmos assuntos de maneira diferente e que esse conhecimento tem que ser aproveitado (ODNI, 2008).

Contudo, a questão mantém-se: "nos dias de hoje, como vamos organizar e priorizar para fazer um uso mais eficiente das fontes abertas, nos próximos 10 anos?" Um dos pontos fortes da OSINT é a língua comum, essa vantagem permite que a partilha seja totalmente compreendida por todos. Por outro lado, Butler defende que o domínio da OSINT deve ser alterado, isto é, deve ser feita fora o ambiente militar e governamental (ODNI, 2008).

Para Robert Steele, antigo operacional da Marinha norte-americana e atual defensor da utilização da OSINT, a informação substitui tempo, dinheiro, espaço e trabalho. Para este especialista, praticar OSINT é uma forma de impressão de dinheiro próprio, isto é, ao praticar OSINT restitui-se poder ao povo, de forma a pedir mais responsabilidades aos decisores políticos, inclinados para a manipulação dos dados, escondendo segredos, ou a lamentarem-se com justificações pelas suas erradas decisões (Steele, 2004).

Resumindo, este autor interroga-se: "não será este um exercício (OSINT) do interesse público?" Steele defende três tipos de escalas de avaliação, que podem ser aplicadas na avaliação do papel da OSINT, em Operações de Informação (OI), em qualquer organização:

a. Custo de sigilo. Os custos de transação são mais elevados e a classificação reduz a concorrência de fornecedores de melhor informação, nacionais e internacionais.
b. Valor relativo. A informação é "suficientemente credível"? Fornece informação "suficientemente credível" para seguir em frente? Permite que a decisão a ser tomada, tenha por base informação "suficientemente credível"? As informações podem ser partilhadas e, portanto, envolver outros interessados?
c. Retorno na partilha. Esta informação, partilhada abertamente, atrai outras informações que são igualmente úteis? Esta informação, partilhada abertamente, faz chegar a outras pessoas, que tenham "necessidade de saber" e, consequentemente, incluí-los e envolve-los numa rede para benefício mútuo?

Por outro lado, Steele defende ainda que a OSINT deve ser realizada em três níveis:

a. Se pode ser feito "em linha" e em menos de 15 minutos, o analista deve fazê-lo.
b. Se vai demorar 15 a 60 minutos, ou requer conhecimento especializado, a célula OSINT deve receber a tarefa.
c. Se vai demorar mais de 60 minutos, ou exige conhecimento muito especializado ou acesso direto, deve ser direcionado para uma terceira fonte ou serviço mais adequado.

2.6. A Perspetiva Nacional

> *"No domínio da cibercriminalidade, impõem-se uma avaliação das vulnerabilidades dos sistemas de informação e das múltiplas infraestruturas e serviços vitais neles apoiados."* (RCM n.º 19/ 2013)

A nível nacional, pode constatar-se que a *Cyber Intelligence* é uma área em que a legislação é escassa e a investigação está muito desprovida de documentação técnico-científica. Contudo, assiste-se a um aumento, que tem sido progressivo nos últimos cinco anos, de instituições e especialistas na área das informações.

Recentemente, a Resolução do Conselho de Ministros (RCM) 12/2012, de 7 de fevereiro, veio, na sequência das conclusões do Grupo de Projeto para as Tecnologias da Informação e Comunicação, definir as linhas gerais de uma Estratégia Nacional de Segurança da Informação (ENSI).

Importa ainda, realçar o trabalho desenvolvido pela AM e pelo GNS, que recorrendo à colaboração do CINAMIL[28] e do CIIWA[29], organizaram o 7º Simpósio Internacional "Ciberespaço: Liderança, Segurança e Defesa na Sociedade em rede" (7º EIN), numa organização conjunta com o 1º Simpósio Internacional "Organizações, Valores e Liderança" (1º OVL), no dia 29 de maio de 2013. Neste âmbito, alguns dos oradores presentes, reforçaram a ideia da importância em desenvolver um conjunto de iniciativas destinadas a garantir uma utilização mais livre, fiável e segura do ciberespaço.

[28]O Centro de Investigação da Academia Militar (CINAMIL) tem por missão promover ou participar em colaboração com outras instituições da comunidade científica nacional ou internacional, na realização de projetos de Investigação e Desenvolvimento e na divulgação de conhecimento científico, nomeadamente em áreas de interesse para a segurança e defesa nacionais.

[29]A "*Competitive Intelligence & Information Warfare Association*" (CIIWA) é uma associação civil, sem fins lucrativos, cujo objetivo primordial é o desenvolvimento de uma comunidade internacional e de uma rede de conhecimento entre entidades, especialistas e consumidores interessados na temática da *Competitive Intelligence* e da Guerra de Informação.

Verificou-se, ainda, que a Segurança da Informação (INFOSEC), não é só do interesse dos governos, pois, por exemplo, no âmbito académico, existe uma grande diversidade de obras publicadas e de trabalhos realizados. Igualmente, no círculo dos meios de comunicação são cada vez mais frequentes notícias sobre este tema e este ligado à Cibersegurança. De forma geral, é notório o aumento do interesse em questões cibernéticas por parte de pessoas, ora anónimos, a considerar pela quantidade de "Blogs*"* relativos ao tema, ora ligados a áreas de investigação, começando pela Segurança e Defesa, à Tecnologia, à Industria, à Economia, às Relações Internacionais e à Política.

Para o SIRP (2012a), o crescente interesse pela supervisão da "rede" é uma questão, inevitavelmente, associada ao problema da reserva da privacidade e de informações de índole pessoal.

Numa conferência dedicada à Cibersegurança, o SIRP afirmou que as empresas privadas possuem uma enorme capacidade de arquivo informático, admitindo-se que o armazenamento e disponibilização de informação possam comprometer a vida das pessoas que, por sua iniciativa e de modo nem sempre avisado, transmitem ou transmitiram no passado dados pessoais e profissionais a empresas (SIRP, 2012b).

Por seu lado, os jovens, que estão entre os principais utilizadores da *Internet*, são extremamente vulneráveis às abordagens via ciberespaço. Por esse motivo, o SIRP dá o seu contributo a iniciativas, como o "Projeto Internet Segura".

Quanto à metodologia utilizada pelo SIRP, a OSINT é um dos métodos de recolha de informações mais utilizados para produzir relatórios confidenciais. Através da OSINT, os analistas testam e graduam a fiabilidade das fontes e a veracidade de certo tipo de informação, como por exemplo, aquela que é publicada pelos Órgãos de Comunicação Social (OCS) (SIRP, 2012b).

Relativamente à segurança no ciberespaço, afirma que a segurança é responsabilidade de todos, isto é, "não podem existir os meios de uns e os meios dos outros, pois estão todos afetos à Segurança Nacional e todos devem responder para o mesmo fim" (SIRP, 2012b).

Por seu lado, o GNS afirma existir necessidade de se criar uma ENC, composta por uma capacidade de nível operacional e uma capacidade de nível estratégico, capaz de garantir uma eficaz gestão de crises (GNS, 2012).

Para além de impor a Cibersegurança como uma prioridade nacional, a proposta do GNS descreve como a ENC deve ser capaz de coordenar a resposta operacional a ciberataques, desenvolver sinergias nacionais e potenciar a cooperação internacional. O principal desafio

que o Estado tem que enfrentar é o de estimular uma utilização livre, segura e eficiente do ciberespaço, por parte de todos os cidadãos, ao mesmo tempo que garante a proteção e defesa da sua infraestrutura de informação crítica (GNS, 2012).

Em suma, a proposta do GNS enfatiza que o País deve procurar atingir as seguintes premissas: garantir a segurança no ciberespaço, fortalecer a Cibersegurança das infraestruturas críticas nacionais e defender os interesses nacionais e a liberdade de ação no ciberespaço.

Por sua vez, o CEGER diz, pela voz de Manuel Honorato, que Portugal, em 2005, era vanguardista na UE e na OTAN, na criação de uma ENSI, e em 2012, já era um dos países mais atrasados (Honorato, 2012).

Algumas das ideias chave defendidas pelo CEGER refletem que a abrangência deverá extravasar o Estado, englobando toda a sociedade da informação e infraestruturas críticas. "O Centro Nacional de Cibersegurança, não é uma opção, é uma obrigação de Portugal perante os seus pares e uma necessidade de sobrevivência" (Honorato, 2012).

Recuando um pouco a 2011, no 5º Simpósio da Academia Militar sobre "A Estratégia de Informação Nacional - Cibersegurança e Ciberdefesa Nacional: levantamento de capacidades, soluções e iniciativas", o Dr. Hayes identificou três territórios distintos de ciberespaço: o ciberespaço governamental, o ciberespaço civil nacional e o ciberespaço internacional, todos com zonas de sombra/comuns, ou seja, partilhando parcelas de território (AM, 2011). Nesta conferência chegou-se a algumas conclusões que seguidamente se transcrevem.

Se por um lado, "hoje, convive-se num mundo digital tipificado pelo designado «*Internet Time*», ou seja existe o acesso à informação, em qualquer instante, em qualquer local, a qualquer sítio, por outro lado, a época é do «*cutting*» e do «*paste*», com poucas cautelas do ponto de vista da qualidade e, muitas vezes, sem atentar em direitos de autor, o contexto é o da *Wikipedia*, da *Web 2.0* e das redes sociais" (AM, 2011).

Por outro lado, "a «computação em nuvem» e as Redes Sociais são um binómio em que um fornece os meios, e o outro fornece os atores. A sociedade é uma rede de redes, e um sistema de sistemas, transversal à atividade humana, onde cada ator é um nó dessa rede" (AM, 2011).

Para Paulo Nunes, "a definição de uma ENC passa por desenvolver um conjunto de iniciativas destinadas a garantir uma utilização mais livre, fiável e segura do ciberespaço. (…) Os novos desafios obrigam os Estados ao levantamento de novas capacidades, à revisão

dos seus modelos de governação e à geração de competências, cada vez mais associadas à exploração das TIC, ao acesso à *Internet* e à utilização do ciberespaço" (Nunes, 2012).

Constata-se, assim, que cada Estado terá de garantir, não só a utilização segura do ciberespaço aos seus cidadãos, mas, também, a salvaguarda da própria soberania. A Estratégia de Cibersegurança defendida por Paulo Nunes visa os vários setores da sociedade ao "disponibilizar benefícios económicos e sociais sustentáveis, estimular a criação de emprego, a sustentabilidade e inclusão social, extraindo o máximo benefício das tecnologias digitais e melhorando a estrutura de enquadramento nacional" (Nunes, 2012).

Por outro lado, a utilização segura e fiável do ciberespaço conduz a vulnerabilidades, que têm de ser cuidadosamente analisadas e, se possível, solucionadas e reduzidas. Deste modo, "a livre utilização da *Internet* tem um valor inegável e pode, assim, ser seriamente comprometido por uma vaga crescente de ciberataques, minando a confiança na segurança global do ciberespaço" (Nunes, 2012).

Deste modo, é através do esforço coletivo, da partilha de responsabilidades e da visão conjunta entre o governo, a administração pública, as forças armadas e de segurança, as empresas e os cidadãos que será possível construir um futuro digital para Portugal, seguro e sustentável (Nunes, 2012).

Recentemente, no 7º Simpósio Internacional sobre o ciberespaço, ficou evidente a vontade do Estado Português em investir no levantamento de capacidades de Cibersegurança, à imagem dos homólogos membros da UE, que encetaram esforços neste âmbito, pela intervenção da Secretária de Estado Adjunta e da Defesa Nacional, Dra Berta de Melo Cabral:

> "O Governo (…) destacou como linhas de ação prioritárias, a definição de uma Estratégia Nacional de Cibersegurança, a montagem de uma estrutura responsável pela Cibersegurança, e a sensibilização dos operadores públicos e privados para a natureza crítica da segurança informática e para o levantamento da capacidade de Ciberdefesa Nacional, reforçada inclusivamente na Reforma Defesa 2020". (AM, 2013)

3. Revisão dos Modelos

3.1. Metodologia de Análise

A primeira etapa do processo de criação de uma proposta de modelo de *Cyber Intelligence* iniciou-se com o estudo de modelos de *Cyber Intelligence*,que já se encontrem implementados em órgãos do Estado ou no setor privado. Porém, antes de se iniciar a revisão dos modelos, foram selecionadas as principais áreas de proveniência das fontes (Tabela 1) desses mesmos modelos. Deste modo, pretende-se abordar, pelo menos, um modelo com incidência nos seguintes âmbitos:

a. Segurança e Defesa (doutrina militar);
b. Governo (legislação estatal);
c. Indústria e Tecnologia (iniciativas do setor privado);
d. Investigação (publicações científicas).

Deste modo, é possível obter diferentes perspetivas e abordagens, permitindo, assim, um maior conhecimento sobre a temática.

Tabela 1 – Área de proveniência dos modelos de Cyber Intelligence

Segurança e Defesa	Governo	Indústria e Tecnologia	Investigação
Doutrina Militar	Legislação estatal	Sector Privado	Publicações científicas
Manuais OSINT OTAN *Política de Cibersegurança OTAN* *Doutrina militar norte-americana* *Robert Steele da OSS.Inc*	*Publicações e estudos* *DOD* *ODNI* *CRS*	*Empresas de Auditoria e Consultoria:* *Deloitte* *MITRE Corp* *SRC* *InfoSphere AB* *AccessData Group*	*Artigos de Institutos, Agências e outros Académicos:* *AFCEA* *INSA* *OSS.Inc*

A primeira ação realizada foi o levantamento dos modelos existentes e os respetivos autores, sendo selecionados, posteriormente, os modelos mais relevantes e a respetiva bibliografia.

A escolha dos modelos, abaixo indicados, baseou-se numa abordagem multidisciplinar, existindo a preocupação de analisar e compreender, pelo menos, um modelo de cada área de proveniência (Tabela 2).

Tabela 2 – Seleção dos modelos para revisão

Área	Autor	Modelo
Segurança e Defesa	OTAN	*Theoretical Framework of the OSINT Information Process*
Governo	*Intelligence Community*	*Cyber Intelligence Sharing and Protection Act*
Investigação	Robert Steele	*Intelligence Reform*
Indústria e Tecnologia	*MITRE Corp*	*Structured Threat Information eXpression*
	SRC	*Cyber Intel & Decision Support*
	AccessData	*Cyber Intelligence & Response Technology*
	InfoSphere	*Open Source Intelligence Support & Training*
	Deloitte	*Cyber Intelligence Risk Management*

Depois de selecionados os modelos a estudar, foi construída uma matriz que reúne as particularidades sobre cada modelo, indicadas de seguida. A compilação destes dados característicos permitiu criar um quadro síntese das características e orientações comuns a todos os modelos analisados, que se consideraram ser fundamentais para o desenvolvimento do presente trabalho:

a. As ideias principais;
b. As características comuns;
c. A metodologia;
d. Os seus planos de ação; e
e. As ferramentas mais relevantes.

3.2. Estudos de Caso

3.2.1. ***Theoretical Framework of the OSINT Information Process***

A OTAN tem vindo a criar doutrina em torno do conceito OSINT desde 2001. Inclusivamente, definiu os conceitos subsidiários de "*Open Source Data*" (OSD) e "*Open Source Information*" (OSI), referindo-se a ambos como a informação em bruto antes de ser objeto de recolha e tratamento. O OSD é relativa a elementos como fotografias e imagens de satélite comerciais, e o OSI são aos OCS, livros e relatórios de todo o género (Graça, 2003).

Importa primariamente, referir que a OTAN é uma organização político/ militar, que tem como objetivo principal preservar a liberdade e a segurança de todos os seus membros, por meios políticos e militares, pelo que as suas tarefas fundamentais são: a Defesa Coletiva, a Gestão de Crises e a Segurança Cooperativa[30] (OTAN, 2010). Por conseguinte, o foco principal da Política de Ciberdefesa da OTAN está relacionada com a proteção das suas redes internas, e com os requisitos de Ciberdefesa das redes nacionais dos estados membros, desta organização, que a OTAN depende para realizar as suas tarefas fundamentais.

Em termos de doutrina, a OTAN dispõe de três manuais essenciais, que definem toda a doutrina da Aliança e como deve ser organizada a OSINT: o "*NATO OSINT Handbook",* de 2001; o *"NATO OSINT Reader",* de 2002; e o *"NATO Intelligence Exploitation of the Internet",* de 2002. Além disso, a OTAN criou formalmente, em 2008, o *Cooperative Cyber Defence Centre of Excellence* (COC DCE), localizado em Tallinn, Estónia, com o fim de aumentar a capacidade de Ciberdefesa da OTAN. É de salientar o esforço deste centro de excelência, nomeadamente, na elaboração *National Cyber Security Framework Manual*, que veio fortalecer a Política de Cibersegurança da OTAN.

Em junho de 2011, a OTAN adotou uma nova Política de Ciberdefesa e respetivo plano de ação, que define uma visão clara de como a Aliança pretende reforçar os seus esforços, no domínio do ciberespaço. Esta política reitera que qualquer resposta de defesa coletiva está

[30] Conceito Estratégico da NATO para a defesa e segurança dos membros da Organização do Tratado do Atlântico Norte, adotado pelos Chefes de Estado e de Governo, na Cimeira da OTAN, em Lisboa, a 19 e 20 de novembro de 2010.

sujeita a decisões do Conselho do Atlântico Norte (NAC), o principal órgão de tomada de decisão política da OTAN (OTAN, 2011).

É de destacar, ainda, o papel do NAC, através da *Cyber Statecraft Initiative*, pelo contributo na cooperação, competição e conflito internacional, no ciberespaço.

Embora, o Modelo de *Cyber Intelligente* da OTAN não se encontre definido em nenhuma publicação dedicada a esta matéria, esta rege-se pelos princípios orientadores defendidos nos manuais de OSINT e são a base de raciocínio, para a sua aplicação no ambiente cibernético. Sendo assim, julgou-se pertinente abordar o modelo genérico de OSINT, procurando encontrar quais as suas linhas gerais e quais os aspetos que tem em comum com outros modelos de *Cyber Intelliegence*.

O presente modelo define como linha orientadora a *Internet*, que apesar de estar em constante mutação e evolução, é (ou deveria ser) o principal veículo de colaboração aberta, ao invés de um repositório de conhecimento. O objetivo da OTAN passa por aumentar a prevenção e a resiliência no ciberespaço, mediante a não-duplicação de informação. Para tal, é necessário aumentar a variedade de informação disponível e facilitar a interação com elementos não-OTAN, através da criação de *Cyber Intelligence* comum e de partilha multilateral, assim como, um entendimento comum entre as forças militares, os seus homólogos civis e organizações não-governamentais (ONG).

A OSINT é o meio mais rápido e importante de satisfazer as necessidades básicas de acesso à informação, incluindo necessidades de antecedentes históricos, contextualização atual e informações geo-espaciais gerais. Uma ferramenta robusta de OSINT aumenta, substancialmente, o número de fontes de informação disponíveis, para que as células de informações observem aos requisitos de informações.

Os princípios defendidos resumem-se a:

a. A ajuda de *Validated Open Source Intelligence* (OSINT-V) é muitas vezes o meio mais eficaz de providenciar apoio à decisão;
b. O "comandante" e os seus funcionários devem digerir, avaliar e fornecer *feedback* sobre toda a informação recebida;
c. O treino de exploração de fontes abertas é extremamente importante;
d. A OSINT pode ser partilhada com quem o "comandante" considere adequado;
e. A OSINT é absolutamente vital para o processo de todas as áreas das informações e deve ser integrada em todos os aspetos relacionados com esse processo.

Importa, então, questionar "O que há de novo sobre OSINT"? OSINT é a nova grande "força" nas OI do século XXI (OTAN, 2001:3). O que há de novo sobre OSINT é a confluência de três tendências distintas: a proliferação da *Internet* como uma ferramenta para a divulgação e partilha de informações claras; a consequente "explosão da informação", na qual o conhecimento publicado cresce exponencialmente; e o colapso de muitas áreas, que anteriormente eram negadas. A matriz de fontes abertas disponíveis é cada vez mais robusta, permitindo que os "comandantes" tentem satisfazer algumas das suas exigências de informação por si (OTAN, 2001:3).

O *NATO OSINT Handbook* (OTAN, 2001:5) define quatro pilares da Estratégia OSINT: as fontes, o *software*, os serviços e a análise, sendo que os três primeiros podem ser obtidos do setor privado (Tabela 3).

Tabela 3 – Tipos de fontes, software e serviços

Fontes	***Software***	**Serviços**
Meios de comunicação tradicionais	*Desktop "toolkit"*[31]	Serviços de recolha
Internet		Serviços de processamento
Fontes comerciais em linha privilegiadas (taxação pelo acesso)		Serviços de análise e produção
Outras formas de informação comercial em linha (Subscrição direta)		
Literatura cinzenta		
Observadores e especialistas		
Reprodução de imagens comerciais		

Por outro lado, a mesma publicação define o ciclo de OSINT em quatro fases principais: deteção, discriminação, destilação e divulgação (OTAN, 2001:15). Contudo, através da Tabela 4, podemos verificar que a evolução tecnológica e a emergência do ciberespaço deram lugar a uma maior delimitação do processo de análise OSINT, o que resulta no aparecimento de etapas importantes, como por exemplo, a etapa inicial de direção (OTAN, 2002b:4).

[31] Conjunto de 18 ferramentas de visualização e manipulação de dados, com instrumentos de modelagem, simulação e análise estruturada de argumentos (OTAN, 2001:13).

Tabela 4 – Diferentes fases de análise OSINT preconizadas pela OTAN

Fase	Ações
Direção	*Seleção e informações apropriadas;* • *Requisitos de informações críticas do comandante (CCIRs);* • *Suporte ao* conhecimento *situacional;* • *Requisitos prioritários de informações (PIRs);* • *Pedidos de informação (RFI).*
Recolha	*Como planear uma recolha de informação na Internet:* • *Determinar os requisitos de pesquisa de informação;* • *Determinar os melhores sítios ou estratégias de busca ("saber quem sabe");* • *Identificar os detalhes para aceder ou encontrar informações específicas;* • *Determine restrições de tempo de busca (Gestão do tempo).*
	Estratégias e ferramentas de pesquisa: • *Preparar antes de pesquisar (catálogos de bibliotecas, bancos de dados de referência, os recursos da Internet);* • *Seis passos para uma pesquisa de sucesso: (1) Identificar conceitos-chave; (2) Identificar os termos possíveis de pesquisa; (3) Decidir qual o método a usar para pesquisar; (4) Construir uma pesquisa própria; (5) Limitar a pesquisa; (6) Refinir a pesquisa;* • *Ferramentas de busca: motores de busca, meta-motores de busca, Deep-Web / "Web invisível".*
	Problemas relacionados: • *OPSEC;* • *Cumprimento com os direitos de autor;* • *Língua estrangeira;* • *Redes externas.*
Processamento e Exploração	• *Requer um conjunto de ferramentas de automação dedicado;* • *Requer um modelo claro de análise, capaz de distinguir o que é militar, civil e informação geográfica e também quais os níveis de análise — estratégico, operacional, tático e técnico;* • *Requer um sistema de autenticação do sítio Web e análise de fontes: precisão, credibilidade e autoridade, moeda, objetividade e relevância.*
Produção	*Os elementos-chave de apoio ao processo interativo e orientado para o consumidor são os relatórios, tabelas dinâmicas, ensino à distância e fóruns de conversação.*
Disseminação e Avaliação	*Alguns produtos OSINT podem ser partilhados abertamente e a sua divulgação pode ser:* • *Via rede interna classificada da OTAN;* • *Diretamente através da Internet;* • *Através do uso de uma rede privada virtual (VPN).*

É de salientar a importância da avaliação, do *feedback* e da formação. A avaliação e o *feedback* são dois conceitos de extrema importância, que se movem juntos em qualquer área de informações (Figura 1).

O processo de OSINT é entendido como um ciclo que nunca se esgota, na medida em que existe sempre um retorno e uma avaliação, para posterior ajustamento e novo ciclo, se necessário. Outra variável é a aprendizagem, pois somente com profissionais, altamente qualificados, treinados e competentes, se garantirá resultados superiores (OTAN, 2002B:4).

Figura 1 – Ciclo do processo de informações

Fonte: Adaptado do JP2_01 (DOD, 2012)

3.2.2. ***Cyber Intelligence Sharing and Protection Act***

O CISPA, acrónimo que significa *Cyber Intelligence Sharing and Protection Act,* entendido por muitos como uma forma de invasão da privacidade na *Internet*, é um projeto de lei, aprovado pela Camara dos Representantes dos EUA, a 19 de abril de 2012, que visa a partilha do tráfego de informações que circulam na *Internet* entre o governo, empresas de tecnologia e de indústria (H.R 3523, 2012).

Os defensores do projeto, argumentam que é necessária uma legislação para promover uma melhor partilha de informação sobre ciberataques ativos, resultando numa defesa de rede

mais efetiva. Os oponentes ao projeto de lei alegam que este permitirá o acesso aos dados pessoais para outros fins que não aqueles declarados (proteção de *Internet Protocol* (IP), a prevenção de pirataria e a supressão dos direitos da primeira emenda).

Contudo, o conceito do CISPA é permitir e incentivar os elementos da IC a partilhar informações de ciberameaças, com entidades do sector privado. Para que tal aconteça:

a. Proporciona a partilha de informações relativas a ciberameaças, entre a IC e entidades responsáveis pela Cibersegurança;
b. Estabelece políticas, atribui responsabilidades e prescreve procedimentos para operações de OSINT dentro do Departamento de Defesa (DOD);
c. Estabelece o *DOD Open Source Council*, como o mecanismo primário de governança para a OSINT do DOD.

No entanto, as perguntas que se colocam são as seguintes:

- Quais os benefícios deste projeto?
- Quais os pontos fracos deste projeto?

Em primeiro lugar, o CISPA conseguiu atrair a si corporações e grupos, como a *Microsoft*, o *Facebook*, a *IBM*, a *Apple Inc*. e a Câmara do Comércio dos Estados Unidos, que vêm o CISPA como um meio simples e eficaz, de partilha de informação importante, sobre ciberameaças, com o governo.

Em segundo lugar, o CISPA contém lacunas na delimitação sobre como e quando o governo pode monitorizar informações de navegação de um particular. Além disso, teme-se que esses novos poderes podem ser usados para espionar o público em geral, ao invés de perseguir os *hackers* maliciosos.

Em suma, o CISPA atribui autoridade ao governo para fornecer informações classificadas de ciberameaças ao setor privado e derruba as barreiras que impedem a partilha de informações de ciberameaças, entre empresas do setor privado e entre estas e o governo.

Tendo em conta, o que foi acima referido e o objetivo deste trabalho, é pertinente estudar este modelo, na medida em que este visa proporcionar a governança de *Cyber Intelligence*, disciplina reconhecida no apoio à tomada de decisões estratégicas de segurança nacional, a fim de facilitar as relações entre funcionários do governo e gestores do setor privado.

Este modelo permite-nos visualizar de que forma o Estado norte-americano perceciona a problemática das informações no ciberespaço.

> *"Informações classificadas relativas a ciberameaças só podem ser partilhadas por um elemento da comunidade de inteligência com entidades certificadas; ou a uma pessoa com um nível de segurança adequado para receber tais informações de*

> *ciberameaça (...) Nenhuma ação civil ou criminal deve encontrar-se ou ser mantida no Tribunal Federal ou Estatal contra uma entidade protegida, entidade auto-protegida, provedor de cibersegurança, ou um agente, empregado ou agente de uma entidade protegida, entidade auto-protegida ou provedor de cibersegurança, agindo de boa fé no uso de sistemas de cibersegurança ou partilha de informações, em conformidade com esta secção; ou por não agir perante informações obtidas ou partilhadas em conformidade com esta secção"* (H.R 3523, 2012).

Por outro lado, analisando o programa do DOD, este pressupõe algumas orientações, nomeadamente:

a. O DOD deve conduzir operações OSINT de uma forma coordenada e colaborativa e prosseguir em prol de uma integração e exploração total dos pressupostos OSINT;
b. Executar as funções especializadas OSINT de análise, de recolha e criar um centro de excelência, que irá apoiar e incentivar todas as agências de informações;
c. Garantir que os agentes e os sistemas de vigilância estão focados na obtenção de informações, que está ativamente encoberta;
d. A obtenção de informações a partir de fontes abertas no ciberespaço é geralmente menos dispendiosa e menos arriscada, do que a recolha de outras fontes de informações;
e. As informações secretas podem ser menos importantes do que a combinação de informações a partir de fontes abertas no ciberespaço, da partilha de informação e das redes de computadores;
f. Todos os analistas OSINT vão exercer práticas apropriadas de segurança de informações e espionagem, em conformidade com as políticas e normas do DNI;
g. Todos os esforços de exploração OSINT vão precaver procedimentos de verificação e validação de fonte/informações adequadas, em conformidade com políticas e normas do DNI.

O *Office of the Director of National Intelligence* (ODNI), em resposta a uma prerrogativa do *Intelligence Reform and Terrorism Protection Act*, de 2004, cria, em 2006, o conceito de *Nacional Open Source Enterprise*, do qual saem alguns princípios (IC, 2006):

a. O estabelecimento da posição do ADNI-OS, com responsabilidade de supervisão geral do esforço pelas fontes abertas;
b. A criação de um grupo de peritos OSINT, num centro de fontes abertas (*Open Source Center*);
c. Um sistema único de gestão de requisitos de fontes abertas;

d. O estabelecimento de uma arquitetura única de fontes abertas, para facilitar o acesso a uma ampla gama de potenciais consumidores, em níveis federais, estaduais, locais e tribais;
e. Criação de uma entidade para desenvolver e adquirir processos e tecnologias de ponta, que avança os esforços para adquirir e utilizar informações a partir de fontes abertas no ciberespaço.

O NOSC é um centro que incorporou e ampliou o *Foreign Broadcast Information Service* (FBIS)[32], serviço que forneceu produtos OSINT ao governo e outros exploradores até 2005, e está sob o comando da *Central Intelligence Agency* (CIA). As suas funções incluem:

a. Gestão da recolha, análise e pesquisa, formação e tecnologias de informação para facilitar o acesso e o uso de todo o governo;
b. Dirigir várias centenas de pessoas, a tempo inteiro, alguns dos quais estão noutras agências, com atribuições temporárias.

O objetivo do NOSC é fornecer um centro de excelência a explorar informações a partir de fontes abertas no ciberespaço, para todo o executivo. Para tal, o NOSC fornece traduções e transcrições de produtos de todo o mundo e mantém uma vasta coleção de material publicado, em formato eletrónico.

Por outro lado, a disponibilidade em rápida expansão de grandes bases de dados eletrónicas e a grande variedade de estratégias de pesquisa, requer treino intensivo e competências que só poderão ser adquiridas em escolas, com elevados padrões de profissionalismo.

O objetivo final do centro é maximizar a conectividade em todos os órgãos do governo e substituir o sistema baseado em formatos incompatíveis e duplicações extensas.

Seguidamente, foi criado, no seio do novo ODNI, o *Information Sharing Environment* (ISE), que pretende estabelecer políticas, procedimentos e tecnologias para interligar pessoas, sistemas e informações às agências do governo. O objetivo é encontrar o melhor equilíbrio entre a partilha de informação adequada e a segurança da informação eficaz.

Este plano tem três grandes ambições: estabelecer políticas e tecnologias consistentes entre as cinco grandes comunidades - Defesa, Informações, Segurança Interna, Negócios Estrangeiros e Justiça; incluir entidades estatais, locais, tribais e o setor privado; fornecer orientações e padrões tecnológicos; e, por fim, uniformizar práticas de segurança e

[32] O FBIS era uma componente de informação de segurança, da Direcção de Ciência e Tecnologia da CIA, que monitorizava, traduzia e divulgava informação disponível publicamente (OSINT), dentro do governo dos EUA, e informação dos *Media,* fora dos Estados Unidos.

metodologias de gestão de risco, para promover a aceitação de todo o governo. Em suma, partilhar informações tornou-se a missão central para as agências de informações (Best, 2007).

Para Army Sands[33], existem quatro categorias de fontes *Cyber Intelligence*: dados e informação disponível, amplamente na *Internet*; dados-alvo comerciais; especialistas; e literatura cinzenta. A OSINT pode, ainda, incluir, apesar de não ser classificada, informação considerada propriedade de uma empresa, sensível a nível financeiro e legalmente protegida ou pessoalmente danosa, abrangendo também informação oriunda da "Blogosfera".

