ACADEMIA DA FORÇA AÉREA

Cibersegurança das Infraestruturas Críticas Nacionais

Eduardo Luís Gonçalves Pequeno de Oliveira e Silva

Aspirante a Oficial-Aluno Piloto-Aviador 137731-A

Dissertação para obtenção do Grau de Mestre em

Aeronáutica Militar, na Especialidade de Piloto-Aviador

Júri

Presidente:	Cor/EngEl Luís Filipe Basto Damásio
Orientador:	Professor Doutor Paulo Cardoso do Amaral
Coorientador:	TCor/EngInf José Manuel António Gorgulho
Vogal:	TCor/EngInf Ana Cristina Domingos de Oliveira Rodrigues Telha

Sintra, março de 2015

Este trabalho foi elaborado com finalidade essencialmente escolar, durante a frequência do Curso de Pilotagem Aeronáutica cumulativamente com a atividade escolar normal. As opiniões do autor, expressas com total liberdade académica, reportam-se ao período em que foram escritas, mas podem não representar doutrina sustentada pela Academia da Força Aérea.

Agradecimentos

A presente dissertação é o terminar do curso de Ciências Militares Aeronáuticas, da Academia da Força Aérea. Considero singular privilégio tal oportunidade, que permitiu, em última análise a realização desta dissertação.

Como culminar de um processo académico, identifico e agradeço a disponibilidade manifestada por várias personalidades.

Em primeiro lugar, gostaria de agradecer ao Professor Doutor Paulo Amaral, que pela sua boa disposição, paciência e profissionalismo nas inúmeras sugestões e conselhos, se revelou essencial para a elaboração desta dissertação.

Os meus sinceros agradecimentos ao meu coorientador, Tenente-Coronel José Gorgulho, pela incansável ajuda demonstrada ao longo de todo o trabalho e incansável esforço de tornar possível a realização das tão importantes entrevistas, bem como ao especial cuidado demonstrado na correção dos textos.

A todos os Oficiais, pela sua prestabilidade e disponibilidade ao concederem o privilégio de os entrevistar, nomeadamente a sua excelência o Senhor Major-General Pedro Melo, Tenente-Coronel Viegas Nunes, Major Paulo Branco, Major António Valente, Major João Farinha bem como ao Capitão-Tenente Francisco Assunção. E ainda ao Engenheiro Lino Santos do Centro Nacional de Cibersegurança.

Um especial agradecimento à minha família, não só pela educação e condições de formação que me proporcionou, bem como pelo auxílio, motivação e apoio que desde o primeiro minuto se revelaram fundamentais para ultrapassar mais esta etapa bem como todas as que a antecederam.

Finalizando os agradecimentos, resta apenas agradecer a todos os que, apoiando ou criticando, tornaram possível o atingir de mais este objetivo que não se trata do fim de um percurso, mas sim do início de uma nova etapa.

Resumo

Segundo o Conceito Estratégico de Defesa Nacional (CEDN) aprovado em 2013, o novo ambiente de segurança obriga a uma capacidade de resposta diferente das Forças Armadas (FFAA), isto é, os investimentos de modernização devem concentrar-se em equipamentos de indiscutível utilidade técnica e estratégica em função das capacidades necessárias ao cumprimento das missões prioritárias assumindo grande importância a definição de uma estratégia civil e militar integrada. Assumindo que os ciberataques se manifestam como uma ameaça crescente às Infraestruturas Críticas (IC) em que os potenciais agressores poderão incapacitar totalmente a estrutura tecnológica de um estado nação moderno (CEDN, 2013), este trabalho discute a proteção das IC na perspetiva da gestão do risco relacionado com a cibersegurança e a ciberguerra, e no envolvimento e contribuição potencial das FFAA e das forças de segurança para a gestão desse mesmo risco. Em particular, este trabalho estuda a possível participação das FFAA na ciberdefesa/cibersegurança das Infraestruturas Críticas Nacionais (ICN).

Com base numa recolha de documentação da União Europeia, Força Aérea Portuguesa e Forças Armadas, bem como da informação recolhida em entrevistas aos especialistas, é realizada uma análise aos conceitos de ciberdefesa e cibersegurança e às metodologias de gestão de risco RAMCAP e ISO 31000, e será da interligação destes conceitos com a informação retirada das entrevistas aos especialistas que serão estabelecidas as conclusões do trabalho.

Conclui-se que as FFAA têm espaço não só na ciberdefesa das ICN mas também na cibersegurança, intervindo não só nos três casos de exceção previstos na lei, mas também na monitorização constante do ciberespaço, sendo a segurança e defesa do ciberespaço o resultado de um trabalho conjunto e combinado.

Finalmente, este trabalho recomenda que as FFAA, como parte interessada na cibersegurança das ICN, passem a apoiar na definição dos requisitos de segurança das mesmas em conjunto com o Centro Nacional de Cibersegurança (CNCS) e com a Autoridade Nacional de Proteção de Civil (ANPC).

Palavras-chave: ICN, FFAA, Ciberdefesa, Cibersegurança, Guerra da Informação

Abstract

In accordance with the 'National Defense Strategic Concept (CEDN)', approved in 2013, the current security environment requires a different response capacity from the Armed Forces. In essence, this means that investment in modernization should focus on equipment of indisputable technical and strategic utility according to the capacities necessary to carry out priority tasks, thus assuming a greater level of importance in defining a civil and military integrated strategy.

Assuming that cyber-attacks manifest themselves as an escalating threat to the CI in which potential aggressors may fully incapacitate the technological structure of a modern nation state (CEDN, 2013), the current paper discusses the protection of the IC within the perspective of risk management related to cyber-security and cyber-warfare, as well as the involvement and potential contribution of the Armed Forces and security forces in the management of the risk in question. In particular, this work studies the possible role of the Armed Forces in ICN cyber-defense/cyber-security.

In this dissertation, a collection of European Union, Portuguese Air Force and Armed Forces documentation, as well as information gathered during interviews with experts, has been used as a basis for analysis in the light of the concepts of Cyber Defense and Cyber Security, and to the risk management methologies RAMCAP and ISO31000. Through linking the information derived both from theory and from the information gathered during the interviews, we find the interconnection that allows us to the conclusions.

We can conclude that the Armed Forces have the necessary space, not only in relation to cyber-defense of the NCI, but also in terms of cyber-security; intervening not only in the three exceptional cases predicted by law, but also in the constant monitoring of cyberspace. The security and defense of cyberspace come as a direct result of this combined work.

Ultimately, this paper recommends that the Armed Forces, as an interested party in ICN cyber-security, take part in defining the respective security requirements jointly with the CNCS and ANPC.

Keywords: National Critical Infrastructure; Armed Forces; Cyber Defense; Cyber Security; Information Warfare.

Índice

Índice de Figuras

Índice de Tabelas

Lista de Acrónimos

ANPC	Autoridade Nacional de Proteção Civil
CCD	Centro de Ciberdefesa
CE	Comunidade Europeia
CEDN	Conceito Estratégico de Defesa Nacional
CEMGFA	Chefe do Estado Maior General das Forças Armadas
CI	Comunicações e Informação
CIRC	*Computer Incident Response Capability*
CLAFA	Comando da Logística da Força Aérea
CNA	*Computer Network Atack*
CND	*Computer Network Defense*
CNE	*Computer Network Exploitation*
CNCS	Centro Nacional de Cibersegurança
CNPCE	Conselho Nacional de Planeamento Civil de Emergência
DCSI	Direção de Comunicações e Sistemas de Informação
DHS	*Department of Homeland Security*
DIRCSI	Direção de Comunicações e Sistemas de Informação
DIVCSI	Divisão de Comunicações e Sistemas de Informação
EMFA	Estado Maior da Força Aérea
EMGFA	Estado Maior General das Forças Armadas
ENSI	Estratégia Nacional de Segurança da Informação
FFAA	Forças Armadas Portuguesas
GCR	Guerra Centrada em Rede
GI	Guerra de Informação
GNS	Gabinete Nacional de Segurança

IC	Infraestruturas Críticas
ICN	Infraestrutura Crítica Nacional
ICE	Infraestrutura Crítica Europeia
IO	*Information Operations*
LOBOFA	Lei Orgânica de Bases da Organização das FFAA
MDN	Ministério da Defesa Nacional
NATO	*North Atlantic Treaty Organization*
PPIC	Planos de Proteção das Infraestruturas Críticas
RFA	Regulamento da Força Aérea
TIC	Tecnologias da Informação e Comunicação
UE	União Europeia

1 Introdução

Atualmente as sociedades mais desenvolvidas encontram-se tendencialmente estruturadas em redes de sistemas de informação e de comunicações dando origem à criação do ciberespaço. Esta caraterística estrutural de funcionamento das sociedades modernas é fundamental para definir e pensar toda a conjuntura estratégica do século XXI. Entendendo a evolução como um desafio e uma oportunidade, é importante garantir que esta aconteça de forma sustentada e, dentro deste contexto, verifica-se que a forma como os diferentes intervenientes utilizam a informação pode ser simultaneamente geradora de oportunidades mas também de novas ameaças.

O ciberespaço toma assim grande relevância e importância nas implicações na condução da política e da estratégia dos Estados. (CARRIÇO, 2013)

As Tecnologias de Informação e Comunicação (TIC) tornaram-se indispensáveis para a sociedade atual. Neste momento dependemos de toda uma infraestrutura de comunicações e informações para as ações governativas da sociedade, para o sector dos negócios, e até para o exercício dos direitos e liberdades dos cidadãos. Na mesma medida, as nações tornaram-se dependentes das suas infraestruturas de comunicações e informação, e por isso, ataques à sua disponibilidade integridade e confidencialidade podem afetar o próprio funcionamento das nossas sociedades. (KLIMBURG, 2012)

Nos termos da constituição e da lei incumbe às Forças Armadas (FFAA) " desempenhar todas as missões militares necessárias para garantir, a independência nacional e a integridade do Estado" e ainda " cooperar com as forças e serviços de segurança, tendo em vista, o cumprimento conjugado das respetivas missões, no combate a agressões ou ameaças transnacionais". (LOBOFA,2009)

É de especial relevância para a eficácia das ações de defesa do ciberespaço, a existência de uma atuação sinérgica e combinada da sociedade Portuguesa, ação essa, que envolva os órgãos do Ministério da Defesa Nacional (MDN), do Estado-Maior General das Forças Armadas (EMGFA) e dos Ramos, mas também a comunidade (Despacho n.º 13687/2013).

1.1 Generalidades

"A cibercriminalidade é uma ameaça crescente às infraestruturas críticas, em que potenciais agressores (terroristas, criminalidade organizada, Estados ou indivíduos isolados) podem fazer colapsar a estrutura tecnológica da organização social moderna;" (CEDN, 2013)

Pressupondo por isso que o estado deve procurar garantir e aumentar a segurança das infraestruturas críticas nacionais, em colaboração direta com os operadores dessas mesmas infraestruturas.

É também importante definir o conceito de Infraestrutura Crítica Nacional (ICN), assim, e assumindo a definição proveniente do enquadramento legal atual, define-se Infraestrutura Crítica Nacional "a componente, sistema ou parte deste situado em território nacional que é essencial para a manutenção de funções vitais para a sociedade, a saúde, a segurança e o bem-estar económico ou social, e cuja perturbação ou destruição teria um impacto significativo, dada a impossibilidade de continuar a assegurar essas funções" (DL 62/2011)

A Resolução do Conselho de Ministros nº12/2012 atribui ao Gabinete Nacional de Segurança (GNS), no âmbito da quarta medida do plano global estratégico de racionalização e redução de custos com as TIC, a missão de coordenação com todas as entidades relevantes na definição e implementação de uma Estratégia Nacional de Segurança da Informação (ENSI), que compreende a criação, instalação e operacionalização de um Centro Nacional de Cibersegurança (CNCS).

Compete assim ao CNCS exercer os poderes de autoridade nacional competente em matéria de cibersegurança, relativamente ao estado e aos operadores das ICN. Bem como assegurar a articulação e a cooperação entre os vários intervenientes e responsáveis nacionais na área da cibersegurança (DL 69/2014).

O Conceito Estratégico de Defesa Nacional (CEDN) reconhece os desafios de segurança do ciberespaço e recomenda a edificação ao nível das FFAA de uma capacidade de ciberdefesa em concreto com a criação de um Centro de Ciberdefesa (CCD) em simultâneo com a criação de um único serviço coordenador

das comunicações e dos sistemas de informação em articulação com os Ramos (Despacho n.º 13692/2013).

1.2 Motivação

"Uma das maiores ameaças que Portugal terá de enfrentar nos próximos anos será sem dúvida a dos ciberataques em larga escala às ICN." (GNS,2011).

Na sociedade de informação atual o ciberespaço constitui-se como um domínio estruturante, o que obriga aos estados a existência de uma visão estratégica clara, com objetivos realistas e linhas de ação concretas, tendo sempre como objetivo final a salvaguarda dos interesses nacionais e o aumento do potencial estratégico. (CARRIÇO,2013)

Assim, o novo CEDN refere que, dado o atual e novo ambiente de segurança, as recentes questões financeiras bem como as exigências das alianças externas obrigam a uma capacidade de resposta diferente das FFAA bem como à definição de uma estratégia integrada, civil e militar, indispensável para dar resposta às ameaças e riscos atuais. (CEDN,2013)

No que concerne à presença de Portugal na *North Atlantic Treaty Organization* (NATO), esta, dado o crescente aumento de ciberataques às suas infraestruturas de informação e redes, optou por desenvolver um esforço conjunto para dar resposta aos novos desafios à segurança global e à evolução das ameaças, elegendo a ciberdefesa como uma prioridade estratégica para a aliança (CARRIÇO,2013).

Assim, e dado o enquadramento estratégico no domínio da cibercriminalidade, é imposto pelo CEDN a avaliação das vulnerabilidades dos sistemas de informação bem como de todas as infraestruturas e serviços vitais por eles suportados. Nesse sentido, é classificado pelo mesmo documento, prioritário garantir a proteção das infraestruturas de informação críticas, criando para esse efeito um sistema de proteção da infraestrutura de informação nacional, bem como definir uma estratégia nacional de cibersegurança e ainda criar a estrutura responsável pelas questões de cibersegurança (CEDN,2013).

1.3 Âmbito e objetivos

De acordo com o enunciado no atual CEDN, esta dissertação encontra-se integrada na atual linha de pensamento estratégico do Estado Português para a defesa dos interesses nacionais nomeadamente na área de cibersegurança sendo também este um tema relevante na Comunidade Europeia (CE), bem como na Aliança Atlântica na qual o Estado Português se insere. (CEDN,2013)

Este trabalho pretende estudar a forma como se encontra organizada a estrutura de cibersegurança e ciberdefesa das ICN e perceber, cumulativamente, se há espaço para um contributo das FFAA nesta matéria. Pretende-se também com este trabalho fazer um levantamento sobre as capacidades de cibersegurança e ciberdefesa do Estado Português, a nível das ICN, dos organismos públicos e das FFAA e, daí perceber, à luz dos conceitos de Guerra de Informação (GI), se estes sectores da sociedade partilham entre si a missão de defesa cibernética, de forma conjunta e cooperativa. E também, de que forma é feita a tutela e supervisão do cumprimento dos pressupostos nacionais e internacionais no âmbito da cibersegurança das ICN junto dos operadores. Sendo que às FFAA, por força da constituição e da lei, está incumbida a missão de salvaguarda dos interesses nacionais, tentaremos com este trabalho concluir se estas deveriam ou não ter mais relevo nas questões de cibersegurança das ICN.

Para a realização deste trabalho assume-se a seguinte hipótese:

"As Forças Armadas têm espaço para contribuir para a Cibersegurança das Infraestruturas Críticas Nacionais"

Assim sendo, a questão que se coloca e que constitui a linha condutora de toda a dissertação é a seguinte:

"As Forças Armadas têm espaço para contribuir para a Cibersegurança das Infraestruturas Críticas Nacionais?"

1.4 Metodologia

Com a pretensão de atingir os objetivos do presente trabalho é adotada como metodologia o modelo enunciado no manual de investigação em ciências socais de *Raymond Quivy e Luc Van Campenhoudt*. Este projeto de investigação apresenta uma série de fases lógicas de abordagem do problema, recolha de dados, análise dos mesmos, tendo por objetivo uma conclusão que se pretende concreta e fundamentada.

Numa primeira fase, é feito um levantamento dos conceitos doutrinários, enquadrados na área de GI, como *Intelligence,* Guerra Centrada em Rede, Guerra de Quarta Geração, *Information Assurance* e Guerra Cibernética, Ciberataque, Ciberdefesa, Cibersegurança, de forma a contextualizar o panorama atual.

Numa segunda fase, para recolha de dados são utilizados vários processos, como a entrevista a representantes do CNCS, aos responsáveis pela área de ciberdefesa das FFAA entre outras que se entenderem por pertinentes, bem como através da leitura da legislação e documentação nacional e internacional (NATO, UE), diretivas e pareceres de especialistas nacionais na área da proteção de infraestruturas críticas e cibersegurança. Pretende-se nesta fase, através do dados apurados, entender qual o contributo das FFAA nas questões de cibersegurança das ICN e se o mesmo é adequado.

Por fim, na terceira fase, após todos os dados recolhidos e tratados, e com o apoio das conclusões intermédias que foram estabelecidas ao longo da análise dos documentos recolhidos, objetiva-se responder à pergunta de partida deste trabalho “As Forças Armadas têm espaço para contribuir para a cibersegurança das Infraestruturas Críticas Nacionais?”. Sendo que o valor das conclusões deste trabalho será subjacente aos dados recolhidos, seja quanto à fonte ou à validade do conteúdo.