O *Congressional Research Service* (CRS), pelas mãos do especialista Richard A. Best (2007), define alguns obstáculos no uso de OSINT, que se passam a enunciar:

a. A falta de cultura (idioma e história) dos analistas;
b. O preconceito relativo à *Cyber Intelligence*;
c. Os prazos apertados associados ao volume e à classificação de informação;
d. A formação e o treino ineficiente;
e. As ferramentas pouco inovadoras ou desatualizadas;
f. O efeito "eco", fenómeno caracterizado pela diferente informação dependendo da fonte;
g. A segurança, pela forma rígida de limitar o acesso à informação.

3.2.3. ***Intelligence Reform***

> *"O único avião sequestrado que não conseguiu atingir o seu alvo no «9/11» foi onde os cidadãos, armados com informações de fonte aberta, tiveram ação direta (...) A Comunidade de inteligência falhou onde alguns bravos cidadãos armados apenas com telefones móveis tiveram sucesso.* (Steele, 2006)

O autor da *Intelligence Reform*, Robert Steele[34], defende uma reestruturação profunda das informações, na medida em que coloca a OSINT como a base de todas as disciplinas de

[33] Cit. por Best, Richard e Cumming, Alfred – *Open Source Intelligence (OSINT): Issues for Congress*, 2007.
[34] Robert David Steele Vivas é o fundador e CEO da OSS.Net, Inc. Foi oficial de Infantaria durante 20 anos e esteve sempre ligado aos Serviços de informações, pelo que é conhecido, no meio, pela sua promoção das informações obtidas através de fontes abertas (Steele, R, *Reinveinting OSINT*, 2006).

recolha de informação "secreta", podendo mesmo ser a base para uma reforma total das informações, ao que alguns chamam de *Collective Intelligence.*

Defende, ainda, que o governo é o elemento catalisador, do chamado "Sistema de Informações a partir de fontes abertas no ciberespaço", e o beneficiário, das contribuições das *Seven Tribes*[35], através da partilha do seu próprio conhecimento direto e tácito. Resumindo, Steele defende que:

a. São necessários acordos de partilha de informações entre estas sete tribos;
b. É possível partilhar o conhecimento com segurança e com integridade financeira e moral, além-fronteiras;
c. É possível alcançar o que os suecos chamam *Multinational, Multiagency, Multidisciplinary, Multidomain Information-Sharing* (M4IS).

A teoria de Steele, aprofundada ao longo de muitos anos de estudos e dedicação, assenta nos basilares da doutrina militar, de coleção/ recolha, processamento e análise de fontes abertas. Contudo, ele vai mais longe, ao entender que o acesso à informação deve ser:

a. Livre, em todas as línguas, em qualquer lugar, a qualquer hora;
b. Interoperável, no processo multidisciplinar de análise de todas as fontes;
c. Integrado, na compreensão da história e cultura de todos os povos;
d. Global, na aceitação de todas as crenças e religiões.

O processo OSINT defendido pelo autor é idêntico ao divulgado pela doutrina OTAN, de forma que se salientam, apenas, os apontamentos reformadores, essenciais para o entendimento geral do modelo defendido.

De início, o processo de recolha visa responder a três reptos iniciais: procurar (*FIND*), obter (*GET*) e comprar (*BUY*), que o autor apelidou de *Collection Management.* Para tal, deve recorrer a sistemas autómatos, que concebem grandes velocidades. Os mesmos sistemas são versáteis o suficiente para permitir as visualizações e reposicionamentos desejados.

De seguida, na fase de processamento, tem lugar a tradução e a análise estatística automática. Com base em padrões de integração global de informações distribuídas, que permite o alerta prévio, deteta anomalias e análise de forma estruturada, permitindo, assim, que esta fase possa ser concluída de uma maneira oportuna e relevante. A necessidade de

[35] Expressão utilizada por Steele para definir as sete realidades da sociedade, envolvidas no processo de partilha de informações: governo, militares, justiça, negócios, meio académico, organizações não-governamentais e órgãos de comunicação social, e cidadania (cidadãos, sindicatos, religiões). (Steele, 2006).

análise automatizada de todas as fontes pressupõe estandardização, atributos geo-espaciais (*Google Earth*, por exemplo) e integração.

Entretanto, na fase de análise, é de salientar a importância de três princípios:

a. Rejuvenescimento do pessoal, ao contratar jovens analistas;
b. Abordagem *Soft*, ao substituir o investimento em máquinas, por formação e estrutura organizacional;
c. O futuro é global, no acompanhamento da evolução tecnológica além-fronteiras.

Steele revela, ainda, os seus conhecimentos numa proposta de reforma no Centro de Informações do DOD, a qual apelidou de *DOD OSINT Program.*

Em síntese, o programa aborda iniciativas OSINT para o DOD, das quais retiramos as nove principais:

a. Projeto de "História em suporte digital", digitalização de informação estrangeira relacionada com história, cultura, política e economia;
b. Armazém de dados de ONG's e redes de partilha de informação;
c. Grupos de trabalho virtuais especializados, com cobertura global;
d. Programa genérico de *Cyber Intelligence* (para todas as sete tribos);
e. Criação de conjuntos de ferramentas genéricas de análise;
f. Criação de cinco Centros Regionais de OSINT (multi-nacional);
g. Criação de um Centro de Negócios Internacional;
h. Implementação do Plano *Marshall* Digital;
i. Criação de uma Universidade da República.

O autor entende que as informações têm uma nova função, que pode ser entendida sob quatro perspetivas:

a. A primeira explora as lições de história;
b. A segunda desenvolve meios de partilha, na *Internet*, tendo em conta a cobertura global;
c. A terceira aproveita a distribuição completa dos recursos de OSINT, a toda a nação;
d. A quarta utiliza espiões e sigilo para garantir melhores resultados.

O principal contributo do plano reformista de Steele é o encentivo à partilha de informações, ao nível global, para reduzir o custo e o tempo, associados a atividades de monitorização global de ameaças, de interesse comum e, em especial, ameaças assimétricas não tradicionais.

Em conclusão, outro aspeto reformista relevante é o fortalecimento de uma estreita colaboração com o governo, no sentido de criar um núcleo genérico de trabalho analítico e um programa de formação de OSINT, ajustado aos interesses nacionais e aos interesses dos parceiros estrangeiros.

3.2.4. ***Structured Threat Information eXpression***

A organização *Mitre Corporation* apresenta um modelo de *Cyber Intelligence*, que se baseia numa linguagem, designada por STIX, que permite a captura, especificação, caracterização e comunicação de informação padronizada de ameaças cibernéticas.

Com este modelo, é possível garantir um apoio mais eficaz na gestão de ciberameaças, através de processos e aplicações de sistemas autómatos, permitindo, assim, o incremento da partilha de indicadores, originando, por sua vez, uma troca crescente e generalizada dos indicadores de gestão (de maior expressão).

O presente modelo baseia-se no princípio de que a ameaça que uma organização A enfrenta hoje, pode muito bem ser uma ameaça que uma organização B vai enfrentar amanhã. Perante esta premissa central, é imprescindível tomar ações, nos seguintes domínios: analisar as ameaças cibernéticas, especificar uma matriz de indicadores de ameaças cibernéticas, gerir as atividades de resposta a ameaças cibernéticas (prevenção e deteção de ciberameaças e resposta a incidentes) e partilhar informações de ameaças cibernéticas.

Porém, estas ações devem ser realizadas tendo em consideração alguns princípios orientadores:

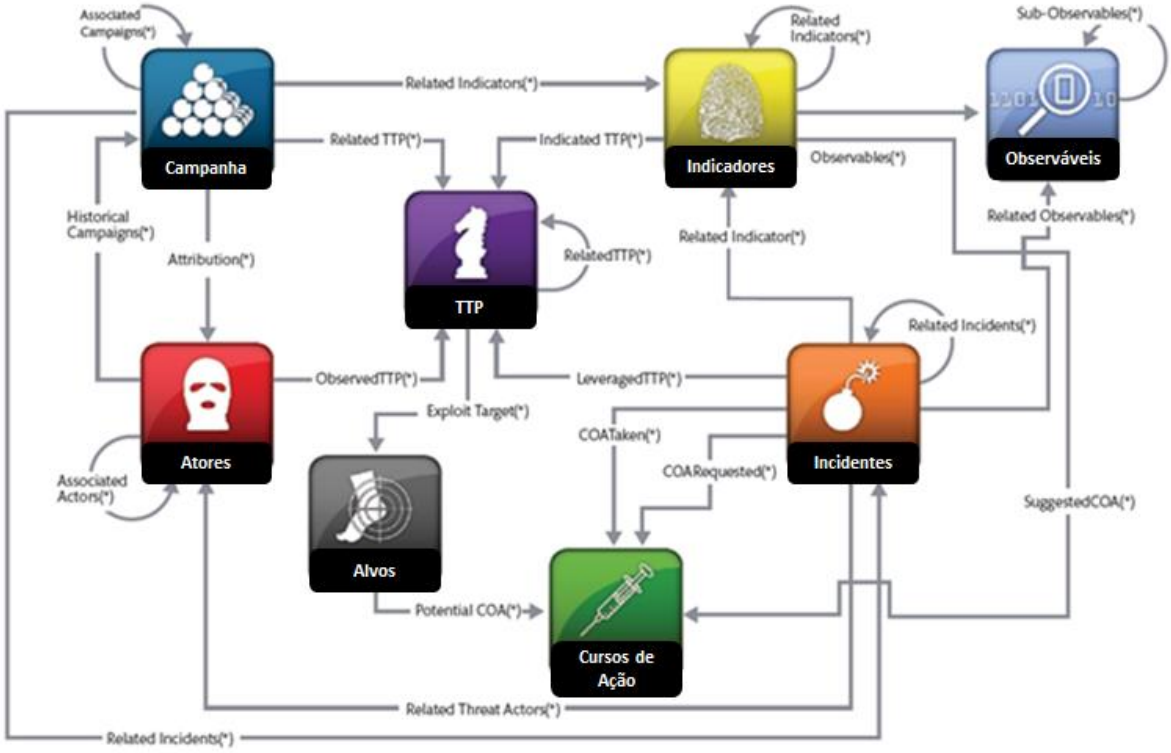
a. A expressividade. Proporciona uma cobertura expressiva agregada a todos os setores de ação.
b. A integração. Evita a duplicação de todas as representações na arquitetura global da STIX.
c. A flexibilidade. Possibilita que os usuários apliquem qualquer parte da representação padronizada, e a extensibilidade assegura o aperfeiçoamento e evolução da linguagem STIX.
d. A automatização. Maximiza a estrutura e consistência para suportar a automação.
e. A legibilidade. Preserva a análise humana a par do processo/consumo autómato.

Tendo em consideração, quais os domínios onde se devem tomar ações e quais os princípios orientadores, importa então conhecer e compreender a arquitetura da linguagem STIX, que se caracteriza pela unidade e similaridade.

A arquitetura estrutura as informações sobre ameaças cibernéticas em oito áreas (Figura 2), que de seguida se enumeram:

1. *Observable* (condições cibernéticas observáveis);
2. *Indicator* (indicadores);
3. *Incident* (incidentes);
4. *TTP* (táticas, técnicas e procedimentos dos adversários, incluindo infraestruturas, alvos, ferramentas e práticas mais comums);
5. *Exploit Target* (alvos, incluindo vulnerabilidades e fraquezas);
6. *Course of Action* (linhas de ação);
7. *Campaign* (campanhas de ciberameaças); e
8. *Threat Actor* (atores de ciberameaças).

Figura 2 – Arquitetura STIX da MITRE



Fonte: Adaptado de MITRE CORP, 2012.

Contudo, existem medidas que são imprescindíveis, para que este modelo alcance a sua máxima eficiência e eficácia:

a. Estimular o esforço colaborativo, orientado pela comunidade;
b. Definir e desenvolver uma linguagem única e comum;
c. Automatizar para apoiar a análise humana ou ações defensivas à velocidade de uma máquina;
d. Definição de representações estruturadas de informações sobre ameaças, que sejam expressivas, flexíveis, extensíveis, automatizadas e legíveis.

Este modelo poderá ser aplicado por organizações e/ou especialistas ligados à Segurança e Defesa, à Industria, à área Científica e ao Governo, incluindo consumidores e produtores de informações de ciberameaças, nas áreas de Departamento de Segurança Interna (DHS), Resposta a Incidentes e Gestão de Processos, Finanças, Investigação e Agencia para a Tecnologia e Informação.

3.2.5. ***Cyber Intel & Decision Support***

Para a *Syracuse Research Corporation* (SRC), *Cyber Intelligence* é sinónimo de "defender e ganhar no ciberespaço". Para isso, é necessário recolher, gerir, analisar e correlacionar dados, não classificados, da *Internet*, para proporcionar o conhecimento necessário para o apoio às operações no ciberespaço.

Deste modo, a SRC criou e implementou um modelo que fornece *Cyber Intelligence* e que estabelece serviços de apoio à decisão em "tempo útil, acionável e partilhável"[36], ao governo e aos operadores de infraestruturas críticas.

Por outras palavras, "é possível, através do presente modelo, fornecer informações de forma oportuna e acionável, aos operadores do ciberespaço, através da correlação de dados não classificados da *Internet* e de redes internas, permitindo que seja partilhável com todos os níveis de decisão do governo e responsáveis por infraestruturas críticas"(SRC, 2012).

Contudo, a SRC defende que, para se atingir a máxima eficiência e eficácia dos serviços de apoio à decisão, é necessário tomar algumas ações, nomeadamente:

a. Recolher dados de uma variedade de fontes abertas no ciberespaço e fazer uso das melhores tecnologias para gerir, analisar, correlacionar e sintetizar dados;
b. Informar e apoiar as operações no ciberespaço, ajudando os clientes a detetar, compreender e erradicar as ameaças, antes que se tornem brechas de segurança;

[36] Tradução do autor de "*on time, actionable and shareable*".

c. Fornecer *Cyber Intelligence* "para além do horizonte" e informação sobre os alvos[37], para uma preparação mais defensiva.

Importa, então, descrever de que modo é possível os serviços de apoio alcançarem um nível de competência tão elevado, que permita fornecer informações, de forma oportuna e acionável, aos operadores do ciberespaço e, além disso, partilhar a informação pelos vários níveis de decisão do governo e responsáveis por infraestruturas críticas.

Em primeiro lugar, para que as informações sejam consideradas "em tempo útil", é necessário garantir algumas condições, que se passam a explicar: deve existir o conhecimento prévio sobre a ameaça; conhecer e compreender, em tempo útil, as táticas, técnicas e procedimentos do adversário; proporcionar, em tempo oportuno, que as operações baseadas em *Cyber Intelligence* contribuam eficazmente para a missão; evitar o dispêndio elevado, em recursos para ações de recuperação e resposta a incidentes; por fim, fornecer, de forma imediata, dados partilháveis, para desenvolver informações acionáveis na condução proactiva de *Computer Network Defense* (CND).

Em segundo lugar, para que as informações sejam "acionáveis", é importante tomar algumas ações, designadamente: a informação baseada em dados da *Internet* deve ser não classificada e imaculada; deve-se construir uma abordagem integrada de *Cyber Intelligence*, ao correlacionar dados externos com dados internos de uma empresa; e, fazer uso de técnicas incisivas de exploração de dados (*Data Mining*), nessa informação fundida, para desenvolver informações acionáveis em operações adversárias, antes que os adversários penetrem na rede.

Por fim, mas não menos importante, é necessário que as informações sejam "partilháveis", sendo que é essencial garantir alguns requisitos como: reconhecer a necessidade de proteger fontes e métodos de partilha de informação; possibilitar a partilha de informação classificada, privilegiada, de redes protegidas; empregar recursos alternativos para colecionar e analisar dados não classificados; e, por último, permitir que a informação do Estado (*eGovernance*) seja convertida em informação passível de ser livremente partilhada com toda a estrutura do governo (da administração central ao poder autárquico), bem como aos responsáveis pelas infraestruturas críticas, no setor privado.

Resumindo, até ao momento foram explanados os requisitos e ações que os serviços de apoio devem observar e empregar para que alcancem a sua máxima eficiência e eficácia. No entanto, a SRC afirma ser fundamental que estes serviços tenham à sua disposição

[37] Tradução do autor de "*cyber intelligence over-the-horizon and target data".*

algumas ferramentas, consideradas fundamentais para que atinjam os seus objetivos com sucesso e que serão descritas de seguida.

a. *"DNSMapper™ Analysis Tool"*

Esta ferramenta proporciona aos analistas de *Cyber Intelligence* a capacidade, em tempo útil, de representar visualmente o domínio e associações de endereço IP. Esta ferramenta amplia o conhecimento situacional do analista, sobre o campo de batalha, isto é, o ciberespaço.

b. *DNSMapper* ™

A *DNSMapper* é uma ferramenta de análise que possibilita aos analistas questionar um determinado endereço IP, ou consultar um domínio e representar graficamente as relações de domínio/IP, ao longo do tempo. Os analistas serão, então, capazes de cruzar os dados de saída, o que permitirá descobrir domínios ou IP's associados anteriormente desconhecidos, com os alvos de interesse, pois exibe graficamente o domínio, o endereço IP e fornece o conhecimento situacional do campo de batalha (ciberespaço).

c. *"Data Collection Architecture Tool"*

Por sua vez, a *Data Collection Architecture Tool* é uma ferramenta de reconhecimento "à escala *Internet*", construída para satisfazer a necessidade de averiguação seletiva, rápida e anónima dos dispositivos de rede globais. Tem, também, a capacidade de realizar "toques" não-imputáveis, de baixa intensidade e *scans* personalizáveis, os rastreamentos e tarefas de coleção, permitindo a pesquisa de dados, de forma discreta e sem deixar um rastro detetável, como também, pode ser delineada uma arquitetura flexível, para requisitos específicos.

d. "Audit-Based Sense and Protection"

Atualmente, a SRC está a desenvolver uma ferramenta, designada por "*Enterprise-Scalable, Defensive Cyber Capability"* que vai permitir monitorizar a rede, de forma contínua, e emitir semanticamente informações sumárias, valiosas e em tempo útil, de estados de alertas de risco.

e. *"C-SCOPE"*

A C-SCOPE é um sistema de monitorização centralizado, capaz de mostrar informações em relação ao estado de prontidão dos vários sistemas CDS (*Content Delivery System*). O *"C-SCOPE"* fornece uma gestão proactiva, ao longo dos diferentes CDSs, presentes na empresa.

f. *"Cyber Intelligence Adversary Model"*

Este é o modelo em que a SRC se baseia para uma compreensão mais completa do ciberespaço e dos seus adversários. Assim, poderá defender-se proactivamente das redes de comunicação e aumentar a sua visão para as fases de uma intrusão, conhecida por "*Cyber Kill Chain*", permitindo que descubra como o seu adversário se configurou para realizar a intrusão (a esta técnica a SRC apelida de "*Supply Chain*").

Por último, a SRC é capaz de desenvolver, proactivamente, contramedidas, assim como informações estratégicas, operacionais e táticas para a exposição do endereço de risco, antes que um incidente ocorra.

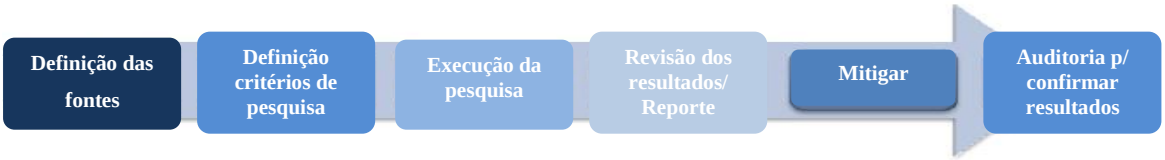
A SRC labora para uma vasta série de organizações, estatais e não estatais, dos vários setores da sociedade, nomeadamente, a Defesa Biológica e Química, os Sistemas de Comunicações, a Cibersegurança, a Guerra Eletrónica, a Análise Ambiental e a Saúde, as Informações/Vigilância/Reconhecimento, a Indústria, a Integração Operacional/ Radares e os Sensores.

Este modelo da SRC, tem aplicabilidade em vários setores, a saber: Organizações governamentais nas áreas da Defesa, Ambiente e Informações, como por exemplo a Marinha norte-mericana, o DHS, a Agência Nacional de Segurança norte-mericana, bem como, tem parcerias com universidades e organizações internacionais, como por exemplo em Taiwan e Israel.

3.2.6. ***Cyber Intelligence & Response Technology***

A *AccessData Group* estabelece um modelo integrado, baseado numa *Cyber Intelligence & Response Technology (CIRT) Security framework.* Esta *framework* de segurança assenta numa única plataforma de segurança, que integra computadores, análise de rede e de *malwares*, auditoria de dados em larga escala e erradicação (Figura 3).

Figura 3 – Metodologia de análise da AccessData



Fonte: Adaptado de AccessData, 2013.

Esta plataforma de segurança caracteriza-se pela integração e automação, possibilitando não só identificar, mas também perseguir e corrigir a fuga de dados. O modelo está desenhado de forma a:

a. Identificar falhas de segurança, reproduzir eventos, analisar registos e correlacionar essas informações com o que está a acontecer, para determinar como se propagam as fugas de dados;
b. Permitir um emprego mais eficaz no combate a qualquer tipo de ameaças de segurança, através da análise integrada e capacidades de mitigação construtivas;
c. Construir uma solução de investigação para atender às necessidades específicas da organização, através de uma recolha de produtos ao nível empresarial, que permita a expansão das capacidades de investigação, conforme as necessidades e a evolução da empresa;
d. Detetar ameaças desconhecidas e reduzir os tempos de resposta.

Assim, existem princípios orientadores que a empresa definiu e que se traduzem em medidas, baseadas na proactividade e reactividade, como por exemplo:

a. Não permitir a fuga de dados que o *Data Loss Prevention* (DLP)**,**erradamente, consente;
b. Detetar novos *malwares* que o *Intrusion Detection System* (IDS) e o antivírus não reconhecem;
c. Monitorizar a atividade dos funcionários na *Internet*, quando estes não estão conectados à sua rede;
d. Criar perfis de ameaça para prevenir a recorrência de ameaça;
e. Colaborar, em tempo real, através de um interface *Internet* seguro, com todos os membros da equipa CIRT, durante um incidente.

De uma forma resumida, a arquitetura/ *framework* pode ser descrita por seis grandes áreas de ação (Tabela 5), que englobam pessoas altamente habilitadas, processos integrados e automatizados e tecnologia de ponta.

A CIRT é ainda constituída por quatro componentes-chave que são: o *AD Enterprise*, o *SilentRunner*, o *Cerberus*, e o *AD eDiscovery*.

Através da estrutura de segurança apresentada pela CIRT, podemos encontrar os recursos críticos que, atualmente, faltam numa infraestrutura de Cibersegurança tradicional, designadamente: a visibilidade, a automação, a integração e a colaboração, numa só plataforma, independentemente, do tamanho da organização, ou seja, pessoas, processos e tecnologia.

Tabela 5 – Arquitetura CIRT

	Área de ação	Processos e Tecnologia
1	Facilidade de utilização, fluxo de trabalho orientado para o processo (*process-oriented*) e comunicações.	- *Web-base Interface* fácil de usar e que permite comunicações em tempo real; - Atribui tarefas e acompanha o progresso.
2	Resposta a incidentes eficaz, incluindo a análise de todos os processos ativos.	- Verificações automáticas (*scans*) em todas as máquinas em busca de anomalias; - Correlaciona dados estáticos e voláteis com o tráfego da rede; - Análise integrada e recolha forense da partilha em rede; - Processador de dados *(Data processing wizard)* fácil de utilizar.
3	Captura rápida e em tempo real de dados na rede.	- Grandes velocidades de captura; - Armazenamento em base de dados centralizado; - Análise e registo correlacionado.
4	Análises de padrões e conteúdos com reprodução de incidentes por solicitação.	- Ferramentas avançadas de ajuda na visualização da *root cause analysis* mais eficaz; - Representações gráficas interativas que ilustram a propagação; - Mapa de proliferação de vírus, ameaças e fugas de dados confidenciais.
5	*Superior Smart-Target*, Auditoria de grande escala.	- Forma eficiente e autómata de detetar fugas de dados; - Determinar onde se encontram dados pessoais ou classificados e categorizá-los; - Conduzir auditorias autómatas usando critérios de pesquisa virtuais.
6	Poder de agir de imediato, eficazmente e com segurança.	- Resposta rápida a alertas, correlacionando o utilizador com o tráfego na rede; - *Right click process kill*;

Em suma, cumprindo as medidas e os princípios orientadores, o presente modelo facilita a monitorização contínua e a *Counter Cyber Intelligence*, possibilitando, assim, uma agenda automatizada das operações em curso, com informações em tempo real.

Por outro lado, permite não só detetar, proactivamente, as ameaças à segurança, como também, correlacionar o registo de eventos. Permite ainda, identificar, analisar e corrigir, rapidamente, as causas.

Por fim, o modelo em questão emprega análises integradas e reúne *Cyber Intelligence* de forma eficiente, possibilitando a construção de perfis para defender a rede.

Este modelo, concebido pela *AccessData* serve organizações que procuram preencher lacunas na deteção, análise e correção, que atualmente subsistem na arquitetura de segurança de informação tradicional, nomeadamente serviços e órgãos governamentais ligados à Justiça, à Segurança e às Finanças.

3.2.7. ***Open Source Intelligence Support & Training***

A InfoSphere AB é uma empresa de consultoria sueca, com experiência na área da Informações e Estratégia do Conhecimento[38], e que tem como principal objetivo assistir no desempenho superior da organização, dando acesso a informações críticas, apoiando, assim, a tomada de decisão e a resolução de problemas, por desbloqueio de ativos de informação. Por outro lado, fornece a base de uma gestão efetiva de risco, peça fundamental na vantagem competitiva, quando falamos de gerir riscos, reputação e relações.

Em suma, pretende responder a três questões essenciais:

a. O quê? - Trabalhar cuidadosamente em conjunto com os clientes na adoção dos requisitos de informações, transformando "*nice to have*" em apenas "*need to know*";
b. Quando? – Operações de 24 horas/7 dias por semana, uma vez que é uma empresa em rede, trabalhando em todos os fusos horários;
c. Como? - Adequar produtos às necessidades do cliente, abrangendo *briefings*, relatórios extensos de multimédia ou implementação de Informação nos portais da empresa.

[38] Tradução do autor de "*Intelligence & Knowledge Strategy".*

Assim sendo, a *InfoSphere AB* oferece três serviços distintos, que visam perseguir os objetivos da empresa e responder às necessidades do cliente:

a. Serviços de apoio à decisão *(Decision Services);*

b. Consultoria de estratégia do conhecimento *(Knowledge Strategy Consulting);*

c. Formação e apoio baseado em informações obtidas a partir de fontes abertas *(Open Source Intelligence Support & Training),* apenas para organizações internacionais e governamentais.

Esta empresa tem provas dadas na utilização e desenvolvimento de metodologias, no campo da OSINT, em combinação com a execução de uma estratégia rentável de Conhecimento Comercial (*Business Knowledge*).

O processo de pesquisa e os serviços de informações (*Research & Intelligence Services*) são caracterizados pela assessoria, aos escalões superiores, de perspetivas imparciais, externas e seguras, críticas para o sucesso da empresa, fornecer aproximações exclusivas para questões complexas e divulgar a informação necessária para tomar as melhores decisões estratégicas e otimizar os resultados.

O modelo defendido pela *InfoSphere AB* é baseado no conceito sueco, cujo termo em inglês se refere a *Multinational, Multiagency, Multidisciplinary, Multidomain Information-Sharing (M4IS)* e que, segundo esta, visa as seguintes premissas:

a. Recolha OSINT (*online e offline*, em mais de 40 idiomas);
b. Formação OSINT (recolha, análise, produção e apresentação);
c. Análise OSINT (*ad-hoc*, *outsourcing*, segunda opinião);
d. Sensibilidade na realização de dados/traduções em multi-formatos;
e. Análises consequentes (culturais, políticas, económicas, éticas, sociais);
f. Recolha, normalização e contextualização de dados, para o formato de importação do cliente;
g. Formação contínua dos métodos utilizados para obter OSINT.

A metodologia seguida desenvolve-se pela integração de uma rede global de profissionais de informações, suportada por tecnologia de ponta, que ajuda a descobrir informação, a criar conhecimento, a fornecer o aviso prévio, a identificar oportunidades e a oferecer uma vantagem superior. De seguida, são mencionadas as suas principais características:

a. Informações coletadas num formato *eXtensible Markup Language* (XML) uniforme;
b. Gestão de dados estruturados e não estruturados;

c. Verificações de antecedentes, análise dos *media* e mapeamento de relações entre pessoas, empresas e organizações;
d. Avaliações, baseadas em previsões futuras;
e. Atualizações de eventos, em tempo quase real, que podem afetar operações comerciais;
f. Análise e monitorização contínua.

Consequentemente, os efeitos pretendidos vão desde as imagens detalhadas, com diferentes modos de visualização (*zoom)*, aos bancos de dados interativos, à confidencialidade, ao acesso anónimo para uma rede de ativos de recolha; as *frameworks*, ao aviso prévio personalizado e estratégias de apoio e aos cenários e indicadores básicos (*road map*).

O Sistema de Gestão de Informações Não-Estruturadas é um sistema que permite minimizar o impacto negativo do uso de diferentes idiomas, na medida em que existe uma grande necessidade de conhecimento linguístico e de tradução, para além da língua inglesa. Por outro lado, o uso de diferentes formatos de informação, tem grande impacto na sustentabilidade das diferentes abordagens.

A *InfoSphere* gera relatórios, rápidos e precisos, a nível tático, operacional e estratégico. A entrega dos conteúdos OSINT da *InfoSphere* é direcionada via *feed RSS* ou XML, ou uso direto, através da plataforma *Able2Act*[39]. Através de uma tabela de diferentes graus de classificação (Tabela 6), os profissionais da *InfoSphere* classificam as informações, de acordo com a credibilidade e precisão das fontes.

Tabela 6 – Graus de classificação da InfoSphere

A	Totalmente confiável
B	Geralmente confiável
C	Razoavelmente confiável
D	Geralmente não confiável
E	Não confiável
F	Confiabilidade não pode ser julgada
1	Confirmada por outras fontes
2	Provavelmente verdadeira
3	Possivelmente verdadeira
4	Duvidosa
5	Improvável
6	Precisão não pode ser julgada

[39]*Able2act* oferece uma gama de produtos de diferentes informações semi-estruturadas, tais como biografias, perfis de organização, perfis de empresas, monitorização dos arquivos Media, cibercrime, guerra de informação.

A *Silobreaker* é um centro virtual de obtenção de informações a partir de fontes abertas no ciberespaço, que incide sobre a informação pública, encontrada em jornais, revistas, boletins informativos, vídeo, sítios da *Internet*, "Blogs".

A *Silobreaker Enterprise Software Suite* apresenta uma rede de relacionamentos, pontos de interesse geográfico, artigos globais, conversas públicas, bem como conexões entre pessoas, empresas, lugares e outras entidades.

Tendo construído capacidades de procura e de análise robustas, o *software* do Silobreaker, lida com textos, vídeos, imagens e outros conteúdos multimédia, apresentando os resultados, para os seus clientes, através de uma variedade de gráficos. Por outro lado, conecta a taxonomias complexas, dicionários de sinónimos, línguas e outros dados internos, para fornecer resultados específicos do mercado e da indústria.

O objetivo é ajudar qualquer pessoa a prever, prevenir e resolver problemas, antes que se tornem crises, e criar uma alta consciencialização, orientada para a resposta e aplicações de pesquisa analítica, numa só plataforma.

3.2.8. ***Cyber Intelligence Risk Management***

O modelo de *Cyber Intelligence*, definido pela *Deloitte*, é baseado na gestão de riscos, relacionados com a segurança e a proteção de infraestruturas criticas. De acordo com o modelo, o risco é tido como um estímulo à decisão e não, como uma consequência de decisões, que já foram tomadas.

Dito isto, a capacidade de gestão de risco de ciberameças complexas é fundamental, sendo que, deve ser salvaguardada a não-partilha de informação não autorizada, bem como o acesso não autorizado à informação.