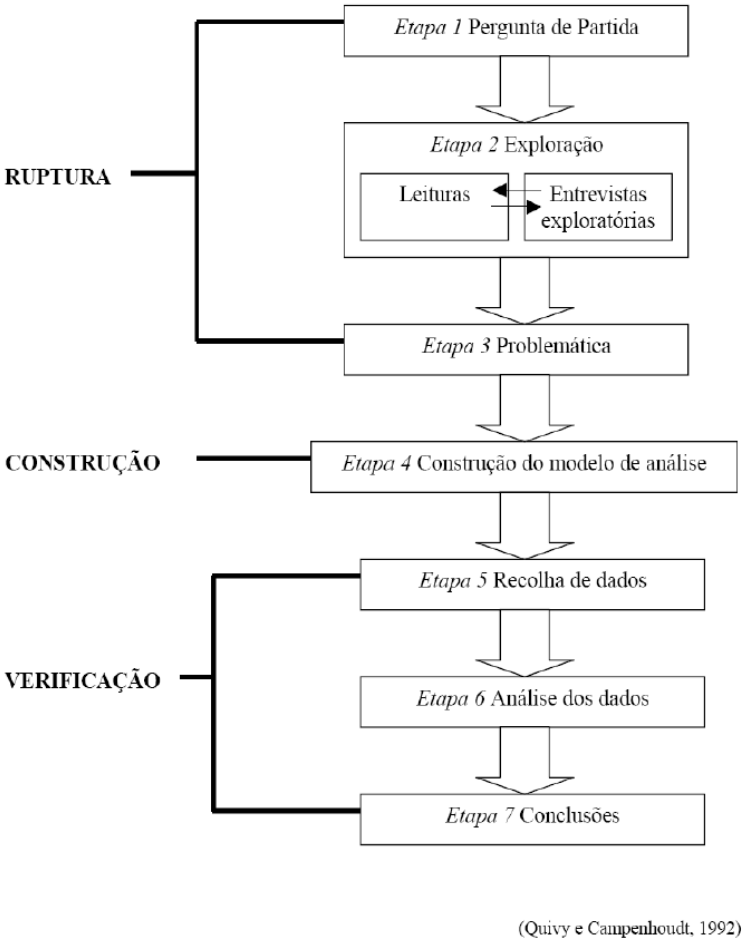

Figura 1 - Modelo de Quivy e Campenhoudt (Quivy e Campenhoudt,1992)

1.5 Modelo de Análise

Partindo da hipótese definida “As Forças Armadas têm espaço para contribuir para a cibersegurança das Infraestruturas Criticas Nacionais" e, com o objetivo de responder à pergunta de partida, “As Forças Armadas têm espaço para contribuir para a cibersegurança das Infraestruturas Criticas Nacionais” é elaborado o presente trabalho que segue como metodologia o método de Quivy e Campenhoudt (Quivy e Campenhoudt, 1992).

A análise consiste na interligação de várias dimensões teóricas com o conhecimento prático retirado das entrevistas realizadas aos peritos nacionais.

De forma a garantir uma resposta cientificamente validade à pergunta de é necessário desenvolver o conceito de ICN, isto é, a sua definição, os tipos de ICN, os seus planos de emergência, legislação aplicável, etc.

Além disso, com o objetivo de estudar as metodologias aplicadas na gestão de risco e proteção das ICN, são analisadas duas metodologias, uma para a gestão de risco, mais generalista - a ISO31000 “Gestão do Risco Princípios e Linhas de Orientação”, e uma outra direcionada para a proteção e gestão de infraestruturas críticas - a RAMCAP. Do estudo destas duas metodologias pretende-se perceber quais os procedimentos e conceitos teóricos previstos pelas mesmas para, posteriormente, verificar se estes são, ou como é que podem ser, aplicados pelos organismos e entidades responsáveis pela ciberdefesa e cibersegurança na proteção das ICN.

Uma vez que a pergunta de partida direciona a investigação para a temática da cibersegurança e, de forma subentendida, para a ciberdefesa, é feita também uma análise aos referidos conceitos. Em termos teóricos, através do estudo e interpretação dos diplomas legais e do ordenamento jurídico nacional, bem como de legislação internacional UE e NATO, e ainda dos regulamentos e normativos internos das FFAA e da Força Aérea. Este levantamento teórico é complementado com os dados retirados da entrevista ao CNCS, e, no caso da ciberdefesa, da informação retirada, entre outras, da entrevista à Direção de Comunicações e Sistemas de Informação (DCSI) do Estado Maior da Força Aérea (EMFA) e ao CCD. O recurso às entrevistas anteriormente referidas torna possível um cruzamento dos fundamentos teóricos com a realidade operacional em Portugal em matéria de cibersegurança e ciberdefesa.

Com o presente estudo pretende-se assim recolher a informação necessária para que, de forma cientificamente sustentada, possa ser respondida a pergunta de partida, bem como estabelecidas algumas conclusões e recomendações no âmbito da cibersegurança e ciberdefesa em Portugal.

1.6 Panorâmica da Dissertação

Esta dissertação encontra-se dividida, fundamentalmente em quatro fases;

- **A 1ª fase**, que serve de introdução ao conteúdo do restante trabalho, evidenciando os seus objetivos, generalidades sobre o tema, a motivação, bem como a metodologia que será utilizada;
- **A 2ª fase**, que corresponde a uma síntese do trabalho já desenvolvido e compilado, onde são apresentados diversos conceitos necessários à compreensão do presente trabalho. São abordados conceitos inseridos na área de GI bem como alguns conceitos importantes para este tema tais como *Information Assurance*, Guerra Centrada em Rede, Guerra Cibernética entre outros;
- A **3ª fase**, tendo por base os conceitos anteriormente recolhidos, analisa a documentação à luz da GI, de forma a produzir informação credível passível de apreciação. A documentação anteriormente referida é proveniente do enquadramento legal do estado Português (Decretos Lei, Despachos, Resoluções de Conselho de Ministros), de legislação e orientações internacionais (UE e NATO) no âmbito da cibersegurança e da proteção das ICN e das orientações internas da Força Aérea e das FFAA em geral no que concerne aos assuntos de ciberdefesa e cibersegurança e, por último, de orientações, recomendações ou propostas provenientes de entidades privadas, grupos de estudo ou universidades. Ao longo deste capítulo são estabelecidas conclusões intermédias que auxiliam a obtenção da conclusão final;
- A **4ª fase**, trata-se de uma síntese de todo o trabalho realizado, que se concretiza na obtenção das conclusões finais. Pretende-se neste capítulo analisar de forma integrada e global da problemática da cibersegurança nas ICN respondendo desta forma à pergunta de partida deste trabalho. Serão também deixadas recomendações para estudos futuros nesta temática.

2 Revisão da Literatura

Este capítulo tem como finalidade dar a conhecer os conceitos e definições necessários para o enquadramento deste trabalho no âmbito da área de GI. Seguidamente é também feito um resumo dos conceitos iniciais mais importantes para a sua compreensão.

2.1 Guerra de Informação

Nos conflitos atuais, a fronteira entre um estado de paz e um estado de guerra, bem como as distinções entre amigo, inimigo ou neutro, são cada vez mais impercetíveis (ALBERTS, 1999).O cenário de conflito alterou-se comparativamente com os conceitos estratégicos e táticos das antigas guerras, em que o inimigo estava perfeitamente definido e identificado, originando, portanto, uma crescente preocupação uma vez que é difícil prever com antecedência o ataque, causa esta que se agrava com o facto de as ferramentas e técnicas necessárias para se fazer GI serem cada vez mais acessíveis e facilmente alcançáveis pelo cidadão normal, criando assim uma possibilidade de guerra assimétrica, fazendo com que a "guerra digital" se torne mais comum que a "guerra física", não sendo necessário que os adversários tenham contato direto com o inimigo, o que altera todo o paradigma da antiga guerra, podendo, atualmente, o ataque ser originário de qualquer sítio do mundo. (ALBERTS, 1999)

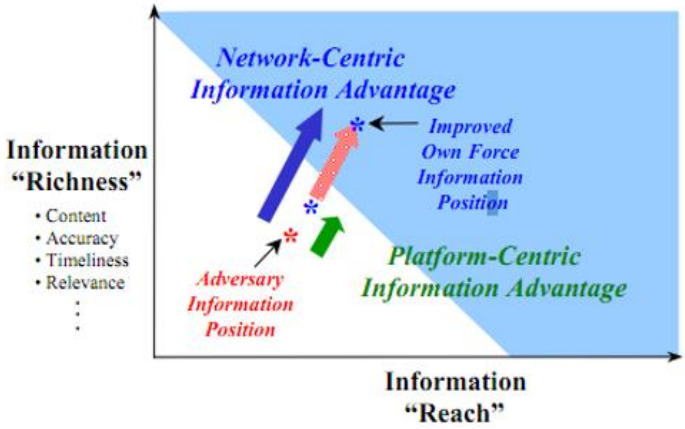

Figura 2 - Nova Perspetiva Sobre a Guerra Centrada em Rede (DOD, 2001)

A GI é atualmente bastante associada à temática do ciberespaço, sendo que nos encontramos numa sociedade caraterizada pela globalização, onde a necessidade de rapidez na transmissão de informação de pessoa para pessoa, em tempo real, origina vários contratempos. “As condições de acesso e de disponibilidade ficam em determinadas circunstâncias prejudicadas pelas necessárias e adequadas medidas de segurança e proteção a implementar.” (DINIS, 2009).

A GI é um conceito resultante da constante evolução do nosso mundo. A forma como cooperamos, competimos e criamos conflitos, muda à medida que as TIC evoluem, pelo que estas mudanças têm então de ser acompanhadas por novas áreas com o intuito de serem melhor interpretadas, sobretudo a nível militar, para que as missões sejam concluídas com a maior eficácia possível (WALTZ, 1998).

.

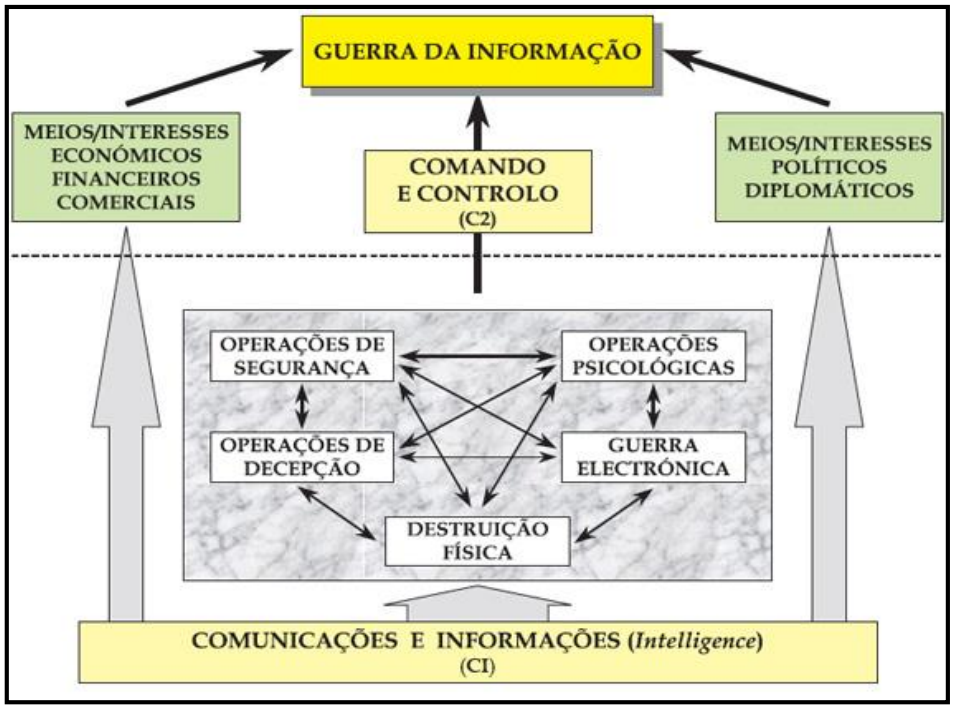

Figura 3 - Elementos GI, (DINIS, 2009)

A GI é “um conjunto de ações com o objetivo de preservar os nossos Sistemas de Informação da exploração, corrupção ou destruição, e ao mesmo tempo explorar, corromper ou destruir os sistemas de informação do adversário ou inimigo”. (FM 100-6,1996). O seu objetivo concretiza-se com o conseguir uma vantagem de informação que permita um domínio rápido sobre o adversário, sendo

que quanto mais depressa esta superioridade for conseguida, maior será a vantagem para o processo de decisão (FM 100-6,1996).

A GI configura-se como “operações de informação conduzidas durante um tempo de crise ou conflito para alcançar ou promover objetivos específicos sobre um adversário específico ou [vários] adversários” (JOINT PUB 1-02, 2001).

Podemos dividir GI em duas áreas distintas, a área ofensiva e a área defensiva. (BATISTA,2003) Assim, tem-se por GI ofensiva a área que trata das ações de intrusão nos chamados sistemas de informação do opositor com o objetivo de provocar a sua degradação ou até mesmo com o objetivo de estes ficarem inoperativos. Sistemas de informação esses que podem ser vitais à ação de comando e controlo de uma organização ou estado, que, sem estes mesmos sistemas, se tornariam alvos fáceis, facilitando as fugas de informação ou provocando danos nos esquipamentos informáticos (BATISTA, 2003).

Por outro lado, da GI defensiva fazem parte todas as ações que têm como objetivo garantir que a informação se encontra segura e que os sistemas de informação se encontram protegidos de eventuais ameaças, sejam estas de índole interna ou externa. (BATISTA, 2003). Relativamente às medidas de proteção da informação, existe uma que se destaca pela sua relevância: a segurança física e eletrónica, que tem como função assegurar que apenas terão acesso à informação, as entidades previamente autorizadas (BATISTA, 2003).

As ações da GI defensiva podem ainda ser agrupadas consoante o seu âmbito, em estratégica, de segurança técnica ou operacional.

A nível estratégico são definidas as políticas de utilização das armas de informação, tais como sistemas de controlo para monitorização de contas de correio eletrónico (BATISTA, 2003).

A segurança operacional está relacionada com tudo o sejam medidas de segurança física, tais como os sistemas de controlo de acessos, que têm como principal objetivo proteger não só *hardware* e *software* como também os utilizadores (BATISTA, 2003).

A segurança técnica pretende apenas não permitir o acesso à informação e aos sistemas de informação por um intruso, tal é conseguido com recurso a *passwords*[1] e *firewall´s*[2] (BATISTA, 2003).

2.2 Information Assurance

São medidas que protegem e defendem as informações e sistemas de informação, assegurando a sua integridade, disponibilidade, veracidade, autenticação e confidencialidade. Inclui a implementação de capacidades de proteção, deteção e reação dos sistemas de informação (JP 3-13, 1998).

"Nunca foi tão verdadeira como hoje a afirmação "saber é poder". Arrisco afirmar que, na atualidade assim como no passado, embora por vezes sem nos darmos consciência disso, o mais importante fator intangível do potencial estratégico de um Estado é precisamente o conhecimento." (SANTOS, 2005).

A informação tem para o decisor diferentes níveis de valor. Esta pode, dependendo do seu valor, mudar decisões, afetar o processo de decisão e talvez mudar o curso de um conflito (HAMILL, 2000).

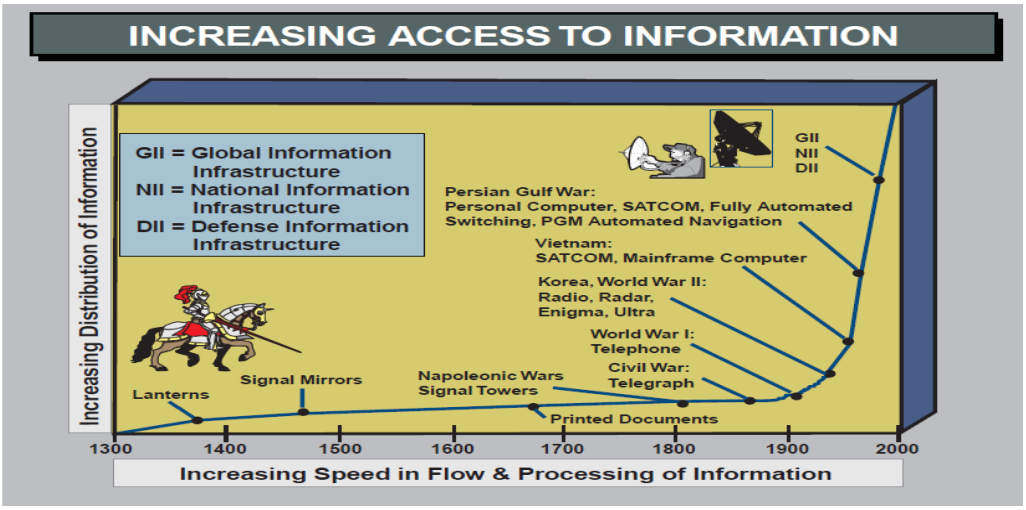

Figura 4 - Nível de Acesso à Informação, (JP 3-13, 1998)

[1] Conjunto de caracteres alfanuméricos que constituem uma "chave" que permite o acesso a um sistema de dados, programas ou sistemas, também conhecido por senha de acesso.

[2] *Software* que permite a passagem seletiva do fluxo de informação entre uma rede interna e a rede pública, assim como a neutralização eventuais tentativas de acesso.

2.3 Superioridade de Informação

O conceito de superioridade de informação materializa-se num estado de desequilíbrio a favor de alguém (vantagem relativa) no domínio da informação, que é atingido pela capacidade de obter a informação correta, para as pessoas certas, na altura certa, negando ao adversário a capacidade de fazer o mesmo (ALBERTS, 2001).

2.4 Guerra Centrada em Rede

"A aplicação de potencial de combate de forças dispersas mas com uma ligação efetiva em rede, para atenuar as condições iniciais de combate, desenvolver elevadas taxas de mudança obtendo o sucesso desejado e bloqueando as estratégias inimigas" (CEBROWSKI, 2005).

O conceito de Guerra Centrada em Rede trata-se de um ajuste ao meio e filosofia militar dos desenvolvimentos tecnológicos e organizacionais, com o objetivo de retirar todo o potencial do funcionamento em rede (RIBEIRO, 2008).

Em termos basilares a Guerra Centrada em Rede assenta em três componentes essenciais: componente organizacional, comportamental e técnica. A sua aplicação origina uma alteração em termos das estruturas, do comportamento e da implementação de novas tecnologias mais avançadas e sofisticadas. Neste sentido, é determinante tanto a existência de superioridade de informação por parte do atacante como uma real partilha da informação entre as várias componentes da força, para que deste modo se ultrapasse a tendência crescente para o aumento da descontinuidade geográfica em termos de espaços de atuação das forças (RIBEIRO,2008).

A Guerra Centrada em Rede combina em si um conjunto de táticas, estratégias, técnicas e procedimentos que têm como objetivo adquirir superioridade num conflito, se esta superioridade não se verificasse significaria que estaríamos no mesmo patamar que o oponente (CEBROWSKI, 2005). Neste sentido, uma força que se encontre ligada em rede parte em considerável vantagem para efetuar as missões, bem como tomar decisões, uma vez que tem mais informação disponível quando comparado com o inimigo. O recurso atual à ligação em rede afeta as três etapas de uma guerra, a estratégica, a operacional e tática (CEBROWSKI, 2005).

A Guerra Centrada em Rede visa aumentar o poder de combate devido à interligação em rede de sensores, decisores e sistemas de armas, por forma a obter uma partilha de consciência, permitindo um aumento da rapidez de comando e controlo e do ritmo das operações, um aumento da letalidade das armas utilizadas contra o adversário, conjugada com um acréscimo da sobrevivência das forças e um elevado grau de sincronização (DoD, 2010).

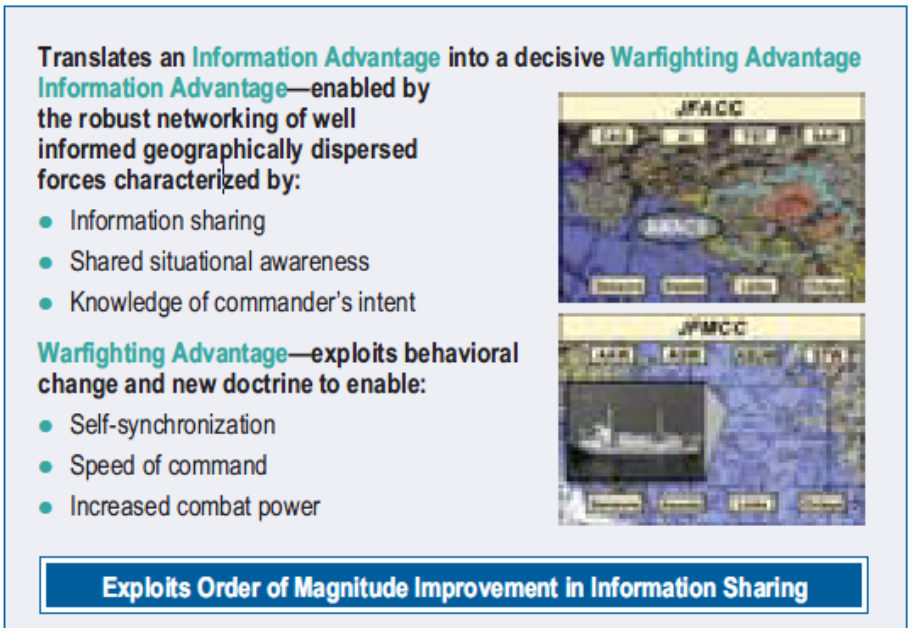

Figura 5 - Vantagens da Guerra Centrada em Rede, (CEBROWSKI, 2005)

2.5 Guerra Cibernética

A guerra cibernética tem vindo a trazer problemas e preocupações com o passar do tempo em relação à segurança de um Estado. As capacidades cibernéticas são, atualmente, um aspeto crítico da guerra moderna e, como tal, têm que ser integradas nas doutrinas militares (COLEMAN 2008).

Tratam-se de "operações militares para corromper ou destruir informações e sistemas de comunicação de modo conhecer o adversário, quem ele é, onde está, e o que é capaz de fazer, significa conhecer toda a informação do inimigo e fazer com que o adversário tenha o mínimo de informação possível." (ARQUILLA, 2000).

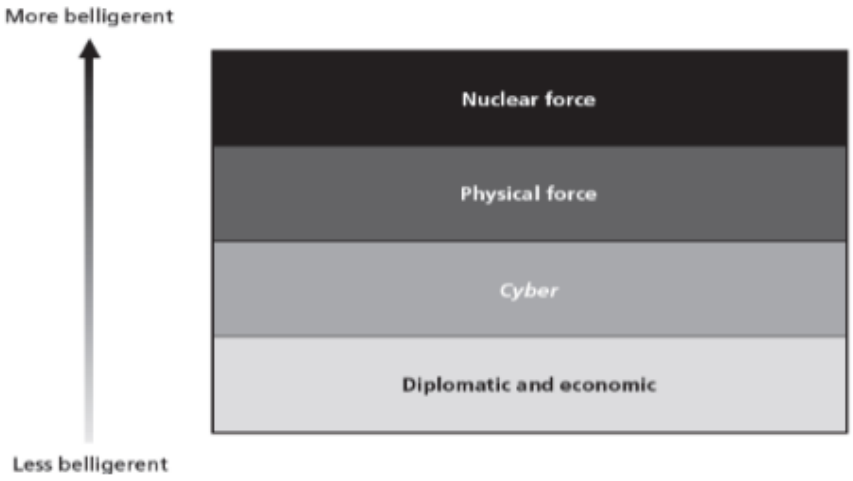

Figura 6 - Nível de Agressividade dos Meios,(LIBICKI, 2009)

Esta guerra cibernética, envolve unidades organizadas segundo um Estado em operações ofensivas e defensivas, usando computadores para atacar outros computadores ou redes através de meios eletrónicos, sendo os *hackers*[3] os principais atores destes ataques (BILLO, 2004). O objetivo final é ganhar vantagem sobre o adversário ao comprometer a sua integridade, confidencialidade e viabilidade do seu dispositivo de computação. Uma prática cada vez mais comum é as unidades individuais executarem ataques contra unidades maiores e mais complexas (BILLO, 2004).

Qualquer indivíduo com acesso ao mundo virtual, pode ter a autoridade, acesso ou habilidade para executar ações de ataque (PARKS;DUGGAN, 2001).

Limites físicos, como distância e espaço, não se aplicam ao mundo cibernético, ou seja, um ataque pode ser feito de outra parte do mundo e ainda assim atingir uma reduzida probabilidade de risco de ineficácia (PARKS;DUGGAN, 2001).

2.6 Sistemas de Informação

Os sistemas de informação definem-se como sendo toda a infraestrutura, organização, indivíduos e componentes que reúnem, processam, armazenam,

[3] Individuo que realiza ataques à segurança dos sistemas informáticos.

transmitem, apresentam, disseminam e operam com informação. Os sistemas de informação também incluem os processos de informação (JP 3.13, 1998).

2.7 Política de Segurança

A política de segurança deve ser elaborada tendo em conta os interesses de um Estado, qual a sua posição e poder perante os outros países, e os seus objetivos devem ser consoante os seus interesses e limitações, por via a conseguir defender com eficácia os seus sistemas e informações (WALTZ, 1998).

Como tal, são apresentados três elementos essenciais para uma segurança eficaz no que toca à GI e, consequentemente, à segurança do ciberespaço (WALTZ, 1998).

- **Interesse Nacional** – Toda a infraestrutura nacional de informação engloba várias organizações, sejam elas militares ou civis, podendo conter alguns elementos privados. É uma infraestrutura que inclui informações e processos passíveis de sofrerem um ataque (WALTZ, 1998).
- **Vulnerabilidades** – As defesas tradicionais, com a evolução, deixam de ser eficazes e já não existe necessidade de um ataque ser efetuado dentro das fronteiras de um país (WALTZ, 1998).
- **Objetivo da Segurança** – Definir níveis para a segurança de informação e classificá-la consoante a sua importância (WALTZ, 1998).

2.8 Estratégia de Segurança

Considera-se a estratégia de segurança nacional como sendo uma arte e uma ciência cuja função é a de conjugar a economia e os aspetos políticos com as FFAA, seja em tempo de paz ou de guerra, de forma a assegurar os objetivos nacionais (WALTZ, 1998). Com a incorporação das FFAA na estratégia de segurança nacional aumentamos a probabilidade de alcançar a vitória e diminuímos o risco de derrota, assegurando assim a eficácia dos objetivos. A estratégia deve ser bem delineada num plano que esteja ao alcance das FFAA e deve obedecer aos seguintes passos: (WALTZ, 1998)

1. Análise situacional das possíveis ameaças às infraestruturas existentes;

2. Criação de objetivos estratégicos, consoante as políticas de segurança nacional, para definir o nível de importância dos sistemas a defender;
3. Criação de planos alternativos caso os principais falhem;
4. As alternativas devem ser medidas em termos de eficácia, custo/benefício e risco;
5. Desenvolvimento de um plano estratégico, consoante os riscos e a sua possibilidade de ocorrência, bem como as consequências;
6. O plano estratégico deve ser adaptado consoante a estrutura das organizações envolvidas, a sua missão e meios;
7. A monitorização é essencial para a implementação do plano, de forma a avaliar o desempenho do mesmo.

Componentes de um plano de estratégia: (WALTZ, 1998)

- Definição das missões militares e não-militares;
- Identificação de todas as políticas de segurança, nacionais ou internacionais em que o país esteja integrado;
- Definição de objetivos a atingir;
- Organizações envolvidas e as suas responsabilidades e papéis;
- Plano de efetividade e desempenho.

Elementos do plano estratégico: (WALTZ, 1998)

- Ameaças e capacidades;
- Estrutura nacional e as vulnerabilidades;
- Capacidades de GI;
- Planos para cada uma das organizações;
- Planos operacionais;
- Plano de estratégia recorrendo às tecnologias;
- Plano de gestão dos riscos.

2.9 Ciberespaço

"Como a utilização do ciberespaço está diretamente relacionada com o meio onde se realizam atividades de guerra de informação, naturalmente que este novo tipo de guerra tem incidência particular no âmbito da segurança e defesa." (DINIS, 2009)

Desde os seus primórdios o Homem foi conquistando áreas de operação, inicialmente estava confinado ao mar e à terra, mais tarde um novo domínio, o espaço aéreo, que no seu início foi mais utilizado pelos militares mas posteriormente, dado a sua importância, a sua utilização alastrou-se para a área comercial. O quarto domínio chegou com a introdução do "espaço" e desta forma, como último domínio, o ciberespaço. (KUEHL, 2009)

O ciberespaço pode ser caracterizado por um conjunto de computadores individuais que estão ligados em rede com o mundo, é também um domínio, com a ligeira diferença de ser construído artificialmente pelo homem, com recurso a material que provém da natureza. (LIBICKI, 2009)

"*Cyberspace is a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers*".(JP 2-0, 2007)

"*Cyberspace is a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange and exploit information via interdependent and interconnected networks using information-communications technologies (ICT) based systems and their associated infrastructures*". (KUEHL, 2009)

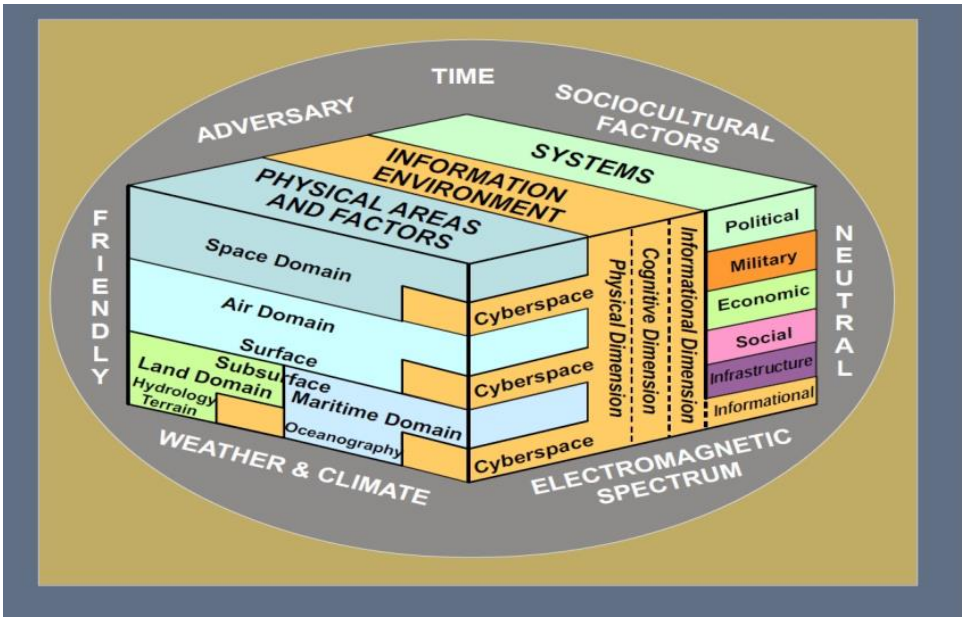

Figura 7 - Envolventes do Ciberespaço, (JP2-03-24, 2009)

2.10 Ciberdefesa

Em termos simplistas, ciberdefesa, está relacionada com a segurança do ciberespaço de um determinado país, não só na componente militar mas também com todas as agências diretamente envolvidas na segurança de um país, sendo composta pelos sistemas e atividades que fornecem a segurança de informação e a segurança física para a infraestrutura digital dentro da área nacional de segurança (HAYES,2011).

Entende-se ciberdefesa como sendo a capacidade de uma nação empregar recursos materiais e humanos ou levar a cabo ações militares com o intuito de proteger os Sistemas de Informação e as infraestruturas críticas contra potenciais inimigos. (COLEMAN, 2008) A ciberdefesa engloba todos os sistemas, programas e tecnologias implicadas na deteção, rastreio e interceção de ataques destrutivos contra as infraestruturas de informação. Engloba ainda todos os procedimentos e métodos necessários para minimizar os efeitos de um eventual ciberataque. (COLEMAN, 2008)

2.11 Cibersegurança

É entendida por cibersegurança toda a área nacional que envolve as tecnologias de informação, em particular os sistemas e tecnologias de informação

civis. Engloba por isso todos os sistemas e atividades que fornecem a segurança de informação e a segurança física para a infraestrutura nacional do ciberespaço (HAYES, 2011).

As ameaças à cibersegurança são denominadas, ciberameaças, isto é, potenciais violações das propriedades de segurança, podendo estas ser de índole acidental ou intencional, sendo as primeiras, tal como o próprio nome indica, desprovidas de qualquer intenção e normalmente caracterizadas por uma falha do *software* ou sistema. Ou, por outro lado, as de índole intencional, consistem na análise da rede através de sistemas de monitorização e podem ainda evoluir para um ciberataque. (ITU, 2012)

Podemos ainda caracterizar as ameaças, segundo o mesmo autor, tendo em conta se estas são ativas ou passivas, sendo que as ativas caracterizam-se por uma tentativa de modificação do estado de normal funcionamento do sistema, como por exemplo, a destruição do equipamento. Já no caso das ameaças passivas estas têm como objetivo retirar informação do sistema sem provocar nenhuma alteração no seu normal funcionamento. Sempre que as ameaças têm sucesso passam a ser classificadas como ataque. (ITU, 2012).

2.12 Guerra da Quarta Geração

O modo como os conflitos armados se desenvolvem atualmente resulta de uma adaptação e evolução de muitos séculos. Após a extinção do Império Romano a guerra tem vindo a ser separada em quatro gerações, sendo que todas as gerações derivam da geração anterior e o fator que está na origem de tal evolução é o constante desenvolvimento e crescimento da tecnologia, de fatores económicos, políticos e sociais (LIND, 2004).

Para que se possa explicar a essência e os conceitos associados à Guerra de Quarta Geração é necessário abordar primeiro as gerações que a precederam.

Na primeira geração de guerra moderna a lógica do campo de batalha era muito simples, entrar em confronto direto com o inimigo e tentar aniquilá-lo (LIND, 2004). O principal e único objetivo nas guerras de primeira geração era o de manter a ordem e a disciplina no campo de batalha. A maioria das características que distinguia os militares dos civis vêm da primeira geração, os uniformes, as continência e os postos, foram impostos com a intenção de reforçar uma forte

cultura militar de ordem. Com o evoluir dos tempos, com o aumento do número de combatentes e consequentemente com a existência de exércitos maiores, toda esta ordem no campo de batalha até então possível começou a não dar resultado (LIND, 2004).

Com o objetivo de resolução do problema anterior, relacionado com a desordem no teatro de operações, surge a guerra de segunda geração desenvolvida essencialmente pelos Franceses durante e após a Primeira Grande Guerra Mundial. Nesta segunda geração o que se pretendia era dividir as forças em grupos mais pequenos com o objetivo de, com recurso à tecnologia existente, atuarem separadamente mantendo a ordem militar no campo de batalha (LIND, 2004).

Desenvolvida em grande maioria pelo exército Alemão surge a guerra de terceira geração, com grande aplicação durante a Segunda Guerra Mundial. Esta guerra de terceira geração não é baseada em poder de fogo mas sim em velocidade, efeito surpresa e perturbação mental e física (LIND, 2004).

"(…) *Fourth Generation marks the most radical change since the Peace of Westphalia*." (LIND 2004).

A guerra de quarta geração tem como suas características essenciais, a descentralização e a iniciativa. A sociedade civil, politica e militar são agora parte integrante do conflito armado, o que não acontecia nas gerações anteriores (LIND, 2004). A guerra de quarta geração, tal como as suas antecessoras, foi marcada pelas novas tecnologias e ideias (LIND,2004). Estas novas tecnologias de comunicação e transportes vieram permitir uma maior troca de informação num menor espaço de tempo, situação característica da era da globalização. Como consequência da era da globalização e dos meios de comunicação social, ações de manipulação bem como as manobras psicológicas que têm como objetivo influenciar a opinião mundial, tornam-se mais facilitadas. (KHAN, 2010)

Khan no seu *"A Response to Fourth Generation Warfare"* disse *"The wars of decolonization, Chinese Civil War, the Vietnam War, the Afghanistan War, the two Intifadas and the current wars in Iraq and Afghanistan all saw the victory of the insurgents. Clearly, irregular warfare is the wave of the future."* (KHAN, 2010).

O JP 3-24 define insurreição como o uso organizado de subversão e violência por parte de um grupo ou movimento que procura derrubar ou mudar à força a autoridade de um governo (JP 3-24, 2009). Até ao século vinte a insurreição era facilmente vencida, mas com o constante crescimento e evolução dos

movimentos políticos, comunicação social e armas eficazes e economicamente mais acessíveis, os insurgentes ficaram capazes de conseguir derrotar qualquer superpotência (KHAN, 2010).

"(…) *insurgency is the wave of the future, able to match and defeat even superpowers*." (KHAN, 2010).

3 Infraestruturas Críticas Nacionais (ICN)

Sendo este trabalho fundamentalmente sobre a ciberdefesa das ICN é conveniente, antes de ser feita a análise do problema, perceber o que se entende por ICN, assim o presente capítulo tem por finalidade esse mesmo objetivo.

Uma definição possível para Infraestrutura Crítica (IC) é a que refere que, se trata dos serviços básicos e das instalações necessárias para o funcionamento da sociedade ou comunidade, identificando como exemplo, os transportes e comunicações, sistemas de abastecimento de água e energia e organismos públicos tais como hospitais, prisões e escolas. (MOTEFF; PARFOMAK, 2004)

Existe contudo uma definição mais completa, na medida em que também se refere ao eventual impacto de uma destruição ou perturbação de uma IC, sendo essa a definição que consta no ordenamento jurídico Português. Segundo o Decreto lei 62/2011 de 9 de Maio entende-se por ICN "a componente, sistema ou parte deste situado em território nacional que é essencial para a manutenção de funções vitais para a sociedade, a saúde, a segurança e o bem-estar económico ou social, e cuja perturbação ou destruição teria um impacto significativo, dada a impossibilidade de continuar a assegurar essas funções".