Em suma, a gestão de risco da *Deloitte* é perspetivada mediante o risco associado, perante determinadas oportunidades ou perante determinadas ameaças. Sendo assim, além das restrições no acesso à informação, o uso de tecnologias e de processos, que monitorizam o tráfego de saída de informações, são a base do presente modelo.

Com a implementação deste modelo é possível sincronizar as iniciativas de Cibersegurança, enquanto são prioritizados os investimentos baseados no risco, desempenho e valor para a missão - desde a ciberforense e as ciberameaças, à força de trabalho na gestão da prontidão e identidade.

Devendo-se, então, primariamente, estabelecer uma estrutura de governança no ambiente cibernético (*Cyber Governance)*, que englobe informações de ciberameaças (*Cyber Threat Intelligence),* mitigação de ciberameaças *(Cyber Threat Mitigation) e* resposta a ciberincidentes *(Cyber Incident Response).*

Deste modo, uma organização que opte por implementar este modelo garante que será mais resiliente para lidar com a adversidade e mais ágil na procura de oportunidades.

Assim, ao realizar uma gestão de risco da ciberameaça mais eficaz, concede à organização uma maior confiança para assumir certos riscos "recompensados", para prosseguir novo valor.

Importa, então, compreender quais as níveis de intervenção, que o modelo em estudo preconiza. Existem três níveis de gestão de risco no seio de qualquer empresa:

a. *Risk Governance Level:* É o nível onde existe envolvimento entre o conselho de administração e a direção executiva, sobre o risco de ciberameaça: uma abordagem formal e disciplinada na monitorização do risco de ameaça cibernética. Pode, por exemplo, ser o *Chief Information Officer;* um quadro de relatórios do conselho de administração pode incluir métricas ou indicadores chave de desempenho (*KPI*);
b. *Risk Infrastructure and Executive Management Level*: É o nível responsável pela implementação e manutenção das pessoas, processos e elementos tecnológicos necessários para fazer a gestão de risco;
c. *Risk Ownership Level:* É o nível onde os funcionários têm responsabilidades bem definidas, apropriadas para o seu papel, para a gestão de risco de ciberameaça; orientações de como usar e partilhar informações; treino funcional apropriado; através de comunicações, avaliações de desempenho, e mesmo incentivos que suportam o comportamento desejado.

Porém, segundo a *Deloitte,* existem quatro princípios orientadores que garantem a resiliência do ciberespaço que devem ser observados, serão explanados de seguida:

a. Reconhecer a interdependência - todas as partes têm um papel na promoção da resiliência num espaço digital partilhado;
b. O papel da liderança - estimular a liderança e consciência do nível executivo para a gestão de riscos cibernéticos;
c. Gestão integrada do risco - desenvolver a implementação de um programa prático e efetivo;

d. Promover a captação - estimular fornecedores e consumidores a desenvolver um nível semelhante de consciência e compromisso, onde apropriado.

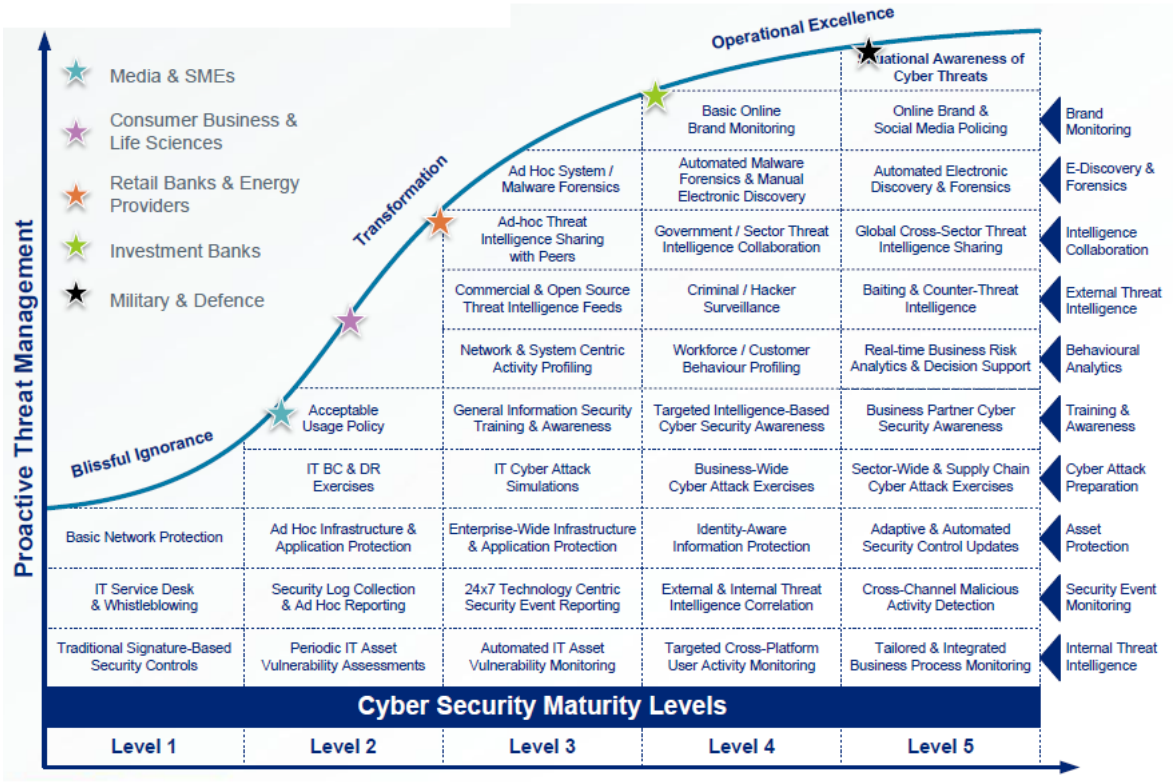
O presente modelo baseia-se numa arquitetura de 5 estágios de maturidade sucessivos (Figura 4), que vão ter repercussões em toda a estrutura da organização:

1. Estágio 1: Inicial;
2. Estágio 2: Fragmentada;
3. Estágio 3: *Top-Down*;
4. Estágio 4: Integrada;
5. Estágio 5*: Risk Intelligent*.

Durante a sua aplicação, estão previstos diferentes comportamentos nos vários escalões, consoante o estágio de maturidade. Mas, quando o modelo atinge o quinto estágio, alcança a maturidade máxima, sendo que para isso, a organização deverá estar dividida em 3 escalões, já anteriormente mencionados:

a. *Risk Governance*: que inclui orientação estratégica e supervisão de risco, liderado pelo conselho de administração;
b. *Risk Infrastructure and Management:* que inclui a conceção, a implementação e a manutenção de um programa de riscos eficaz. São quatro os grupos responsáveis envolvidos neste nível:
    i. Grupo dos gestores executivos;
    ii. *Enterprise Risk Group*;
    iii. Grupo dos auditores internos e
    iv. Grupo de gestão de risco;
c. *Risk Ownership:* que inclui a identificação, a medição, a monitorização e a elaboração de relatórios sobre riscos específicos, liderado pelas funções de apoio e unidades comerciais.

Figura 4 – Modelo de maturidade da Deloitte



Fonte: Deloitte, 2012.

Ainda assim, o modelo em estudo prevê que para se garantir a sua máxima eficiência e eficácia é indispensável o uso das seguintes medidas:

a. Avaliação da ameaça: Compreender o valor dos ativos da sua organização e as vulnerabilidades atuais;
b. Rede de informações: Estabelecer contínuas parcerias no sentido de partilhar boas práticas, experiências e conhecimentos;
c. Gestão de risco: Integrar todos os sistemas internos transacionais e de segurança;
d. Trazer o Chief Executive Officer **(**CEO) para a tomada de decisão: os *Chief Security Officer* (CSO) devem ser assessores e líderes de negócios;
e. Relação Comercial: usar a *Cyber Intelligence* para permitir a redução do risco e o prejuízo no negócio.

Este modelo, defendido pela *Deloitte*, tem aplicabilidade em vários setores da sociedade, designadamente: organizações ligadas à Tecnologia, à Industria, ao Setor Financeiro e à Administração Pública**.** Por último, a *Deloitte* desenvolveu, também, recentemente, um *Cyber Intelligence Center* que visa ajudar a monitorizar as empresas, analisar e responder a ciberameaças.

3.3. Análise Comparativa dos Modelos

O objetivo desta análise comparativa é confrontar as diferentes perspetivas da utilização de *Cyber Intelligence*, nas diferentes áreas de atuação e níveis organizacionais, segundo requisitos e capacidades comuns a todos os modelos. O levantamento e seleção destes requisitos e capacidades preconizam o primeiro passo na definição das variáveis-chave que, posteriormente, serão alvo de estudo.

Assim, as linhas orientadoras desta análise prendem-se, essencialmente, com uma leitura abreviada dos objetivos, metodologia e principais medidas de ação e respetivas ferramentas.

Para proceder à análise comparativa dos modelos, que neste capítulo estão descritos, apresenta-se de seguida um quadro síntese das principais características de cada abordagem (Tabela 7).

Tabela 7 – Quadro síntese da análise comparativa dos modelos

Modelo	Objetivos	Metodologia	Ferramentas
Theoretical Framework of the OSINT Information Process da OTAN	- **Prevenir e detetar** ciberataques; - **Integrar** a OSINT no processo de todas as disciplinas de Informações; - **Aumentar** o leque de informações disponíveis aos analistas; - **Estabelecer** um processo interativo com outros órgãos de Informações; - **Facilitar** a interação com elementos não-OTAN; - **Cooperar** com a Europa e outros países não-OTAN (PfP);	Ciclo OSINT: - **Procura,** - **Discriminação,** - **Produção e** - **Disseminação**.	- **Arquitetura partilhada**, com *hardware* e *software* interoperacional. - Ferramentas que permitem o cumprimento de OPSEC, salvaguarda dos direitos de autor, **tradução**, **análise de tráfego de redes** internas e externas, **autenticidade**, **reporte**, fóruns. - Uso de **VPN**. - Transferir o risco para o setor privado; - **Equipa de monitorização 24h**..
Cyber Intelligence Sharing and Protection Act dos EUA	- **Obter e partilhar** informação que tem sido escondida (classificada); - **Colecionar** informação com menos risco e menos dispendiosa; - **Verificar e validar** informações apropriadas; - **Criar** um centro de excelência de exploração de fontes abertas; - **Providenciar** transcrições de produtos em linha; - **Manter** uma vasta coleção de material publicado em suporte eletrónico.	- **Projeto de digitalização** de informação cultural e histórica (estrangeira); - **Treino e formação** específica OSINT para todos os atores dos *Seven Tribes*; - **Desenvolvimento e aquisição de tecnologias e processos** avançados;	- **Bases de Dados** extensíveis; - ***Generic Analítical Tool-Kit***; - **Monitorização global**; - **Formatação única**; - **Formatação de requisitos única**; - **Tradução** em vários idiomas; - **Prioritização de documentos**; - **Imagens de Satélite** (*Geospacial Intellegence Agency*); - **Armazenamento e acesso livre** a todas as redes ONG's; - **In-Q-Tel** (empresa de desenvolvimento de tecnologia com parcerias com o setor privado);

Intelligence Reform de Robert Steele	- **Ter acesso** a todas as informações, em todas as línguas, o tempo todo; - **Investir** fortemente na compreensão da história e cultura de todos os povos; - **Desenvolver** monitorização em tempo real (24/7) e em contexto geoespacial, a todos os níveis de governação; - **Investir** na educação e treino dos operacionais; - **Promover** as oportunidades em prol das ameaças; - **Partilhar** conhecimento de forma segura e com integridade financeira e moral.	Ciclo do processo OSINT: - **Definição de requisitos,** - **Processo de Recolha,** - **Processamento e exploração,** - **Processo de Análise,** - **Produção,** - **Avaliação,** - **Disseminação e** - ***Feedback*.**	-**Automação** e **interoperabilidade** de todo o processo de análise de fontes; - **Uniformização** de procedimentos e protocolos/ linguagens. - **Digitalização** e **visualização** instantânea;
Structured Threat Information eXpression da MITRE Corp	- **Apoiar** mais eficazmente a gestão de ciberameaças através de processos e aplicações de sistemas autómatos; - Ampliar a partilha de indicadores para permitir a troca generalizada de conjuntos significativamente mais expressivos dos indicadores de gestão; - **Gerir** atividades de resposta a ameaças cibernéticas (Prevenção e deteção de ciberameaças e resposta a incidentes).	**Arquitetura única e comum** que interliga o conjunto de informação de ciberameaças em 8 principais áreas: - Condições cibernéticas observáveis, - Indicadores, - Incidentes, - *TTP's*, - Alvos, - Linhas de ação, - Campanhas de ciberameaças, - Atores de ciberameaças.	- **Análise de ciberameaças**; - **Partilha de informação** de ciberameaças; - Estrutura e consistência capaz de suportar a automação; - Usuários capazes de aplicar qualquer parte da representação padronizada; - **Integração** vez de duplicação de todas as representações na arquitetura geral STIX;

Cyber Intel & Decision Support da SRC	- **Recolher** dados de uma variedade de fontes e fazer uso das melhores tecnologias. - **Coletar, gerir, analisar e correlacionar** dados não classificados da Internet, para apoiar as operações no ciberespaço; - **Fornecer** informação partilhável com todos os níveis de decisão do governo e responsáveis por infraestruturas críticas.	- Representação visual do domínio e associações de endereço IP. - Averiguação seletiva, rápida e anónima de dispositivos de rede globais. - Monitorização e emissão de informações sumárias de estados de alertas de riscos. - Gestão proactiva ao longo dos diferentes CDS's presentes na empresa.	- **Orientação para a preparação defensiva**. - **Ferramenta de análise**. - **Ferramenta de reconhecimento.** - **Sistema de monitorização e gestão proactiva**.
Cyber Intelligence & Response Technology da AccessData	- **Identificar** falhas de segurança, reprodução de eventos e análise de registos; - Detetar proactivamente as ameaças desconhecidas e reduzir os tempos de resposta; - **M**onitorizar a atividade dos funcionários na Internet, quando estes não estão conectados à sua rede; - **Colaborar**, em tempo real, através de um interface Web seguro, com todos os membros da equipa CIRT, durante um incidente.	Uma plataforma de segurança integrada e autómata**:** ***- Incident Response & Cyber Intelligence*** ***- Information Assurance & Compliance Auditing*.** As quatro componentes-chave do CIRT: ***- AD Enterprise***, ***- SilentRunner***, ***- Cerberus,*** ***- AD eDiscovery***.	- Integra **as pessoas, os processos e a tecnologia**. - **Facilidade de utilização**, fluxo de trabalho orientado para o processo (*process-oriented*) e comunicações; - **Captura rápida** e em tempo real; - Criação de **perfis de ameaça** para prevenir a recorrência de ameaça; - ***Superior Smart-Target***; - **Auditoria** de grande escala;

Open Source Intelligence Support & Training da InfoSphere	**- Assistir** no desempenho superior da organização, dando acesso a informações críticas; **- Apoiar** a tomada de decisão e resolução de problemas por desbloqueio de ativos de informação; **- Fornecer** uma perspetiva imparcial, externa e segura, crítica para o sucesso da empresa; **- Trabalhar** cuidadosamente em conjunto com os clientes na adoção dos requisitos de Informações; **- Adequar** produtos às necessidades do cliente, abrangendo *briefings*, relatórios extensos de multimedia ou implementação de Informação nos portais do empresa.	**- Coleção de informações de fonte aberta** em mais de 40 idiomas; **- Formação em informações de fonte aberta** (coleção, análise, produção e apresentação); **- Análise de informações de fonte aberta** (*ad-hoc*, *outsourcing*, segunda opinião); **- Sensibilidade de realização de dados/traduções em multi-formatos**; **- Análises consequentes** (culturais, políticos, económicos, éticos, sociais); **- Coleção, normalização e contextualização de dados para o formato de importação do cliente**; **- Formação contínua** dos métodos utilizados para obter Informações de Fonte Aberta. *Baseado no conceito sueco, cujo termo em inglês é *Multinational, Multiagency, Multidisciplinary, Multidomain Information-Sharing (M4IS)*	- Integração de uma rede global de **profissionais** de informações, suportado por **tecnologia** de ponta; **- Operações 24/7**, uma vez que é uma empresa em rede, trabalhando em todos os fusos horários; - Informações coletadas em um **formato XML uniforme**; **- Gestão de dados estruturados e não estruturados**; - Verificações de antecedentes, análise de *media* e **mapeamento** de relacionamento de pessoas, empresas e organizações; **- Avaliações** baseadas em previsões futuras; **- Atualizações** de eventos**,** de tempo quase real, que podem afetar operações comerciais; **- Análise e monitorização contínua**. ***Silobreaker Enterprise Software Suite*** - apresenta uma rede de relacionamentos, pontos de interesse geográfico, artigos globais, conversas públicas, bem como conexões entre pessoas, empresas, lugares e outras entidades.

Cyber Intelligence Risk Management da Deloitte	- Garantir a resiliência do Ciberespaço; - Sincronizar iniciativas de Cibersegurança enquanto prioriza investimentos baseados no risco, desempenho e valor para a missão; - Estabelecer uma estrutura de *Cyber Governance*; - Dispor de tecnologias e processos que monitorizam o tráfego de saída de informações. - Estimular a liderança e consciência do nível executivo para a gestão de riscos cibernéticos; - Desenvolver a implementação de um programa prático e efetivo - Gestão integrada do risco.	Programa de maturidade baseado em 5 estágios sucessivos: - Estágio 1: Inicial, - Estágio 2: Fragmentada, - Estágio **3: *Top-Down*,** - Estágio **4: Integrada, e** - Estágio **5*: Risk Intelligent*.** As organizações estão divididas em 3 escalões: - ***Risk Governance*:** - ***Risk Infrastructure and Management:*** - ***Risk Ownership:***	- ***Risk Governance Level****:* envolvimento entre o conselho de administração e a direção executiva, sobre o risco de ameaça cibernética; - *Risk Infrastructure and executive management Level:* é responsável pela implementação e manutenção das pessoas, processos e elementos tecnológicos; - *Risk Ownership Level:* Os funcionários têm responsabilidades bem definidas, orientações de como usar e partilhar informações.

4. Proposta de Modelo

4.1. O Modelo

4.1.1. Descrição geral do Modelo

O modelo proposto de *Cyber Intelligence* descreve as variáveis, ou os parâmetros, principais do problema, seguido da identificação do espectro de valores ou condições que cada parâmetro expressa nas possíveis soluções para o problema. As variáveis e condições do modelo resultam de dados empíricos, obtidos da análise de conteúdos efetuada sobre os diferentes modelos adotados, nos diversos setores da sociedade (Militar, Governamental, Setor Privado).

O presente modelo é orientado pelos conceitos de multidisciplinariedade, complementaridade e integração. Em primeiro lugar, segue a metodologia tradicional em informações, de uma forma lógica, estruturada e objetiva, baseando-se num processo de recolha, exploração, análise e disseminação da informção.

Contudo, este é apenas um dos métodos para produzir informações, pelo que se deve considerar outros, de forma complementar e integrada, para que seja possível obter outras perspetivas, entre o entendimento e a razão (Racionalismo Crítico)[40]. A título exemplificativo, outro processo complementar que pode ser adotado é o processo não linear. É um processo de diálogo entre especialistas e analistas que se caracteriza pela interatividade e conectividade, baseado na capacidade de ramificação de conhecimentos, isto é, tudo o que se passa fora do gabinete, num sistema de redes, rede de comunicações e de relações.

Sendo assim, o modelo apresentado é baseado na taxonomia de diferentes modelos de risco, de segurança e de informações no ciberespaço, utilizados por empresas do setor privado, na oferta de serviços de *Cyber Security & Intelligence*, nomeadamente o

[40] O racionalismo crítico de Kant defende "O que conhecer?". Para haver conhecimento é preciso que haja coisas para conhecer e que entremos em contacto com elas, isto é, que algo nos seja dado. Conhecer cientificamente é explicar, dizer por que razão algo acontece aqui e agora e não simplesmente que algo acontece aqui e agora. Embora não despreze o papel da experiência, conhecimento empírico, pretende mostrar quais as condições de possibilidade *a priori* do conhecimento (Silveira, Maria João – "Pensamento Contemporâneo", Conferência no Centro de Estudos Aeronáuticos, da Academia da Força Aérea).

Structured Threat Information eXpression (MITRE CORP, 2012); o *Cyber Intel & Decision Support* (SRC, 2013); o *Cyber Intelligence & Response Technology* (AccessData Group, 2013); o *Open Source Intelligence Support & Training* (InfoSphere AB, 2013); e o *Cyber Intelligence Risk Management* (Deloitte, 2011).

Associam-se a este modelo, a doutrina militar norte-americana e da OTAN de referência, no que diz respeito ao ciclo de informações, ou seja, os objetivos e o método utilizados pelos militares para fazer *Intelligence*, nomeadamente o *Theoretical Framework of the OSINT Information Process* (OTAN, 2002b), o *Cyber Intelligence Sharing and Protection Act* (HR, 2012) e as propostas de Robert Steele condensadas na *Intelligence Reform* (Steele, 2008).

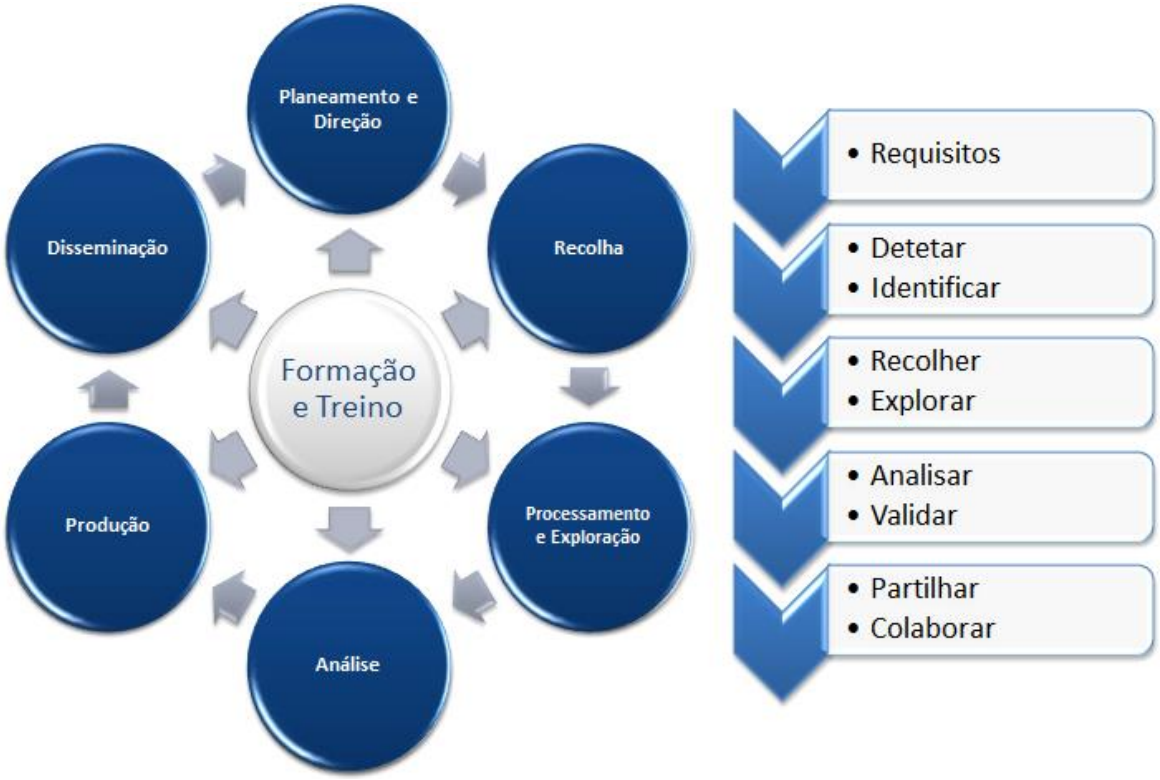
Dada à escassa produção científica e intelectual na área de informações no ciberespaço, a nível nacional, apenas foram consideradas as disciplinas académicas mais intimamente ligadas com esta temática, como a *Competitive Intelligence* (Graça, 2010) e a Cibersegurança e Estratégia Militar (Nunes, Santos & Martins, 2012).

As variáveis deste modelo identificam, inicialmente, os domínios, os atores e as fontes, como que circunscrevendo as origens da informação e enquadrando-a nos diferentes níveis de atuação organizacional (Político, Estratégico, Operacional e Tático/ Técnico). Tem, também em consideração, a forma como a informação é exposta (isto é, as pessoas, os processos e a tecnologia), pois só através destes três vetores é possível atingir os objetivos e obter os efeitos desejados (Figura 5).

Figura 5 – Relação entre fontes, ferramentas e os efeitos desejados

Para assegurar que a informação necessária chega ao processo de decisão, o presente modelo permite identificar algumas das vulnerabilidades, como por exemplo a cultura, o idioma, a formatação, manifestas ao longo das várias fases de produção de informações. Por fim, o modelo apresentado identifica, claramente, o método que é seguido para se realizar *Cyber Intelligence*, de uma forma sistemática, rigorosa e efetiva, que vai desde o planeamento, à formação de especialistas de *Cyber Intelligence* (Figura 6).

Figura 6 – Método e objetivos da Cyber Intelligence

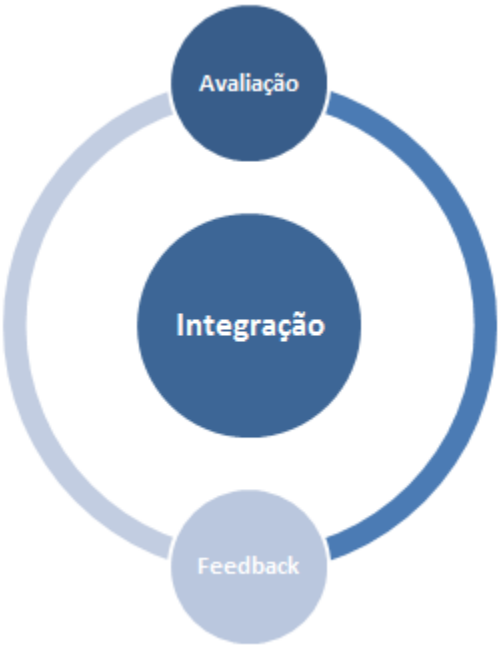


Durante este processo, existem duas etapas fundamentais e que caracterizam este modelo: a Avaliação e a Integração (Figura 7). Estas duas condições são *sine qua non* para a produção efetiva e credível de informações no ciberespaço. Existe ainda uma relação muito próxima entre a Avaliação e o *Feedback*, que mais não é que o retorno da veracidade da informação produzida.

Por outro lado, a Avaliação, em conjunto com o *Feedback*, é uma função essencialmente humana, nesta etapa final de validação da informação. É um passo elementar para credibilizar e autenticar a informação, classificando-a consoante o seu grau de confiabilidade e precisão das fontes.

Por outro lado, pela Integração entende-se que toda a informação obtida de fonte aberta deverá der correlacionada e verificada por outras áreas das informações, nomeadamente ELINT, GEOINT, MASINT, SIGINT e HUMINT. Assim, procura-se cruzar a informação com outras informações, obtidas por outras fontes e analisadas por outras disciplinas, para obter maior credibilidade no resultado final.

Figura 7 – Processo de avaliação, feedback o e integração da Cyber Intelligence



Logo, só conhecendo com rigor as fontes utilizadas pela *Cyber Intelligence*, qual o domínio de ação e respetivos atores, as ações (no essencial a tecnologia) e as vulnerabilidades, é possível apoiar a tomada de decisão em situação de crise. A tecnologia, partilhada e explorada eficientemente; as pessoas, em número adequado e altamente qualificados; e os processos, bem definidos e orientados para o conhecimento aberto, segundo os interesses ou as prioridades dos decisores, permite consequentemente refletir sobre as oportunidades e os riscos e qual a equação certa para atingir os objetivos da organização.

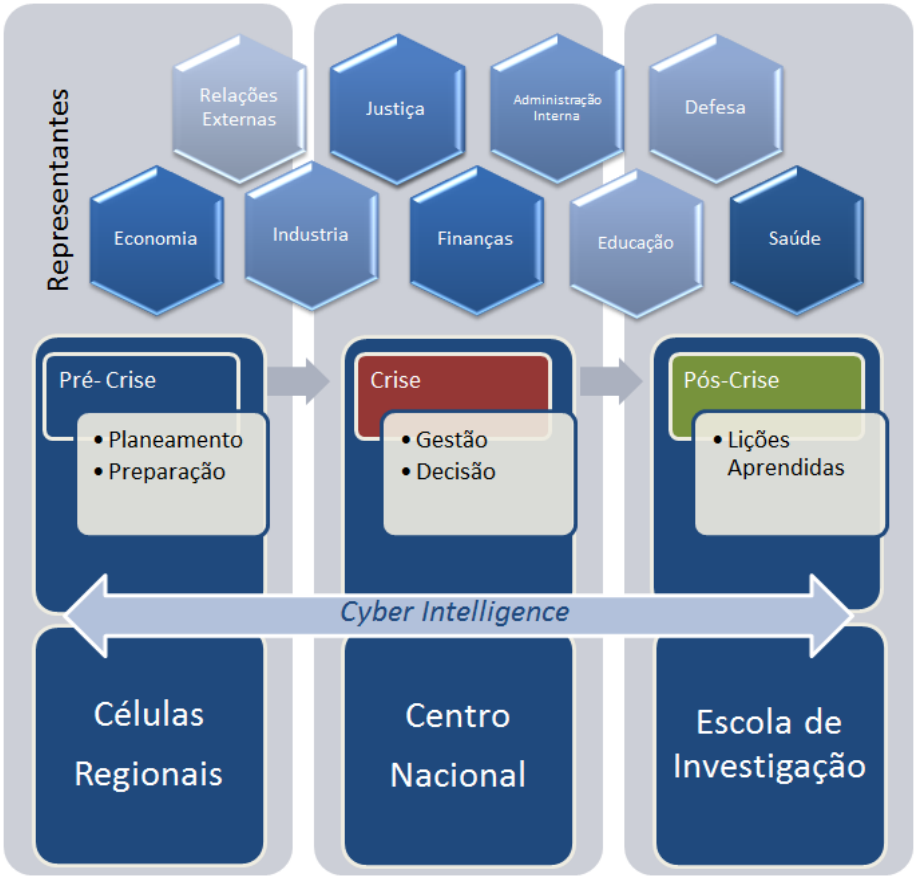
Em suma, a organização deve ser capaz de aumentar as suas oportunidades e reduzir os riscos que estão associados, através do apoio da *Cyber Intelligence*. Estas operações só serão conduzidas eficazmente na integração das várias fontes de informação. Com o recurso à *Cyber Intelligence* é possível obter avaliações das várias áreas das informações, na produção de informações e retorno, ou *Feedback*, dos resultados das projeções e da ação das informações na tomada de decisão.

4.1.2. Aplicação do Modelo na Gestão de Crises no Ciberespaço

Os Estados e as organizações exigem conceitos e capacidades para antecipar, dissuadir, prevenir, proteger e responder a uma perturbação ou uma negação de acesso nos vários domínios (terrestre, marítimo, aéreo, espacial e ciberespaço), para garantir a liberdade de ação e as suas inter-relações (Fiori, 2012).

O contributo da *Cyber Intelligence*, na gestão de crises no ciberespaço, terá que ser equacionada em três fases distintas: Pré-Crise, Crise e Pós-Crise[41] (Figura 8). A fase de Pré-crise é caracterizada por uma aparente estabilidade, onde existe grande competição pela obtenção de informação dos concorrentes, fornecedores e clientes, ética e legalmente, através da *Competitive Intelligence* (Fiori, 2012).

Figura 8 – Cyber Intelligence e as 3 fases de conflitualidade



Nesta fase, a *Cyber Intelligence* realiza um trabalho de campo, digamos "*off-line*", pois o objetivo é recolher toda a informação relevante, acompanhar os eventos mais significativos, fornecer aviso prévio de potenciais agressores, trabalhando na preparação e

[41] "*Cyber Eco-System",* SVP Strategy Finmeccanica (Fiori, 2012).

planeamento de cenários e fazendo parte de uma equipa de resposta preventiva de ciberameaças. Um núcleo de tomada de decisão bem informado é, hoje, uma condição indispensável de competitividade e sucesso para qualquer empresa, tanto a nível nacional como internacional (Graça, 2012).