A Comissão das Comunidades Europeias, em 2004, num comunicado intitulado "Proteção das Infraestruturas Críticas no âmbito da luta contra o terrorismo" define que "as infraestruturas críticas são as instalações físicas e de tecnologia de informação, redes, serviços e bens, os quais, se forem interrompidos ou destruídos, provocarão um sério impacto na saúde, na proteção, na segurança ou no bem-estar económico dos cidadãos ou ainda no funcionamento efetivo dos governos nos Estados-Membros." (Comunicação das Comunidades Europeias, 2004).

O referido comunicado acrescenta ainda que, para além das infraestruturas propriamente ditas existem ainda cadeias ou redes de abastecimento que são vitais para a circulação do produto ou da prestação de um serviço, dando como exemplo o abastecimento alimentar ou de água nas áreas urbanas (Comunicação das Comunidades Europeias, 2004).

Para além da definição de ICN é ainda importante referir que, segundo dados da Proteção Civil constantes no seu sítio *online* (Autoridade Nacional de Proteção Civil, 2012) o número de ICN tem vindo a aumentar de forma exponencial e que, para além desse fato estas desempenham funções fundamentais para a economia e segurança dos países, logo a sua inoperacionalidade, se ocorrer de forma prolongada, causará elevados prejuízos.

Adianta ainda a referida entidade que, a proteção das ICN em Portugal teve início em 2004, em simultâneo com as primeiras iniciativas da União Europeia (UE) para a construção de uma estratégia e de um plano de ação para a proteção e aumento da resiliência das Infraestruturas Críticas Europeias (ICE). Numa primeira fase foi criado um grupo de trabalho coordenado pelo então Conselho Nacional de Planeamento Civil de Emergência (CNPCE) cujas atribuições passaram agora para a Autoridade Nacional de Proteção Civil (ANPC), sendo o trabalho dividido em três fases, a primeira passava pela identificação e classificação das ICN, nesta fase as ICN foram classificadas de acordo com critérios que traduzem a sua importância relativa para o país e catalogadas numa base de dados georreferenciada, sendo nesta fase classificadas como ICN cerca de 290 infraestruturas das quais, aproximadamente metade ligadas aos sectores da energia e transportes. Posteriormente, numa segunda fase, foi feita a análise e avaliação do risco associado à disfunção de cada IC bem como o estudo e difusão das medidas para reforço da sua proteção, sendo esta uma etapa central da proteção das ICN, uma vez que, é nesta fase que são apuradas as vulnerabilidades face às ameaças. Por último, a terceira fase, consiste na implementação de medidas de monitorização do risco. (Autoridade Nacional de Proteção Civil, 2012)

Atualmente, a Comissão Europeia incentiva os seus estados membros a desenvolverem programas nacionais para proteção das ICN e a requisitarem apoio para a sua elaboração sempre que entenderem por necessário. Quando se trata da proteção de ICN se a metodologia e os planos de proteção forem análogos entre os estados-membros permite que todos intervenientes a nível europeu beneficiem de não estarem sujeitos a enquadramentos diferentes o que permite, por exemplo, a redução de custos. Os referidos programas têm que necessariamente abordar, no mínimo, as seguintes questões:

- Identificação e designação pelo estado-membro das ICN de acordo com critérios nacionais predefinidos;

- Estabelecimento de um diálogo com os proprietários/operadores IC;
- Identificação de interdependências geográficas e sectoriais;
- Elaboração de planos de emergência ligados às infraestruturas críticas nacionais, quando considerado relevante.

Sendo que este trabalho tem como foco as ICN é conveniente perceber quais os critérios que levam a que uma IC seja assim considerada. Assim, segundo a doutrina em uso na Comunidade Europeia, existem três fatores que permitem identificar potenciais IC, sendo eles: (Comunicação das Comunidades Europeias, 2006)

- **O alcance ou extensão** – a destruição ou perturbação de um elemento de uma dada infraestrutura é avaliada em função da extensão da área geográfica que pode ser afetada pela sua perda ou indisponibilidade – internacional, nacional, provincial/territorial ou local;
- **A Magnitude ou gravidade** – consequências da perturbação ou destruição de uma dada infraestrutura. É conveniente também salientar que existem critérios que apoiam a avaliação da magnitude potencial:
    - O impacto na população (número de pessoas afetadas, perda de vidas, doença, prejuízos graves, evacuação);
    - Os efeitos na economia (efeitos no PIB, importância das perdas económicas e/ou degradação de produtos ou serviços);
    - A incidência ambiental (impacto no público e em áreas vizinhas);
    - A interdependência (em relação a outros elementos de infraestrutura crítica);
    - Efeitos políticos (confiança na capacidade do governo);
    - Efeitos psicológicos, que podem agravar acontecimentos que, em si mesmo, seriam de menor importância;
    - Efeitos na saúde pública.
- **Efeitos no tempo** – este critério permite verificar até que ponto a perda de um elemento perpétua no tempo.

3.1 Planos de Emergência

Como parte integrante dos Planos de Proteção das Infraestruturas Críticas (PPIC) surgem como elemento fundamental, os planos de emergência. Estes têm

como objetivo minimizar os eventuais efeitos da perturbação ou destruição de uma IC. Com o desenvolvimento dos planos de emergência pretende-se a criação de uma abordagem que, numa situação de emergência, envolva de forma coordenada e cooperante a participação dos proprietários/operadores das IC, das autoridades nacionais e ainda o intercâmbio de informações entre países vizinhos.

Assim, segundo o Decreto-lei 62 de 9 de Maio, a identificação de potenciais ICN é permanente e é conduzida pelo CNPCE, atual ANPC. Cada ICN dispõe de um plano de segurança da responsabilidade do seu operador que é revisto anualmente, o referido programa identifica os elementos da ICN bem como as soluções de segurança a executar, incluindo (DL 62/2011);

- A identificação dos elementos importantes;
- Uma análise de risco baseada em cenários de ameaça grave, na vulnerabilidade de cada elemento e nos impactos potenciais;
- A identificação, seleção e priorização de contramedidas e procedimentos de segurança permanentes;
- A identificação, seleção e priorização de contramedidas e procedimentos de segurança progressivos a ativar consoante o grau de ameaça aplicável à IC ou o estado de segurança decretado.

As contramedidas e procedimentos de segurança permanentes incluem (DL 62/2011);

- A instalação de meios de deteção, controlo do acesso, proteção e prevenção;
- Procedimentos de alerta e gestão de crises;
- Medidas de controlo e verificação;
- Comunicação, sensibilização e formação;
- A segurança dos sistemas de informação;
- Medidas de minimização dos danos e impactos e de reposição da normalidade.

3.2 Tipos de Infraestruturas Críticas

Segundo dados da proteção civil e da comunidade europeia as infraestruturas críticas estão distribuídas pelas seguintes áreas e sectores (Comunicação da Comissão ao Conselho e ao Parlamento Europeu, 2004);

- **Sector da energia** – sendo exemplo, infraestruturas e instalações de produção e de transporte de eletricidade; infraestruturas de produção, refinação, tratamento, armazenagem e transporte de petróleo por oleodutos; infraestruturas de produção, refinação, tratamento, armazenagem e transporte de gás por gasodutos e terminais para gás natural em estado líquido (GNL).
- **Sector dos transportes** – sendo exemplo, transportes rodoviários, marítimos e aéreos, transportes por vias navegáveis interiores;
- **Tecnologia da informação e comunicação -** sendo exemplo, as telecomunicações, os sistemas de radiodifusão, programas e equipamentos informáticos e redes, incluindo a Internet;
- **Finanças** – sendo exemplo, atividades bancárias, valores mobiliários e investimento;
- **Saúde** – sendo exemplo, hospitais, centros de assistência médica e bancos de sangue, laboratórios e empresas farmacêuticas, serviços de busca e de primeiros socorros, serviços de urgência;
- **Alimentação** – sendo exemplo, segurança alimentar, meios de produção, distribuição por grosso e indústria alimentar;
- **Água** – sendo exemplo, barragens, armazenamento, tratamento e redes;
- **Produção, armazenamento e transporte de mercadorias perigosas** – sendo exemplo, materiais químicos, biológicos, radiológicos e nucleares;
- **Administração** – sendo exemplo, serviços de base, instalações, redes de informação, bens, sítios e monumentos de importância nacional.

Tal como evidenciado ao longo do presente capítulo, as ICN representam especial importância para o Estado Português, e materializam-se em variados sectores, dada a sua criticidade constituem-se como um alvo de interesse também

no domínio ciber, assim é justificada a existência de entidades dedicadas à segurança e defesa também no domínio ciber.

4 Ciberdefesa

Para uma abordagem correta ao conceito de ciberdefesa, em primeiro lugar é analisada a morfologia da própria palavra, o prefixo *"ciber",* tem origem Grega e significa "controlo" (RFA 390-6,2011). Nos anos 40 o físico *Norbert Wiener* atribuiu ao termo "cibernética" o significado de ciência do controlo e da comunicação entre os seres vivos e as máquinas (RFA 390-6,2011), sendo a partir dessa altura o prefixo *"ciber"* associado aos vários temas relacionados com o domínio da computação e das "máquinas inteligentes". (RFA390-6,2011)

A *NATO Consultation, Command and Control Agency* (NC3A) entende que ciberdefesa se pode definir como "a aplicação de medidas de segurança para a proteção e resposta a ciberataques lançados contra as infraestruturas de Tecnologias de Informação e Comunicações (TIC), requerendo uma capacidade de preparação, prevenção, deteção, resposta, recuperação e extração de lições aprendidas a partir dos ataques que podem afetar a confidencialidade, integridade e disponibilidade da informação, assim como os recursos e serviços dos sistemas de TIC que a processam". (CARRIÇO,2013).

Segundo o documento que uniformiza a Política de Ciberdefesa da Força Aérea, ciberdefesa é definida como a aplicação de medidas de segurança destinadas a proteger os componentes de uma infraestrutura de um Sistema de Informação e Comunicação (SIC) e a informação por este processada contra um ciberataque." (RFA 390-6, 2011).

Na opinião do Engenheiro Lino Santos do CNCS "cibersegurança é o conjunto de capacidades, nos vários domínios de atuação, com vista a melhorar a insegurança das redes, o que inclui as medidas de proteção simples, inclui o ramo civil e militar, inclui a prossecução criminal no âmbito do cibercrime e inclui a defesa mas não em forma subsidiária" (SANTOS, 2014).

Uma análise aos dois conceitos permite estabelecer que: (HAYES, 2011)

- A ciberdefesa depende apenas em parte do setor civil (cibersegurança);
- A cibersegurança necessita de pesquisa e capacidades da ciberdefesa;

- As ameaças e ataques internacionais poderão necessitar da intervenção de ambos;
- As ferramentas de proteção da informação são semelhantes;
- O treino e exercício são iguais para os dois;
- Os especialistas de uma área podem cooperar com a outra.

Sendo tal relação demonstrada, graficamente, na figura seguinte;

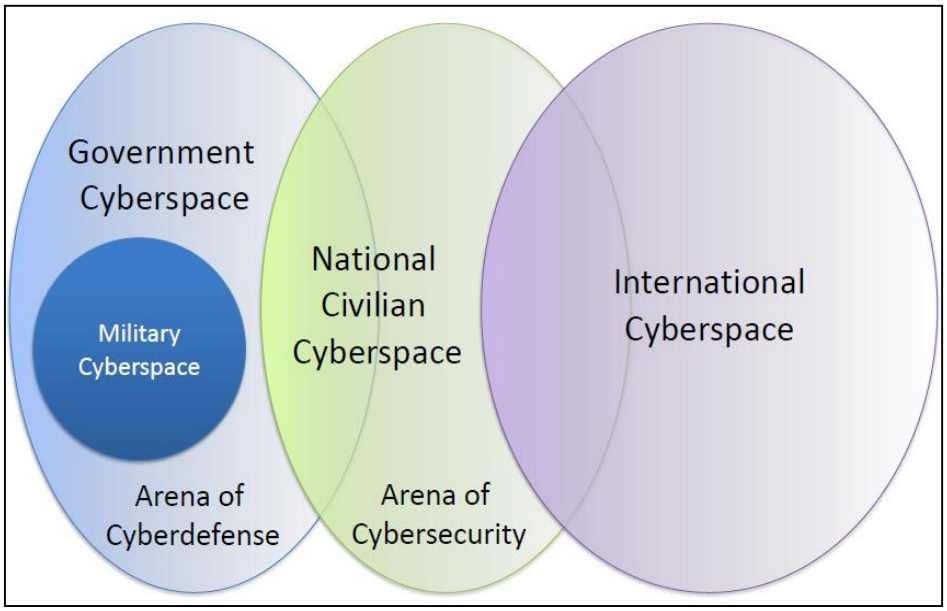

Figura 8 - Ciberdefesa Versus Cibersegurança, (HAYES, 2011)

Considerando a estreita relação verificada entre a segurança e a defesa nacional também no domínio ciber, a cibersegurança e a ciberdefesa, revelam-se indissociáveis (CARRIÇO, 2013). Assim não se conseguirá garantir uma capacidade de cibersegurança sem o levantamento de uma capacidade de ciberdefesa (CARRIÇO,2013).

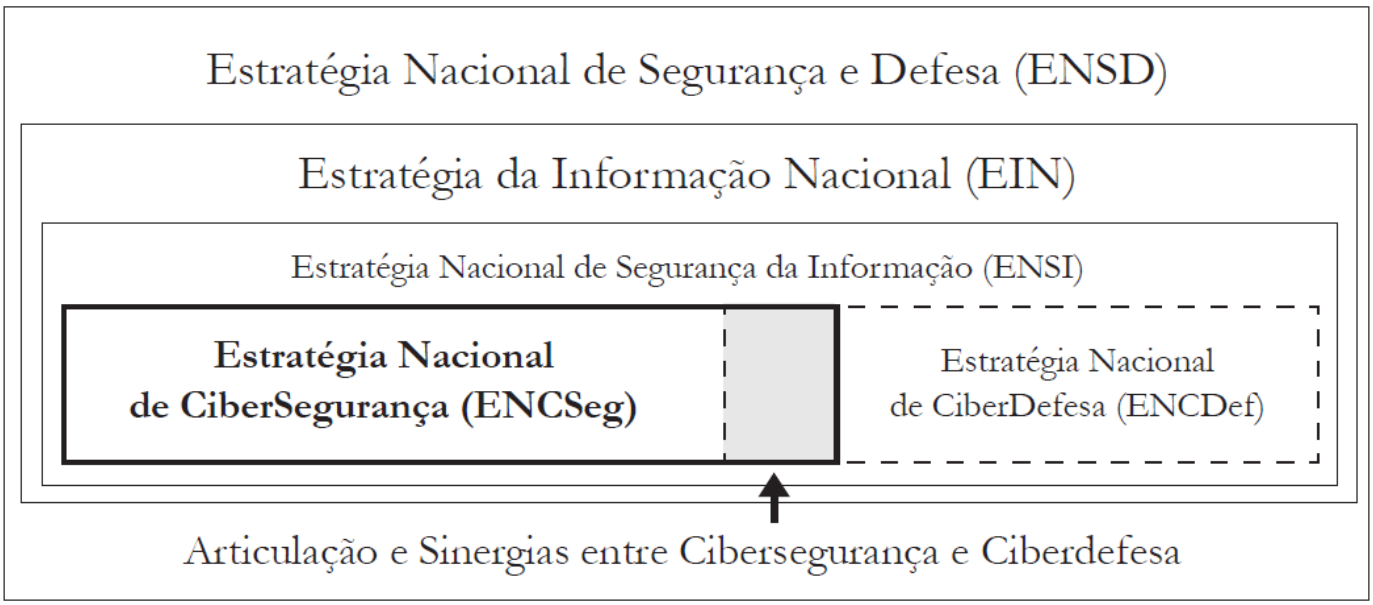

Figura 9 - Enquadramento da Estratégia Nacional de Cibersegurança (CARRIÇO,2013).

Como apresentado na figura 9, a estratégia nacional de cibersegurança, para além dos processos de segurança da informação no ciberespaço deverá ainda, de forma sinérgica e articulada, apoiar o levantamento dos mecanismos de ciberdefesa necessários mobilizar de forma a garantir a própria cibersegurança do estado. (CARRIÇO,2013).

4.1 Domínios de Atuação

Para o combate aos ciberataques podem ser considerados três domínios de atuação, sendo que se entende por domínio de atuação "o conjunto dos meios técnicos e humanos (atores), bem como do enquadramento legal, envolvidos na prossecução de um conjunto de objetivos, os quais são em parte determinados por uma perspetiva relativamente ao fenómeno da ciberconflitualidade". Os respetivos domínios são, o domínio da proteção simples, da prossecução criminal e da defesa do Estado ("Proteção do Ciberespaço: Visão Analítica",2012).

Tabela 1 - Domínios de atuação na proteção do ciberespaço (Proteção do Ciberespaço: Visão Analítica, 2012)

	Protecção Simples	Prossecução criminal	Defesa do Estado
Caracterização	Os ciberataques são vistos como ameaças à disponibilidade, integridade e confidencialidade da informação e de outros activos.	Os ciberataques são vistos como actos criminalmente relevantes.	Os ciberataques são vistos como um acto de Guerra, pondo em risco a existência do Estado.
Objectivos	Proteger potenciais alvos contra ciberataques.	Prevenir crimes e identificar e condenar os responsáveis.	Eliminar uma ameaça que coloque em causa a Soberania Nacional ou ganhar uma vantagem competitiva sobre outro Estado.
Aspectos legais e constitucionais	Salvaguarda dos direitos individuais e da privacidade dos cidadãos.	Actuação dentro do quadro da legislação aplicável e segundo as regras do sistema judicial.	Actuação sujeita à Constituição da Republica, Lei do Estado de Sítio e do Estado de Guerra, bem como ao Direito Internacional dos Conflitos Armados e dos Direitos Humanos.
Actores	Técnicos de sistemas e de redes, Indústria TIC, autoridades reguladoras sectoriais, CSIRT, utilizadores TIC.	Órgãos de polícia criminal, Ministério Público e Magistrados Judiciais.	Forças Armadas e Serviços de Informações.

Tal como é evidenciado pela tabela 1, a cada domínio de atuação está associada uma perspetiva do ciberataque e consequentemente diferentes objetivos, aos quais correspondem determinados atores envolvidos, bem como os meios e enquadramento jurídico aplicável (Proteção do Ciberespaço: Visão Analítica, 2012).