Este esforço deverá ser executado por qualquer célula de *Cyber Intelligence*, no seio de uma empresa privada, uma organização estatal ou um departamento militar. Entretanto, as células devem trabalhar em simultâneo com empresas ligadas à cibersegurança e aos SIS, para definir e controlar problemas de indicadores e aviso prévio, para avisar, particularmente a OTAN, sobre os mais prováveis cenários de ciberataques (Healey, 2012). Contudo, a competição entre empresas nacionais, no cenário internacional, está a evoluir para um nível de conflitualidade de facto próximo da guerra económica (Graça, 2012). Em situação de crise declarada, a *Cyber Intelligence* é uma mais-valia, preponderante no conhecimento situacional do espectro global da ameaça. Todo o investimento concedido às equipas de análise de *Cyber Intelligence* terá o seu retorno positivo, aquando da necessidade de aplicar ações de resposta eficazes, na resposta a incidentes no ciberespaço.

Por seu lado, a OTAN e a UE defendem uma abordagem inovadora para a elaboração de *Info-data* de múltiplas fontes de informação e correlação/integração relevantes, no que apelida de *Common Operational Picture* (termo inglês para Imagem Operacional Comum), para reforçar as capacidades de Ciberdefesa, através de técnicas de correlação, *Cyber Intelligence* e integração das múltiplas fontes de informação (Fiori, 2012).

Actualmente, as células de *Cyber Intelligence*, através de novas fontes e métodos de informação, ajudam a responder a ataques em curso, mas não preveem novos ataques. Nesse sentido, a OTAN defende que se deverão expandir as células de *Cyber Intelligence* para uma equipa robusta de *Cyber Intelligence* (Healey, 2012).

Resumindo, em situação de crise, é evidente a necessidade de dotar os decisores políticos de análise de ciberameaças, através de uma equipa de *Cyber Intelligence,* e de ações de resposta proactiva a ciberataques, por pessoal ligado à Cibersegurança/ Ciberdefesa de redes, com as ações e as ferramentas apropriadas para a situação. Para tal acontecer, é indispensável uma colaboração público-privada, para a partilha e implementação de práticas, conhecimentos e estratégias de Cibersegurança, a par de normalização abrangente e análoga a todos os setores, de forma a garantir a continuidade dos "serviços mínimos" e a rápida recuperação (Figura 9).

Para Fiori, em situação de crise declarada, é difícil acreditar que uma ameaça desenvolvida no ciberespaço e disseminada ao longo de um sistema aberto, como a *Internet*, possa ser neutralizado isoladamente (Fiori, 2012).

Figura 9 – Cyber Intelligence na gestão de crises no ciberespaço

A terceira fase diz respeito ao Pós-Crise que é, juntamente, com a fase de Pré-Crise, de extrema importância na gestão de crises eficaz. Esta fase é uma fase de investigação, em que o principal objetivo é retirar lições aprendidas de eventos anteriores, que poderão ser fundamentais na condução de operações de resposta a incidentes futuros.

Por um lado, ao nível operacional/ tático, a investigação é local e deverá ser disseminada pelos canais apropriados, de forma a todos aprenderem e se preparem para futuras ameaças. Quanto que ao nível estratégico, deveria ser instituída uma verdadeira Universidade da Informação, onde se estaria a pensar nas futuras gerações, na educação informacional, na cultura de segurança da informação, no desenvolvimento de competências de gestão de sistemas de informação e na partilha de conhecimentos.

4.1.3. Descrição das Varáveis-chave

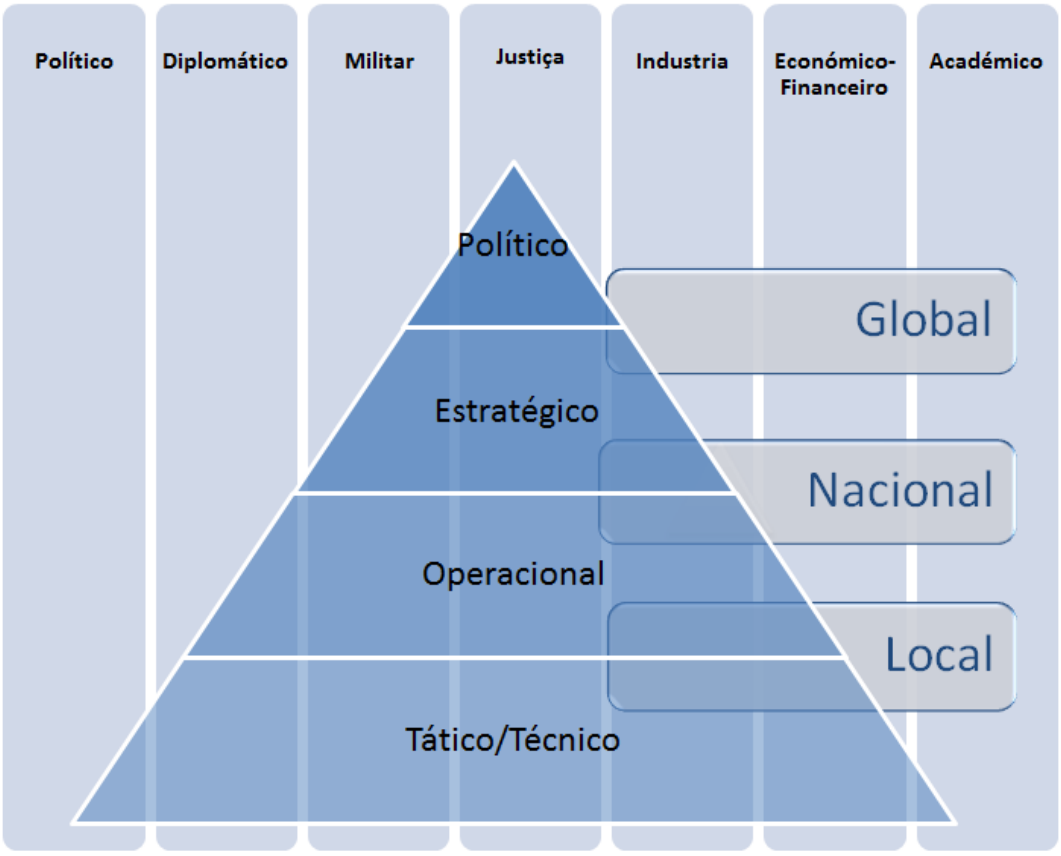
A totalidade dos parâmetros (isto é, variáveis do modelo) e seus valores ou condições é um campo morfológico, que pode ser reduzido a um número de configurações em que somente

aquelas que satisfazem determinados critérios permanecem no final, ou seja no modelo de representação do problema (Martins, et al., 2012, p.59).

Com esta proposta, pretende-se responder a algumas questões primordiais no campo da *Cyber Intelligence*: *Onde, Quem, O quê, Como, Para quê e Porquê*? Descrevem-se, então, sumariamente, as variáveis do modelo, apresentadas no Apêndice IV, as quais definem o espaço de soluções para o problema da *Cyber Intelligence*, no apoio à tomada de decisão e gestão de crises eficaz. Assim, o modelo apresentado identifica as principais variáveis (exemplo: Fonte) e as possíveis condições (exemplo: *Internet*, Redes internas e externas), que serão descritas de seguida.

O ***Domínio*** e o ***Ator*** podem ser considerados como a base do modelo e responde a duas questões essenciais: "*Onde?/ Quem?"*. A variável Domínio encontra-se dividida em dois campos naturalmente agregados – Área de Responsabilidade e Nível Organizacional.

Figura 10 – Domínios e atores em Cyber Intelligence



A área de responsabilidade é entendida como sendo o campo de ação, isto é, cada unidade organizativa põe em prática um conjunto de procedimentos na respetiva área de

responsabilidade, seja esta global, nacional ou local. Os níveis organizacionais expostos no modelo são os defendidos e aplicados pela grande parte das organizações, em todo o mundo. De realçar que a distinção entre os diferentes níveis (político, estratégico, operacional e tático/técnico) é encarada à luz do que são considerados os níveis de poder.

A tipologia de ação nestes domínios define qual a origem do ator - setor público ou setor privado, estatal ou não-estatal.

Por outro lado, a *Cyber Intelligence* é uma área das informações que tanto pode ser realizada ou requerida por uma entidade ligada à Política ou Diplomacia, como pode ser efetuada, ou esse serviço solicitado, a empresas ligadas ao setor económico-financeiro ou industria, por exemplo (Figura 10).

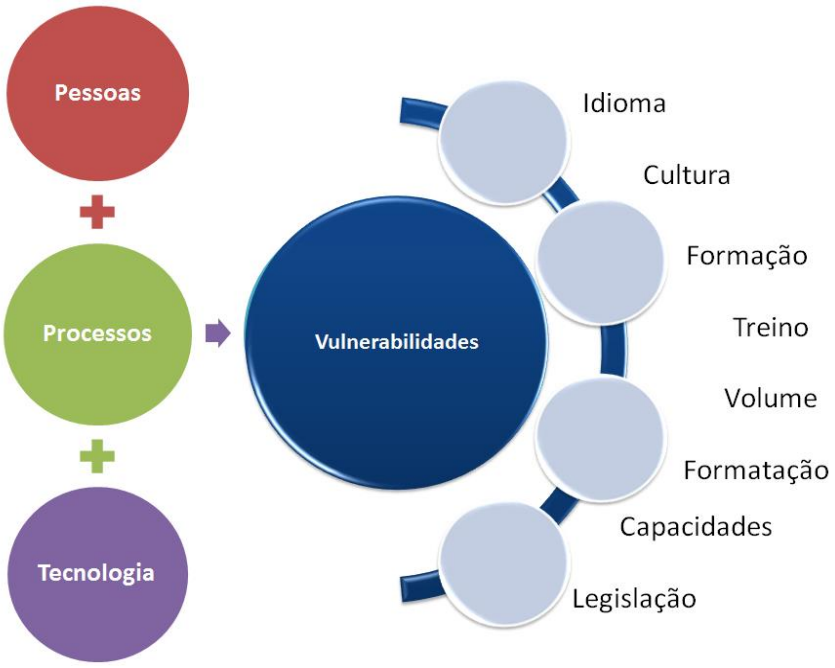
Assim, a título exemplificativo, podemos definir o Centro de Informações e Segurança Militar (CISMIL), como sendo um organismo nacional (área de responsabilidade), operacional (nível organizacional) e militar (tipo de ator).

A *Cyber Intelligence* diferencia-se da OSINT tradicional exatamente pelas ***Fontes*.** Este é o campo onde se procura responder à questão: "*O quê?".* Toda a informação que veicula no ciberespaço é matéria de *Cyber Intelligence*, contudo a *Internet* não é a única fonte de informação, outras redes e dispositivos *offline* podem ser alvo de *Cyber Intelligence*, tais como redes locais e internas e centrais de bases de dados. O acesso às fontes "em linha" pode ser feito livremente, ora através de "*Blogs*", das redes sociais e das páginas *Web* institucionais, ou carece de requisitos de acesso, que normalmente têm associado contratos de fidelização e subscrições (sujeitas ao pagamento de taxas).

Para responder à questão "*Como?"* aborda-se de seguida o campo de ***Ações***. A informação está exposta fundamentalmente em três componentes: as pessoas, ou seja todos os *stakeholders*, que podem aceder à informação, através de redes privadas e da *Internet*; os processos de negócio utilizados na manipulação da informação; e a tecnologia que permite realizar o ciclo de produção de *Cyber Intelligence*, desde a *Hardware*, *Software* e bases de dados, a redes de computadores.

Estes elementos constituem o campo de ações, ou conjunto de ações, que são meios ou ferramentas, que assistem a *Cyber Intelligence* na procura e exploração das ***Vulnerabilidades*** (Figura 11), com a recolha, armazenamento, exploração, análise e disseminação da informação (Martins, et al., 2012:59).

Figura 11 – Campo de ações e vulnerabilidades da Cyber Intelligence



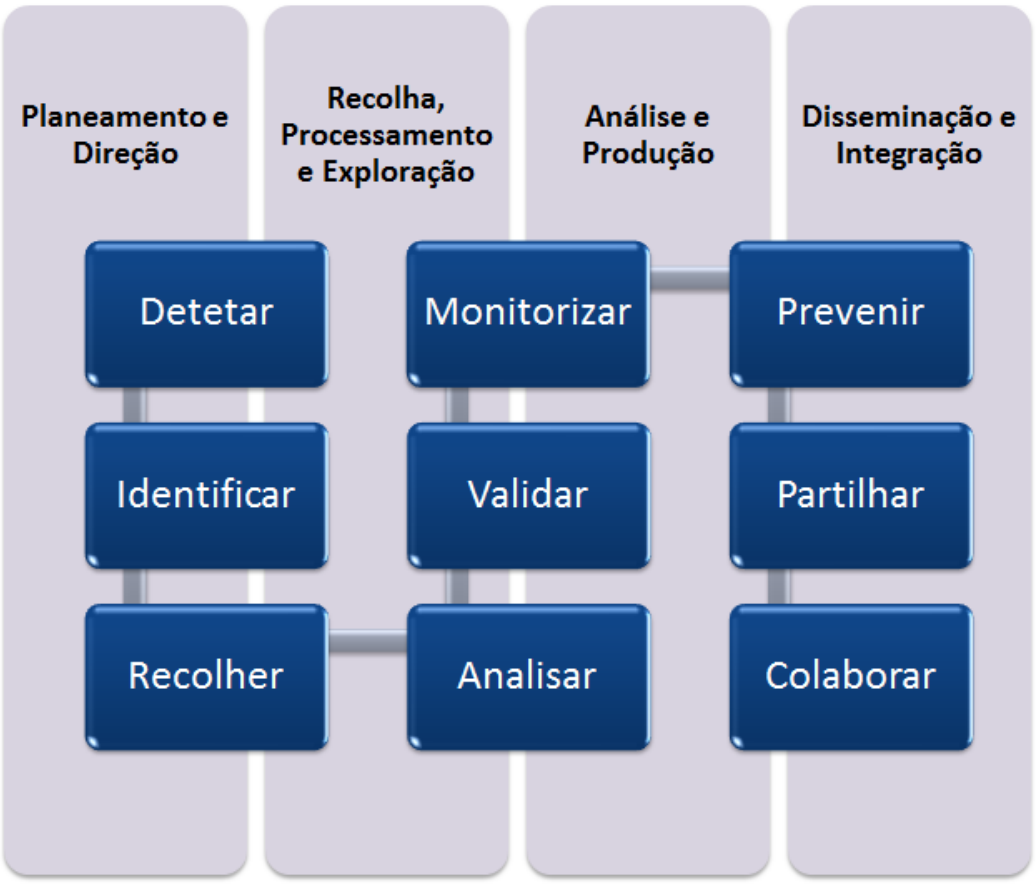
A exploração de vulnerabilidades, permite direta ou indiretamente provocar ***Efeitos*.** Estes efeitos podem ser alcançados por ações, realizadas indiretamente por pessoas e processos, no incentivo pela colaboração público-privada e legislação, que vise uma maior Cooperação Internacional; ou diretamente por tecnologia, no uso de plataformas que ofereçam, por exemplo, aviso prévio, conhecimento situacional, avaliação da ameaça, rede de informações e níveis de autenticidade.

Resumidamente, o conjunto de ações expostas permitem uma maior integração da informação, que se materializará numa maior gestão de riscos e segurança proactiva (Figura 12), no auxílio à tomada de decisão. Assim respondemos à questão "*Para quê*?", se fazer *Cyber Intelligence*.

Figura 12 – Campo de ações e efeitos da Cyber Intelligence

Os efeitos produzidos permitem, desta forma, atingir diretamente os ***Objetivos*** ou contribuir para os alcançar. A pergunta que se coloca neste ponto é "*Porquê?"*, e compreenderemos a razão para existir *Cyber Intelligence*. Os objetivos da obtenção de informações a partir de fontes abertas no ciberespaço dividem-se em quatro grandes fases, preconizados na metodologia aplicada nas informações: Planeamento e Direção; Recolha, Processamento e Exploração; Análise e Produção; e Disseminação e Integração (Figura 13). Os objetivos permitem orientar a *Cyber Intelligence* a produzir os efeitos desejados, através de pessoas, processos e tecnologia robustas.

Figura 13 – Método e objetivos da Cyber Intelligence



Estas quatro grandes fases de aplicação do modelo são em parte similares às áreas subsidiárias de qualquer célula de *Cyber Intelligence*, onde se prevê que as atividades sejam acompanhadas por pessoal altamente qualificado e habilitado, ferramentas atuais e estandardizadas e processos integradores e comuns.

O ***Método*** prevê ainda uma "fase adicional", isto é, um processo que acompanha a disseminação e integração das informações, que é caracterizado pela Avaliação e Feedback.

Por outro lado, a capacidade ao nível da Formação e Treino é essencial e indispensável, exigindo um processo amplo e contínuo (Figura 14), que está presente em qualquer fase do ciclo de *Cyber Intelligence.*

Figura 14 – O método da Cyber Intelligence

4.2. Validação do Modelo

4.2.1. Caso Prático 1

4.2.1.1 Entrevistas

Para se validar, primariamente, o presente modelo de *Cyber Intelligence*, aplicado à gestão de crises no ciberespaço, a metodologia seguida foi a técnica de entrevista semiestruturada. As entrevistas seguiram um processo de planeamento, formulação do guião e respetivas questões, realização da entrevista propriamente dita, transcrição, análise de conteúdos e elaboração do relatório (Oliveira, 2000; Boni e Quaresma, 2005; Costa, et al., 2004).

Após a revisão de literatura dos modelos existentes de *Cyber Intelligence*, em particular os modelos de análise de informações obtidas a partir de fontes abertas no ciberespaço, sendo estes os dados objetivos de pesquisa, foi possível obter dados subjetivos, através do recurso às entrevistas, que se relacionam com valores, atitudes e opiniões dos sujeitos entrevistados (Boni e Quaresma, 2005).

Para o método de investigação presente neste trabalho, o tipo de entrevista mais adequado é a entrevista semiestruturada, pois pretende-se verificar e aprofundar um estudo efetuado pelo pesquisador (Costa, Rocha, Acúrcio, 2004). A entrevista semiestruturada foi realizada com perguntas abertas e fechadas, previamente definidas. No plano prático, criou-se um ambiente muito semelhante ao de uma conversa informal, pois a interação entre o entrevistador e o entrevistado favoreceu respostas mais espontâneas (Boni e Quaresma, 2005).

Na fase de preparação da entrevista, foram definidos os objetivos gerais e o formulário com as questões importantes, que se materializaram no guião da entrevista, conforme Apêndice V. Nesta fase foram, ainda, selecionados os entrevistados, de acordo com dois critérios: familiaridade com o tema e setor de atividade. Pretendeu-se entrevistar especialistas de informações e/ou entidades relacionadas com a segurança da informação no ciberespaço, de cada uma das seguintes áreas: Militar, Governo, Setor Privado e Académico.

A principal vantagem da entrevista semiestruturada é que nesta técnica as respostas espontâneas dos entrevistados fizeram surgir questões, que foram de grande utilidade na pesquisa. De realçar, também, que as entrevistas foram realizadas nos locais de trabalho dos entrevistados, sem condicionamentos. Não houve nenhuma limitação digna de registo,

para além, da possível insegurança do entrevistado em relação ao seu anonimato e por esse motivo possa ter omitido algumas informações importantes.

4.2.1.2. Análise de conteúdo das Entrevistas

Após a realização das entrevistas, foram elaborados os respetivos relatórios, contendo os objetivos da entrevista, os principais pontos abordados e as opiniões dos entrevistados. Os entrevistados, ora são militares do CISMIL, ora especialistas ligados à área dos Serviços de Informações do Estado ou à Inteligência Competitiva (*Competitive Intelligence*).

De seguida, serão descritos os aspetos mais relevantes a fixar nestas entrevistas e qual o seu contributo na validação do modelo que se apresenta.

O Sr. Tenente Coronel Lima Alves é militar e presta serviço no CISMIL, há mais de 20 anos, sempre ligado às Informações Militares, particularmente na área de análise de informações. Hoje em dia, a sua área de atuação é extensa, desde África, ao Médio Oriente, até mesmo América Latina. Tendo em conta, a sua experiência como analista, foram-lhe colocadas algumas questões relacionadas com o tema *Cyber Intelligence*.

Assim, os temas abordados foram os seguintes: a importância da OSINT e a relação com o ciberespaço; os tipos de fontes OSINT, que utiliza e as ferramentas de recolha de informação "em linha"; o que entendia por Fontes Abertas (*Open Sources)* e Fontes Livres (*Free Sources)*; e as vulnerabilidades do serviço de informações, nomeadamente, a falta de recursos humanos na análise de informações.

Esta entrevista (Apêndice VI) serviu, principalmente, para reforçar a importância do ciberespaço na análise de informação, pois é evidente a dependência dos analistas na informação que veicula na *Internet*, nomeadamente nos "Blogs", por exemplo, na questão dos Países Africanos de Língua Oficial Portuguesa (PALOP).

Contudo, toda esta informação é integrada e analisada segundo outras fontes ou disciplinas, sobretudo através dos Adidos Militares, colocados nessas regiões, e as operações de HUMINT. Por outro lado, estes analistas têm acesso a redes internas classificadas da OTAN, que, por sua vez, também validam, ou invalidam, toda a informação recolhida por fontes abertas.

De seguida, foi entrevistado o Sr. Tenente Coronel Gonçalves, que é, também, militar do CISMIL, que, neste momento, está a trabalhar na área da pesquisa e da disseminação de informação.

Nesta entrevista foi possível conhecer o quadro orgânico do CISMIL, a sua missão e responsabilidades (Apêndice IX); quais as suas áreas de interesse e de influência e, deste modo, conhecer os *Priority Intelligence Requirements* (PIR's); quais as redes e plataformas usadas para obter informação; que ferramentas ou agregadores de informação são utilizados; as vantagens e desvantagens na utilização de OSINT; a falta de cultura e de uma Escola de Informações; e da importância do CISMIL, na gestão de crises no ciberespaço.

Através desta entrevista (Apêndice VII), foi possível ver o outro lado das informações - o "Antes" e o "Depois", ou seja, o que acontece antes e depois da fase de análise. Por outras palavras, fala-se das responsabilidades, das fontes, da cultura, das vantagens e desvantagens, da gestão de crises no ciberespaço.

Sem desprimor pela análise de dados, que tem uma enorme importância no processo de informações, existem outras variáveis que são, também, importantes, tais como as origens da informação, as áreas de atuação, as fontes, as pessoas, a formação, a cultura, a cooperação e a integração interdisciplinar, com outras fontes não classificadas e classificadas.

Rumando para o mundo empresarial, foi fundamental ouvir a voz de um especialista de informações ligado ao setor privado. O Prof. Dr. Pedro Borges Graça é professor associado do Instituto Superior de Ciências Sociais e Políticas (ISCSP) da Universidade Técnica de Lisboa, docente de vários cursos ligados às Informações e à Estratégia. As suas atividades de investigação estão relacionadas com Estudos de Informações e de Segurança, Estudos Africanos, História Contemporânea, Relações Internacionais, Estratégia e Geopolítica. Em comissão de serviço, foi Diretor de Departamento do Serviço de Informações Estratégicas de Defesa e Militares.

Na entrevista (Apêndice VIII) foram abordados alguns assuntos pertinentes que ajudam a entender a problemática da *Cyber Intelligence* e da livre e segura partilha de informações, entre o setor público (serviços) e o setor privado (empresas). Assim, são de realçar alguns pontos mais relevantes abordados nesta entrevista.

a. Inteligência Competitiva. No mundo empresarial fala-se neste conceito para abordar as informações no meio empresarial.

b. "*Correspondant Honorable*". Figura de ligação, dos "serviços" a determinadas "empresas".

c. As relações de confiança (ou promíscuas) entre serviços de informações e uma componente empresarial.

d. O caso da *Ongoing*. Se uma empresa é conhecida no mercado por ter relações privilegiadas com um serviço de informações, de que país for, à partida, poderá ter efeitos nefastos para a imagem da empresa.
e. Espionagem económica. Todos os serviços, sem exceção e de acordo com as suas capacidades, têm um correspondente muito secreto de espionagem económica. Não transparecem cá para a opinião pública, a não ser quando acontecem escândalos e se deslumbram um pouco as operações em curso.
f. O célebre caso "*Vallery Plan*" é um caso típico de uma operação de espionagem económica.
g. Tecnologia e investigação. Os grandes desenvolvimentos tecnológicos são feitos no ambiente militar. Existem relações ou contratantes privados para preencher determinadas necessidades.
h. Libertação de informação desclassificada. O segredo de Estado está mal desenhado e consagrado, juridicamente, em Portugal, ao não permitir a "desclassificação" de informação.
i. Valorização das informações. Do ponto de vista das empresas não existe uma valorização do valor das informações.
j. O "Pronto-a-vestir" das informações. É muito fácil, hoje, ir buscar informação por fontes abertas à *Internet*, se bem que com recurso a uns pequenos truques e bem orientado.
k. Células de informações. É importante que cada empresa tenha a sua célula de informações. Se for bem organizada, essa célula deverá estar fisicamente à parte e estará disfarçada com outro nome e função (por exemplo a consultadoria ou a análise estatistica).
l. Unidade sectorial de informações. Poderá existir uma unidade sectorial que interligue a informação do privado e do Estado, com uma plataforma de informação "Pronto-a-vestir".

4.2.2. Caso Prático 2

4.2.2.1. O Exercício "Ciber Perseu 2013"[42]

O Exercício "Ciber Perseu 2013", decorreu entre os dias 5 e 7 de novembro de 2013. Este exercício enquadra-se no levantamento da capacidade de Ciberdefesa do Exército e constitui o segundo exercício desta natureza, a realizar pelas Forças Armadas Portuguesas.

Materializando uma oportunidade para avaliar procedimentos técnicos e operacionais, este exercício pretendeu exercitar e avaliar a capacidade de resposta do Exército, face à ocorrência de ciberataques, de âmbito nacional e internacional que, afetando as CSI, que suportam o C2 do Exército, ponham em causa a obtenção da Superioridade de Informação do seu Sistema de Forças, no moderno campo de batalha. Por outro lado, o exercício pretendeu, também, contribuir para a consolidação do levantamento da Capacidade Nacional de Ciberdefesa.

Tendo por base esta finalidade, foram definidos os seguintes objetivos para o exercício:

a. Exercitar o processo de decisão e testar os diversos níveis de responsabilidade e competências, de forma a garantir uma resposta coordenada a todos os níveis da Organização (nível planeamento, autoridade de gestão, resposta operacional e tática), face à ocorrência de ciberataques;
b. Exercitar os procedimentos técnicos e operacionais existentes no Exército, de resposta a ciberataques, que afetem os sistemas C2 e a segurança CSI do seu Sistema de Forças;
c. Exercitar, testar e avaliar os mecanismos de cooperação com Entidades e Organizações externas ao Exército e os processos de troca de informação técnica existentes;
d. Preparar a participação do Exército no Exercício "*Cyber Coalition 2013"*.

Incorporando a experiência adquirida noutros exercícios, este permitiu envolver elementos da Estrutura de Comando, da Estrutura Base e elementos da componente operacional do Sistema de Forças do Exército, testando, desta forma, a Política, a Estrutura e os procedimentos de Ciberdefesa e Segurança da Informação, aos diversos níveis que intervêm na reação contra ciberataques.

[42] De acordo com o briefing de preparação para o Exercício de Ciberdefesa "Ciber Perseu 13", realizado no Comando das Forças Terrestres (CFT), em Oeiras, no dia 4 de novembro de 2013, pelo EXCON do exercício, Tenente Coronel Paulo Viegas Nunes.

À semelhança do anterior Exercício "Ciber Perseu 2012", o Exército pretendeu envolver outras organizações (Armada e Força Aérea) e entidades externas não militares, num exercício e treino conjunto, ora com o estatuto de participante ora como observador, de forma a que estes, também, conseguissem testar os seus próprios procedimentos locais.

Uma vez que o ciberespaço, enquanto espaço de interação social, materializa uma área de responsabilidade coletiva, em última estância, todos são responsáveis pela proteção e defesa das Redes e SI. A atribuição de responsabilidades e competências na Cibersegurança deverá obedecer à mesma lógica e fundamentos que caracterizam a Segurança e a Defesa do Estado.

Os objetivos de treino, tendo em conta as audiências de treino internas do Exército e os participantes externos, foram os seguintes:

a. Exercitar o processo de tomada de decisão estratégica/operacional;
b. Testar e validar os procedimentos operacionais e técnicos;
c. Testar e validar os canais e acordos estabelecidos para cooperação multinacional;
d. Exercitar, testar e validar os procedimentos de cooperação com organizações nacionais públicas e/ou privadas;
e. Sensibilizar e treinar o pessoal que vai participar no *Cyber Coalition 2013*.

No quadro do esforço cooperativo na área da Cibersegurança Nacional, os objetivos do Exército foram bem sucedidos, ao congratular-se com a participação ativa de entidades externas, tais como o *CERT.PT*, a *Portugal Telecom*, a *COMPTA*, a *Vodafone* e a *Critical Software*.

4.2.2.2. A Criação da Célula de *Cyber Intel* no Centro de Ciberdefesa

O Exercício "Ciber Perseu 2013" surgiu como uma excelente oportunidade, para colocar em funcionamento uma célula de *Cyber Intel*, de apoio à tomada de decisão, neste caso particular, o Chefe do Centro de Ciberdefesa (plano operacional).

A convite do *Exercise Control* (EXCON), a implementação de uma célula de *Cyber Intel* teria como objetivo a aplicação prática de um modelo de *Cyber Intelligence*, desenvolvido para a gestão de crises no ciberespaço, sendo que esta participação serviria igualmente para validar o estudo e modelo consequente de *Cyber Intelligence,* em cenário de crise nacional no ciberespaço.

Os objetivos da célula *Cyber Intel* para o exercício foram os seguintes[43]

1. Explorar o emprego de algumas ferramentas, utilizadas no planeamento do Exercício "O dia seguinte … no ciberespaço"[44], nomeadamente, a análise de atores[45], o planeamento baseado em efeitos[46] e *Framework* de Guerra de Informação[47], destinadas a avaliar o impacto das OI nas organizações;
2. Desenvolvimento de atividades OSINT, de acordo com a orientação recebida;
3. Construção de uma base de conhecimento situacional no ciberespaço, para apoiar o planeamento de *Computer Network Operations* (CNO) e o processo de tomada de decisão do Chefe do Centro de Ciberdefesa.

4.2.2.3. A Célula de *Cyber Intel* na Gestão de Crises no Ciberespaço

A fase de identificação dos atores e a recolha de dados sobre as ameaças estava concluída e foi produzida durante a fase de planeamento do exercício. Esta informação estava contida num documento, apelidado na gíria militar de *Exercise Plan* (EXPLAN), que foi entregue, antecipadamente, a todas as audiências de treino.

Esta fase diz respeito à fase de preparação, onde se dá lugar à Análise do Risco Social (compreensão do Ambiente Estratégico) e à Construção de Cenários (fase de síntese), que carateriza o primeiro passo a desenvolver pela Célula de *Cyber Intel.*

Finda esta parte, a finalidade da célula de *Cyber Intel*, no Centro de Ciberdefesa, era concluir, em primeiro lugar, a análise dos atores e do ambiente estratégico, para dar resposta aos pedidos de informação (RFI) sobre o possível impacto da ameaça.

Após os incidentes iniciais e os indícios que foram chegando de possíveis intrusões, ações exploratórias e ataques, foi necessário saber quais os cenários possíveis de encontrar.

A Ferramenta de Análise Morfológica (Apêndice XIII) serviu, antes de mais, para antever qual a probabilidade do ataque, que tipo de atores e ações que se poderiam enfrentar. Através da triangulação de dados e mediante os parâmetros constantes na tabela, pode-se descortinar qual será a abordagem "mais eficaz", a "mais provável" e a "mais perigosa".

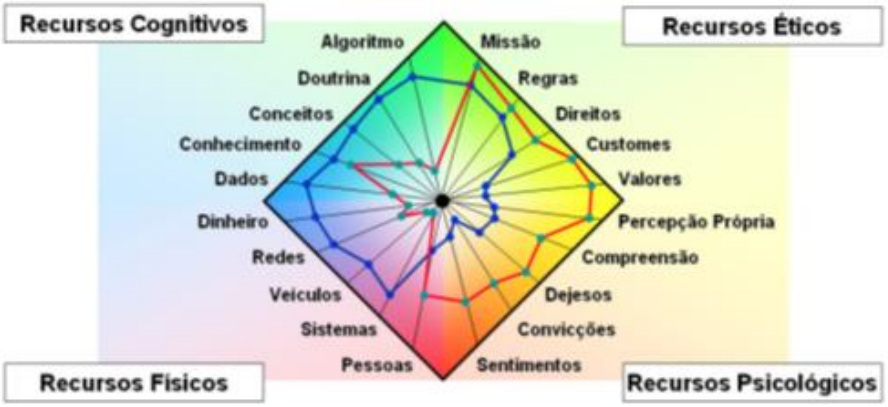
[43] De acordo com informação recolhida por correio eletrónico do EXCON, enviado à célula de *Cyber Intel* e assessores externos.
[44] Exercício integrante da unidade curricular (UC) do Curso de Mestrado em Guerra de Informação (MGI), com o nome de "Seminário de Gestão de Crises no Ciberespaço".
[45] "Formulário de Análise de Atores", ferramenta integrante da UC do MGI "Seminário de Gestão de Crises no Ciberespaço".
[46] "Ferramenta de Planeamento Operacional Baseada em Efeitos no Ciberespaço (FPOBE)", ferramenta integrante da UC de MGI "Seminário de Gestão de Crises no Ciberespaço".
[47] "Ferramenta de Análise Morfológica", ferramenta integrante da UC do MGI "Seminário de Gestão de Crises no Ciberespaço".

Esta ferramenta foi, sem dúvida, útil numa primeira abordagem ao conhecimento da ameaça. Ao nível operacional, no Centro de Ciberdefesa, foi importante na monitorização e recolha de informações e na ajuda à análise do impacto da ciberameaça.

O Formulário de Análise de Atores (Apêndice XIV) visa estudar os atores principais, suscetíveis de análise, descrevendo os parâmetros necessários para identificar o ator, tais como os seus pontos fortes, pontos fracos, centro de gravidade, motivações, estado final pretendido e presença geográfica.

Ao determinar o centro de gravidade, tendo em conta os recursos cognitivos, éticos, físicos e psicológicos dos atores, conforme ilustrado na Figura 15, é possível fazer a análise das implicações.

Figura 15 – Determinação do centro de gravidade dos atores



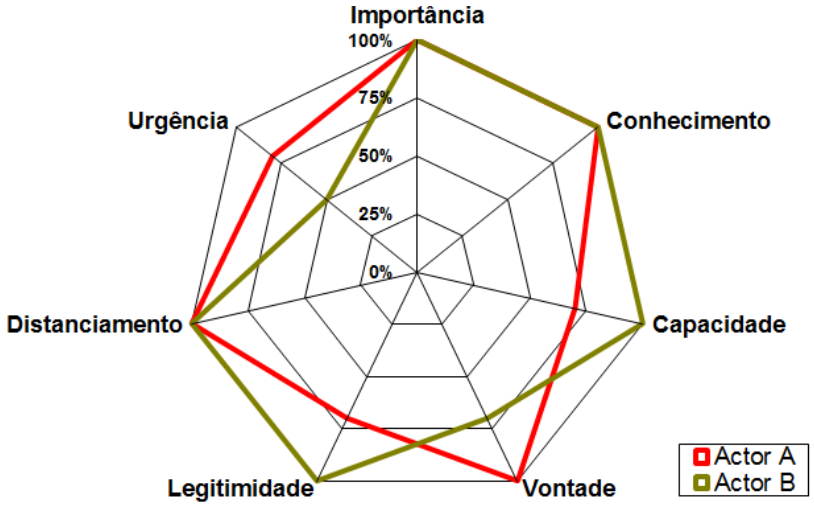
Fonte: Adaptado de Nunes, 2011.

Seguidamente, é elaborada a análise das relações relevantes, do ator em questão com terceiros e, por fim, são calculados a Representação dos Interesses e os Recursos dos Atores em Jogo, numa escala percentual e os resultados representados graficamente, conforme ilustrado na Figura 16.

Através de representações gráficas é possível comparar os interesses e os recursos dos atores, isoladamente como "forças opositoras" ou em simultâneo com as "forças aliadas", principalmente aqueles que se identificaram como sendo a principal ameaça/ ator.

Por conseguinte, para se obter uma comparação abrangente e integrada, foi necessário analisar os "atores potencialmente amigos", assim como, também, se incluiu a "nossa força", isto é, o "nosso país" como ator.

Figura 16 – Representação dos interesses / Recursos dos atores em jogo



Fonte: Adaptado de Nunes, 2011

Através do exemplo representado na Figura 16, sendo o Ator A a ameaça/ adversário, constata-se que a mesma está mais forte nos setores da Urgência e da Vontade, enquanto o Ator B, sendo este um ator potencialmente amigo, está mais forte na Capacidade e na Legitimidade.

Portanto, com base no que for anteriormente referido, elaboraram-se duas folhas de análise de atores, de forma a perspetivar duas visões diferentes: uma perspetiva defensiva e uma perspetiva ofensiva.

Da perspetiva defensiva foi possível visualizar, através de uma breve leitura gráfica, as nossas fragilidades, face às potencialidades do adversário e encetar deste modo as adequadas operações defensivas (ou seja, CND). O objetivo é mitigar as nossas vulnerabilidades (ou até mesmo eliminálas se possível) e aumentar a nossa resiliência, face ao adversário, nestas áreas ou setores.

A perspetiva ofensiva é uma visão mais orientada para CNO. Estas operações podem ser empregues através de *Computer Network Exploitation* (CNE), na identificação da origem da ameaça e na exploração de vulnerabilidades nessa origem; ou podem ser operações com vista a negar, degradar ou destruir a capacidade do adversário (*Computer Network Attack* - CNA), no quadrante mais vulnerável do seu perfil (por exemplo, recorrendo à Figura 16, a Capacidade ou a Urgência).

À medida que se assistia a um escalonamento da situação para uma crise nacional, e após decisão do Nível Estratégico (Poder Político), dão-se origem a ações militares de resposta à ameaça (ofensivas e defensivas). Nesta fase, em particular, a metodologia do planeamento

a seguir está de acordo com a lógica baseada em efeitos [AJP 3.10, 2009 e "*Multinational Information Operations Experiment*" (MNIOE)].

Utilizou-se, para este fim, a Ferramenta de Planeamento Operacional Baseada em Efeitos (FPOBE), pois é um instrumento que permite analisar, projetar e decidir quais as ações mais adequadas a tomar, por parte do Centro de Ciberdefesa, que neste exercício comandava estas ações.

O último passo a realizar foi, portanto, a Análise do Estado Final e do Critério de Sucesso, o Desenvolvimento de Efeitos, o Desenvolvimento de Ações de Sincronização e Refinamento do Plano. Deste modo, foram elaboradas duas folhas, consoante a perspetiva defensiva e a perspetiva ofensiva (Apêndice XV). Para cada uma das perspetivas, foram definidos os seguintes campos:

1. Descrever o Estado Final Desejado e o Critério para o Sucesso;
2. Listar as Restrições e as Limitações (incluindo regras de empenhamento, quadro legal e político, como organizações governamentais e ONG's);
3. Determinar o Centro de Gravidade e o Objetivos/ Intenção (Tipo de efeito a obter, das quais se salientamas ações de: prevenir, enganar, influenciar, diminuir, explorar, degradar, negar, disrupção, destruir, proteger);
4. Definir o Alvo (o nosso e do adversário, no processo de decisão, tendo em conta a vontade, a capacidade e o conhecimento);
5. Definir o tipo de Impacto necessário (lento, rápido, permanente e transitório);
6. Escolher os Métodos possíveis (cinéticos ou não-cinéticos, que podem passar por efeitos físicos, Operações Psicológicas (PSYOPS), CNO, *Information Assurance* (IA), *Electronic Warfare* (EW), Operações de Segurança (OPSEC), Informações, *Network Block Device* (NBD));
7. Escolher a Ferramenta ou o Meio de transmissão (nomeadamente computador, arma, *Media*, comunicações, elementos físicos, mensagem, significado, postura);
8. Definir a Matriz de Sincronização e as Métricas para avaliar a eficácia dos efeitos produzidos (tendo em conta a natureza da variável medir e forma de medição).

O objetivo desta ferramenta é permitir a operação da *Cyber Intel* no apoio à tomada de decisão, na identificação de iniciativas, que ajudem a minimizar as implicações negativas da ocorrência de crises, como a enfrentada durante o exercício. Por outro lado, ajudar a mitigar as suas consequências e reduzir a probabilidade de que estas voltem a ocorrer novamente.

4.3. Revisão do Modelo

4.3.1. O Contributo das Entrevistas

Através da análise das entrevistas foi possível sublinhar algumas condições já preconizadas no modelo, mas, também, foi possível verificar alguns requisitos novos, que ajudam a completar um diagrama único e transversal de *Cyber Intelligence* (Tabela 8).

Portanto, no campo das Fontes, os entrevistados referem que existem outras fontes, essenciais, na obtenção de informações, nomeadamente através de Adidos Militares, Espionagem Económica e Redes Internas da OTAN. Contudo, estas fontes asseguram que a informação obtida por fontes abertas é válida, ou seja, o que estas fontes fazem é uma validação complementar, que pode ser aberta (Adidos Militares), encoberta (Espionagem Económica) e/ ou classificada (Redes Internas OTAN).

No campo das Ações, os entrevistados reconhecem que o conhecimento prévio das fontes (como o caso dos autores de "Blogs") permite construir perfis de potenciais fontes de informação. Por outro lado, há quem defenda que através de uma plataforma única de partilha de informação é possível obter um "pronto-a-vestir" de informação útil, como por exemplo, na gestão de riscos e avaliação de ameaças. Ainda neste campo, outra orientação dada é no processo de recrutamento de pessoas, dentro do serviço, que possam ser "representantes", e ter uma relação institucional-pessoal de confiança com outra pessoa dentro de outra instituição.

No campo das Vulnerabilidades, é necessário dar resposta e controlar algumas áreas referentes às relações interinstitucionais e pessoais, entre serviços e empresas, à valorização e respeito pela disciplina das informações, à "desclassificação" e libertação de informação "obsoleta", e às áreas de atuação inóspitas, desprovidas de tecnologia ou de meios de comunicação, como é o caso, por exemplo, de muitos países africanos.

No que diz respeito aos Efeitos, é de salientar a importância dada à integração interdisciplinar do processo analítico, através, de outras fontes e áreas de informações. Assim como, a vantagem competitiva que é proporcionada pela superioridade da informação.

Quanto ao Método, é de realçar o incentivo no desenvolvimento de Células de Informações ligadas à *Cyber Intelligence*, que por sua vez, podem e devem ser incluídas em qualquer organização, como também fazer parte de uma Unidade Sectorial de Informações, que reúna capacidades de análise e de partilha de informações, pertinentes para o setor.

Por último, é de salientar a relevância dada à formação e à cultura, no seio da comunidade das informações e dos cidadãos em geral. A criação de uma Escola de Informações surge, aqui, apontada como uma lacuna no nosso ambiente literário e intelectual.

Tabela 8 – Quadro síntese da análise de conteúdo das entrevistas

Varáveis-chave	Doutrina Militar	Inteligência Competitiva
Domínio	Áreas de interesse e áreas de influência do Estado Português.	Global e a todos os níveis da organização.
Ator	Nível de atuação puramente militar.	Empresarial (Económico-financeiro), Indústria, Diplomático e Académico.
Fonte	*Internet* ("Blogs"). **Adidos militares.** Agências noticiosas. Órgãos Comunicação Social. **Uso de redes internas classificadas da OTAN para validar as informações.**	**"*Correspondant Honorable*".** **Espionagem económica**.
Ação	Recursos Humanos. **Conhecimento prévio das fontes (Perfil de autores de "Blogs").** Ferramentas ou agregadores de informação em linha.	Tecnologia e Investigação, desenvolvida em ambiente militar, com parcerias privadas. **"Pronto-a-vestir" das informações** (plataforma única de partilha). **Processos de recrutamento.**
Vulnerabilidades	Falta de cultura de informações. Falta de uma Escola de informações. **As origens da informação.** **Áreas inóspitas de atuação, com poucas fontes credíveis de informação.**	**Relações de confiança** entre uma componente empresarial e um serviço de informações. **Valorização das informações**. **Libertação de informação desclassificada.**
Efeitos	Cooperação militar internacional. Aviso prévio. Avaliação da ameaça. **Integração interdisciplinar** com outras fontes não classificadas e classificadas.	Segurança e gestão de riscos. **Vantagem competitiva.**
Objetivo	**Dirigir**, **Coordenar**, **Orientar**, Produzir, Difundir, Comunicar, Colaborar.	Monitorizar, analisar, assessorar.
Método	Planeamento, Coordenação e Gestão de Pesquisa, Produção, **Ligação aos Adidos de Defesa e Militares.**	**Células de informações.** **Unidades sectoriais** que interligue a informação do privado e do Estado.

Para sistematizar os contributos das entrevistas na revisão do modelo proposto, recorreu-se a um quadro comparativo de variáveis e condições, dispostas pelos entrevistados, que são fundamentais para a revisão do modelo que se apresenta (Apêndice XII).

4.3.2. O Contributo do Exercício "Ciber Perseu 2013"

O Exercício "Ciber Perseu 2013" enquadra-se no Plano de Ação para a Superioridade de Informação. Os exercícios e o treino permitem validar competências, facultando um melhor entendimento da Capacidade de Ciberdefesa Nacional, pois permitem exercitar e testar:

a. Política de *Information Assurance* (Ciberdefesa e INFOSEC) do Exército;
b. Processo de decisão, níveis de responsabilidade e competências (resposta coordenada nível planeamento, autoridade gestão, operacional e tático);
c. Capacidades operacionais e procedimentos técnicos existentes;

Por outro lado, através da decisão Sua Excelência, o Chefe de Estado-Maior General das Forças Armadas (CEMGFA), de novembro de 2011, a Ciberdefesa será incluída em todos os Exercícios Conjuntos, afirmando competências residentes no Exército (nível interno e externo) e oferecendo uma oportunidade única de treino conjunto.

Este exercício permitiu, pela primeira vez, empregar uma célula de *Cyber Intel*, com procedimentos e técnicas de análise, avaliação e impacto da ameaça, com vista a apoiar o Centro de Ciberdefesa na tomada de decisão, em ambiente de crise no ciberespaço.

A finalidade da célula de *Cyber Intel* no Centro de Ciberdefesa, à medida que ia decorrendo o exercício e a análise dos atores e do Ambiente Estratégico estando concluída, foi definida em 3 pontos essenciais:

a. Avaliação das ameaças;
b. Impacto das ameaças;
c. Futuras ações (medidas).

A Tabela 9, demonstra, sinteticamente, quais os passos a seguir na metodologia de análise da célula de *Cyber Intel*. O primeiro passo é uma "fase de síntese", pois diz respeito à análise do Risco Social, ou seja a compreensão do Ambiente Estratégico, e à construção de cenários.

O segundo passo é a análise dos atores e do Ambiente Estratégico, onde a definição correta dos atores é um verdadeiro desafio, assim como a determinação do Centro de Gravidade dos atores, que dá origem à análise das implicações.

No terceiro passo e último, é estruturada a análise do Estado Final e do Critério de Sucesso, seguido pelo plano de desenvolvimento de efeitos e de ações, de sincronização e refinamento do mesmo.

A mesma tabela refere, ainda, quais as ferramentas que podem ajudar a célula de *Cyber Intel*, na condução deste processo de análise, salientando que estas são meros instrumentos de fonte aberta e livre, de fácil abordagem e compreensão.

Tabela 9 – Quadro síntese das ações Cyber Intel na gestão de crises

Passo	Metodologia de análise	Ferramentas
1º Passo	Análise do Risco Social e Construção de Cenários	Formulário de Análise Morfológica
2º Passo	Análise de Atores e Análise do Ambiente Estratégico	Formulário de Análise de Atores
3º Passo	Análise do Estado Final e do Critério de Sucesso, o Desenvolvimento de Efeitos e o Desenvolvimento de Ações de Sincronização e Refinamento do Plano	Ferramenta de Planeamento Operacional Baseado em Efeitos

Os pontos identificados como necessários à preparação da participação da célula de *Cyber Intel* no Exercício "Ciber Perseu 2013", após uma sessão de avaliação da condução do exercício, foram os seguintes:

1. Fase de Planeamento e Preparação. A célula de *Cyber Intel* deverá fazer parte do processo de planeamento do exercício, na construção dos cenários, pois este passo é muito importante no decorrer do trabalho desta célula. Por outro lado, a célula deverá ter mais tempo para se preparar e fazer a análise de atores, a relação entre eles,o levantamento das capacidades e as intenções das forças potencialmente amigas e das forças potencialmente agressoras. Em suma, devem ser considerados mais dias de preparação do exercício.
2. O Formulário de Análise de Atores. Este formulário, utilizado noutros exercícios, pode ser mais dinâmico, de forma a poder ser otimizado facilmente para diferentes cenários. Esta ferramenta tem um lado subjetivo de análise, pelo que deverá ser necessário ter em conta um sistema de métricas e critérios de análise bem definidos e fundamentados, para diminuir esta análise empírica dos atores. Como

recomendação pode se ter em conta algo como um *Checklist*, com os passos e critérios que precisam ser considerados para avaliar um ator e suas ações.

3. O FPOBE. Esta ferramenta requer estudo antecipado dos atores e quais as suas vulnerabilidades e pontos fortes, e por conseguinte, requer conhecimentos de outras áreas mais técincas, como por exemplo CNO, para elaborar todo o processo de definição do FPOBE. É uma ferramenta com enorme potencial, mas que requer conhecimentos e treino para que seja eficaz.
4. Ferramentas de Análise. O Chefe do Centro de Ciberdefesa, e demais intervenientes no processo de decisão, devem ter conhecimento prévio destas ferramentas para agilizar, em tempo, o entendimento das soluções e propostas apresentadas pela *Cyber Intel* para a gestão da crise eficaz.
5. Os Assessores Externos. Estes assessores deveriam estar mais "presentes", principalmente, nesta fase e nesta área "pioneira". Conclui-se que fez falta alguém com o "s*aber fazer*" da matéria, para auxiliar os participantes no entendimento do exercício e no uso das ferramentas, pois o interesse não é avaliar mas exercitar, treinar e aprender.
6. Local de trabalho. Neste exercício a célula não dispôs de um local pré-definido para operar, nem um sistema ou rede de comunicação próprio. É sem dúvida essencial um local estritamente dedicado a este fim.
7. Pessoal na célula de *Cyber Intel.* Esta célula deve conter no mínimo 3 pessoas dedicadas, em exclusivo, a este serviço: o chefe da célula e 2 analistas. Pelo menos, uma destas pessoas necessita de ter conhecimentos ou experiência adquirida, anteriormente, nesta área.

Estas "lições aprendidas" são muito importantes para fortalecer a importância da existência de células de *Cyber Intel*, no seio do Centro de Ciberdefesa, mas também, ajudam a definir os procedimentos e técnicas usadas, principalmente, no apoio à tomada de decisão em cenários de crise.

Conclusões

Considerações Finais

A *Cyber Intelligence* é responsável pela recolha, análise e exploração da informação, dita de fontes abertas, e pelo seu posterior contributo para o conhecimento atempado das respetivas ciberameaças, colmatando, assim, uma falha na leitura e avaliação do espectro das ameaças, emergentes do ciberespaço. Dito de outro modo, a *Cyber Intelligence*, deve garantir a gestão de informação aberta, a utilização das demais extensões do ciberespaço, de forma a assegurar uma decisão mais eficaz e em tempo oportuno.

O objetivo principal desta dissertação foi a criação de um modelo de *Cyber Intelligence*, isto é, a criação de um conjunto de passos que, de forma proactiva e preventiva, permite obter informações através de fontes abertas no ciberespaço. Acrescenta-se ainda, que este estudo propôs-se colaborar na definição de orientações, para melhorar o conhecimento situacional de Ciberdefesa e fortalecer as missões atuais e futuras contra as ciberameaças.

Desta forma, o modelo desenvolvido teve em consideração, primariamente, outros modelos de *Cyber Intelligence*, utilizados por entidades governamentais e privadas, na sua gestão de risco da informação no ciberespaço, como o caso da *Deloitte* e da *InfoSphere*.

Assim, foi elaborado um quadro síntese de análise comparativa, que reúne e confronta as diferentes perspetivas da utilização de *Cyber Intelligence*, nas diferentes áreas de atuação e níveis organizacionais. O levantamento e seleção de requisitos e capacidades, comuns a todos os modelos, preconizaram o primeiro passo na definição das variáveis-chave e condições do modelo proposto.

As variáveis deste modelo identificam, inicialmente, os domínios, os atores e as fontes, como que circunscrevendo as origens da informação e enquadrando-a nos diferentes níveis de atuação organizacional. Para assegurar que a informação necessária chega ao processo de decisão, o presente modelo permite identificar algumas das vulnerabilidades manifestas ao longo das várias fases de produção de informações. Por fim, o modelo apresentado identifica, claramente, o método que é seguido para se realizar *Cyber Intelligence*, de uma

forma sistemática, rigorosa e efetiva, que vai desde o planeamento, à formação de especialistas de *Cyber Intelligence*. Durante este processo, existem duas etapas fundamentais: a Avaliação e a Integração, indispensáveis na produção efetiva e credível de informações no ciberespaço.

Conclui-se que conhecendo as fontes utilizadas pela *Cyber Intelligence*, qual o domínio de ação e respetivos atores, as ações e as vulnerabilidades, é possível apoiar a tomada de decisão em situação de crise. A tecnologia, partilhada e explorada eficientemente; as pessoas, em número adequado e altamente qualificados; e os processos, bem definidos e orientados para o conhecimento aberto, segundo os interesses ou as prioridades dos decisores; permitem refletir sobre as oportunidades e os riscos e qual a equação certa para atingir os objetivos da organização.

Este modelo foi, posteriormente, submetido a verificação e validação, realizadas ora por entrevistas a especialistas na matéria, ora pelo trabalho de campo efetuado pela célula de *Cyber Intel*, no exercício anual de Ciberdefesa do Exército.

Numa fase inicial, foram atendidas as opiniões de algumas individualidades, civis e militares, ligadas a este tema. Importa aqui salientar a importância revelada no campo da "Blogosfera" como fonte de informação, assim como a espionagem económica e os adidos militares, no campo da recolha de informação. Salienta-se ainda, a falta de cultura de informações, da inexistência de uma escola de ensino especial nesta área, assim como a relevância da "desclassificação" da informação e da implementação de células de informações, como vulnerabilidades presentes na produção de informações.

Numa fase final, o modelo criado foi posto em prática, no exercício anual de Ciberdefesa do Exército, onde se questionou, confirmou e aperfeiçoou ideias defendidas na proposta de modelo. Nesta fase, foi possível aferir, a proximidade entre o setor público e o setor privado, entre as empresas e as organizações estatais, entre militares e forças de segurança, num ambiente de ameaças comuns e com objetivos e metodologias idênticos. Neste contexto operacional, as diferenças são reduzidas e a complementaridade e a partilha de conhecimentos é altamente relevante.

No campo operacional, a operação da célula de *Cyber Intel* durante o exercício serviu para redefinir qual a metodologia a seguir: (i) o primeiro passo foi a análise do risco social e a construção de cenários, com vista a perceber as capacidades e as intenções de potenciais atacantes, ou seja a avaliação e impacto da ameaça; (ii) o segundo passo foi a análise de atores e a análise do ambiente estratégico, nomeadamente a identificação dos atores e as

suas inter-relações, ou seja, compõem-se perspetivas defensivas e ofensivas, tendo em conta os pontos positivos e negativos e o centro de gravidade; e finalmente (iii) o terceiro passo foi a análise do estado final e do critério de sucesso, o desenvolvimento de efeitos e o desenvolvimento de ações de sincronização e refinamento do plano. Nesta última fase, delineiam-se os objetivos e as medidas, agrupando-se em operações defensivas, de exploração e de ataque.

A criação da célula de *Cyber Intel* no Centro de Ciberdefesa, revelou ser um fator indispensável, na produção de um conhecimento situacional do ciberespaço, comum a todas as audiências. Esta célula comprovou a relevância desta capacidade no apoio à tomada de decisão, nomeadamente na condução de operações no ciberespaço, através do aviso prévio, na avaliação do impacto da ameaça e na escolha das operações mais eficazes, para diminuir ou anular a evolução da ameaça.

A metodologia seguida pela *Cyber Intelligence* é baseada na doutrina das informações, pelo que, a análise dos atores e do ambiente estratégico se torna essencial para enfrentar qualquer cenário de crise. Para além da preparação, a exploração, a recolha e o processamento da informação, é uma tarefa diária e inacabada, que requer pessoal dedicado a tempo inteiro, ferramentas adequadas e legislação própria.

Deste modo, o presente trabalho pretendeu não só reforçar e dar visibilidade ao tema, mas sobretudo demonstrar que esta matéria tem uma importância fulcral para a construção do projeto de futuro na Cibersegurança, para Portugal.

A inclusão de uma célula de *Cyber Intel*, em qualquer empresa ou departamento do Estado, é uma prerrogativa e nunca é tarde para o reconhecer e investir nesta matéria. O desinteresse, associado ao desconhecimento, demonstrado nesta área, é fruto de uma lacuna na formação dos nossos gestores. É tempo de apostar numa verdadeira Escola de Informações e numa "Biblioteca de Conhecimentos", partilhada por todos e que ofereça o acesso, a proteção e a segurança da informação.

A proposta de criação de um centro nacional de *Cyber Intel* pode ser entendida como o conjunto de atividades e pessoas ligadas a empresas e a entidades do sistema científico e tecnológico nacional, às entidades públicas (incluindo capacidades orgânicas das FA) e privadas, com capacidade para fomentar a divulgação da informação "classificada" através de meios e processos "não classificados", de forma a possibilitar a partilha desta informação. Serviria também como aglutinador das diversas células de *Cyber Intel* espalhadas pelo país, sendo que seria acionado apenas em situações especiais ou de crise.

Portanto, respondendo à questão central do presente trabalho:"Como poderão as informações de fontes abertas no ciberespaço melhorar a Cibersegurança/ Ciberdefesa nacional, garantindo assim que, através de uma adequada gestão de informação, a cooperação interinstitucional contribua para uma gestão de crises mais eficaz?", pode concluir-se que:

1. O ciberespaço livre, aberto e seguro, pode garantir uma decisão mais informada e segura. A gestão de informação aberta associada à utilização (des)cuidada do ciberespaço evidenciam um fator fundamental na cooperação, de carácter interinstitucional civil-militar, ou de carácter público-privada.
2. A Cibersegurança e a Ciberdefesa devem ser consideradas como um dever, único e indissociável, do Estado e não como obrigações, distintas e distantes, uma vez que o ciberespaço, enquanto espaço de interação social, materializa uma área de responsabilidade coletiva. Em última estância, todos (Governo, setor privado, ONG's, militares, forças de segurança, cidadãos) são responsáveis pela proteção e defesa das Redes e SI. A atribuição de responsabilidades e competências na Cibersegurança deve obedecer à mesma lógica e fundamentos que caracterizam a Segurança e a Defesa do Estado.
3. O Estado tem um papel fundamental como legislador e regulador de normas e procedimentos, essenciais ao bom funcionamento do ciberespaço. O Estado é o primeiro responsável pela segurança e defesa do pais, pelo que deve incrementar esforços na criação de condições, que permitam assegurar um normal exercício e resiliência das funcionalidades das Redes e SI.

   Enquanto Estado-membro da UE, aliado estratégico da OTAN e membro das Nações Unidas, Portugal necessita proteger os seus compromissos internacionais e desenvolver células setoriais de *Cyber Intel*, de forma articulada com as necessidades de Ciberdefesa e Cibersegurança nacionais. Deste modo, evita a duplicação de esforços e de capacidades, em particular associadas à disponibilidade operacional dos meios militares, direcionando as políticas e atividades de Investigação e Desenvolvimento de Defesa, para o desenvolvimento de tecnologias de duplo-uso (militar e civil), que respondam a requisitos operacionais de médio e longo prazo.
4. O setor privado traz a si inúmeras responsabilidades e vantagens de negócio. As responsabilidades são partilhadas por todos, pelo que o setor privado é parte

integrante, ora porque é usuário deste domínio, ora depende dele para gerir a sua vantagem competitiva. O setor empresarial apelida esta área de Inteligência Competitiva e vai mais além, na partilha e segurança da informação. O setor privado vê neste ambiente uma oportunidade, um desafio, com riscos e vulnerabilidades que esperam ser postas à prova a todo e a qualquer instante.

Na Inteligência Competitiva, também, se conhece um lado mais hostil, pelo que a Guerra Económica é um assunto incandescente, sempre no ponto de ebulição. Assim, as empresas privadas têm uma necessidade natural de se munir de informações privilegiadas, sendo a área da *Cyber Intelligence*, normalmente associada à gestão do risco no apoio à tomada de decisão.

5. A *Cyber Intelligence* é um conceito que herdou a doutrina da disciplina OSINT e aplica a sua metodologia num ambiente altamente dinâmico e criativo que é o ciberespaço. Esta nova disciplina é tida como fundamental na recolha, processamento, análise e disseminação de informações para tomada de decisão, em qualquer empresa ou organismo vivo, que utilize o mais ínfimo sistema de comunicações.

   O desenvolvimento da estrutura OSINT nacional deverá ter em consideração as mudanças que atualmente ocorrem, nomeadamente, no que diz respeito aos conceitos de segurança e defesa e na dificuldade, que os Estados têm em delimitar os campos de atuação destes dois conceitos.

   Para além disso, para um país de pequenas dimensões como Portugal, o desenvolvimento de *Cyber Intelligence* pode ser perspetivado como uma oportunidade estratégica de potenciar as capacidades e oportunidades do ciberespaço na área da Defesa, tornando a sua afirmação e atuação no mercado nacional e internacional de defesa e de segurança, mais eficaz, competente e competitiva.

6. As forças armadas e de segurança são o pilar na defesa e segurança do país, das pessoas e das infraestruturas que as sustentam, representando deste modo um pilar fundamental para a soberania das Nações. Neste sentido, é evidente a necessidade de comprometimento conjunto, neste que é um ambiente partilhado por todos. Para garantir a Cibersegurança, estas forças têm que se capacitar de recursos, materiais e humanos, para continuar a existir segurança nas nossas comunicações e ligações às diferentes redes espalhadas, pelo país e pelo mundo.

7. A gestão de crises eficaz é o *status quo* que a *Cyber Intelligence* deseja alcançar, com a sua metodologia de análise, avaliação e seleção de ações, defensivas ou ofensivas, para enfrentar qualquer ciberameaça.

   Uma resposta eficaz, e em tempo oportuno, a ciberincidentes e a condução de operações no ciberespaço, dependem da análise atempada da *Cyber Intel*, nomeadamente, da avaliação de potenciais ameaças, suas intenções e vulnerabilidades, capaz de operacionalizar um aviso prévio e uma resposta assertiva, por parte dos decisores políticos.

Face ao exposto, reconhecendo-se a existência de um nível nacional e supranacional da Cibersegurança, cada Estado terá que garantir não só a utilização segura do ciberespaço aos seus cidadãos, como a salvaguarda da própria Soberania.

Neste contexto, importa analisar o risco social e o impacto dos diversos tipos de ciberataques, separando os de motivação criminosa daqueles que, por apresentarem um maior poder disruptivo, possam colocar em risco a Segurança e Defesa do Estado.

De modo a responder às questões derivadas e verificar as respetivas hipóteses, foi elaborado um quadro resumo (Apêndices X e XI), onde o leitor pode encontrar a indicação das respostas ao longo do trabalho.

Em síntese, este modelo apresenta uma configuração prática da área de informações no ciberespaço, como fator preponderante na criação de uma Estrutura Nacional de Cibersegurança. Este estudo evidencia ainda a capacidade e o contributo, que esta área de operação pode fornecer na proteção, resiliência e segurança do ciberespaço, contra ciberataques. Essencialmente, traduz-se no apoio à tomada de decisão, ao nível estratégico, mas também no apoio na condução de operações no ciberespaço, ao nível operacional e tático.