4.1.1 Proteção Simples

A proteção simples "engloba os meios técnicos, processuais e humanos que realizam diariamente as componentes preventiva, reativa e de gestão da qualidade da segurança", tem o objetivo de proteger as organizações e os indivíduos e é

realizada, em primeiro lugar, pelas próprias infraestruturas, bem como pelos fabricantes de *hardware* e *software*, os técnicos que administram os sistemas de rede, os CSIRT – C*omputer Security Incident Response Team,* mas também pelo Estado, através das suas forças e serviços de segurança e autoridades reguladoras (Proteção do Ciberespaço: visão Analítica, 2012).

No domínio da proteção simples, um ciberataque "é entendido como uma sequência de ações destinadas a produzir um resultado não autorizado ou uma perturbação indesejada na confidencialidade, na integridade ou na disponibilidade de um serviço ou produto", sendo por isso a necessidade de proteção do ciberespaço relacionada com a racional de mercado e de continuidade da prestação de um dado serviço (Proteção do Ciberespaço: visão Analítica, 2012).

Neste domínio existem ainda algumas considerações a ter em conta (Proteção do Ciberespaço: visão Analítica, 2012);

- A indústria das TIC, se por um lado é responsável pelas vulnerabilidades existentes nos seus produtos, por outro é quem fornece juntamente com a investigação as soluções de segurança;
- Existe a necessidade de investimento público e privado, não só em tecnologia, mas também em pessoas capazes de executar a monitorização, deteção, reação e gestão da segurança;
- As IC não são obrigadas a acatarem as normas existentes na área da cibersegurança, logo a sua adoção está dependente da visão das mesmas relativamente ao grau de ameaça e da análise custo-benefício.

Para além das medidas de proteção de perímetro normalmente associadas à cibersegurança existem ainda as CERT – *Computer Emergency Response Team* – cujas funções são o alerta e resposta a incidentes de segurança informática, sendo que estas equipas, dado o carácter transnacional que é característico dos incidentes informáticos, trabalham num sistema de cooperação nacional e internacional exigindo às vezes a participação de várias entidades e a existência de uma rede de contactos (Proteção do Ciberespaço: Visão Analítica, 2012).

4.1.2 Prossecução Criminal

Já no domínio da prossecução criminal, entendem-se os ciberataques como sendo “atos criminalmente relevantes, passíveis de sancionamento dentro do edifício jurídico do respetivo país.” (Proteção do Ciberespaço: Visão Analítica, 2012) Sendo objetivo principal do sistema judicial Português a dissuasão da prática criminal com recurso à prevenção geral, isto é, pelo “exemplo” dado pela retribuição social através da sanção penal e, posteriormente, caso o ilícito o justifique, através da prevenção especial, isto é, da condenação concreta do autor do crime. Uma vez que uma grande percentagem dos ciberataques configuram prática criminal, segundo a legislação nacional e internacional, é importante identificar e julgar os infratores e, verificada a importância da proteção das ICN, a nova lei da ciberdefesa prevê inclusivamente um agravamento substancial das medidas de coação a quem realizar ataques contra as mesmas. (Proteção do Ciberespaço: Visão Analítica, 2012)

É ainda importante referir que, por lei, em Portugal a prevenção e investigação dos cibercrimes esta atribuída à Polícia Judiciária. (DL 49/2008)

4.1.3 Domínio da Defesa do Estado

No domínio da Defesa do Estado, ciberataque é definido como “ato de guerra, pelo que a resposta se centra na ação militar, com todos os recursos disponíveis, apenas sujeita na ação, no plano nacional, à Constituição da República, à Lei do Estado de Sítio e do Estado de Guerra e, no plano internacional, ao Direito Internacional dos Conflitos Armados e ao Direito Internacional dos Direitos Humanos.” (Proteção do Ciberespaço: Visão Analítica, 2012)

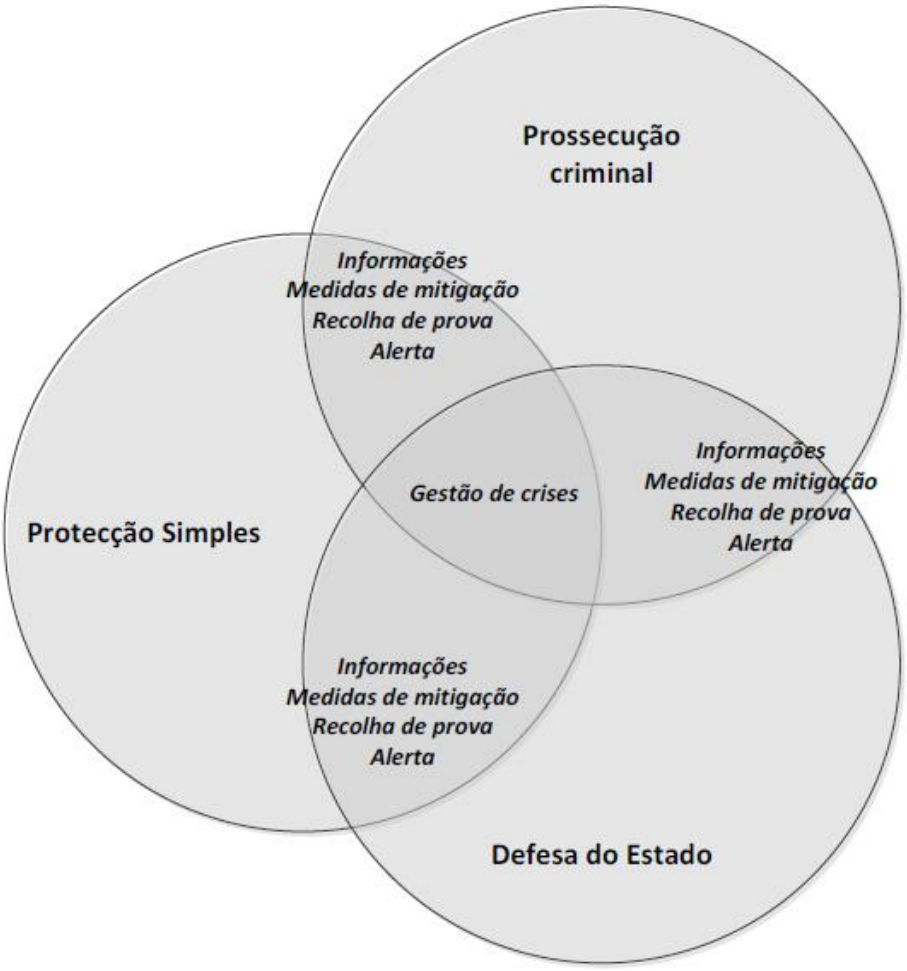

Figura 10 - Domínios de Atuação na Proteção do Ciberespaço, (Proteção do Ciberespaço: Visão Analítica,2012)

4.2 A Ciberdefesa na Força Aérea

A política de ciberdefesa da Força Aérea encontra-se vertida no RFA 360-6, regulamento esse cuja finalidade é "estabelecer a política de ciberdefesa na Força Aérea, potenciando a capacidade de proteger os seus SIC e a informação neles armazenada, processada ou transmitida, com importância crítica para o desempenho da missão, contra um ciberataque." (RFA 390-6, 2011). Sendo o seu conteúdo totalmente aplicado aos sistemas de comunicação e informação da Força Aérea e à informação neles contida. (RFA 390-6, 2011).

Este regulamento avança ainda que só será possível alcançar os objetivos de ciberdefesa se existirem princípios doutrinários, procedimentos de operação e

normas devidamente instituídas e treinadas, que permitam uma resposta célere, eficiente e eficaz contra eventuais incidentes de segurança informática (RFA 390-6, 2011). Sendo esta eficiência e eficácia resultado de um elevado conhecimento técnico, e da existência de coordenação e comunicação entre os indivíduos envolvidos. (RFA 390-6, 2011).

Segundo a política de ciberdefesa da Força Aérea são cinco as bases da Ciberdefesa;

1. **“Política de Segurança, Diretivas e Documentação de Segurança”.** Isto é, o “conjunto de princípios orientadores de aplicação da estratégia de segurança definida e que deve focar-se no pessoal, na tecnologia e na informação.” Sendo que a sua implementação requer o envolvimento de diversas entidades no seu planeamento e execução, que incluem a formação, o treino, análise das lições aprendidas, a condução de exercícios, a gestão de recursos necessários, a definição dos instrumentos legais de atuação e dos protocolos de cooperação adequados. (RFA 390-6, 2011). A política de ciberdefesa da Força Aérea está estruturada em três níveis, o de Estado- Maior, o de operação e o de apoio; (RFA 390-6,2011)
    1.1. **EMFA/DIVCSI** – é competência desta Divisão elaborar a referida política de ciberdefesa e, posteriormente, mantê-la atualizada relativamente a novas ameaças e à evolução dos procedimentos e tecnologias. Esta divisão integra ainda a Comissão Coordenadora da Capacidade de Resposta a Incidentes de Segurança Informática (CC-CRISI), com o papel Coordenador dos Grupos de Reação a Incidentes de Segurança Informática (GRISI) seja na Força Aérea, quando o incidente afetar apenas os seus sistemas internos, quer no exterior em sistemas conjuntos. Mantém ainda atualizado um registo de ocorrência dos incidentes e das suas características.
    1.2. **CLAFA/DCSI** – é competência desta direção implementar os procedimentos promulgando as publicações necessárias para adequar as soluções tecnológicas às ameaças. São os recursos humanos desta direção que constituem os GRISI.
    1.3. **Centro de Informática das Unidades** – é competência destas entidades, em coordenação com os Oficiais de Segurança Local dos Sistemas de Segurança e Informação e Comunicação (OSSIC) e dos Administradores Locais dos Sistemas de Informação e Comunicação (ALSIC),

implementarem os procedimentos estabelecidos pela DCSI de forma adequada ao local em que se inserem.

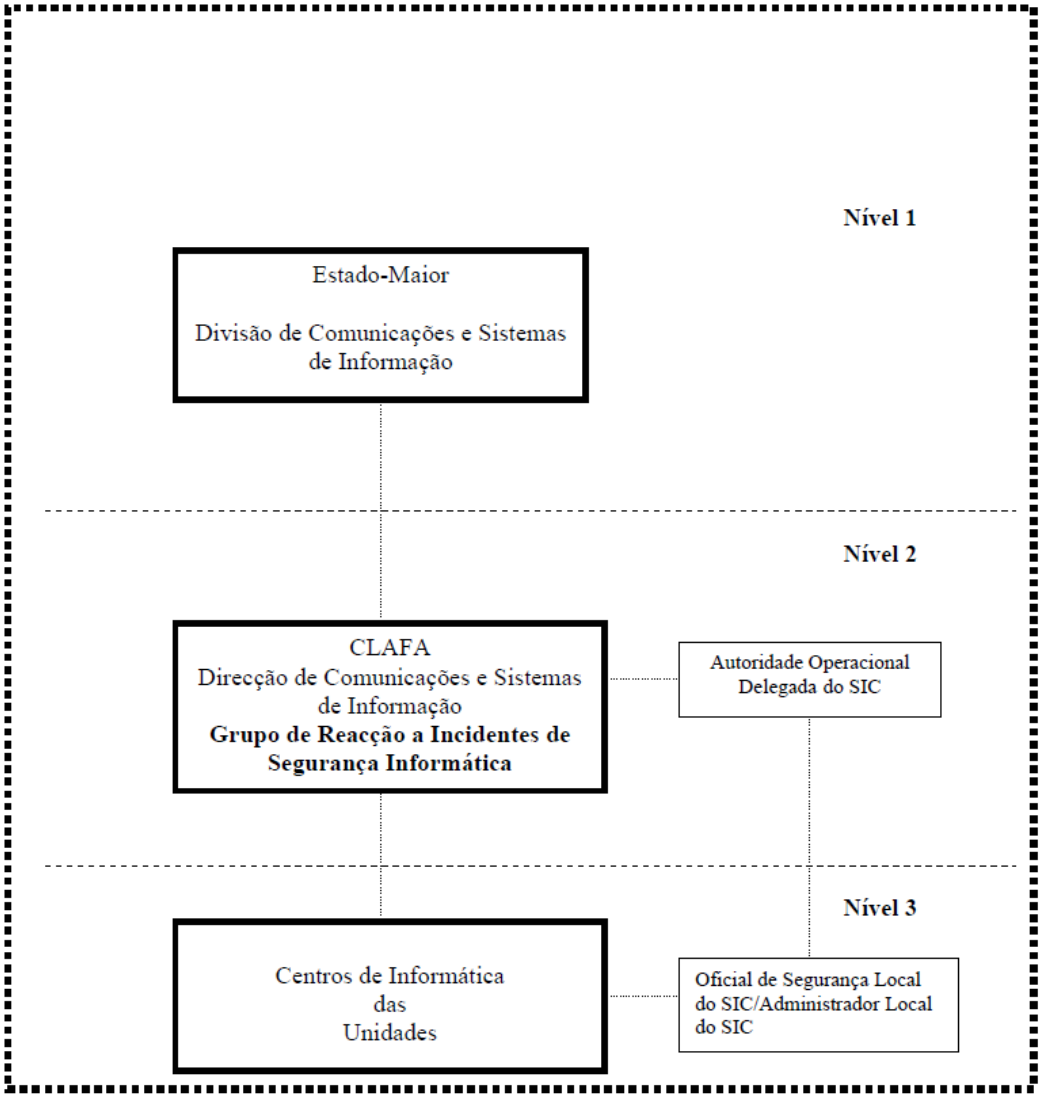

Figura 11 - Organigrama Ciberdefesa Força Aérea Portuguesa. (RFA 390-6,2011)

2. **“Gestão e Análise de Risco”.** Trata-se de um processo complexo que, para além do conhecimento das ferramentas informáticas, implica ainda um profundo conhecimento da estrutura da organização, dos sistemas existentes e da cultura organizacional com o objetivo de avaliar as vulnerabilidades e ameaças a que a organização está sujeita e também desenvolver as medidas de segurança a implementar em cada sistema. Este processo está dividido em várias fases que passam pela, análise do risco, mitigação da ameaça ou

das vulnerabilidades e pela avaliação e ajustamento das medidas. (RFA 390-6,2011)

3. **“<u>Deteção de Intrusões”.</u>** Sistemas de deteção de intrusões são sistemas que “permitem a monitorização de computadores e das redes que os interligam detetando atividades maliciosas e/ou violações da política de segurança, produzindo relatórios e acionando alertas.”. São sistemas de grande importância uma vez que sem eles muitos dos ataques poderiam acontecer sem sequer serem detetados. Sendo precisamente os ataques que, não provocando nenhum tipo de dano no equipamento, acedem ou retiram informação de forma dissimulada comprometendo desta forma recursos e informações. (RFA 390-6,2011)
4. **“Equipas de Reação”.** Estas equipas deverão encontrar-se habilitadas a lidar com incidentes de segurança informática e, para tal, os seus elementos deverão possuir formação específica. Estando estas equipas na direção técnica da DCSI, desejavelmente funcionando em regime de H24. (RFA 390-6,2011)
5. **“Cultura de Segurança”.** Considerando que são os recursos humanos os responsáveis por colocarem em prática as politicas e os procedimentos de segurança, se estes não possuírem a formação e o treino adequado não estarão capazes de prevenir, detetar e reagir perante os eventuais incidentes de segurança, ficando ainda desta forma mais vulneráveis às práticas utilizadas com o objetivo de obter acesso a informações dos sistemas por meio de engano ou exploração da confiança dos utilizadores, práticas bastante comuns atualmente sendo que é aceite que a maioria dos incidentes informáticos têm origem interna, quer por intenções maliciosas, quer por puro desconhecimento e inocência dos operacionais.

A Força Aérea, no contexto da ciberdefesa, entende que o sistema defensivo deve ser assente no princípio da “ defesa em profundidade”. Este sistema estabelece um anel defensivo que permite uma operação segura dos sistemas através da aplicação integrada de alguns componentes de segurança, tais como, a segurança física, a segurança pessoal, segurança documental, segurança da emissão, segurança da transmissão, segurança criptográfica e segurança da informação. (RFA 390-6, 2011)

O RFA 390-6 de 2011 define ainda os pilares da ciberdefesa como sendo os elementos que constituem o ciclo de gestão de incidentes de segurança informática, nomeadamente: (RFA 390-6, 2011).

- **"Formação e treino".** É considerado um pilar fundamental para a construção de uma cultura de segurança e é constituído por "todas as medidas de antecipação, como a elaboração de planos de instrução, definição procedimentos de operação seguros e a condução de exercícios e treinos adequados de todo o pessoal envolvido na operação e manutenção dos sistemas." Sendo o objetivo da formação e do treino não só dotar os recursos humanos do conhecimento técnico relacionado com a área da ciberdefesa mas também a criação de uma consciência sobre esta realidade, os riscos e os cuidados necessários.
- **"Prevenção".** Isto é, a "capacidade de proteger a informação e os sistemas que a processam da perda de confidencialidade, integridade e disponibilidade." Considera-se a dissuasão como sendo um elemento fundamental uma vez que pretende "convencer" o inimigo de que as medidas de segurança dos sistemas tornarão o seu ataque ineficaz. Outro aspeto que o RFA considera importante é o acompanhamento por parte da *intelligence* de todo o processo de forma a que exista uma avaliação da credibilidade das ameaças numa tentativa de permitir a existência do tempo necessário para o levantamento das capacidades de defesa e análise de risco. Dada a dificuldade e baixa probabilidade de conseguir ser antecipado um ataque cibernético, muito do esforço da ciberdefesa é despendido na reação a uma agressão o que implica um investimento na robustez dos sistemas mantendo-os tecnologicamente atualizados.
- **"Deteção, Resposta e Atenuação".** Este pilar consiste na capacidade de monitorização dos sistemas com vista à deteção e identificação de atividades suspeitas prevendo o seu impacto e a aplicação de medidas que permitam isolar a ameaça e os sistemas afetados, atenuando desta forma as consequências de um eventual ataque. Para isso os sistemas devem possuir a capacidade de operar mesmo no decurso de um ataque e serem robustos o suficiente para recuperarem a normal operação tão breve quanto possível.

- **“Recuperação e Análise”.** Após a existência de um ataque aos sistemas a sua recuperação envolve não só a restauração da informação e do sistema responsável pelo processamento mas também a análise do incidente com vista a que sejam retirados ensinamentos que permitam, no futuro, aumentar a capacidade de resiliência dos sistemas através da alteração ou modificação nos mesmos. É ainda recomendado que, tendo em vista a partilha de informação, sejam gerados avisos de ameaça e técnicas de resposta para a restante comunidade envolvente.