Recomendações e Trabalhos Futuros

Dos ensinamentos retirados do Exercício "Ciber Perseu 2013", enumeram-se aqui algumas recomendações:

1. O Formulário de Análise de Atores pode ter em conta algo como um *lista de indicadores*, com os passos e critérios que precisam ser considerados para avaliar um ator e suas ações.

2. A FPOBE é uma ferramenta com potencial, mas que requer conhecimentos e treino para que seja eficaz. A sugestão passa por partilhar esta ferramenta no Centro de Ciberdefesa, pelos seus participantes, em que cada um poderia acrescentar a sua vertente mais técnica (Por exemplo, as ferramentas a utilizar por parte da equipa CNO).
3. A preparação de sessões de esclarecimento, numa fase introdutória ou de preparação para o exercício, para explicar as ferramentas de análise e outros procedimentos que se julguem oportunos, aos intervenientes, de forma a maximizar e otimizar o seu uso.
4. A existência de pelo menos uma pessoa que faça o acompanhamento, ou a avaliação da célula de *Cyber Intel*, pois com esta aproximação, os resultados, tendencialmente, serão melhores. O exercício pretende treinar as equipas e que estas aprendam a operar eficazmente em situações reais, segundo orientações pré-concebidas.
5. A definição de um espaço e respetivas condições para a célula de *Cyber Intel* operar é fundamental, seja na sala de operações do Centro de Ciberdefesa, ou noutra sala adjacente. Este local deve ter no mínimo dois computadores, com respetivos acessos à rede, para ter acesso a toda a informação, elaborar relatórios, *briefings* e outros documentos, se necessário.
6. A criação de uma célula com caráter permanente, que se dedique a tempo inteiro à produção de *Cyber Intel*, preparada para realizar exercícios mas, essencialmente, pronta para agir em caso de situação de crise real declarada.
7. Outra sugestão é incluir pessoas do Curso de Mestrado em Guerra de Informação (MGI), ou outros equivalentes, servindo como analistas de *Cyber Intel*. Os alunos têm os conhecimentos adequados e seriam uma mais-valia para o exercício e para o curso em questão.
8. Outro desafio interessante é a elaboração de um manual ou equivalente, com todos os procedimentos e técnicas previstas para operacionalizar a célula de *Cyber Intel*, em qualquer cenário de crise, procurando tipificar acima de tudo regulamentar este tipo de análise e sua respetiva gestão.

O Exercício de Ciberdefesa do Exército "Ciber Perseu 2014", liderado pelo Exército Português, está já em fase de planeamento, pelo que as conclusões e recomendações deste estudo poderão ser consideradas e melhoradas, se tidas em conta no próximo exercício.

No âmbito da análise de literatura de modelos de *Cyber Intelligence* existentes, apenas foram considerados modelos dos quadrantes Segurança e Defesa, Governo, Investigação e Indústria e Tecnologia. Porém outros segmentos podem ser igualmente abordados, numa visão mais económica/ empresarial, tendo em conta a emergente área da Inteligência Competitiva.

No campo da proposta de um modelo proactivo de *Cyber Intelligence*, o presente trabalho apenas propõe e descreve as principais variáveis do modelo, no entanto em futuros trabalhos será importante relacionar as variáveis e as condições identificadas neste modelo e descrever mais, detalhadamente, os parâmetros e as componentes de cada variável e condição.

Um exemplo prático é a definição de quais os atores nacionais plausíveis de contribuir na recolha e produção de *Cyber Intelligence*, e a identificação e implementação de uma plataforma ou sistema único de partilha de informação.

Outras questões estão ligadas à "computação em nuvem", pouco afloradas neste estudo e alvo de futuros estudos, que são a avaliação dos riscos e limites para conceder autoridade para operar na "nuvem"; a reação à contenção da fuga de informações, num ambiente altamente virtualizado ou "grande nuvem"; e as implicações da transição de uma rede corporativa de IPv4 para IPv6.

Referências Bibliográficas

ACADEMIA MILITAR – Conclusões de Simpósio e Seminário. **Proelium - Revista Científica da Academia Militar** [Em Linha]. Série VII, n.º1 (2011), 319-330. [Consult. 24 Jan. 2013]. Disponível em WWW:<URL:http://www.academiamilitar.pt/proelium-serie-vii-n.o-1.html>.

ACADEMIA MILITAR – **7º EIN Simpósio Internacional sobre o Ciberespaço: Liderança, Segurança e Defesa na Sociedade em Rede** [Em Linha]. 2013. [Consult. 18 Jul. 2013]. Disponível em WWW:<URL:http://www.academiamilitar.pt/7o-simposio-internacional.html>.

ACCESSDATA – **The only solution to integrate network analysis, host analysis and data auditing** [Em Linha]. 2011. [Consult. 18 Jul. 2013]. Disponível em WWW:<URL:http://www.archives.gov/applied-research/pdf/accessdata.pdf>.

ACCESSDATA – **CIRT: What you don't know can hurt you** [Em Linha]. 2013. [Consult. 18 Jul. 2013]. Disponível em WWW:<URL:http://www.accessdata.com/products/cyber-security/cirt>.

AED – **A Stock take of Capabilities for Cyber Defence in the military domain (milCyberCAP)** [Em Linha]. Bruxelas: AED, 2011. [Consult. 15 Jan. 2013]. Disponível em WWW:<URL:http://www.eda.europa.eu/procurement-gateway/opportunites/eda-procurement/procurement-view/11-cap-op-111---a-stock-take-of-capabilities-for-cyber-defence-in-the-military-domain-(milcybercap)>.

AED – **Cyber Intelligence for EU-led Operations (CyTelOPS)** [Em Linha] Bruxelas: AED, 2012. [Consult. 15 Jan. 2013]. Disponível em WWW:<URL:http://www.eda.europa.eu/procurement-gateway/opportunites/eda-procurement/procurement-view/11-cap-np5-415---cyber-intelligence-for-eu-led-operations-(cytelops)>.

AFCEA – **Intelligence and the New National Security Environment** [Em Linha]. Fairfax: AFCEA Intelligence Committee, 2004. [Consult. 18 Jul. 2013]. Disponível em WWW:<URL:http://www.afcea.org/mission/intel/documents/innse.pdf>.

AFONSO, Patrícia – **Implicações da mudança de paradigmas dos conceitos de Segurança e de Defesa no desenvolvimento da Base Tecnológica e Industrial de**

Defesa (BTID) Nacional [Em Linha]. Lisboa: Repositório da Universidade Técnica de Lisboa, 2011. Dissertação de Mestrado. [Consult. 24 Jul. 2013]. Disponível em WWW:<URL:https://www.repository.utl.pt/bitstream/10400.5/3403/1/Implica%c3%a7%c3%b5es%20da%20Mudan%c3%a7a%20de%20Paradigmas%20na%20BTID%20nacional_Patr%c3%adcia%20Afonso.pdf>.

BEST, Richard A. – Intelligence Information: Need to Know vs Need to Share. **CRS Report for Congress** [Em Linha]. N.º 7-5700 (2011). [Consult. 26 Jul. 2013]. Disponível em WWW:<URL:http://www.fas.org/sgp/crs/intel/R41848.pdf>.

BEST, Richard A. e CUMMING, Alfred – Open Source Intelligence (OSINT): Issues for Congress. **CRS Report for Congress** [Em Linha]. N.º 34270 (2007). [Consult. 26 Jul. 2013]. Disponível em WWW:<URL:http://www.fas.org/sgp/crs/intel/R41848.pdf>.

BONI, Valente e QUARESMA, Sílvia – **Aprendendo a entrevistar: como fazer entrevistas em Ciências Sociais.** Revista Eletronica dos Pós-Graduandos em Sociologia Política da UFSC [Em Linha]. Vol. 2 n.º 1 (2005), 68-80. [Consult. 12 Out. 2013]. Disponível em WWW:<**URL:http://www.emtese.ufsc.br/3_art5.pdf>.**

BUCCI, Steven P.; ROSENZWEIG, Paul e INSERRA, David – A congressional guide: seven steps to US Security Prosperety and Freedom. **The Heritage Foundation Backgrounder** [Em Linha]. N.º 2785 (2013). [Consult. 23 Jul. 2013]. Disponível em WWW:<URL:http://www.heritage.org/research/reports/2013/04/a-congressional-guide-seven-steps-to-us-security-prosperity-and-freedom-in-cyberspace>.

BUDNICK, Kris – **Cyber Intelligence** [Em Linha]. 2011. [Consult. 12 Fev. 2013]. Disponível em WWW:<URL:https://www.deloitte.com/assets/Dcom-SouthAfrica/Local%20Assets/Documents/Cyber_Intelligence.pdf>.

C4ISR JOURNAL – **12th Annual Conference: Cyber Security, Stop Treating Cyber as Alien** [Em Linha]. Arlington: C4ISR Journal, 2013. [Consult. 04 Ago. 2013] Disponível em WWW:<URL:http://c4isrjournal.com/blogs/insider/2013/04/25/experts-stop-treating-cyber-as-alien/>.

COMISSÃO EUROPEIA – **Comunicação Conjunta ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões: Estratégia da União Europeia para a Cibersegurança: Um ciberespaço aberto, seguro e protegido** [Em Linha]. Bruxelas: Alta Representante União Europeia, 2013. [Consult. 22

Jul. 2013]. Disponível em WWW:<URL:http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=JOIN:2013:0001:FIN:PT:PDF>.

COMISSÃO EUROPEIA – **Plano de Cibersegurança da UE para proteger a *Internet* aberta, a liberdade e as oportunidades em linha** [Em Linha]. Bruxelas: Relações Externas da União Europeia, 2013. [Consult. 22 Jul. 2013]. Disponível em WWW:<URL:http://europa.eu/rapid/press-release_IP-13-94_pt.htm>.

CONSTANTIN, Lucian – Flame part of US-Israeli cyberattack campaign against Iran. **Computer World Online** [Em Linha]. N.º 9228283 (2012). [Consult. 6 Jan. 2013]. Disponível em WWW:<URL:http://www.computerworld.com/s/article/9228283/Report_Flame_part_of_US_Israeli_cyberattack_campaign_against_Iran>.

COSTA, Cristina; ROCHA, Guida e ACÚRCIO, Mónica – **A Entrevista** [Em Linha]. Lisboa: DEFCUL - Metodologia de Investigação, 2004. [Consult. 12 Out. 2013]. Disponível em WWW:<**URL:http://www.educ.fc.ul.pt/docentes/ichagas/mi1/entrevistat2.pdf**>.

DELOITTE – Risk Intelligent governance in the age of cyber threats - What you don't know could hurt you. **Risk Intelligence Series** [Em Linha]. Issue n.º23 (2012). [Consult. 12 Fev. 2012]. Disponível em WWW:<URL:http://www2.deloitte.com/global/en/pages/governance-risk-and-compliance/articles/risk-intelligent-governance-age-cyber-threats.html>.

DEZABALA, Ted – **Getting Smart About Cyber Intelligence** [Em Linha]. Londres: Center for Security & Privacy Solutions, 2012. [Consult. 12 Fev. 2012]. Disponível em WWW:<URL:http://www.deloitte.com/assets/Dcom-UnitedKingdom/Local%20Assets/Documents/Services/ERS/Security/uk-ers-getting-smart-about-cyber-intelligence.pdf>.

DOA – **ATP2-22-9 Open Source Intelligence** [Em Linha] US Army Headquarters: Doctrine and Training Publications, 2012. [Consult. 26 Jul. 2013]. Disponível em WWW:<URL:http://www.fas.org/irp/doddir/army/atp2-22-9.pdf>.

DOD – **JP 2-01 Doctrine for Joint and National Intelligence Support to Military Operations** [Em Linha]. Joint Electronic Library: Joint Publications, 2012. [Consult. 19 Jul. 2013]. Disponível em WWW:<https://www.fas.org/irp/doddir/dod/jp2_01.pdf>.

DOD – **JP 3-0 Doctrine for Joint Operations** [Em Linha]. Joint Electronic Library: Joint Publications, 2012. [Consult. 19 Jul. 2013]. Disponível em WWW:<URL:https://www.fas.org/irp/doddir/dod/jp3_0.pdf>.

ENISA – Setting the course for national efforts to strengthen security in cyberspace. **National Cyber Security Strategies** [Em Linha]. Heraklion: Resilience and CIIP Program, 2012. [Consult. 22 Jul. 2013]. Disponível em WWW:<URL:http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/cyber-security-strategies-paper/at_download/fullReport>.

ENISA – Practical Guide on Development and Execution **National Cyber Security Strategies** [Em Linha]. [Consult. 22 Jul. 2013]. Disponível em WWW:<URL:http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-an-implementation-guide/at_download/fullReport>.

FERNANDES, José P. T. – Utopia, Liberdade e e Soberania no Ciberespaço. **In Cibersegurança**. Lisboa: IDN - Nação e Defesa, 2012. ISSN 0870-757X. Nº133 – 5ª Série, 11-31.

FIORI, Lorenzo – **Which approach to cooperation in the Cyber Defense and Information Security: the Finmeccanica initiatives** [Em Linha]. Roma: SVP Strategy Finmeccanica, 2012. [Consult. 18 Jul. 2013]. Disponível em WWW:<URL:http://w3.uniroma1.it/mastersicurezza/images/materiali/convegni/18_06_2012/fiori.pdf>.

GRAÇA, Pedro Borges – **Metodologia da Análise nas Informações Estratégicas.** In Moreira, Adriano (Coord.), Informações e Segurança: Estudos em Honra do General Pedro Cardoso. Lisboa: Prefácio, 2003. P. 429-438. ISBN 972-8816-13-8.

GRAÇA, Pedro Borges – **Mundo Secreto: História do presente e Intelligence nas Relações Internacionais.** Lisboa: Instituto de Informações e Segurança de Angola, 2010.

GRAÇA, Pedro Borges – **Inteligência Competitiva no mundo dos negócios** In Curso de especialização de Competitive Intelligence, GRAÇA, Pedro Borges (Coord.). Lisboa: ISCSP-UTL, 2012.

GNS – **Proposta de Estratégia Nacional de Cibersegurança** [Em Linha] Lisboa: CEGER, 2012. [Consult. 15 Jul. 2013]. Disponível em

WWW:<URL:http://www.gns.gov.pt/media/1247/PropostaEstrat%C3%A9giaNacionaldeCiberseguran%C3%A7aPortuguesa.pdf>.

H.R. 3523 **– The Cyber Intelligence Sharing and Protection Act** [Em Linha]., (2012-04-17). [Consult. 18 Jul. 2013]. Disponível em WWW:<URL:http://www.gpo.gov/fdsys/pkg/BILLS-112hr3523rh/pdf/BILLS-112hr3523rh.pdf>.

HEALEY, Jason e BOCHOVEN, Leendert van **– NATO's Cyber Capabilities Yesterday, Today, and Tomorrow** [Em Linha]. Washington DC: Atlantic Council Issue Brief, 2011. [Consult. 6 Jan. 2013]. Disponível em WWW:<URL:http://www.atlanticcouncil.org/publications/issue-briefs/natos-cyber-capabilities-yesterday-today-and-tomorrow>.

HEALEY, Jason e BOCHOVEN, Leendert van **– Strategic Cyber Early Warning A Phased Adaptive Approach for NATO** [Em Linha]. Washington DC: Atlantic Council Issue Brief, 2012. [Consult. 6 Jan. 2013]. Disponível em WWW:<URL:http://www.atlanticcouncil.org/en/publications/issue-briefs/strategic-cyber-early-warning-a-phased-adaptive-approach-for-nato>.

HLOSEK, Andrea L. – Covering your digital footprints. **C4ISR Digital Edition** [Em Linha]. Washington: Defense News, 2012. [Consult. 22 Jul. 2013]. Disponível em WWW:<URL:http://www.defensenews.com/article/20120628/C4ISR02/306280008/>.

HONORATO, Manuel – CEGER: A Ciberseguranca - a visão do Estado. **II Conferência de Hiperíon - Cibereseguranca em Portugal: Aonde nos encontramos?** [Em Linha]. Universidade Lusófona: Instituto de Estudos de Segurança. [Consult. 15 Jul. 2013]. Disponível em WWW:<URL:http://conferenciashiperion.files.wordpress.com/2012/11/ciberseguranc3a7a-uma-visc3a3o-do-estado-universidade-lusc3b3fona-21nov2012.pdf>.

IANNOTTA, Ben – Securing the cloud. **C4ISR Digital Edition** [Em Linha]. Washington: Defense News, 2011. [Consult. 22 Jul. 2013]. Disponível em WWW:<URL:http://www.defensenews.com/print/article/20111101/C4ISR02/111010312/Securing-cloud>.

INFOSPHERE DB – **Intelligence Primer** [Em Linha]. Stockholm: Infosphere DB, 2006. [Consult. 18 Jul. 2013]. Disponível em

WWW:<URL:http://www.infosphere.se/extra/pod/?id=66&module_instance=1&action=pod_show>.

INTELLIGENCE Community – **ICD 301 National Open Source Enterprise** [Em Linha]. Virginia: Director of National Intelligence, 2006. [Consult. 18 Jul. 2013]. Disponível em WWW:<URL:https://www.fas.org/irp/dni/icd/icd-301.pdf>.

INSA – Expectations of Intelligence in the Information Age. **INSA Cyber Intelligence White Paper** [Em Linha]. Arlington: Rebalance Task Force, 2012. [Consult. 22 Jul. 2013]. Disponível em WWW:<URL:http://www.insaonline.org/i/d/a/Resources/Expectations_of_Intelligence.aspx>.

INSA – Setting the landscape for an emerging discipline. **INSA Cyber Intelligence White Paper** [Em Linha]. Arlington: Rebalance Task Force, 2012 [Consult. 22 Jul. 2013]. Disponível em WWW:<URL:http://www.insaonline.org/i/d/a/resources/Cyber_Intelligence.aspx>.

KUJAWSKI, Guilherme – Realidades Virtuais, Riscos Reais. **RAE Publicações** [Em Linha]. Vol.2, n.º3 (2003), p.49-53. [Consult. 6 Ago. 2013]. Disponível em WWW:<URL:http://rae.fgv.br/sites/rae.fgv.br/files/artigos/2065.pdf>.

LEI n.º 67/98 – **Lei da proteção dos dados pessoais** [Em Linha]. DR I Série, 247 (5536-5546). [Consult. 15 Jan. 2013]. Disponível em WWW:<URL:http://www.cnpd.pt/bin/legis/nacional/lei_6798.htm >.

LEI n.º 109/2009 – **Lei do Cibercrime** [Em Linha]. DR I Série, 179 (2009-09-15), 6319-6325. [Consult. 15 Jan. 2013]. Disponível em WWW:<URL:http://www.cnpd.pt/bin/legis/nacional/LEI109-2009-%20CIBERCRIME.pdf>.

LEI 109-163 – **National Defense Authorization Act for Fiscal Year 2006** [Em Linha]. Nº 1815, (2006-01-06), 3135-3557. [Consult. 13 Mar. 2013]. Disponível em WWW: <URL: http://www.dod.mil/dodgc/olc/docs/PL109-163.pdf>.

LEXISNEXIS – **OSINT 2020: The Future of Open Source Intelligence** [Em Linha]. Washington D.C.: The National Press Club, 2010. [Consult. 6 Jul. 2013]. Disponível em WWW:<URL:http://www.opensourceintelligence.eu/ric/doc/OSINT%202020%20The%20Future%20of%20Open%20Source%20Intelligence.pdf>.

MINAS, Harry – Can the Open Source Intelligence Emerge as an Indispensable Discipline for the Intelligence Community in the 21st Century? **RIEAS Publications** [Em Linha]. Research Paper n.º 139 (2008). [Consult. 16 Jul. 2013]. Disponível em WWW: <URL: <URL:http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?ots591=0c54e3b3-1e9c-be1e-2c24-a6a8c7060233&lng=en&id=111330>.

MITRE CORP – **Structured Threat Information eXpression** [Em Linha]. 2012. [Consult. 18 Jul. 2013]. Disponível em WWW:<URL:https://msm.mitre.org/docs/STIX-Whitepaper.pdf>.

MINISTÉRIO da Defesa Nacional – **Despacho n.º 5590/2012, de 11 de abril de 2012** [Em Linha]. DR II Série, 82 (2012-04-26), 14784. [Consult. 15 Jan. 2013]. Disponível em WWW:<URL:http://dre.pt/pdf2sdip/2012/04/082000000/1478414784.pdf>.

NUNES, Paulo e MARTINS, José – **A *Internet* como fator de transformação social e das relações de poder**. In Proelium - Revista da Academia Militar, Lisboa: Academia Militar, 2006. N.º9, p.135-158.

NUNES, Paulo – **Gestão do risco social na Sociedade em rede: a definição de uma estratégia da Informação Nacional.** Seminário: As TIC para um Mundo Mais Seguro - Segurança na Era Digital. Lisboa: Instituto de Estudos Superiores Militares, 2010.

NUNES, Paulo – **Impacto das ciberameaças na segurança e defesa: da ciberdefesa ao levantamento da Estratégia das Informação Nacional.** In Moreira, Adriano e Ramalho, Pinto (Coord.), Estratégia. Lisboa: Instituto Português da Conjuntura Estratégica, 2011. Vol X, p.359-388. ISSN1645-9083.

NUNES, Paulo – Apontamentos da Unidade Curricular do Curso de Mestrado em Guerra de Informação. **Seminário de Gestão de Crises no Ciberespaço**. Lisboa: Academia Militar, 2011.

NUNES, Paulo; SANTOS, Henrique e MARTINS, José – Modelo de Segurança da Informação para Organizações Militares em Ambiente de Guerra de Informação. **In Proelium - Revista Científica da Academia Militar**. Lisboa: Academia Militar, 2012. Série VII, n.º2, p.31-66.

NUNES, Paulo – A Definição de uma Estratégia Nacional Cibersegurança. **In Cibersegurança**. Lisboa: IDN - Nação e Defesa, 2012. ISSN 0870-757X. Nº133 – 5ª Série, 113-127.

ODNI – **ODNI Open Source Conference** [Em Linha]. Washington D.C. - Ronald Reagan Center: Open Source Conference Blog, 2008. [Consult. 16 Jul. 2013]. Disponível em WWW:<URL:http://dniopensource.wordpress.com/>.

OLIVEIRA, José Valente – **Entrevistas** [Em Linha]. Faro: Universidade do Algarve, 2000. [Consult. 12 Out. 2013]. Disponível em WWW:<**URL:http://w3.ualg.pt/~jvo/ep/entre.pdf>.**

OTAN – **NATO OSINT Handbook** [Em Linha] Norfolk: SACLANT Intelligence Branch, 2001. [Consult. 16 Jul. 2013]. Disponível em WWW:<URL:http://www.oss.net/dynamaster/file_archive/030201/ca5fb66734f540fbb4f8f6ef759b258c/NATO%20OSINT%20Handbook%20v1.2%20-%20Jan%202002.pdf>.

OTAN – **NATO OSINT Reader** [Em Linha] Norfolk: SACLANT Intelligence Branch, 2002. [Consult. 16 Jul. 2013]. Disponível em WWW:<URL:http://www.oss.net/dynamaster/file_archive/030201/254633082e785f8fe44f546bf5c9f1ed/NATO%20OSINT%20Reader%20FINAL%2011OCT02.pdf>.

OTAN – **NATO Intelligence Exploitation of the *Internet*** [Em Linha] Norfolk: SACLANT Intelligence Branch, 2002. [Consult. 16 Jul. 2013]. Disponível em WWW:<URL:http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB436/docs/EBB-005.pdf>.

OTAN – **AJP 3.10 Allied Joint Doctrine For Information Operations** [Em Linha]. Bruxelas: NSA, 2009. [Consult. 19 Jul. 2013]. Disponível em WWW:<URL:http://info.publicintelligence.net/NATO-IO.pdf>.

OTAN – **NATO Strategic Concept** [Em Linha] Bruxelas: NATO e-Library, 2010. [Consult. 26 Fev. 2013]. Disponível em WWW:<URL:http://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf>.

OTAN – **Defending the networks: NATO Cyber Defence Policy** [Em Linha] Bruxelas: OTAN Public Diplomacy Division, 2011. [Consult. 18 Jul. 2013]. Disponível em WWW:<URL:http://www.nato.int/nato_static/assets/pdf/pdf_2011_09/20111004_110914-policy-cyberdefence.pdf>.

OTAN – **Resolution 387 on Cyber Security** [Em Linha] Bucareste: Committee on the Civil Dimension of Security, 2011. [Consult. 18 Jul. 2013]. Disponível em WWW:<URL:http://www.nato-pa.int/default.asp?SHORTCUT=2629>.

OTAN CCD COE – **National Cyber Security Framework Manual** [Em Linha]. Tallinn: OTAN CCD COE Publications, 2012. [Consult. 26 Jul. 2013]. Disponível em WWW:<URL:http://www.ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf>.

PARKHOUSE, Tom e BOCHOVEN, Leendert van **– An Agenda for NATO- EU-Private Sector cyber Collaboration** [Em Linha]. Washington DC: Atlantic Council Issue Brief, 2012. [Consult. 6 Jan. 2013]. Disponível em WWW:<URL:http://www.atlanticcouncil.org/en/publications/issue-briefs/an-agenda-for-natoeuprivate-sector-cyber-collaboration>.

PARLAMENTO Europeu **– Recomendação referente ao reforço da segurança e das liberdades fundamentais na *Internet*, de 26 de março de 2009** [Em Linha]. Estrasburgo: Parlamento Europeu, 2009. [Consult. 15 Jan. 2013]. Disponível em WWW:<URL:http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2009-0194+0+DOC+XML+V0//PT>.

PARLAMENTO Europeu **– Relatório sobre a proteção das infraestruturas críticas da informação - realizações e próximas etapas: para uma Ciberseguranca mundial, de 16 de maio de 2012** [Em Linha]. Estrasburgo: Comissão da Indústria, da Investigação e da Energia, 2012. [Consult. 15 Jan. 2013]. Disponível em WWW:<URL:http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2012-0167+0+DOC+XML+V0//PT>.

PARLAMENTO EUROPEU **– Relatório sobre uma Estratégia para a Liberdade Digital na Politica Externa da EU** [Em Linha]. Bruxelas: Comissão dos Assuntos Externos do Parlamento Europeu, 2012. [Consult. 22 Jul. 2013]. Disponível em WWW:<URL:http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2012-0374+0+DOC+XML+V0//PT>.

PARLAMENTO Europeu **– Resolução do Parlamento Europeu sobre Cibersegurança e Ciberdefesa, de 22 de novembro de 2012** [Em Linha]. Estrasburgo: Comissão dos Assuntos Externos, 2012. [Consult. 15 Jan. 2013]. Disponível em WWW:<URL:http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2012-0457&language=PT>.

QUIVY, Raymond e CAMPENHOUDT, Luc Van **– Manual de investigação em ciências sociais.** 5.ª Edição. Lisboa: Gradiva Publicações, 2008. ISBN: 9789726622758.

RADABAUGH, Gregory **–** The envolving cyberspace threat. **The journal of the JAPCC** [Em Linha]. Ed. 15, (2012), 62-66. [Consult. 06 Jan. 2013]. Disponível em WWW:<URL:http://www.japcc.de/fileadmin/user_upload/journal/Edition_15/2012-03-22_Journal_Ed-15_web.pdf>.

RCM n.º 42/2012, de 5 de abril [Em Linha]. DR I Série, 74 (2012-04-13), 1925-1926. [Consult. 15 Jan. 2013]. Disponível em WWW:<URL:http://www.gns.gov.pt/media/1924/rcm-42-2012.pdf>.

RCM n.º 19/ 2013, de 21 de março [Em Linha]. DR I Série, 67 (2013-04-05), 1981-1995. [Consult. 15 Jul. 2013]. Disponível em WWW:<URL:https://dre.pt/pdf1sdip/2013/04/06700/0198101995.pdf>.

RCM n.º 26/2013, de 11 de abril [Em Linha]. DR I Série, 77 (2013-04-19), 2285-2289. [Consult. 15 Jul. 2013]. Disponível em WWW:<URL:http://www.defesa.pt/Documents/20130419_RCM_Defesa_2020.pdf>.

ROSENZWEIG, Paul **–** 10 Conservative Principles for Cybersecurity Policy. **The Heritage Foundation Backgrounder** [Em Linha]. N.º 2513 (2011). [Consult. 24 Jul. 2013]. Disponível em WWW:<URL:http://www.heritage.org/research/reports/2011/01/10-conservative-principles-for-cybersecurity-policy>.

SILVEIRA, Maria João – **Pensamento Contemporâneo**. Conferência no âmbito do Curso Básico de Comando. Sintra: Centro de Estudos Aeronáuticos, Academia da Força Aérea, 2013.

SILOBRAKER – **Silobreaker Enterprise Software Suite** [Em Linha]. Stockholm: Silobraker Ltd, 2013 [Consult. 18 Jul. 2013]. Disponível em WWW:URL:http://www.silobreaker.com/products/silobreaker-enterprise-software-suite>.

SIRP **– Cibersegurança - o papel do SIRP** [Em Linha]. Braga: Universidade do Minho, 2012. [Consult. 26 Fev. 2013]. Disponível em WWW:<URL:http://www.sirp.pt/cms/view/id/90/>.

SIRP **– Informações Estratégicas e Segurança: O SIRP** [Em Linha]. Lisboa: IDN, 2012. [Consult. 26 Fev. 2013]. Disponível em WWW:<URL:http://www.sirp.pt/cms/view/id/92/>.

SRC – **Cyber Intel & Decision Support** [Em Linha]. 2012. [Consult. 18 Jul. 2013]. Disponível em WWW:<URL:http://www.srcinc.com/what-we-do/cybersecurity/cyber-intel-and-decision-support.html>.

STEELE, Robert **– The new craft of Intelligence** [Em Linha], Strategic Studies Institute, U.S. Army War College, 2002. [Consult. 18 Jul. 2013]. Disponível em WWW:<URL:http://www.oss.net/dynamaster/file_archive/060428/0a0990fda32047654d6115ed7310269f/Book.pdf>. ISBN 1-58487-083-4.

STEELE, Robert **– SOF OSINT Handbook** [Em Linha], Virginia: OSS.Net, 2004. [Consult. 16 Jul. 2013]. Disponível em WWW:<URL:http://www.oss.net/dynamaster/file_archive/060322/17c1874f675af107a11872c1a76dbf37/SOF%20OSINT%20Handbook%20(Draft).pdf>.

STEELE, Robert **– Reinveinting OSINT** [Em Linha], 2006. [Consult. 18 Jul. 2013]. Disponível em WWW:URL:<http://www.oss.net/dynamaster/file_archive/060325/e7ce2981d1eef3658878e9a046c499aa/REINVENTING%20INTELLIGENCE%20FINAL.doc>.

STEELE, Robert **– Smart Nation Act** [Em Linha], Virginia: OSS International Press, 2006. [Consult. 18 Jul. 2013]. Disponível em WWW:<URL:http://www.oss.net/dynamaster/file_archive/060908/07186f23e0e0f63f4d54f9941fa7f3b1/Smart%20Nation%20Act%20PDF%20for%20Web.pdf>.

STEELE, Robert – Operational OSINT [Em Linha], In Loch Jonhson (ed.), **Handbook of Intelligence Studies**, NY: Routledge, 2007. Chapter 10 pp. 129-147. [Consult. 16 Jul. 2013]. Disponível em WWW:<http://www.oss.net/dynamaster/file_archive/060409/5432a5e19def62b82684a111fe03f899/STEELE%20OSINT%20FOR%20HANDBOOK%203.3%20Chapter.doc>.

STEELE, Robert **– Collective Intelligence** [Em Linha]. Virginia: Earth Intelligence Network, 2008. [Consult. 18 Jul. 2013]. Disponível em WWW:<URL:http://www.oss.net/dynamaster/file_archive/080227/8580f18843bf5c10f17c38f7ad9fdf71/Complete_022508-C%20FINAL%201420.pdf>.

Apêndices

Apêndice I – Glossário

Agenda Digital para a Europa - Estratégia europeia para uma economia digital florescente por volta de 2020. Estabelece políticas e ações para maximizar os benefícios da revolução digital. Para tal, a Comissão Europeia trabalhará em estreita ligação com os governos nacionais e organizações envolvidas. (Glossário da Sociedade da Informação, APDSI, 2011).

Autenticidade – Num contexto informacional, propriedade de uma informação cuja origem e integridade são garantidas (Glossário da Sociedade da Informação, APDSI, 2011).

Blogs – É a abreviatura do termo original da língua inglesa *weblog*. O termo *weblog* parece ter sido utilizado pela primeira vez em 1997 por Jorn Barger. Na sua origem e na sua aceção mais geral, um *weblog* é uma página na Web que se pressupõe ser atualizada com grande frequência através da colocação de mensagens – que se designam "*posts*" – constituídas por imagens e/ou textos normalmente de pequenas dimensões (muitas vezes incluindo *links* para sites de interesse e/ou comentários e pensamentos pessoais do autor) e apresentadas de forma cronológica, sendo as mensagens mais recentes normalmente apresentadas em primeiro lugar (Maria João Gomes, Universidade do Minho, 2005).

Botnet-for-hire – Rede de aplicativos (*bots*), capaz de se comunicar com os invasores que o colocaram. O *bot* pode ser um programa independente, propaga-se pelo computador, cria redes e espalha conteúdo perigoso através dela (*Kaspersky Lab*, 2011).

Business Intelligence – (ou *eBusiness*) Conjunto de processos organizacionais para reunir e analisar informação relevante para o negócio, incluindo a tecnologia usada e a informação obtida. Por vezes utilizada como sinónimo de "apoio à decisão", a "inteligência empresarial" é no entanto de um âmbito mais abrangente, envolvendo potencialmente gestão do conhecimento, planeamento de recursos empresariais e exploração de dados (*data mining*), entre outras práticas (Glossário da Sociedade da Informação, APDSI, 2011).

Ciclo de Produção OSINT – Para a produção de informações é fundamental seguir um ciclo que é composto por cinco fases: planeamento e orientação; recolha; processamento; análise e produção; e disseminação ou distribuição. Este ciclo será mais ou menos eficaz conforme a presciência dos decisores, a qualidade dos analistas, a fiabilidade das fontes e a capacidade de os sistemas informáticos de registar, integrar, cruzar e disponibilizarem as informações de forma fácil, simples e rápida. (*NATO OSINT Handbook*, 2001).

Computação em nuvem – (ou *Cloud Computing*) Paradigma de computação baseado na *Internet*, em que recursos escaláveis e muitas vezes virtuais da *Internet* são fornecidos a pedido, como serviços, aos utilizadores, que não têm necessidade de gerir a infraestrutura técnica, a "nuvem", que sustenta este modelo de computação (Glossário da Sociedade da Informação, APDSI, 2011).

Dados – (ou *Data*) Representação da informação sob uma forma convencional adequada à comunicação, à interpretação ou ao processamento. Os dados podem ser processados através de meios humanos ou automáticos (Glossário da Sociedade da Informação, APDSI, 2011).

Data Mining – (Exploração de Dados) Processo de análise de dados que busca identificar padrões e semelhanças, em registos de ficheiros ou bases de dados, assim como extrair informações e conhecimentos neles contidos implicitamente (Glossário da Sociedade da Informação, APDSI, 2011).

Data Warehouse – Estrutura informatizada, centralizando um grande volume de dados consolidados provenientes de diversas origens, organizados de forma a fornecerem informação útil aos decisores de uma organização (Glossário da Sociedade da Informação, APDSI, 2011).

Domínio – Grupo de computadores e dispositivos de uma rede, em particular da *Internet*, que são administrados como uma unidade com regras e procedimentos comuns e que partilham um nome comum (nome do domínio) (Glossário da Sociedade da Informação, APDSI, 2011).

e-Government – Utilização de tecnologias da informação e da comunicação (tais como *Internet*, *Intranets*, *Extranets*, bases de dados, sistemas de apoio à decisão e sistemas de vigilância) para facilitar e agilizar as relações entre as estruturas do Governo e entre o Governo e os cidadãos e as empresas, melhorando assim a sua eficiência/eficácia e habilitando-o a prestar melhores serviços (Glossário da Sociedade da Informação, APDSI, 2011).

Em linha – (ou *on-line*) Qualificativo da operação de uma unidade funcional, quando subordinada ao controlo direto de um computador (Glossário da Sociedade da Informação, APDSI, 2011).

Flame – *Malware* modular que ataca computadores que operam o *Windows* da *Microsoft*. Programa usado para espionagem cibernética, sobretudo em países do Médio Oriente. Segundo a *Kaspersky*, em maio de 2012, o "FLAME" tinha infetado cerca de 1000 máquinas, incluindo organizações não-governamentais (ONG's), instituições de ensino e particulares (*Kaspersky Lab*, 2011).

Firewall – Sistema abrangente de medidas de segurança que deve impedir o acesso eletrónico não autorizado a um computador ou serviços específicos na rede. Além disso, é um sistema ou conjunto de dispositivos, que podem ser configurados de modo a permitir, proibir, criptografar ou de-criptografar ou agir como um mediador (*proxy*) para todas as comunicações entre computadores em diferentes domínios de segurança, com base num conjunto de regras e outros critérios. *Firewall* pode ser implementada como hardware ou software, ou uma combinação de ambos (AFCEA, 2004)

IP address – Endereço de 32 *bits* de um computador ou outro dispositivo ligado à *Internet*, representado habitualmente por uma notação decimal de quatro grupos de algarismos separados por pontos. Exemplo: 195.23.245.193 (Glossário da Sociedade da Informação, APDSI, 2011).

Literatura Cinzenta – A literatura cinzenta refere-se a toda a documentação produzida nos ministérios, agências governamentais, organizações privadas, ONG's, instituições culturais e académicas e a gerada em reuniões, congressos e foros de natureza

diversificada. A literatura cinzenta converteu-se atualmente na forma mais ágil, a que a comunidade científica recorre para difundir os resultados dos seus trabalhos e investigações (Universidade de Coimbra, 2012).

Metadata – Em geral "dados sobre os dados"; funcionalmente, "dados estruturados sobre dados". Informação sobre um recurso de informação. Exemplo: Cartão de um catálogo de uma biblioteca, que contém dados sobre o conteúdo de um livro: são dados sobre os dados no livro referido pelo cartão (Glossário da Sociedade da Informação, APDSI, 2011).

Open Source Data **(OSD)** – Informação em bruto, relativa a elementos como fotografias e imagens de satélite comerciais, antes de ser objeto de recolha e tratamento (*NATO OSINT Handbook*, 2001).

Open Source Information **(OSI)** – Informação em bruto, antes de ser objeto de recolha e tratamento, relativo aos meios de comunicação social, livros e relatórios de todo o género (*NATO OSINT Handbook*, 2001).

Rede Social – Rede virtual inter-relacional que permite estabelecer laços de conhecimento entre pessoas. Este tipo de rede pode ser estabelecido em diversos contextos, do profissional ao pessoal, em volta de interesses ou objetivos comuns, ou simplesmente para o estabelecimento de relações humanas. Este conceito apareceu nos EUA, em 2003, simultaneamente, com a criação da primeira rede social na *Internet* (*Friendster*). Atualmente, existem várias redes sociais na *Internet*, sendo algumas das mais visitadas as seguintes: *Facebook*, *Twitter*, *MySpace* e *YouTube* (Glossário da Sociedade da Informação, APDSI, 2011).

Seven Tribes – (ou *Seven Intelligence Tribes*) é o termo utilizado por Robert Steele para identificar quais as áreas setoriais principais, produtoras de informações, que fazem parte de uma Rede Global de Agências Nacionais, com capacidades distintas mas que cooperam entre si. As "tribos" são as seguintes: Nacional, Militar, Empresarial, Académico, Justiça, ONG's e Media, e Religião e Cidadania (Robert Steele, 2003)

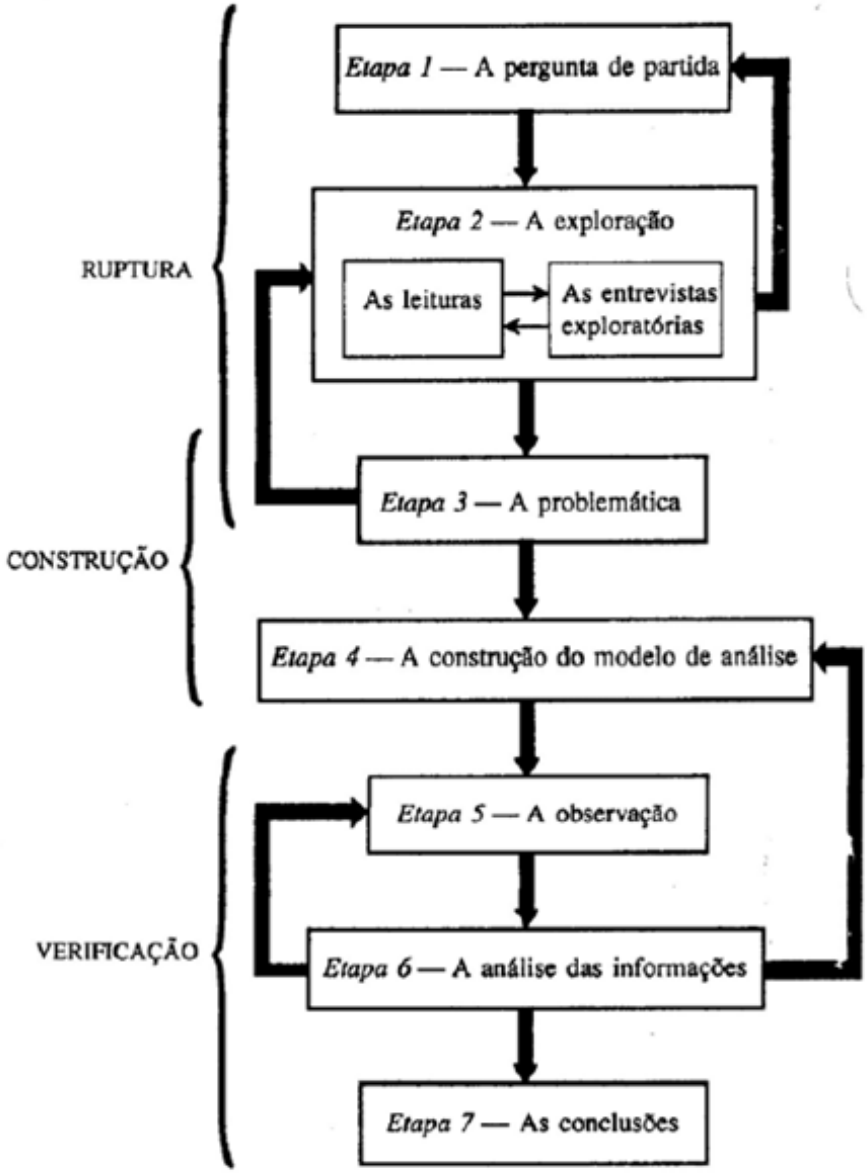
Sítio *Web* – Conjunto de hipertextos organizados por uma determinada pessoa ou organização, armazenados e disponibilizados na *World Wide Web*, com informações de diferentes espécies (texto, fotos, animações gráficas, sons e vídeos). Um sítio *Web* é normalmente composto por páginas residentes num mesmo hospedeiro, e o seu acesso é conseguido através do endereço URL da sua página principal (Glossário da Sociedade da Informação, APDSI, 2011).

Stuxnet – É um *worm* (vírus) que controla e monitora processos industriais e projetado especificamente para atacar o sistema de controlo industrial SCADA. É um protótipo funcional e temível de uma arma cibernética, que dará início a uma nova corrida ao armamento mundial (Kaspersky Lab, 2011).

***Validated Open Source Intelligence* (OSINT-V)** – É uma informação que pode ser atribuída a um grau de certeza muito elevado. Pode ser produzida por todos os profissionais das várias disciplinas de informações, com acesso a fontes de informações confidenciais, trabalhando para uma nação ou para um gabinete de coligação. Também, pode vir de uma fonte aberta segura, ao qual nenhuma pergunta pode ser levantada sobre a sua validade (exemplo de imagens de uma aeronave que chegue a um aeroporto e que são transmitidas nos Media) (*NATO OSINT Handbook*, 2001).

WWW – Sistema baseado na utilização de hipertexto, que permite a pesquisa de informação na *Internet*, o acesso a essa informação e a sua visualização. Utiliza a linguagem HTML e o protocolo HTTP para apresentar e transmitir texto, gráficos, som e vídeo, e incorpora também outros protocolos *Internet* tradicionais como *Gopher, FTP, WAIS* e *Telnet* (Glossário da Sociedade da Informação, APDSI, 2011).

Apêndice II – Método de Investigação Científica de Quivy e Campenhoudt



Apêndice III – Modelo e principais Variáveis-chave

Domínio	Ator	Fonte	Ação	Vulnerabilidades	Efeitos	Objetivo	Método
Global	Político	Internet	Pessoas	Capacidades	Segurança proativa	Detetar	Planeamento e Direção
Nacional	Diplomático	Redes Internas e Externas	Liderança Interdependência	Cultura	Aviso prévio	Identificar	Coleção
Local	Militar	Informação em suporte eletrónico	Processos	Formação e Treino	Avaliação da Ameaça	Colecionar	Processamento e Exploração
Político	Justiça	Literatura cinzenta	Gestão integrada Auditoria	Volume de Informação	Gestão de Riscos	Analisar	Análise
Estratégico	Industria	Especialistas	Tecnologia	Formatação	Rede de Informações	Validar	Produção
Operacional	Económico-Financeiro	Informação comercial (*Pay-to-see*)	Plataforma única Automação	Idioma	Percepção Situacional	Monitorizar	Disseminação e Integração
Tático/ Técnico	Académico	Informação geospacial comercial	Uniformização Digitalização	Segurança	Autenticidade	Prevenir	Avaliação
		Fontes com requisitos de acesso	Representação estruturada	Legislação	Colaboração Publico Privado	Partilhar	*Feedback*
			Ferramentas de Coleção e Análise	Classificação	Cooperação Internacional	Colaborar	Formação
			Imagem Interativa Geoespacial				
			Mapeamento de rede				
			Monitorização 24h Reporte				
			Alertas Tradução				
			Gestão de perfis de ameaça				

Apêndice IV – Tabela comparativa dos Modelos existentes e das Variáveis em estudo

Modelo	Domínio/ atores	Fontes	Objetivos	Método	Ação	Vulnerabilidades/ Efeitos
Theoretical framework of the OSINT information process da OTAN	A OTAN é uma organização **política** e **militar**. Os níveis de análise preconizados são: **Político**, **Estratégico, Operacional, Tático/ Técnico**.	- Media, - ***Internet,*** - Informação em **suporte eletrónico,** - **Informação geospacial comercial,** - Fontes com **requisitos de acesso.**	Fundamentais: Defesa Coletiva, Gestão de Crises e Segurança Cooperativa. - **Prevenir e detetar** ciberataques; - **Integrar** a OSINT no processo de todas as disciplinas de informações; - **Aumentar** o leque de informações disponíveis aos analistas; - **Estabelecer** um processo interativo com outros órgãos de informações; - **Facilitar** a interação com elementos não-OTAN; - **Cooperar** com a Europa e outros países não-OTAN (PfP);	Ciclo OSINT: - **Procura,** - **Discriminação,** - **Produção e** - **Disseminação**.	- ***Desktop toolkit.*** - **Arquitetura partilhada**, com *hardware* e *software* interoperacional. - Ferramentas que permitem o cumprimento de OPSEC, salvaguarda dos direitos de autor, **tradução**, **análise de tráfego de redes** internas e externas, **autenticidade**, **reporte**, fóruns. - Uso de **VPN**. - Transferir o risco para o setor privado; - Gabinete OTAN/PfP **Virtual "NATO *Web*";** - **Equipa de monitorização 24h** e permanente.	Efeitos: - **Entendimento comum** entre as forças militares, os seus congéneres civis e organizações não-governamental. - Apoio no **aprontamento de forças e no apoio à decisão**, em tempo oportuno, para uma resposta a incidentes eficazes. - Informações ***"just enough, just on time"***
Cyber Intelligence Sharing and Protection Act	O NOSC depende diretamente da CIA e é parte integrante da	- Informação e dados **disponíveis em linha**, - **Especialistas**,	- **Obter e partilhar** informação que tem sido escondida (classificada); - **Colecionar** informação com	- **Projeto de digitalização** de informação cultural e histórica (estrangeira); - **Treino e formação**	- **Bases de Dados** extensíveis; - ***Generic Analítical Tool-Kit***; - **Monitorização global**; - **Formatação única**;	Vulnerabilidades: - **Formação e treino;** - **Volume de informação;** - **Ferramentas;**

(CISPA) dos EUA	**política nacional** de informações norte-americana. Os atores são os *Seven Tribes* (**Nacional, Militar, Religião/Tribo, ONG's/ Media, Academia, Sector Empresarial e Justiça**)	- **Empresas privadas**, - **Material sensível do setor financeiro**, - *Internet* (***blogues*, redes sociais**) e - **Literatura cinzenta.**	menos risco e menos dispendiosa; - **Verificar e validar** informações apropriadas; - **Criar** um centro de excelência de exploração de fontes abertas; - **Providenciar** transcrições de produtos em linha; - **Manter** uma vasta recolha de material publicado em suporte eletrónico.	específica OSINT para todos os atores dos *Seven Tribes*; - **Desenvolvimento e aquisição de tecnologias e processos** avançados;	- **Formatação única de requisitos**; - **Tradução** em vários idiomas; - **Prioritização de documentos**; - **Imagens de Satélite** (*Geospacial Intellegence Agency*); - **Armazenamento e livre acesso** a todas as redes ONG's; - **In-Q-Tel** (empresa de desenvolvimento de tecnologia com parcerias com o setor privado);	**- Efeito eco;** **- Segurança;** **- Classificação;** **- Cultura;** **- Idioma;** **- Aptidão do analista.**
Intelligence Reform de Robert Steele	**Os decisores políticos** são catalisadores benfeitores da estratégia de partilha de informação, pelo que devem	*Information Commons*, termo inglês para denominar as "**indústrias de informações**": - *Intelligence Community*,	- **Ter acesso** a todas as informações, em todas as línguas, o tempo todo; - **Investir** fortemente na compreensão da história e cultura de todos os povos; - **Desenvolver** monitorização em tempo real (24/7) e em contexto	Ciclo do processo OSINT: - **Definição de requisitos,** **- Processo de Recolha,** **- Processamento e exploração,** **- Processo de Análise,** **- Produção,** **- Avaliação,**	-**Automação** e **interoperabilidade** de todo o processo de análise de fontes; - **Uniformização** de procedimentos e protocolos/ linguagens. **- Digitalização** e **visualização** instantânea;	Vulnerabilidades: - Conhecimento de diferentes **Idiomas**; - Conhecimento da **História e Cultura** dos povos; - **Educação** das futuras gerações;

	estimular acordos entre os ***Seven Tribes.*** O conceito *Collective Intelligence* remete para um domínio global.	- Governo e - Setor privado.	geoespacial, a todos os níveis de governação; - **Investir** na educação e treino dos operacionais; - **Promover** as oportunidades em prol das ameaças; - **Partilhar** conhecimento de forma segura e com integridade financeira e moral.	- **Disseminação e** - ***Feedback*.**		- Crise económica/ restrições orçamentais que se traduzem na diminuição de **capacidades**; - **Segurança** e compartimentação;
Structured Threat Information eXpression da MITRE Corp	Organizações e especialistas ligados à **Segurança e Defesa**, à **Industria**, à **Academia** e ao **Governo**. **Estados** **Grupos Hacktivistas** **Terroristas** **Criminosos**	*Internet* e redes internas.	- **Apoiar** mais eficazmente a gestão de ciberameaças através de processos e aplicações de sistemas autómatos; - **Ampliar** a partilha de indicadores para permitir a troca generalizada de conjuntos significativamente mais expressivos dos indicadores de gestão; - Gerir atividades de resposta a ameaças cibernéticas (Prevenção e deteção de ciberameaças e resposta a incidentes).	**Arquitetura única e comum** que interliga o conjunto de informação de ciberameaças em 8 principais áreas: - ***Observable*** (Condições cibernéticas observáveis); - ***Indicator*** (Indicadores); - ***Incident*** (Incidentes); - ***TTP*** (táticas, técnicas e procedimentos dos adversários, incluindo infraestruturas, alvos, ferramentas e práticas mais	- **Análise de ciberameaças**; - **Partilha de informação** de ciberameaças; - Estrutura e consistência capaz de suportar a **automação**; - Usuários capazes de aplicar qualquer parte da **representação padronizada**; - **Integração** em vez de duplicação de todas as representações na arquitetura geral STIX;	Vulnerabilidade: - Desenvolvimento de uma **linguagem única e comum**; Efeito: - **Esforço colaborativo** orientado pela comunidade.

	Crime organizado.			comums); - ***Exploit Target*** (Alvos, incluindo vulnerabilidades e fraquezas); - ***Course of Action*** (Linhas de ação); - ***Campaign*** (Campanhas de ciberameaças); - ***Threat Actor*** (Atores de ciberameaças);		
Cyber Intel & Decision Support da SRC	Organizações governamentais nas áreas da **Defesa, Ambiente e Informações**: - Defesa Biológica e Química; - Cibersegurança; - Análise Ambiental e Saúde;	*Internet* e redes internas.	- **Recolher** dados de uma variedade de fontes e fazer uso das melhores tecnologias. - **Coletar, gerir, analisar e correlacionar** dados não classificados da *Internet*, para apoiar as operações no ciberespaço; - **Fornecer** informação partilhável com todos os níveis de decisão do governo e responsáveis por infraestruturas críticas.	*"**DNSMapper™ Analysis Tool**"* - Representação visual do domínio e associações de endereço IP. *"**Data Collection Architecture Tool**"* - Averiguação seletiva, rápida e anónima de dispositivos de rede globais. **"Audit-Based Sense and Protection"** - Monitorização e emissão de informações sumárias de	- *Over-the-horizon cyber intelligence and target data* para uma **preparação defensiva**; - **Ferramenta de análise**; - **Ferramenta de reconhecimento** "à escala *Internet*"; - *"Enterprise-scalable, defensive cyber capability".* - **Sistema de monitorização e gestão proactiva**.	Efeitos: - Informações e serviços de apoio à decisão em tempo oportuno, acionável e partilhável - "***on time, actionable and shareable*";** - **Conhecimento situacional do ciberespaço**;

	- Informações / Vigilância / Reconhecimento; - Industria; **Atores estatais, Políticos dissidentes, Crime organizado.**			estados de alertas de riscos. ***"C-SCOPE"*** - Gestão proactiva ao longo dos diferentes CDS's presentes na empresa.		
Cyber Intelligence & Response Technology da AccessData	Na **aplicação da lei** (Justiça), **em agências governamentais** (Administração Central do Governo), em empresas e escritórios de **advocacia.** **Atores ligados à Indústria e à Economia.**	*Internet* e redes internas.	**- Identificar** falhas de segurança, reprodução de eventos e análise de registos; **- Detetar** proactivamente as ameaças desconhecidas e reduzir os tempos de resposta; - **Monitorizar** a atividade dos funcionários na *Internet*, quando estes não estão conectados à sua rede; - **Colaborar**, em tempo real, através de um interface *Web* seguro, com toda a equipa CIRT, durante um incidente;	Plataforma de segurança integrada e autómata**.** **- *Incident Response & Cyber Intelligence*** **- *Information Assurance & Compliance Auditing*.** As quatro componentes-chave do CIRT: **- *AD Enterprise***, **- *SilentRunner***, **- *Cerberus,*** **- *AD eDiscovery***.	- Integra **as pessoas, os processos e a tecnologia**: - *Threat Identification;* - *Network forensics;* - *Host forensics;* - *Malware analysis;* - *Large-scale data auditing;* - *Remediation;* - *Collaboration and* - *Reporting.* - **Facilidade de utilização**, fluxo de trabalho orientado para o processo (*process-oriented*) e comunicações;	Efeitos: **- Proactividade;** **- Reatividade**.

					- **Captura rápida** e em tempo real; - Criação de **perfis de ameaça** para prevenir a recorrência de ameaça; - ***Superior Smart-Target***; - **Auditoria** de grande escala;	
Open Source Intelligence Support & Training da InfoSphere	Apenas para **organizações internacionais e governamentais**.	*Internet* e redes (*on-line* e *off-line).*	- **Assistir** no desempenho superior da organização, dando acesso a informações críticas; - **Apoiar** a tomada de decisão e resolução de problemas por desbloqueio de ativos de informação; - **Fornecer** uma perspetiva imparcial, externa e segura, crítica para o sucesso da empresa; - **Trabalhar** cuidadosamente em conjunto com os clientes na adoção dos requisitos de informações; - **Adequar** produtos às necessidades do cliente,	- **Recolha de informações de fonte aberta** (*online* e *offline*) em mais de 40 idiomas; - **Formação de informações de fonte aberta** (recolha, análise, produção e apresentação); - **Análise de informações de fonte aberta** (*ad-hoc*, *outsourcing*, segunda opinião); - **Sensibilidade de realização de dados/ traduções em multi-formatos**; - **Análises consequentes**	- Integração de uma rede global de **profissionais** de informações, suportado por **tecnologia** de ponta; - **Operações 24/7**, uma vez que é uma empresa em rede, trabalhando em todos os fusos horários; - Informações coletadas em um **formato XML uniforme**; - **Gestão de dados estruturados e não estruturados**; - Verificações de antecedentes, análise de *media* e **mapeamento** de relacionamento de pessoas,	Efeitos: - **Imagens detalhadas,** com diferentes modos de *zoom*; - **Bancos de dados interativos**; - **Confidencialidade**; - **Acesso anónimo** para uma rede de ativos de recolha; - *Frameworks*, **aviso prévio personalizado** e estratégias de apoio; - **Cenários e indicadores** básicos (*a road map*). Vulnerabilidades:

			abrangendo *briefings*, relatórios extensos de multimédia ou implementação de Informação nos portais do empresa.	(culturais, políticos, económicos, éticos, sociais); - **Recolha, normalização e contextualização de dados para o formato de importação do cliente**; - **Formação contínua** dos métodos utilizados para obter informações de Fonte Aberta. *Baseado no conceito sueco, cujo termo em inglês é *Multinational, Multiagency, Multidisciplinary, Multidomain Information-Sharing (M4IS)*	empresas e organizações; - **Avaliações** baseadas em previsões futuras; - **Atualizações** de eventos**,** de tempo quase real, que podem afetar operações comerciais; - **Análise e monitorização contínua**. ***Silobreaker Enterprise Software Suite*** *Silobreaker* apresenta uma rede de relacionamentos, pontos de interesse geográfico, artigos globais, conversas públicas, bem como conexões entre pessoas, empresas, lugares e outras entidades.	- Diferentes **idiomas** que não só o inglês; - Diferentes **formatos** de informação.

Cyber Intelligence Risk Management da *Deloitte*	Organizações ligadas à **Tecnologia, Industria, Setor Financeiro e Administração Pública.** **Ciberterrorismo, *Hacketivismo, Hackers,* Crime organizado e Organizações apoiadas pelos Estados.**	*Internet* e redes internas	- **Garantir** a resiliência do ciberespaço; - **Sincronizar** iniciativas de Cibersegurança enquanto prioriza investimentos baseados no risco, desempenho e valor para a missã**o**; - **Estabelecer** uma estrutura de *Cyber Governance*; - **Dispor** de tecnologias e processos que monitorizam o tráfego de saída de informações. - **Estimular** a liderança e consciência do nível executivo para a gestão de riscos cibernéticos; - **Desenvolver** a implementação de um programa prático e efetivo - Gestão integrada do risco.	- Programa de maturidade baseada em 5 estágios sucessivos: **- Estágio 1: Inicial,** **- Estágio 2: Fragmentada,** **- Estágio 3: *Top-Down*,** **- Estágio 4: Integrada, e** **- Estágio 5*: Risk Intelligent.*** - As organizações estão divididas em 3 escalões: ***- Risk Governance*:** ***- Risk Infrastructure and Management:*** ***- Risk Ownership:***	***- Risk Governance Level:*** envolvimento entre o conselho de administração e a direção executiva, sobre o risco de ameaça cibernética; ***- Risk Infrastructure and executive management* Level:** é responsável pela implementação e manutenção das **pessoas**, **processos** e **elementos tecnológicos;** ***- Risk Ownership Level*:** Os funcionários têm responsabilidades bem definidas, orientações de como usar e partilhar informações.	Efeitos: **- Avaliação da ameaça**: o valor dos ativos da sua organização e as vulnerabilidades atuais; **- Rede de informações:** contínuas parcerias no sentido de partilhar boas práticas, experiências e conhecimentos; **- Gestão de riscos:** Integração dos sistemas internos transacionais e de segurança; **- Relação Comercial**: "*Cyber Intelligence*" para permitir a redução do risco e o prejuízo no negócio.

Apêndice V – Guião de Entrevista e Formulário de Questões

Guião de entrevista a Especialistas de Informações e Entidades relacionadas com a Segurança da Informação no Ciberespaço

Formulário de questões

Tema

Cyber Intelligence – A obtenção de informações a partir de fonte aberta no ciberespaço

Objetivos gerais

Conhecer as atividades e experiência acumuladas de cada entrevistado e que juízos fazem sobre a importância da *Cyber Intelligence*.

Recolher informação relevante que contribua para validar o modelo de *Cyber Intelligence,* proposto pelo autor do presente trabalho.

Avaliar o contributo da *Cyber Intelligence* na gestão de crises no ciberespaço.

Obter do entrevistado a sua visão de qual poderia ser o modelo militar, governamental e empresarial de *Cyber Intelligence.*

Guião de entrevista

Blocos	Objetivos específicos	Questões	Tópicos
Bloco 1 Legitimação da entrevista	Informar acerca das finalidades da investigação. Motivar o entrevistado a participar, realçando o valor da colaboração. Assegurar a confidencialidade e anonimato das declarações prestadas. Obter autorização para a gravação da entrevista. Informar a duração aproximada da entrevista. Fazer a transcrição.		

Bloco 2 Perfil do entrevistado (percurso académico e profissional)	Caracterizar o sujeito.	Formação Inicial – breve descrição Percurso académico/profissional.	Como tem sido o seu percurso Profissional. Quanto tempo de serviço tem. Que cargos tem desempenhado.
	Conhecer o seu percurso académico e profissional.	Formação contínua.	Adquiriu alguma formação específica para o exercício do cargo. Que funções desempenha atualmente.
Bloco 3 Caracterizar o departamento onde o entrevistado exerce funções	Conhecer o contexto profissional.	Referenciar dados relativos à localização do local de trabalho.	Como tem gerido a sua formação contínua. Organização interna do departamento – dependências e níveis hierárquicos.

Bloco 4 A importância da *Cyber Intelligence*	Descrever o contexto da atividade de informações. Descrever o processo de elaboração de informações adotado, em particular a *Cyber Intelligence.*	Como apareceu e qual a importância dada às informações, no contexto atual. Como nasceu a *Cyber Intelligence*. Como é constituído o processo: - Que dificuldades foram sentidas. - Como foram resolvidas. - Quais as referências e as propensões.	Descrição geral Quando começaram. Quem teve a iniciativa e qual o contexto. Como começaram. Como era formada a primeira equipa. Como foram selecionadas. Alguma decisão formal ou informal. Qual o modelo adotado. Como está estruturado. Quais as capacidades.

	Descrever a forma como funciona a equipa/ centro neste momento. Descrever que alterações ocorreram ou estão a decorrer.	Como recolhem informação. Que atividades desenvolveram. Como fizeram a avaliação na prática. Quais os produtos resultantes. Como foram divulgados os resultados. Quem tem conhecimento. Como são redigidos os relatórios. Neste momento como é constituída a equipa. A equipa mantém-se a mesma ou mudou. A atuação da equipa/ serviço. Como minimizar os riscos e potenciar as oportunidades.	Mantém a mesma atuação do início ou mudou. O que motivou as alterações. Quais as prioridades da equipa. A importância para a tomada de decisão. Ferramentas *Web* indispensáveis para assegurar os serviços.