A figura seguinte esquematiza as diferentes bases e pilares da ciberdefesa anteriormente abordados permitindo assim uma melhor compreensão do seu posicionamento neste conceito:

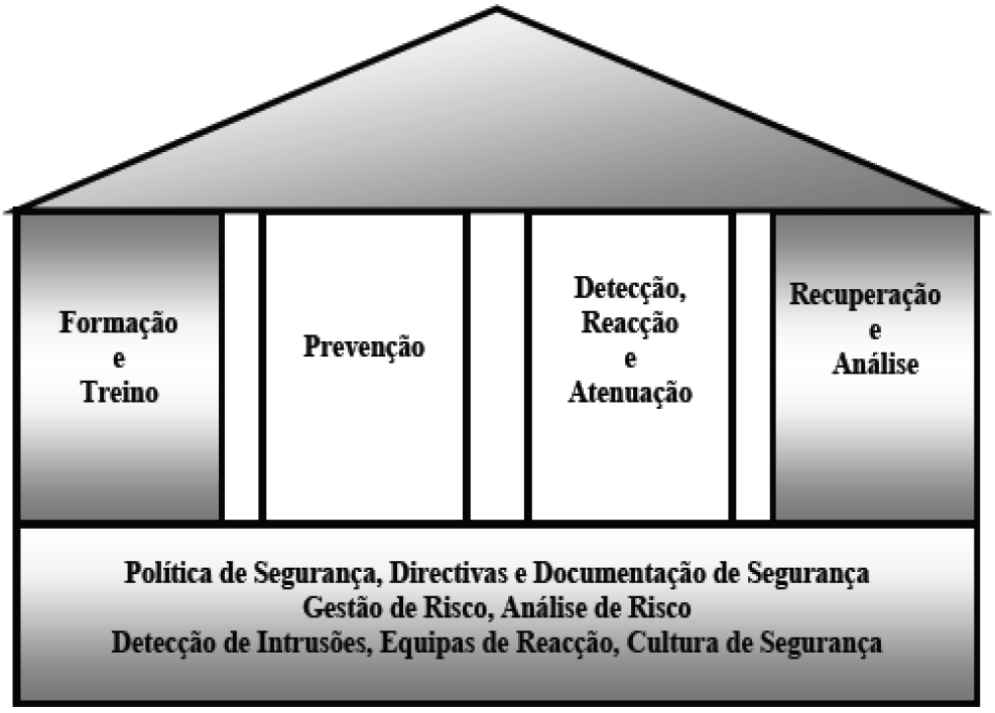

Figura 12 - Bases e Pilares da Ciberdefesa Tipificadas pela Força Aérea Portuguesa. (RFA 390-6, 2011)

4.3 A Ciberdefesa e Cibersegurança nas Forças Armadas.

Segundo o Decreto-Lei nº 184 de 29 de dezembro de 2014, é missão da Direção de Comunicações e Sistemas de Informação do EMGFA (DIRCSI), no âmbito da ciberdefesa, “ coordenar a proteção dos valores da integridade,

confidencialidade e disponibilidade da informação e dos sistemas de informação das FFAA". No sector da cibersegurança da defesa nacional é missão da DIRCSI " coordenar a proteção dos valores da integridade, confidencialidade e disponibilidade da informação e dos sistemas de informação e dos sistemas de informação do restante universo da defesa nacional".

A DIRCSI é "chefiada por um comodoro ou brigadeiro-general" e a sua estrutura é constituída por; (DL 289/2014)

- Repartição de coordenação e integração;
- Repartição de sistemas de comunicações;
- Repartição de sistemas e tecnologias de informação;
- Repartição de segurança;
- Centro Ciberdefesa;
- Serviço de comunicações e sistemas de informação;
- Centro de comunicações e Cifra.

A DIRCSI desenvolve a sua atividade tendo como orientação a política definida para a área dos sistemas de informação e das tecnologias de informação e comunicação na área da defesa nacional e de forma coordenada com o Ministério da Defesa Nacional e no âmbito das competências do Chefe do Estado-Maior General das Forças Armadas (CEMGFA), tendo como atribuições no domínio da ciberdefesa (DL 289/2014):

- Dirigir e coordenar a capacidade de ciberdefesa nacional;
- Planeamento, coordenação e gestão dos ciberincidentes de maior relevância para a ciberdefesa;
- Aprovisionamento de soluções de proteção da informação e seus sistemas das ameaças do ciberespaço, no âmbito da ciberdefesa;
- Coordenação e colaboração com os núcleos *Computer Incident Response Capability* (CIRC) dos Ramos e do EMGFA;
- Partilha de informação e colaboração com o CNCS e com os CIRC nacionais e internacionais;

- Participar nas operações de informação na componente C*omputer Network Operations*[4] *(CNO)*;
- Atualização do panorama do ciberespaço, no domínio das FFAA;
- Planeamento e organização de um programa de exercícios de treino.

Já no âmbito da "cibersegurança sectorial da defesa nacional", são atribuições da DIRCSI; (DL 289/2014)

- Planeamento, coordenação e gestão dos ciberincidentes de maior relevância para a cibersegurança sectorial da defesa nacional;
- Aprovisionamento de soluções de proteção da informação e seus sistemas das ameaças do ciberespaço, no âmbito da cibersegurança sectorial da defesa nacional;
- Colaboração e partilha de informação com os CIRC da área da defesa nacional de forma "articulada com as competências de coordenação da cooperação nacional e internacional do CNCS;
- Cooperação com as entidades nacionais responsáveis pela cibersegurança, ciberespionagem, cibercrime e ciberterrorismo.

Com a promulgação do PEMGFA/CSI/301 "Organização e normas para resposta a incidentes de segurança informáticos nos SIC das FFAA" em 23 de Setembro de 2008, documento este que se destinava ao estabelecimento da estrutura orgânica, das normas e procedimentos necessários para garantir a capacidade de resposta a incidentes de segurança informática no seio das FFAA foi estabelecida a estrutura, as normas e os procedimentos que corporizam esta capacidade com atuação em sistemas conjuntos. (CARRIÇO,2013).

A estrutura de ciberdefesa nas FFAA assenta, basicamente, em duas entidades: (RFA 390-6, 2011)

- **O Centro de Coordenação da CRISI (CC-CRISI) –** Entidade onde se encontram os representantes diretamente relacionados com a definição das políticas de segurança da informação, coordenação das respostas aos incidentes de segurança informática e ciberdefesa dos 3 Ramos. Esta

[4] Termo amplo de aplicação civil e militar que é constituído pelas componentes de CNA, CNE e CND.

entidade é ainda a responsável pela coordenação da capacidade de resposta aos incidentes sempre que estes afetem um sistema conjunto dos 3 Ramos e permite ainda a discussão e debate das politicas e procedimentos a definir nos Ramos e no EMGFA.

- **O Grupo de Resposta a Incidentes de Segurança Informática (GRISI)** – Consiste num grupo técnico, cujos recursos humanos são nomeados pelas direções técnicas de cada ramo e cuja missão primária é a reação a incidentes e a recuperação dos sistemas afetados.

A proteção dos sistemas de informação e comunicações militares críticos, requer não apenas a implementação e gestão de medidas de segurança adequadas, mas também uma capacidade de resposta a incidentes de segurança informática das FFAA (CRISI-FA). Assim, tal como é definido pela estrutura de ciberdefesa das FFAA, apresentada anteriormente, a CRISI-FA recorre, de forma coordenada, às estruturas existentes nos Ramos das FFAA e no EMGFA, com o objetivo de maximizar as valências existentes em recursos humanos e equipamento técnico, bem como a estrutura orgânica, normas e procedimentos garantindo, desta forma conjunta e combinada, a disponibilidade, integridade e confidencialidade nos SIC das FFAA (CARRIÇO,2013).

É missão do CRISI "coordenar a resposta a incidentes de segurança informática nas FFAA" (CARRIÇO,2013). Materializando-se no Grupo de Resposta a Incidentes de Segurança Informática (GRISI), cuja responsabilidade é "receber, analisar e responder a notificações e atividades relacionadas com incidentes de segurança em sistemas informáticos. As atividades do GRISI são dirigidas à área CSI das FFAA." (CARRIÇO,2013).

A promoção da implementação da política conjunta de segurança da informação com o objetivo de garantir a autonomia, sobrevivência e interoperabilidade dos sistemas das FFAA é da competência do EMGFA. Sendo o Centro de Coordenação da CRISI (CC-CRISI), o órgão responsável pela ligação com a Estrutura Nacional de Cibersegurança (CARRIÇO,2013).

Uma vez estudadas as duas entidades responsáveis pela defesa e segurança do ciberespaço e o seu papel junto das infraestruturas críticas, o próximo passo será o estudo da metodologia de gestão de risco ISO31000, com o objetivo de

perceber se as entidades anteriormente referidas levam a cabo a sua missão de acordo com os pressupostos teóricos metodologicamente previstos.

5 ISO 31000 – “Gestão do risco Princípios e Linhas de Orientação”

Atualmente qualquer tipo de organização, independentemente da sua dimensão, está exposta a fatores internos e externos que tornam incerto se serão atingidos os objetivos a que se propõem. A este estado de incerteza numa organização dá-se o nome de “risco”. (NP ISO31000, 2013)

Assim, e visto todas as organizações terem de alguma forma que gerir o risco, a norma portuguesa ISO31000 de 2013 “ Gestão do Risco Princípios e Linhas de Orientação”, estabelece um conjunto de orientações que deverão ser cumpridas para tornar eficaz a gestão do risco. Assim, esta norma recomenda que “ as organizações desenvolvam, implementem e melhorem continuamente uma estrutura cujo objetivo é integrar o processo para gerir o risco na governação, estratégia e planeamento, gestão, processos de comunicação, políticas, valores e cultura.

Para uma gestão de risco eficaz toda a infraestrutura deverá desenvolver a sua atividade tendo por base os seguintes princípios orientadores; (NP ISO31000, 2013)

1. **“A gestão do risco cria e protege o valor”** – uma política eficaz de gestão de risco permite que os objetivos da organização sejam atingidos e ainda um maior desempenho na qualidade dos produtos, na proteção ambiental, na reputação, etc.
2. **“A gestão do risco é parte integrante de todos os processos organizacionais”** – A gestão de risco não pode ser dissociada das atividades principais da infraestrutura em questão uma vez que esta tem de ocorrer de forma integrada, como uma responsabilidade da gestão, que deverá estar incluída no planeamento estratégico bem como nos processos de gestão dos projetos.
3. **“A gestão do risco é parte da tomada de decisão”** – uma vez que esta define as ações a serem tomadas bem como a ordem pela qual são tomadas tendo em conta o seu nível de importância.
4. **“ A gestão do risco considera explicitamente a incerteza”** – tendo em conta a sua natureza e a forma como deve ser tida em consideração.

5. **“ A gestão do risco é sistemática, estruturada e atempada” –** pois só assim é possível esperar resultados consistentes e fiáveis que permitam uma maior eficiência da organização.
6. **“ A gestão do risco baseia-se na melhor informação disponível” –** uma vez que as fontes desta mesma informação são tendencialmente arquivos históricos, previsões, dados recolhidos pela própria experiência das partes interessadas, bem como o recurso a pareceres de especialistas. Assim a quando da decisão das ações a tomar deve ser tido em consideração a limitação dos dados disponíveis bem como a existência de divergências entre as fontes.
7. **“A gestão do risco é feita à medida” –** uma vez que forçosamente terá de ter em consideração e estar adaptada ao contexto interno e externo da organização bem como ao seu perfil
8. **“ A gestão do risco tem em conta fatores humanos e culturais” -** tendo em consideração a potencialidade das capacidades e intenções de pessoas internas ou externas à organização com potencial de impedirem a consecução dos objetivos definidos.
9. **“ A gestão do risco é transparente e participada” –** de forma a ser atual e pertinente e ainda para que todas as partes envolvidas no processo tenham o seu ponto de vista tido em consideração na determinação dos critérios de risco. Para tal deverá existir não só um envolvimento dos decisores a todos os níveis como também de todas as partes interessadas.
10. **“A gestão do risco é dinâmica, iterativa e reativa à mudança”-** uma vez que sempre que há uma alteração do contexto ou o nível de conhecimento se altera emergem novos riscos e outros deixam de existir.
11. **“A gestão do risco facilita a melhoria contínua da organização” –** a elaboração e implementação de estratégias melhora não só a maturidade da gestão do risco como de outros sectores da organização.

5.1 Estrutura da Política de Gestão de Risco

Tal como todos os processos, a gestão do risco também deve obedecer a uma estrutura bem definida que permita o envolvimento de todos os níveis da organização e que garanta também que a informação relativa ao risco seja corretamente reportada e assim utilizada como base para a tomada de decisão.

Serão agora descritas as componentes constituintes da estrutura de gestão do risco e a forma como estas, de um modo iterativo, se relacionam. Tal como é representado na figura seguinte.

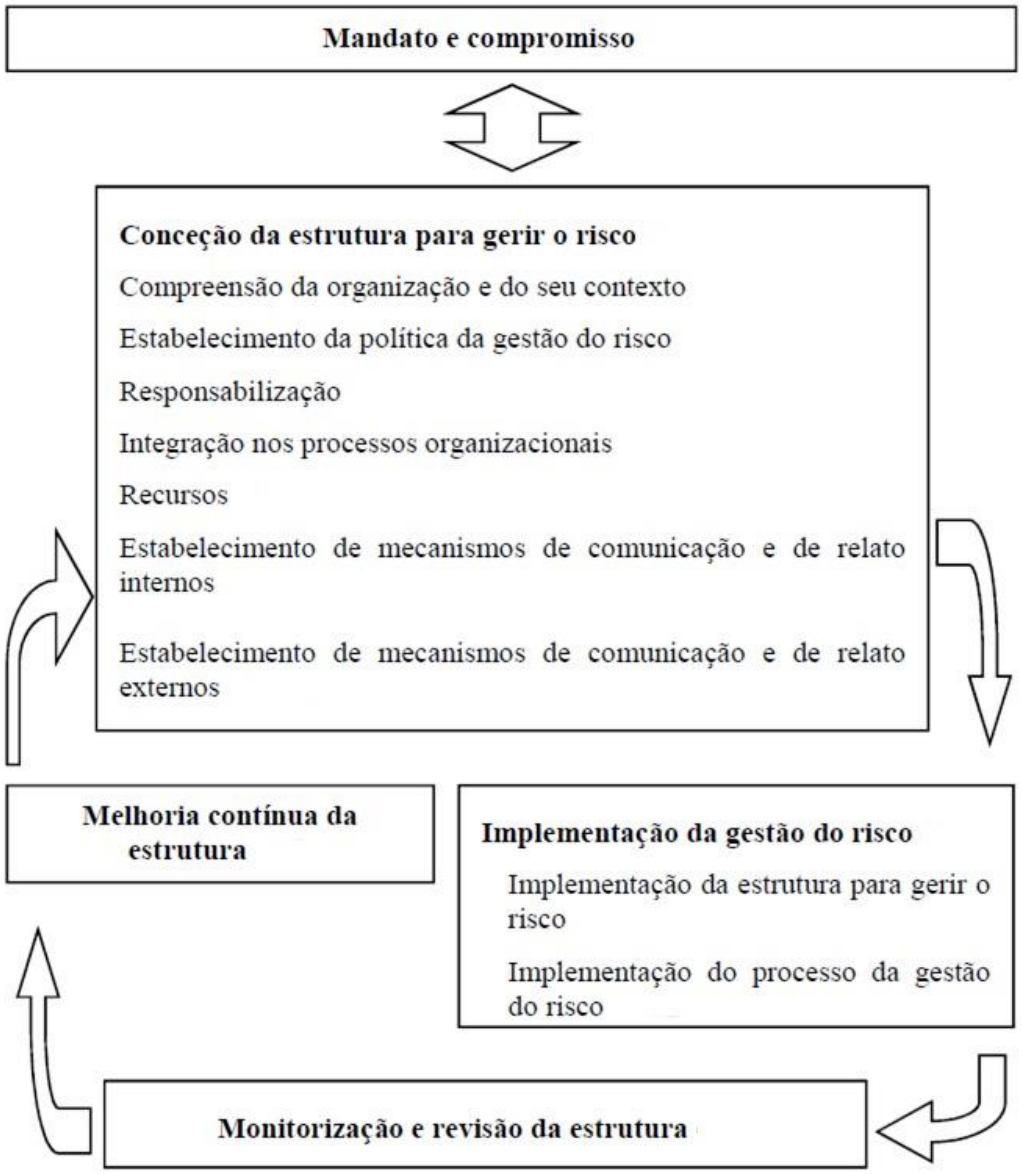

Figura 13 - Relações entre as Componentes da Estrutura de Gestão do Risco (NP ISO 31000, 2013)

Mandato e compromisso – Quando uma organização pretende introduzir uma política de gestão de risco de forma contínua e eficaz é necessário que exista um compromisso e um planeamento estratégico e rigoroso por parte da gestão de topo, sendo que esta deverá (NP ISO 31000):

- Definir e aprovar a política de gestão de risco;
- Assegurar o alinhamento entre a política de gestão de risco e a cultura da própria organização;
- Definir indicadores de desempenho da política de gestão de risco coerentes com os indicadores de desempenho da organização;
- Alinhar os objetivos da gestão de risco com os objetivos e estratégias da organização;
- Garantir que os parâmetros legais e regulamentares estão em conformidade;
- Atribuir a cada nível da organização as responsabilidades apropriadas;
- Disponibilizar os recursos necessários à gestão do risco;
- Garantir que a estrutura de gestão de risco se mantém adequada aos interesses da organização e comunicar as suas vantagens às partes interessadas.

5.2 "Conceção da Estrutura Para Gerir o Risco"

5.2.1 **"Compreensão da Organização e do seu Contexto"**

O primeiro passo antes da criação e implementação da estrutura de gestão de risco é a avaliação e compreensão do contexto interno e externo da organização uma vez que estas podem alterar significativamente a mesma. Assim a avaliação do contexto externo de uma organização deverá incluir (NP ISO31000, 2013):

- Todas as envolventes internacionais, nacionais, regionais e locais em termos políticos, culturais, sociais, tecnológicos, naturais;
- Tendências e outros fatores críticos para os objetivos da organização;
- Relações com os parceiros externos e seus valores.