Bloco 5 Os efeitos sentidos	Analisar e interpretar qual é o contributo da *Cyber Intelligence*.	Contributo da *Cyber Intelligence* em geral na organização. Contributo da *Cyber Intelligence* na gestão de crises eficaz. Impacto das conclusões dos relatórios. De que forma a *Cyber Intelligence* é percecionada pela gestão de topo. Que mudanças houve e em que sentido existiram.	Gestão de riscos. Segurança Proactiva. Cooperação interinstitucional. Plataforma única de partilha de informação. Estado regulador ou interventivo. O futuro da *Cyber Intelligence*.
Bloco 6 Modelo de *Cyber Intelligence*	Saber qual o modelo de *Cyber Intelligence* defendido pelo entrevistado	Como especialista, qual o modelo militar, governamental e empresarial de *Cyber Intelligence* melhor se aplicaria.	Tem algum modelo de *Cyber Intelligence* de referência? Qual o modelo que defenderia ou recomendaria?

Apêndice VI – Entrevista Tenente Coronel Alves

Entrevistado: TCor Lima Alves (CISMIL) **Data:** 25-10-2013

Entrevistador: Óscar Frias **Assunto:** *Cyber Intelligence*

Objetivos:

1. Recolher informação relevante que contribua para validar o modelo de *Cyber Intelligence*, proposto pelo autor do presente trabalho.
2. Conhecer as atividades e experiência acumuladas do entrevistado e que juízos faz sobre a importância da *Cyber Intelligence*.
3. Avaliar o contributo da *Cyber Intelligence* na gestão de crises no ciberespaço.

Principais pontos abordados:

Função, área de atuação e limitações.

A importância da OSINT.

A OSINT e o ciberespaço (sobretudo a *Internet*).

Fontes de informação OSINT e sua importância.

Fontes abertas e fontes pagas.

Falta de recursos humanos na análise.

Ferramentas de recolha de informação em linha.

Opiniões do entrevistado:

A OSINT é fundamental e quem menospreza a OSINT é um idiota.

A *Internet* veio mudar a forma de trabalhar informações.

Nesta região (África) nós fazemos OSINT com base em "Blogs", porque nesta região existe muito poucas fontes de informação, a não ser um jornal ou outro, ou como por exemplo a agência noticiosa LUSA.

Mas é preciso conhecer as pessoas. Porque também há muita informação em "Blogs" que não interessa e é incorreta (por exemplo propaganda enganosa de falsos tumultos).

É preciso ter muito cuidado, nem tudo o que se diz na *Internet* é verdade.

É preciso conhecer bem as fontes, as pessoas e ir ao terreno.

Não há aqui espionagem, é tudo informação aberta, disponível através de pessoas que estão no local, observam e colocam na *Internet*.

Normalmente são pessoas da oposição (ao regime vigente) que procuram informação que ponha em causa as elites e quem detém o poder.

Não confundir OSINT com HUMINT. HUMINT é feito por operacionais que trabalham para os SIS, com vista a atingir um objetivo em particular.

Os Adidos, por exemplo, são muito importantes, porque embora não estando a trabalhar para as informações, são um contacto privilegiado.

É preciso uma monitorização constante e existem poucas pessoas, neste momento, a fazer análise.

Cada analista tem a sua área de responsabilidade e somos poucos, não fazemos *brainstorms.*

Não confundir fonte aberta com fonte livre. Existem muitas fontes em linha que se pagam muito bem.

A minha maneira de escolher as fontes é muita leitura e ler *à posteriori*. Leio uma notícia, guardo-a e depois volto-a a ler passados uns tempos para verificar a veracidade dela.

Apêndice VII – Entrevista Tenente Coronel Gonçalves

Entrevistado: TCor Gonçalves (CISMIL) **Data:** 25-10-2013

Entrevistador: Óscar Frias **Assunto:** *Cyber Intelligence*

Objetivos:

1. Recolher informação relevante que contribua para validar o modelo de *Cyber Intelligence*, proposto pelo autor do presente trabalho.
2. Conhecer as atividades e experiência acumuladas do entrevistado e que juízo faz sobre a importância da *Cyber Intelligence*.
3. Avaliar o contributo da *Cyber Intelligence* na gestão de crises no ciberespaço.

Principais pontos abordados:

Funções do CISMIL (Decreto-Lei n.º 234/2009 de 15 de setembro).

Os PIR's nacionais.

Área de influência e área de interesse.

Fontes de OSINT (plataformas e redes entre países NATO e PfP).

Ferramentas OSINT (agregadores de informação).

Escola de informações.

Cultura de informações.

Recursos Humanos e especialização.

Vantagens na utilização de OSINT.

Integração de disciplinas de informações.

Gestão de Crises no Ciberespaço.

Opiniões do entrevistado:

Quando falamos em fonte, falamos também na origem do sítio.

Por exemplo se o servidor estiver alojado nos EUA, a fonte é pró-ocidental.

Plataforma de rede informática, de países NATO e outros parceiros/ coligações (ISAF).

PIR's nacionais: apoiar os Estados-Maiores dos Ramos em prol das FND's, acompanhar os PALOP e acompanhar a diáspora portuguesa (são as áreas de influencia).

A *Internet* tem muitas ferramentas. A OSINT faz-se com o cruzamento de fontes e origens da informação.

Em África: usamos a análise de "Blogs" (escrita de rua), redes sociais, organização social, LUSA, jornais.

É preciso ter em atenção o espectro e as ligações a grupos financeiros, dessas fontes. Qual a história recente e passada dessas fontes.

Os cursos permitem esquematizar as nossas ideias, a nossa pesquisa e sabermos através de outras pessoas o que é que existe, com as mesmas ferramentas.

A nível NATO, dentro da área de influência da NATO, mais as áreas de interesse, nós temos muita informação, derivada das redes proprietárias da NATO e não proprietárias da NATO.

Onde é que temos as nossas grandes falhas? Em África, onde temos os nossos interesses. Aí tem que ser mesmo OSINT.

A informação que nos chega também é um bocado desvirtuada da realidade. É muito tendenciosa. Nós sabemos que os jornais nesses locais, por exemplo, os jornais da oposição, não têm meios, não têm financiamento, logo não sobrevivem.

Em Portugal, temos um problema que é: não temos uma Escola de Informações que aborde todas as disciplinas das informações.

E temos outro problema que é: há uma cultura, que se calhar já vem de trás, em que não há separação interlinguísticos dentro das informações.

Não temos uma Escola de Informações ou de Inteligência que forme pessoas dentro desta área, porque as pessoas fazem análise muito *adoc*, vêm para esta área por gosto e acabam por aprender aqui a trabalhar.

Um centro que não tenha um bom reforço humano não consegue abranger essas disciplinas todas. Hoje em dia temos que pensar na especialização.

Focalizamo-nos no essencial e o quem é nos dá o essencial? O BICES, dá-nos isso já trabalhado.

É nossa obrigação partilhar informação com os outros países da NATO. É uma responsabilidade nossa. Nós isolados, ou conjuntamente com outros países, temos obrigatoriamente de fazer análise, partilhar e fazer uma avaliação de risco nesses países.

Se uma empresa está sediada em Portugal, se a empresa é nacional, se a empresa contribui para o desenvolvimento de Portugal, porque não serem os órgãos

portugueses a apoiar essas empresas, de que maneira for, com partilha de informação.

Quanto mais informações conseguirmos obter da *Internet*, quanto mais resumida, mais agregada tiver melhor é.

Hoje em dia, informação é poder. Hoje em dia, a rapidez da chegada da informação ao analista é importante.

Normalmente, passamos o ato da notícia primeiro, vamos recolhendo mais informação, vamos fazendo a atualização dessa mesma informação, até termos um *assessmen*t eficaz.

Os meus meios de pesquisa são: o BICES, o SIGINTCOINS, O MMHS, a *Internet* e outros (adidos, pessoal em determinados cargos e as FNDs).

Numa situação de gestão de crise no ciberespaço, nós o que podemos fazer é realizar algum estudo, termos alguma história para trás. Por quem fomos atacados? Porque razão fomos atacados? É um ataque de *hackers* ou de um país?

Hoje em dia, vamos para a *Open Source* porque nos sai mais barato.

A OSINT pode por si só produzir informações se não houver mais nada. Mas toda essa *Open Source* vale o que vale, essa análise vale o que vale, tem que ser integrada noutras informações que venham de outras disciplinas.

Apêndice VIII – Entrevista Prof. Dr. Pedro Borges Graça

Entrevistado: Prof. Dr. Pedro Borges Graça **Data:** 25-10-2013

Entrevistador: Óscar Frias **Assunto:** *Cyber Intelligence*

Objetivos:

1. Recolher informação relevante que contribua para validar o modelo de *Cyber Intelligence*, proposto pelo autor do presente trabalho.
2. Conhecer as atividades e experiência acumuladas do entrevistado e que juízos faz sobre a importância da *Cyber Intelligence*.
3. Avaliar o contributo da *Cyber Intelligence* na gestão de crises no ciberespaço.

Principais pontos abordados:

Competitive Intelligence.

"*Correspondant Honorable*".

Relações de confiança entre serviços de informações e uma componente empresarial.

O caso da *Ongoing.*

Espionagem económica.

O célebre caso "*Vallery Plan*".

Tecnologia e investigação.

Libertação de informação desclassificada.

Valorização das informações**.**

O "pronto-a-vestir" das informações.

Células de informações.

Unidade sectorial de informações.

Opiniões do entrevistado:

As empresas do eixo anglo-americano, tradicionalmente, sempre tiveram essa componente de procurar junto dos meios oficiais, nomeadamente militares, informações que os ajudassem a fazer negócios na parte comercial.

A figura do "*Correspondant Honorable*" é uma figura de ligação dos serviços a determinadas empresas.

O princípio do "*Correspondant Honorable*", significa uma relação de alguém dentro do serviço muito secreta, classificada muito secreta, do conhecimento de uma ou duas pessoas.

Promover como missão dos serviços, a ligação às empresas, ora isso é uma coisa que não se diz e que não se faz.

A maior dificuldade é a promiscuidade de que se pode gerar a partir de um determinado discurso, de favorecimento de umas empresas em detrimento de outras, em termos de relações institucionais.

No mercado, se uma empresa é conhecida no mercado por ter relações privilegiadas com um serviço de informações, de que país for à partida, está queimada no mercado.

As relações entre serviços e empresas não promíscuas e, em último caso, quem se prejudica é a empresa.

Todos os serviços sem exceção e consoante mais capacidades têm, têm um correspondente muito secreto de espionagem económica. Todos os serviços desenvolveram mecanismos de espionagem económica.

Não transparecem cá para fora a não ser quando acontecem escândalos é que nós conseguimos deslumbrar um bocado as operações em curso. O célebre caso "*Vallery Plan"* nos EUA, é um caso típico de uma operação de espionagem económica

Os serviços de informação devem fazer processos de recrutamento, de acordo com um plano de interesses e de alvos dentro das empresas e ter uma relação institucional-pessoal, ou seja, alguém dentro do serviço a quem é atribuída essa missão de ter uma relação também com outra pessoa dentro de outra instituição.

Os grandes desenvolvimentos tecnológicos são feitos no ambiente militar. Há relações ou há contratantes privados para preencher determinadas necessidades.

O segredo de Estado está muito mal desenhado e consagrado juridicamente em Portugal, que dá espaço, por exemplo, dentro dos serviços, passados 20, 30, 40 anos, não haja libertação de informação desclassificada.

Do ponto de vista das empresas não existe uma valorização do valor das informações.

O gestor português tem a mania que pega no telefone e fica logo a saber tudo ou vai de viagem com o Primeiro-Ministro a Angola e fica logo a conhecer toda a gente.

Aquela coisa de carregar num botão e já está que é o "pronto-a-vestir" das informações.

É muito fácil hoje ir buscar informação por fontes abertas à *Internet*, se bem com uns pequenos truques e bem orientado.

Se for bem organizado, essa célula (de informações) deverá estar completamente à parte, fisicamente.

Existe uma unidade sectorial que interliga a informação do privado e do Estado. Há uma plataforma de acesso comum, onde existe informação de "pronto a vestir".

Mas o mais importante é que cada empresa tenha a sua célula de informações. Há muita gente a perder dinheiro com a falta de informação.

Apêndice IX – Centro de Informações e Segurança Militares

Missão e atribuições

(De acordo com o Decreto-Lei n.º 234/2009, de 15 de setembro)

O Centro de Informações e Segurança Militares (CISMIL) tem, nos termos da lei, por missão, a produção de informações necessárias ao cumprimento das missões específicas das Forças Armadas e à garantia da segurança militar.

Cabe ao CISMIL, no âmbito das suas atribuições específicas, promover, de forma sistemática, a pesquisa, a análise e o processamento de notícias e a difusão e arquivo das informações produzidas, devendo, nomeadamente:

a) Produzir as informações necessárias para a preparação e execução de missões e operações militares;

b) Acionar os meios técnicos e humanos das Forças Armadas, necessários à produção de informações e à garantia da segurança militar, desenvolvendo a sua atividade de acordo com orientações e diretivas emanadas do CEMGFA, em coordenação com os ramos;

c) Dirigir as células de informações militares, quando constituídas;

d) Difundir as informações produzidas, de forma pontual e sistemática, às entidades que lhe sejam indicadas;

e) Colaborar na definição da doutrina militar conjunta e combinada nos vários domínios da sua área específica;

f) Orientar a instrução de informações nas Forças Armadas;

g) Recolher, processar e disseminar a informação geoespacial para apoio ao planeamento e conduta das operações militares;

h) Dirigir a exploração dos sistemas de informação geoespacial de natureza conjunta;

i) Coordenar as atividades dos adidos de defesa, de acordo com orientações e diretivas emanadas pelo CEMGFA;

j) Assegurar a ligação com os adidos de defesa ou militares acreditados em Portugal;

k) Assegurar e participar na representação nacional nos organismos nacionais e internacionais, no âmbito das informações militares, segurança militar e informação geoespacial;

l) Comunicar às entidades competentes para a investigação criminal e para o exercício da ação penal os factos configuráveis como ilícitos criminais, salvaguardado o que nos termos da lei se dispõe sobre segredo de Estado;

m) Comunicar às entidades competentes, nos termos da lei, as notícias e as informações de que tenha conhecimento e respeitantes à segurança do Estado e à prevenção e repressão da criminalidade.

Estrutura

O CISMIL é dirigido por um contra-almirante ou major-general e tem a seguinte estrutura:

a) Repartição de Planeamento;

b) Repartição de Coordenação e Gestão da Pesquisa;

c) Repartição de Produção;

d) Repartição de Segurança e Contra -Informação;

e) Gabinete de Ligação aos Adidos de Defesa e Militares;

f) Secção de Apoio.

As atividades de informações levadas a cabo pelas Forças Armadas, necessárias ao cumprimento das suas missões específicas e à garantia da segurança militar, regem--se por legislação própria, de acordo com as atribuições que decorrem da Lei Quadro do Sistema de Informações da República Portuguesa.

Apêndice X – Quadro Resumo das Questões e respetivas Hipóteses

Questão central	Questões derivadas	Hipóteses
Como poderão as informações de fontes abertas no ciberespaço melhorar a Cibersegurança/ Ciberdefesa nacional, garantindo assim que, através de uma adequada gestão de informação, a cooperação interinstitucional contribua para uma gestão de crises mais eficaz?	Como poderá a *Cyber Intelligence* minimizar os riscos e potenciar as oportunidades que a *Internet* oferece?	Portugal deverá munir-se imediatamente de recursos e ferramentas necessários, para melhorar as capacidades no âmbito da Ciberdefesa.
	Como tornar a *Cyber Intelligence* uma ferramenta indispensável para assegurar os serviços providenciados pela *Internet* e garantir a confiança dos seus utilizadores?	A *Cyber Intelligence* é uma ferramenta indispensável na consecução plena dos serviços de informações no ciberespaço, que visam dotar o Estado e o setor privado de condições de troca e partilha de informação privilegiadas pelo meio da *Internet*.
	De que forma a cooperação interinstitucional garante uma decisão mais informada e segura, permitindo a gestão de crises mais eficaz?	A abordagem integrada, que reúne capacidades civis e militares a trabalhar em conjunto para atingir um objetivo único, é o veio principal na colaboração para a definição de orientações que melhorem o conhecimento situacional de Ciberdefesa.
	Será possível definir um modelo de gestão de informação interinstitucional integrado (órgãos do Estado e setor privado) no ciberespaço, capaz de melhorar a resiliência nacional, face à ocorrência de ciberataques?	A educação e a perceção política, isto é a intervenção do Estado, nesta matéria são fundamentais para criar sinergias positivas na sensibilidade, conceptualização e decisão dos cidadãos, em matérias relacionadas com a segurança da informação na *Internet*, nomeadamente redes sociais e "Blogosfera".

Apêndice XI – Diagrama de Validação

	Questões derivadas		Hipóteses		
QD1	Como poderá a *Cyber Intelligence* minimizar os riscos e potenciar as oportunidades que a *Internet* oferece?	§§ 7,8,9,10,11,22,23,24 e 25 de 2.1.; §§ 16,17, 18 e 19 de 2.2.; §§ 5, 7, 8,10,11,15, 17 e 21 de 2.3.; §§ 2,3,4,5 e 6 de 2.4; §§ 6,19, 20, 21 e 26 de 2.5; §§ 12,18,19,20,22 e 23 de 2.6; § 7 de 3.2.1; §§ 3,6 e 7 de 3.2.8.	H1	Portugal deverá munir-se imediatamente de recursos e ferramentas necessários, para melhorar as capacidades no âmbito da Ciberdefesa.	C
QD2	Como tornar a *Cyber Intelligence* uma ferramenta indispensável para assegurar os serviços providenciados pela *Internet* e garantir a confiança dos seus utilizadores?	§§ 13,16,17,18,19,20, 21,22, 23,24 e 25 de 2.1.; §§ 8,9,12, 13, 14 e 15 de 2.2.; §§ 3, 4, 5, 6, 10, 11, 13 e 17 de 2.3; §§ 15 e 16 de 2.4; §§ 14, 15, 16 e 22 de 2.5; §§ 18 e 19 de 2.6; §§ 6, 7, 15 e16 de 3.2.2;§§ 2, 10 e 11 de 3.2.3.	H2	A *Cyber Intelligence* é uma ferramenta indispensável na consecução plena dos serviços de informações no ciberespaço, que visam dotar o Estado e o setor privado de condições de troca e partilha de informação privilegiadas pelo meio da *Internet*.	C
QD3	De que forma a cooperação interinstitucional garante uma decisão mais informada e segura, permitindo a gestão de crises mais eficaz?	§ 14 de 2.3; §§ 16 e 17 de 2.4; §§ 11, 12, 13 e 21 de 2.5; §§ 14, 15, 16 e 23 de 2.6; §§ 6, 7, 15 e16 de 3.2.2;§§ 2, 10 e 11 de 3.2.3; § 3 de 3.2.4.	H3	A abordagem integrante, que reúne capacidades civis e militares a trabalhar em conjunto para atingir um objetivo único, é o veio principal na colaboração para a definição de orientações que melhorem o conhecimento situacional de Ciberdefesa.	C
QD4	Será possível definir um modelo de gestão de informação interinstitucional integrado (órgãos do Estado e setor privado) no ciberespaço, capaz de melhorar a resiliência nacional, face à ocorrência de ciberataques?	4.1.2; 4.2.2.3; 4.3.	H4	A educação e a perceção política, isto é a intervenção do Estado, nesta matéria são fundamentais para criar sinergias positivas na sensibilidade, conceptualização e decisão dos cidadãos, em matérias relacionadas com a segurança da informação na *Internet*, nomeadamente redes sociais e "Blogosfera".	C

QD – Questão Derivada H – Hipótese C - Confirmada

Apêndice XII – Diagrama de Revisão

Varáveis-chave	Presente Modelo	Doutrina Militar	Inteligência Competitiva	Exercício Ciberdefesa
Domínio	Área de responsabilidade: Global, Nacional, Local. Nível organizacional: Político, Estratégico, Operacional, Técnico/ Tático.	Áreas de interesse e áreas de influência do Estado Português.	Global e a todos os níveis da organização.	Estratégico (Política), Operacional e Tático (Forças armadas e de segurança/ setor privado).
Ator	Político, Diplomático, Militar, Industria, Económico-financeiro, Justiça, Académico.	Nível de atuação puramente militar.	Empresarial (Económico-financeiro), Indústria, Diplomático e Académico.	Estados, Grupos, *Hacktivistas*, Terroristas, Criminosos e Crime organizado.
Fonte	*Internet*, Redes Internas e Externas, Informação em Suporte Eletrónico, Literatura cinzenta, Especialistas, Informação Comercial (*Pay-to-See*), Informação Geoespacial Comercial, Fontes com Requisitos de Acesso.	*Internet* (“Blogs”) **Adidos militares.** Agências noticiosas. Órgãos Comunicação Social. **Uso de redes internas classificadas da OTAN para validar a informações.**	**“*Correspondant Honorable*”. Espionagem económica**.	**Redes de Comunicação e Sistemas de Informação**

Ação	Pessoas, Processos, Tecnologia.	Recursos Humanos. **Conhecimento prévio das fontes (Perfil de autores de "Blogs").** Ferramentas ou agregadores de informação em linha.	Tecnologia e Investigação, desenvolvida em ambiente militar, com parcerias privadas. **"Pronto-a-vestir" das informações,** através de uma plataforma única de partilha. **Processos de recrutamento.**	Formulário de **Análise Morfológica;** Formulário de **Análise de Atores;** Ferramenta de **Planeamento Operacional Baseado em Efeitos.**
Vulnerabilidades	Capacidades, Cultura, Formação e Treino, Volume de Informação, Formatação, Idioma, Segurança, Legislação, Classificação.	Falta de cultura de informações. Falta de uma Escola de Informações. **As origens da informação.** **Áreas inóspitas de atuação, com poucas fontes credíveis de informação.**	**Relações de confiança** entre uma componente empresarial e um serviço de informações. **Valorização das informações**. **Libertação de informação desclassificada.**	Processo de **planeamento e construção dos cenários;** **Análise empírica** dos atores; **Local pré-definido para operar;** **Adequação de conhecimentos e treino.**
Efeitos	Segurança proactiva, Aviso prévio, Avaliação da Ameaça, Gestão de Riscos, Rede de Informações, Conhecimento Situacional, Autenticidade, Colaboração Público-Privado,	Cooperação militar internacional. Aviso prévio. Avaliação da ameaça. **Integração interdisciplinar** com outras fontes não	Segurança e gestão de riscos. **Vantagem competitiva.**	**Apoio à tomada de decisão, na gestão de crises eficaz no ciberespaço.**

	Cooperação Internacional.	classificadas e classificadas.		
Objetivo	Detetar, Identificar, Colecionar, Analisar, Validar, Monitorizar, Prevenir, Partilhar, Colaborar.	**Dirigir**, **Coordenar**, **Orientar**, Produzir, Difundir, Comunicar, Colaborar.	Monitorizar, analisar, assessorar.	**Avaliação dos perfis das ameaças;** **Avaliação do Impacto das ameaças;** **Projeção das futuras ações (medidas).**
Método	Planeamento e Direção, Recolha, Processamento e Exploração, Análise, Produção, Disseminação e Integração, Avaliação, Feedback, Formação.	Planeamento, Coordenação e Gestão de Pesquisa, Produção, **Ligação aos Adidos de Defesa e Militares.**	**Células de Informações.** **Unidades sectoriais** que interligue a informação do privado e do Estado.	**Análise do Risco Social e Construção de Cenários;** **Análise de Atores e Análise do Ambiente Estratégico;** **Análise do Estado Final e do Critério de Sucesso;** **Desenvolvimento de Efeitos;** **Desenvolvimento de Ações de Sincronização e Refinamento do Plano**

Apêndice XIII – Ferramenta de Análise Morfológica

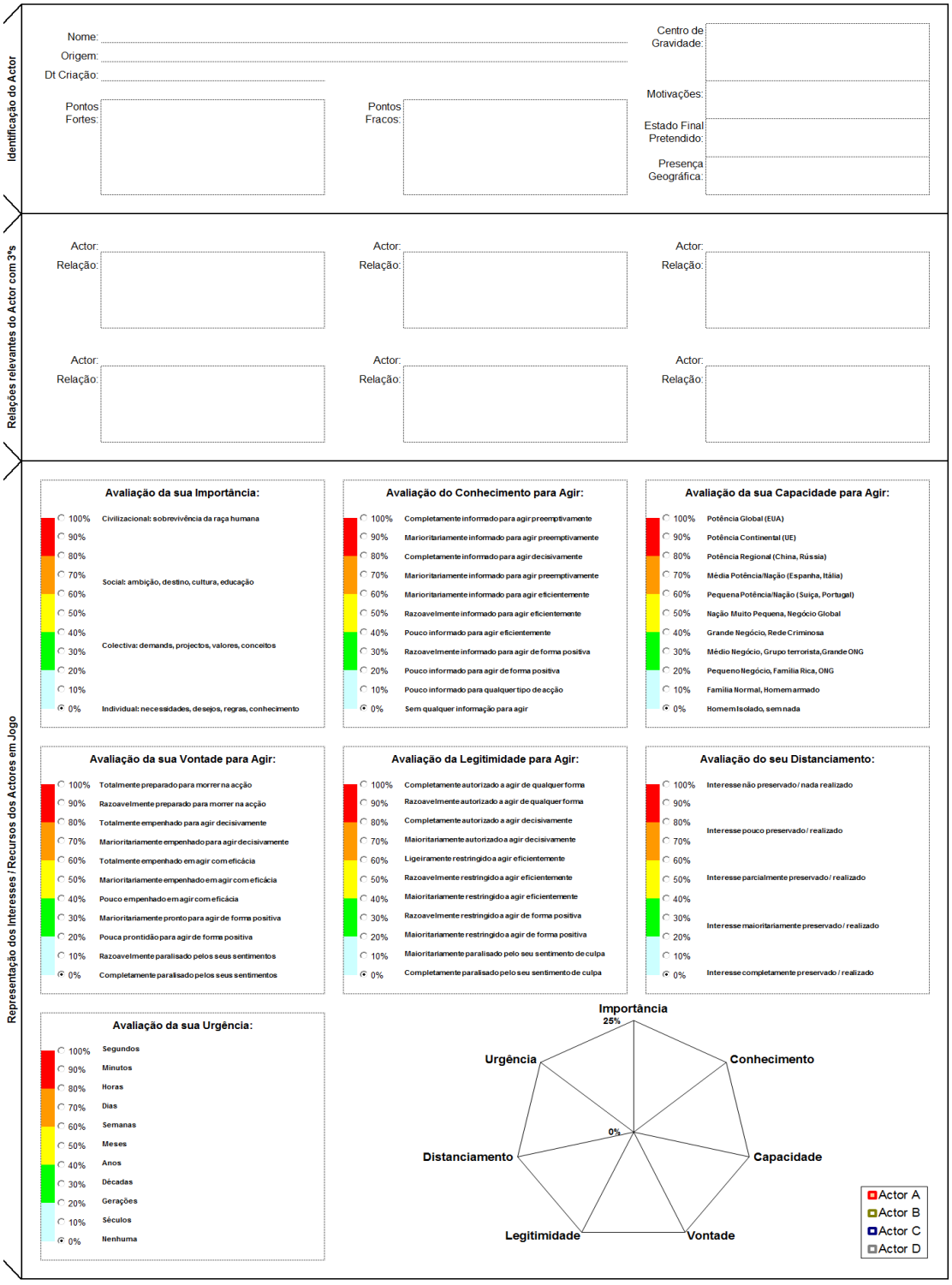
Dimensões / Vectores do Poder	Infra-estructuras Críticas Nacionais	Efeitos das Armas de GI	Probabilidade de Ataque	Tipos de Actores
☐ Política/Diplomática	☐ Rede Eléctrica	☐ Físico	☐ Muito Alta	☐ Amadores
☐ Informação	☐ Redes Telecom.	☐ Sintaxe	☐ Alta	☐ Hackers
☐ Militar	☐ Sist. Transportes	☐ Semântico	☐ Moderada	☐ Crackers
☐ Económica	☐ Sist. Financeiro		☐ Baixa	☐ Activistas
	☐ Defesa		☐ Nula	☐ Crime Organizado
	☐ Serviços Emergência			☐ Terroristas
	☐ Outras IE Críticas			☐ Estados

Legenda:
condição de parâmetro seleccionada
condição de parâmetro disponível
condição de parâmetro indisponível

Limpar Selecção

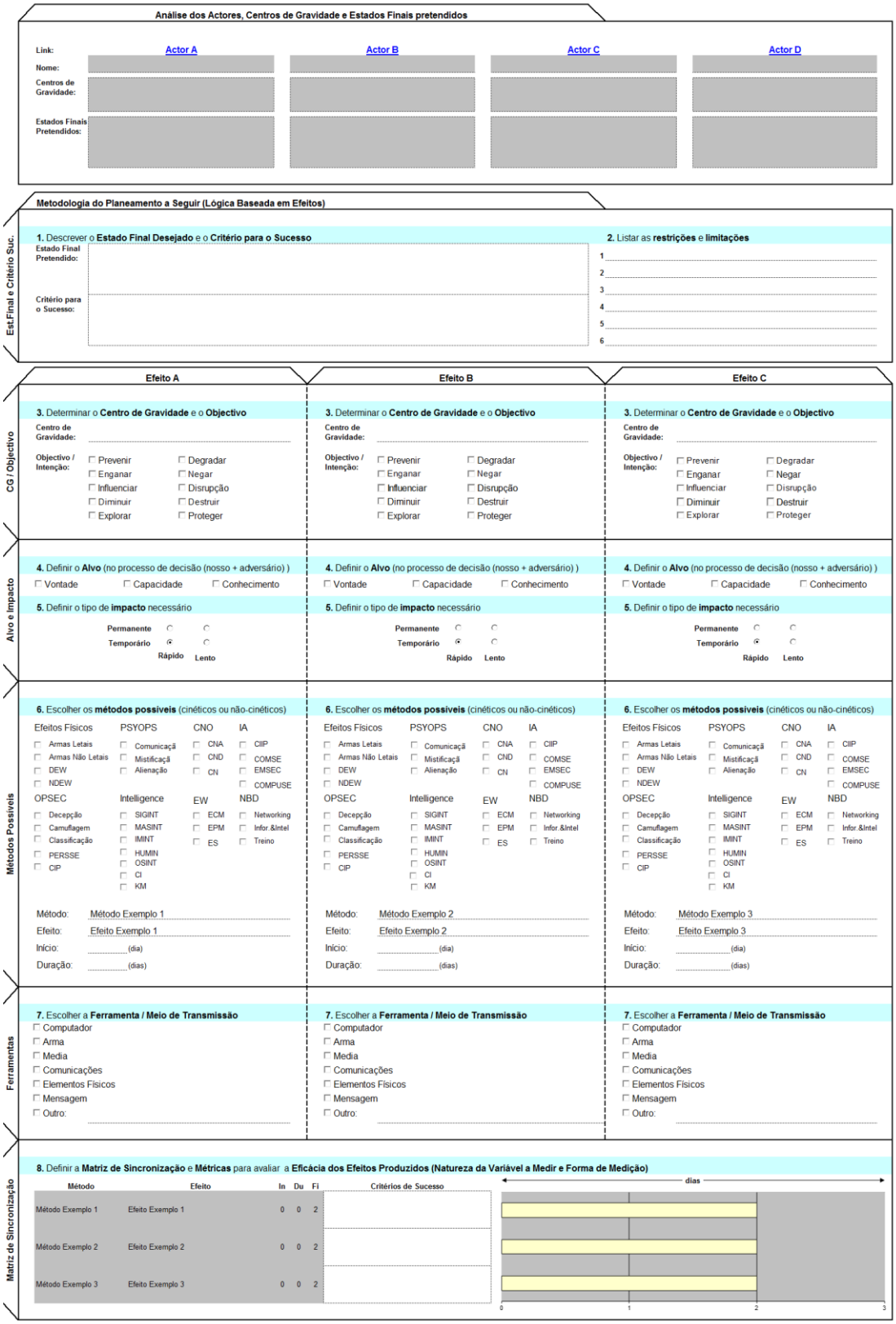
Fonte: Adaptado de Nunes, 2011

Apêndice XIV – Formulário de Análise de Atores



Fonte: Adaptado de Nunes, 2011

Apêndice XV – Ferramenta Operacional de Planeamento Baseado em Efeitos



Fonte: Adaptado de Nunes, 2011