A avaliação do contexto interno da organização deverá por sua vez incluir:

- Os recursos e o conhecimento disponível;
- Processos de decisão, os sistemas de informação e consequentes fluxos informativos;
- Relações com parceiros internos e seus valores;
- Modelos, linhas de orientação e normas adotadas pela organização;

- A cultura da própria organização;
- Os objetivos mas também as políticas e as estratégias implementadas para os concretizar;
- As relações contratuais quanto à sua forma e extensão;
- As responsabilidades e funções resultantes da estrutura organizacional.

5.2.2 "Estabelecimento da Política da gestão do risco"

Que permita definir inequivocamente os objetivos e o compromisso da organização neste âmbito da gestão do risco. Esta política deve ter em consideração os seguintes aspetos:

- Qual a necessidade da organização para a existência de uma gestão do risco;
- Definição de responsabilidades em matéria de gestão de risco;
- Gestão de conflitos de interesse;
- A ligação entre as políticas de gestão de risco e as próprias políticas da organização em termos de objetivos;
- Definição dos parâmetros de medição e reporte do desempenho das politicas de gestão do risco;
- Estabelecimento da obrigatoriedade de disponibilização dos recursos necessários aos elementos responsáveis pela gestão do risco;
- Estabelecimento da obrigatoriedade de revisão e melhoramento continuo e periódico da estrutura e da política de gestão de risco acompanhando assim a eventual alteração das circunstâncias.

5.2.3 "Responsabilização"

Deverá ser garantida pela organização, não só a existência de responsabilização do processo de gestão de risco, como também a existência da autoridade e da competência necessária para que todo o referido processo seja mantido de forma eficaz e eficiente. Para esse efeito são recomendadas as seguintes práticas:

- Identificação do responsável ou responsáveis pela definição, implementação e manutenção da estrutura de risco bem como de responsabilidades existentes em todos os níveis da organização no processo de gestão do risco;
- Identificação dos proprietários do risco, que por sua vez são os detentores da autoridade e responsabilidade de gestão do mesmo;
- Avaliação dos processos e do desempenho do sistema de reporte quer interno quer externo e de transmissão da informação relativa à gestão do risco a todos os níveis da organização.

5.2.4 "Integração nos Processos Organizacionais"

De modo a que, o processo de gestão de risco possa ser eficaz, eficiente e pertinente, o mesmo terá de ser integrado nos restantes processos da organização, especialmente no que concerne à sua integração no desenvolvimento da política, no planeamento estratégico do negócio e sua revisão, bem como nos processos de gestão da mudança.

5.2.5 "Recursos"

Tal como já referido anteriormente deverá existir a preocupação da organização de afetar ao processo de gestão de risco todos os recursos necessários para o seu cumprimento, devendo nomeadamente ter em conta:

- A competência, experiência e aptidões existentes nos recursos humanos disponíveis;
- As necessidades em termos dos processos, ferramentas e métodos a serem utilizados;
- Os programas de formação;
- A documentação relativa aos procedimentos e processos já existentes;
- Os sistemas de gestão da informação e do conhecimento.

5.2.6 "Estabelecimento de Mecanismos de Comunicação e de Relato Internos"

Como já foi evidenciado repetidas vezes anteriormente é essencial a existência e implementação de mecanismos de comunicação e de relato internos de forma a suportar e aumentar a responsabilização e a apropriação do risco na organização. Estes mecanismos deverão, para além de nos casos necessários permitir a consolidação das informações relativas ao risco quando estas forem provenientes de diversas fontes, ter ainda em consideração que parte ou a totalidade desta informação poderá ter caracter sensível, bem como garantir:

- Que a informação útil que resulta da aplicação dos processos de gestão do risco se encontra disponível no tempo e aos níveis adequados;
- Que são efetuados os devidos relatos internos, relativos não só aos resultados como também à eficácia da estrutura da gestão do risco;
- Que os elementos estruturantes da gestão do risco bem como qualquer modificação são comunicados.

5.2.7 "Estabelecimento de Mecanismos de Comunicação e de Relato Externos"

Para além dos mecanismos de comunicação internos é ainda importante a existência e implementação de um plano de comunicações com as partes externas interessadas, sendo que estes deverão permitir a consolidação das informações relativas ao risco quando estas forem provenientes de diversas fontes, e terem ainda em consideração que parte ou a totalidade desta informação poderá ter caracter sensível. Assim, o plano de comunicações externas deverá contemplar:

- Uma troca eficaz da informação através do envolvimento das partes externas interessadas;
- Os reportes das entidades externas para o cumprimento dos requisitos legais, regulamentares da governação;
- Que a ocorrência de uma crise ou contingência seja comunicada às partes interessadas;
- Que a comunicação com as entidades externas permite a criação de confiança na organização.

5.3 “Implementação da Gestão do Risco”

5.3.1 “ Implementação da Estrutura para Gerir o Risco”

Com vista a concretização deste objetivo a organização deverá;

- Calendarizar todo o processo, definindo a melhor estratégia para a sua implementação;
- Garantir o cumprimento de todas as normas regulamentares;
- Fazer uso, nos processos organizacionais, da política e dos processos de gestão de risco.
- Levar a cabo ações de formação e informação;
- Garantir que, aquando do estabelecimento e desenvolvimento dos objetivos, os decisores têm em linha de consideração os resultados dos processos de gestão de risco;
- Manter contacto com as partes interessadas garantido assim a adequabilidade da estrutura de gestão do risco.

5.3.2 “Implementação do Processo da Gestão do Risco”

Deverá ocorrer de forma a garantir que o processo de gestão do risco analisado seguidamente, é aplicado a todos os níveis e funções da organização, seguindo o plano elaborado para o efeito.

5.4 “Monitorização e Revisão da Estrutura”

Com o objetivo de garantir uma gestão de risco eficaz e que proporcione um apoio contínuo ao desempenho da organização esta deve;

- Reavaliar a eficácia da estrutura de gestão do risco, isto é, rever se a estrutura, a política e o plano da gestão de risco continuam adequados às alterações do contexto interno e externo da mesma;
- Avaliar o desempenho do processo com recurso a indicadores que devem ser revistos periodicamente quanto à sua adequabilidade;

- Verificar, com periodicidade, a existência de desvios ao plano de gestão de risco bem como os progressos alcançados elaborando relatórios com as referidas informações.

5.5 “ Melhoria Contínua da Estrutura”

Com recurso aos resultados obtidos pela monitorização e revisão da estrutura deverá proceder-se a uma otimização e melhoria constante, seja da estrutura, da política ou mesmo do plano da gestão do risco.

5.6 Processo de Gestão de Risco

Tal como como tem sido descrito, o processo de gestão do risco deve ocorrer como parte integrante da gestão, da cultura e das práticas organizacionais e adaptado aos processos organizacionais de negócio. Este processo compreende várias atividades ilustradas na figura seguinte e que serão descritas de seguida;

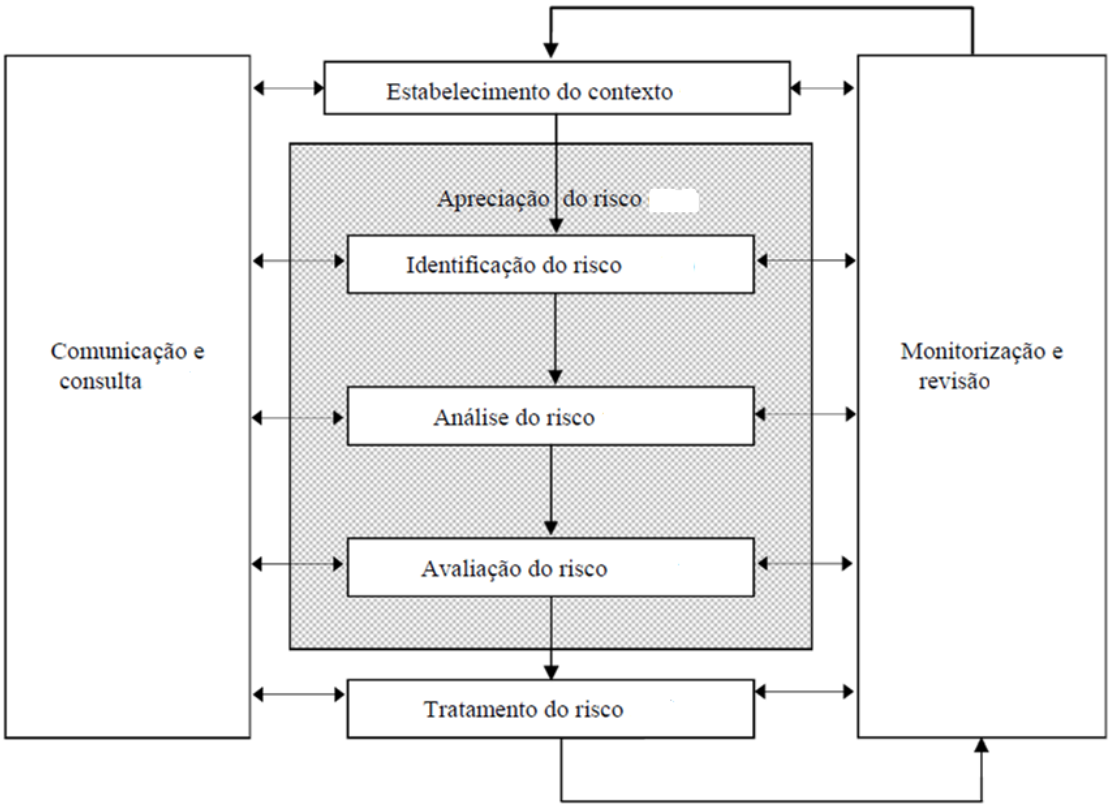

Figura 14 - Processo da Gestão do Risco

5.6.1 Comunicação e Consulta

Tal como evidenciado pela figura 14, a comunicação e consulta deve ser uma constante durante todas as fases do processo. Assim, os planos de comunicação e consulta das partes interessadas, apesar de serem desenvolvidos numa fase inicial, deverão abordar as várias questões diretamente relacionadas com o risco, isto é, as suas causas, consequências e as contramedidas. Sendo que existindo uma comunicação e consulta eficaz ,quer em termos internos quer externos, será possível garantir às partes interessadas bem como aos responsáveis pela implementação do processo da gestão do risco que estes compreendem as justificações e objetivos das decisões tomadas.

A ISO 1000 avança ainda que a existência de uma política de consulta em equipa trará algumas vantagens, nomeadamente;

- O diálogo entre as várias áreas de especialização para uma melhor análise do risco;
- O garante de que os vários pontos de vista são tidos em consideração na definição e avaliação do risco;
- Um maior envolvimento de toda a organização, o que permite uma maior adesão e apoio relativamente ao tratamento do risco;
- Garantir que tanto os riscos como o seu contexto são identificados de forma adequada;

Tal como exposto anteriormente a consulta e comunicação entre as várias partes interessadas na área de gestão é de extrema importância uma vez que, através da troca de valores, pressupostos, necessidades, conceitos e preocupações do coletivo permite uma tomada de decisão mais efetiva e eficaz. Sendo o objetivo primeiro da consulta e comunicação a existência de uma troca de informação mais verdadeira, precisa e compreensível tendo em consideração a sensibilidade da informação e a sua integridade.

5.6.2 Estabelecimento do Contexto

Este passo da gestão do risco, entenda-se, o estabelecimento do contexto seja ele o contexto externo ou interno, permite que a organização tipifique os seus

objetivos, defina quais os parâmetros internos ou externos a ter em conta na gestão do risco. Nesta fase é elaborada uma análise mais detalhada de parâmetros similares aos considerados no estabelecimento do contexto do processo da gestão do risco.

5.6.2.1 Estabelecimento do Contexto Externo

O contexto externo é compreendido pelo ambiente externo onde qualquer organização se propõem atingir os seus objetivos. Compreender o ambiente externo inclui:

- A envolvente social, cultural, politica, legal, regulamentar, financeira, tecnológica, económica seja a nível local, regional, nacional ou mesmo internacional;
- As tendências e os elementos mais importantes com impacto para a consecução dos objetivos da organização;
- As relações com as partes interessadas externas no que respeita aos seus valores e perceções,

Esta compreensão do contexto externo vem garantir que, aquando do desenvolvimento dos critérios de risco, os objetivos e preocupações de todas as partes são tidas em consideração.

5.6.2.2 Estabelecimento do contexto interno

O contexto interno é compreendido pelo ambiente interno onde qualquer organização se propõem atingir os seus objetivos. A compreensão do contexto interno deve incluir;

- Os sistemas de informação bem como os fluxos de informação e os processos formais ou informais de tomada de decisão;
- A cultura da organização e as relações das partes internas nomeadamente as suas perceções e seus valores;
- As capacidades existentes tanto em termos de recursos como de conhecimento;

- As políticas, objetivos e as estratégias implementadas para os atingir;
- Os modelos, normas e linhas de orientação adotadas pela organização, bem como a sua estrutura, as suas funções, e estilo governativo;

O estabelecimento deste contexto interno deverá ocorrer uma vez que a gestão do risco acontece no contexto dos objetivos da organização, qualquer objetivo ou critério de um projeto ou atividade específico deverão ter sempre em consideração os objetivos da organização como um todo. Sendo certo que algumas organizações por vezes falham ao não aproveitarem oportunidades que lhes permitiriam atingir os seus objetivos estratégicos e isso leva a que a sua credibilidade, confiança e valor afetado.

5.6.2.3 "Estabelecimento do contexto do processo da gestão do risco"

Partindo da necessidade de justificar todos os recursos utilizados na implementação da gestão do risco e de serem especificados todos os recursos pretendidos bem como as responsabilidades e autoridades que devem ser respeitadas durante todo o processo, é necessário que sejam definidos de forma clara os objetivos, estratégias, o âmbito, bem como os parâmetros das atividades em que o processo será aplicado. Assim, o contexto do processo de gestão do risco deverá focar;

- Definição das responsabilidades, metas, metodologias e objetivos das atividades da gestão do risco;
- Especificação do âmbito, extensão, objetivos dos estudos necessários bem como os recursos disponíveis para os mesmos;
- Estabelecer os parâmetros de avaliação do desempenho e da eficácia da gestão do risco;
- Procurar localizar no tempo e no espaço cada atividade, projeto, processo, produto e serviço inerentes á gestão de risco.

5.6.3 “Definição dos Critérios do Risco”

Sendo que estes serão posteriormente utilizados para avaliar o grau de impacto de cada ameaça associado ao risco que esta representa, estes deverão estar perfeitamente alinhados com os valores e objetivos da organização bem como com os recursos disponíveis. Sendo necessário ter também em linha de conta que alguns desses critérios poderão não ser de caracter facultativo, isto é, estes poderão ser resultado de exigências legais ou de requisitos regulamentares subscritos pela organização. Por fim os critérios de risco deverão ainda ter em linha de consideração a política de gestão do risco previamente definida, devendo incluir:

- O nível de tolerância ao risco e a forma como este é determinado;
- As variadas causas e respetivas consequências que podem ocorrer e a forma como são medidas;
- As opiniões das partes interessadas;
- Caso seja oportuno a consideração da existência de combinação de múltiplos riscos, quais as combinações que deverão ser consideradas;
- O modo como será definida a probabilidade de ocorrência de cada combinação.

5.6.4 “Apreciação do Risco”

Isto é, o “ processo global de identificação, análise e avaliação do risco”.

5.6.5 “Identificação do Risco”

Trata-se de uma fase crucial de todo o processo uma vez que um risco que não seja conveniente identificado como tal, não será considerado durante as fases seguintes. Assim pretende-se identificar, não só as fontes do risco, como também as áreas de impacto, as causas e respetivas consequências, para assim cumprir o objetivo de constituir uma lista abrangente dos riscos “ baseada nos eventos que possam, criar, melhorar, prevenir, degradar, acelerar ou retardar a consecução dos objetivos”.

É importante que nesta fase de identificação dos riscos a organização esteja na posse da informação mais pertinente e atualizada, para que esta consiga identificar riscos, seja a sua fonte controlada ou não pela própria organização. Esta

fase deverá ainda ter em conta a análise das reações em cadeia bem como os efeitos cumulativos e em cascata.

Tal como são identificados os riscos, isto é, aquilo que poderá vir a acontecer, é também importante nesta fase identificar as causas e posteriores consequências.

5.6.6 “Análise do Risco”

Nesta fase é feita uma compreensão do risco para que posteriormente se possa passar para a fase seguinte denominada “ Avaliação do Risco”, a análise do risco é então o primeiro passo na tomada de decisão, esta análise implica uma identificação das causas e fontes do risco, das consequências tanto negativas como positivas bem como da probabilidade dessas mesmas consequências ocorrerem.

A forma como as consequências e a suas respetivas probabilidades são calculadas, apresentadas e posteriormente combinadas para determinação do nível de risco deve estar de acordo com o tipo de risco, a informação disponível e a utilização que lhe será empregue, sendo esta análise sempre feita tendo por base os critérios de risco e a interdependência dos vários tipos de risco e suas fontes.

Aquando da análise de risco, fatores que possam de alguma forma descredibilizar a mesma devem ser também enunciados e até realçados, sendo que os decisores deverão ser conhecedores dos referidos fatores podendo estes ser, “ divergência de opinião entre especialistas, incerteza, disponibilidade, qualidade, quantidade e pertinência da informação ou limitações na modelação”.

É ainda de realçar que, consoante o tipo de risco ou a própria finalidade da análise e da informação, dos dados e dos recursos disponíveis, a análise do risco pode ser feita com níveis de detalhe variáveis e pode ainda ser de caracter qualitativo, semi-quantitativo, quantitativo ou uma combinação das anteriores.

5.6.7 “Avaliação do Risco”

Com recurso aos resultados obtidos na análise do risco, é agora feita uma avaliação do risco sendo o objetivo apoiar a tomada de decisão sobre quais os riscos mais prioritários e que necessitam de maior atenção.

Esta avaliação consiste na comparação dos critérios de risco definidos aquando da elaboração do contexto, com o nível do risco identificado durante a fase de análise, surgindo assim desta comparação a necessidade ou não de tratamento de um dado risco, sendo possível que, após a avaliação, seja determinado que apesar serão mantidos os controlos já existentes.

5.6.8 “Tratamento do Risco”

Quando, após a avaliação, é determinado a necessidade de tratamento de um dado risco é desencadeado um processo cíclico de inclui;

- Avaliar o tratamento a aplicar;
- Avaliar se o nível de risco residual é aceitável e caso não seja aplicar um novo tratamento do risco;
- Avaliar a eficácia do tratamento aplicado;
- A organização dispõem de algumas opções de tratamento do risco podendo estas incluir, conforme as circunstancias, o seguinte;
    - Remoção da fonte do risco;
    - Alteração das probabilidades;
    - Partilha do risco com terceiros (contratos e financiamento do risco);
    - Alteração das consequências;
    - Retenção do risco;
    - Interromper, ou não dar início, a uma dada atividade portadora do risco;
    - Assumir a existência do risco ou até aumentá-lo com o objetivo de perseguir uma oportunidade.

5.6.9 “Seleção de Opções de Tratamento do Risco”

As várias opções de tratamento existentes e disponíveis podem ser consideradas e aplicadas seja individualmente ou e de forma combinada, sendo que normalmente existe um maior benefício quando há uma combinação de várias opções de tratamento. O processo de seleção das opções passa por uma avaliação dos custos e implicações da implementação de cada opção quando comparado com os benefícios resultantes, sempre tendo em linha de consideração os requisitos legais e regulamentares. Deverá ainda ser feita uma de risco para avaliar se o mesmo justifica o custo do tratamento a aplicar.

Também na seleção do(s) tratamento(s) do risco deverá ser tido em consideração os valores e cultura da organização e das partes interessadas. Deverá ser elaborado um plano de tratamento que, de forma clara e objetiva, identifique a ordem e a prioridade dos tratamentos.

É ainda importante ter em consideração que a aplicação do tratamento, só por si, já poderá introduzir riscos, nomeadamente a falha ou ineficácia de um dado tratamento, sendo por isso recomendável a monitorização constante de todo o processo de tratamento.

5.6.10 “Preparação e Implementação dos Planos de Tratamento do Risco”

Que têm como objetivo tipificar a forma como as diversas opções de tratamento escolhidas serão implementadas, devendo incluir;

- A calendarização da implementação e o cronograma;
- Todos os recursos necessários;
- Os responsáveis, não só pela aprovação do plano, como pela sua implementação;
- O justificativo das opções escolhidas, com a identificação dos objetivos que se pretendem atingir;
- As medidas de desempenho e eventuais contratempos.

Contudo deverá estar sempre presente na ação dos decisores e das partes interessadas que, mesmo após a implementação dos planos de risco, existirá um risco residual, devendo os mesmos estar conscientes da sua natureza e dimensão. O risco residual deverá, por isso, estar devidamente documentado e ser monitorizado e revisto sempre que necessário.

5.6.11 Monitorização e Revisão

Esta fase do processo deverá também estar planeada, devendo os seus responsáveis estar claramente definidos. Deverá ter uma visão global de todas as restantes fases do processo tendo como objetivo;

- Identificar eventuais alterações de contexto, quer externo quer interno, bem como alterações nos critérios de risco uma vez que estas alterações podem implicar uma alteração dos tratamentos do risco e das prioridades;
- Identificar novos riscos;
- Manter uma supervisão constante de novos eventos, mudanças, tendências, sucessos e falhas. para que com a sua análise se retirem lições aprendidas;
- Garantir que os mecanismos de controlo são eficazes e eficientes tanto na conceção como na operação.

A informação resultante deste constante processo de monitorização e revisão de todas as fases deverá ser registada e reportada a todas as partes interessadas, sejam elas internas ou externas, devendo posteriormente ser usada para a revisão da estrutura da gestão do risco.

5.6.12 Registo do Processo da Gestão do Risco

Todas as fases do processo de gestão do risco são registadas, sendo que, estes registos deverão ser utilizados na melhoria constante de todos os métodos e ferramentas. Assim quando se discute a criação de registos deverá ser tido em consideração que;

- Existe uma necessidade de aprendizagem contínua de todas as organizações;
- As exigências legais, regulamentares e operacionais dos registos;
- O período de conservação;
- O nível de sensibilidade da informação;
- Os custos envolvidos na criação e manutenção dos registos;
- Definir os critérios de acessibilidade bem como os meios de armazenamento.

Com análise da metodologia ISO31000 abordamos uma metodologia de gestão do risco generalista aplicável a qualquer organização que tenha por necessidade a gestão de algum tipo de risco. Seguidamente será analisada a metodologia RAMCAP uma vez que esta se encontra mais direcionada para a proteção de ICN em concreto.

6 Metodologia RAMCAP

RAMCAP (Risk Analysis and Management for Critical Asset Protection), é uma metodologia de análise e gestão de risco associado a um ataque terrorista contra uma IC. Esta metodologia permite identificar, analisar, quantificar e comunicar as várias características e potenciais impactos de ataques terroristas a um determinado alvo. Trata-se de um processo de identificação de vulnerabilidades bem como das opções para corrigir essas mesmas vulnerabilidades. (ASME-ITI,LLC, 2005)

A metodologia RAMCAP foi desenvolvida com o intuito de dar resposta a 3 objetivos base: (ASME-ITI,LLC, 2005)

1. Definir uma metodologia comum que pudesse ser utilizada pelos proprietários e operadores das IC como instrumento de avaliação das consequências e vulnerabilidades a um eventual ataque terrorista às suas instruturas ou sistemas;
2. Fornecer orientações sobre os métodos que podem ser utilizados para avaliar o risco através de uma metodologia comum;
3. Criar um mecanismo consistente e eficiente, que pudesse ser aplicado tanto no sector privado como no setor do estado, para reporte das informações resultantes das avaliações de risco das suas IC para o *Department of Homeland Security* (DHS).

RAMCAP é composta por sete áreas de análise inter-relacionadas: (ASME-ITI,LLC, 2005)

1. **Caracterização de ativos** (*Asset Characterization*) – A caracterização de ativos permite determinar os ativos que, quando perturbados ou destruídos, seja por causas naturais, acidentes ou por um qualquer ataque, podem provocar interrupções prolongadas das operações, ferimentos, mortes, impossibilidade de acesso à própria infraestrutura ou sistema, impactos económicos negativos ou qualquer combinação dos anteriores. Em última avaliação a caracterização de ativos permite obter uma compilação dos ativos críticos de interesse a serem considerados nas etapas posteriores. Trata-se da análise de uma instalação ou sistema operacional com o objetivo de identificar pontos críticos ao mesmo

tempo que é feita uma previsão preliminar de potenciais consequências de um ataque. Esta análise é efetuada nos dois domínios de ação, físico e ciber. Esta avaliação pode ainda ser feita em duas fases, numa primeira fase é feita uma avaliação à infraestrutura como um todo e posteriormente uma análise mais detalhada e individualizada a cada sector da infraestrutura ou sistema. O processo de caracterização de ativos está divido em seis passos: (ASME ITI, 2010)

i) **Identificação de funções críticas,** isto é, determinar os ativos que realizam ou apoiam as funções ou missões críticas.

ii) **Identificar ativos potencialmente críticos,** isto é, os ativos que são necessários para realizar ou apoiar as funções ou missões críticas. Estes podem incluir, recursos humanos, equipamentos, produtos, informações, dependendo do tipo de infraestrutura ou sistema que está a ser avaliado.

iii) Identificar Infraestruturas críticas (externas ou internas), como por exemplo, infraestruturas de telecomunicações, energia, transportes, serviços de emergência bem como todas as interdependências que suportam cada IC. Importa ainda nesta fase avaliar o impacto da perda de uma ou mais destas IC.

iv) Identificar contramedidas e estratégias de mitigação existentes, incluindo a segurança física, segurança cibernética, controlos administrativos bem como outros mecanismos existentes.

v) Estimar o pior razoável cenário possível, resultante da destruição, ou perda de acesso, para cada ativo. Isto é, considerar o potencial para perdas de vidas humanas ou feridos graves, graves perdas económicas para a própria infraestrutura ou para a comunidade que serve, perdas de confiança ou ainda inibição efetiva das funções dos serviços de administração pública, segurança e defesa nacional em qualquer nível.

vi) Priorizar os ativos críticos, isto é, utilizando a previsão de consequências resultante do passo anterior, identificar os ativos mais prioritários.

2) **Caracterização da ameaça** (*Threat Characterization*) – Trata-se da identificação de potenciais tipos de ataque, sejam eles de caracter geral ou específico, que poderão ser usados contra um dado alvo. As ameaças podem incluir vários tipos de ataque (Ex: Aéreo, Terrestre ou Marítimo) bem como podem atingir várias

dimensões (Ex: pequena, media ou grande). As ameaças poderão ser terrorismo ou tempestades, tornados, incêndios, ataques cibernéticos, pandemias, incidentes de origem alimentar. Assim no que respeita à análise de ameaças esta deve contemplar: (ASME ITI, 2010)

i) Descrição, no caso de ataques terroristas, das capacidades dos envolvidos incluindo tipos de armamento, táticas e meios disponíveis;
ii) Descrição, no caso das causas naturais, de todos os furacões, terramotos, inundações, incêndios, erupções vulcânicas, etc. que ocorreram ou poderão ocorrer num dado local. Deve ser ainda estabelecido um intervalo de magnitudes espectáveis com os danos associados;
iii) Elaboração de pares ameaça-ativo, este processo implica que para cada ativo seja considerada cada ameaça possível. Isto é, para uma dada infraestrutura pode fazer sentido considerar um furacão como uma potencial ameaça mas dada a sua localização esta não ser, por exemplo, vulnerável a *tsunamis.* Desta análise as combinações lógicas resultantes são chamadas pares ameaça-ativos. Se um dado ativo (A) pode ser suscetível a todas as ameaças (T) o número máximo de pares ameaça-ativo é dado por A*T;
iv) Descrever, no caso dos denominados perigos de dependência, todos os possíveis, tais como, interrupções de serviços públicos, fornecedores, funcionários, clientes, transportes etc;
v) Estabelecer um *ranking* dos pares ameaça-ativo de acordo com a magnitude prevista das consequências;
vi) Selecionar os pares ameaça-ativo de maior relevância para a restante análise, os pares selecionados serão os que representarem maiores consequências. Contudo uma ameaça que exija um maior investimento por parte do adversário ou que tenha menor probabilidade de ocorrência (desastres naturais) pode representar menor risco que uma ameaça de menores consequências mas de maior probabilidade de ocorrência.

3) **Análise das Consequências** (*Consequence Analysis*) – Consiste na identificação das piores razoáveis consequências que determinada ameaça poderia gerar. Neste passo a infraestrutura ou sistema é analisado em termos da sua organização, estrutura e operação com o intuito de identificar os tipos de

consequências que podem ser esperadas, em termos quantitativos no que respeita a custos financeiros, fatalidades ou ferimentos causados e, em termos qualitativos, aos impactos psicológicos e aos efeitos na segurança nacional ou nas funções governativas. No campo da análise de consequências devem ser seguidos os seguintes passos: (ASME ITI, 2010)

i) Aplicar as piores hipóteses razoáveis para cada tipo de incidente. No caso de ataques terroristas deve ser assumido que o adversário é inteligente e tem a capacidade de se adaptar com o objetivo e otimizar ou maximizar as consequências de um cenário. No caso das ameaças naturais devem ser assumidas todas as razoáveis magnitudes do incidente;

ii) Devem ser estimadas as consequências em termos de perdas de vidas humanas, ferimentos graves bem como perdas económicas para a instituição;

Tabela 2 - Escala de consequências para as fatalidades (ASME,2006)

	CONSEQUENCE SCALES - FATALITIES													
	CONSEQUENCE RANGE													
RAMCAP Consequence Criteria	0	1	2	3	4	5	6	7	8	9	10	11	12	13
Number of Fatalities	0 - 25	26 - 50	51 - 100	101 - 200	201 - 400	401 - 800	801 - 1,600	1,601 - 3,200	3,201 - 6,400	6,401 - 12,800	12,801 - 25,600	25,601- 51,200	51,201 - 102,400	102,401+

Tabela 3 - Escala de consequências para os feridos (ASME,2006)

	CONSEQUENCE SCALES - INJURIES													
	CONSEQUENCE RANGE													
RAMCAP Consequence Criteria	0	1	2	3	4	5	6	7	8	9	10	11	12	13
Number of Injuries	0 - 25	26 - 50	51 - 100	101 - 200	201 - 400	401 - 800	801 - 1,600	1,601 - 3,200	3,201 - 6,400	6,401 - 12,800	12,801 - 25,600	25,601 - 51,200	51,201 - 102,400	102,401+

Tabela 4 - Escala de consequências para as perdas económicas (ASME,2006)

	CONSEQUENCE SCALES - ECONOMIC IMPACTS (As measured in $milliion)													
	CONSEQUENCE RANGE													
RAMCAP Consequence Criteria	0	1	2	3	4	5	6	7	8	9	10	11	12	13
Economic Impacts (in $-million)	0 - 25	26 - 50	51 - 100	101 - 200	201 - 400	401 - 800	801 - 1,600	1,601 - 3,200	3,201 - 6,400	6,401 - 12, 800	12,801 - 25,600	25,601 - 51,200	51,201 - 102,400	102,401 +

iii) Ter em consideração a existência de consequências adicionais. Tais como consequências sociopolíticas, perda da capacidade estratégica e/ou da confiança do público, impactos psicológicos, etc.;

iv) Desenvolver um plano de resposta aos média. Uma vez que, como já visto, publicidade negativa pode representar consequências inesperadas e indesejáveis a longo prazo. Por outro lado os média podem também ser um meio de comunicação valioso para informar a comunidade sobre um eventual incidente e sua recuperação;

v) Identificar os danos que dado ataque possa desenvolver, não só na infraestrutura em si mas também em outras infraestruturas ou serviços dos quais esta depende. Uma vez que um dado dano pode impossibilitar que recursos essenciais á operação da IC lhe sejam fornecidos, como por exemplo, impossibilidade de fornecimento de água, luz, alimentação etc.

4) **Análise de Vulnerabilidades** (*Vulnerability Analysis*) – Este passo consiste na análise dos pontos fortes e das vulnerabilidades de cada ativo bem como de cada sistema de proteção e das estratégias de mitigação correspondentes a cada ameaça. Desta análise deverá resultar a determinação da probabilidade de um ataque ser bem-sucedido tendo em conta uma dada ameaça e um determinado alvo. Esta análise deve ser conduzida com base num procedimento de 4 fases;

1. Rever todos os detalhes pertinentes da construção das instalações e dos sistemas. Nesta revisão devem ser incluídas as contramedidas e todos os mecanismos de defesa da ameaça, tais como características topográficas, de estrutura ou equipamentos de dissuasão bem como os sistemas de deteção.

2. Analisar a vulnerabilidade de cada ativo crítico ou sistema para estimar a probabilidade de, dado a ocorrência de uma ameaça, ocorrem as consequências previstas no ponto 3.
3. Documentar o método usado para a realização da análise de vulnerabilidades, dos piores casos razoáveis pressupostos, e os resultados da análise de vulnerabilidade.
4. Guardar um registo das estimativas de vulnerabilidades numa escala de probabilidades. A probabilidade de sucesso de um ataque pode ser expressa como uma fração, uma probabilidade, ou o número de sucesso entre tentativas.

Tabela 5 - Escala de Probabilidades de Sucesso de um ataque (ASME, 2006)

Likelihood of "Attack Success" Scale				
Bin		Decimal Description	Percentage Range	Success Per Attempts
5	C	0.9 - 1.0	90% +	9/10 > L > 1
	B	0.75 - 0.9	75% - 90%	3/4 > L > 9/10
	A	0.5 - 0.75	50% - 75%	1/2 > L > 3/4
4		0.25 - 0.5	25% - 50%	1/4 > L > 1/2
3		0.125 - 0.25	12% - 25%	1/8 > L > 1/4
2		0.0625 - 0.125	6% - 12%	1/16 > L > 1/8
1		0.0312 - 0.0625	3% - 6%	1/32 > L > 1/16
0		< 0.0312	< 3%	1/32 > L

5) **Avaliação da ameaça** (*Threat Assessment*) – a avaliação das ameaças é composta por dois passos, em primeiro lugar é feita uma avaliação do nível de interesse dos ativos e posteriormente uma avaliação completa das ameaças. O nível de interesse de determinado ativo para um determinado ataque terrorista é avaliado tendo em conta a forma como cada recurso é percebido pelo eventual atacante quando considera as medidas de segurança e robustez do potencial alvo, esta avaliação de interesse é feita pelo próprio operador da IC. A avaliação da ameaça é feita pelo *Department Of Homeland Security* (DHS) com recurso á *Intelligence* com o objetivo de perceber quais são os objetivos dos grupos

terroristas bem como as suas capacidades. No caso das ameaças naturais a avaliação é feita com base no registo histórico de um dado local especifico.

6) **Avaliação do Risco** (Risk Assessment) – consiste num processo sistemático e abrangente de análise da informação previamente recolhida relacionada com atos terroristas para um dado sistema ou instalação. Este tipo de avaliação permite ao operador da IC criar uma base de dados para a seleção de estratégias e táticas a adotar para a defesa contra ataques terroristas estabelecendo prioridades com base no risco. Nesta fase a IC deve:
   a) Calcular o risco para cada par ameaça-ativo como a resultante de um produto entre a análise de consequências, a análise de vulnerabilidades e a avaliação de vulnerabilidades, assim;

Risco = Consequências x (Probabilidade da ameaça x Vulnerabilidade)

Onde:

- **Risco**, deve ser expresso na unidade monetária por ano (Ex: euros/ano), fatalidades ou feridos graves bem como a combinação de ambos caso seja aplicável;
- **Probabilidade da Ameaça,** tal como visto no ponto 5, trata-se de uma probabilidade de uma ameaça especifica ocorrer para um ativo em particular. A unidade de medida é o próprio valor da probabilidade ou frequência de ocorrência ao longo de um determinado período de tempo.
- **Vulnerabilidade,** tal como visto no ponto 4, é também uma probabilidade, desta feita, a de que uma ameaça a um alvo especifico resulta nas consequências estimadas no ponto 3, sempre que a ameaça ocorra.
- **Consequências,** tal como visto no ponto 3, são expressas para cada par ameaça-ativo relativamente ao numero de vitimas, feridos graves, perdas económicas quer seja para o operador/dono da IC quer seja para a região onde a mesma opera ou serve.

Quando é feita a avaliação do risco, o número de fatalidades, ferimentos graves e consequências económicas devem ser calculados separadamente. Por outro lado, se for atribuído um valor monetário à vida humana e/ou a

cada tipo de ferimentos já se torna possível combinar as fatalidades com os ferimentos e com as perdas económicas.

7) **Gestão do Risco** (*Risk Management*) – Neste passo é determinado qual o nível de risco aceitável e a que custo. A gestão de risco é um processo que pretende compreender os riscos das decisões relativas à implementação de ações, tais como a implementação de contramedidas de segurança ou de mitigação de consequências, com o objetivo de alcançar num nível risco/ custos aceitável. A avaliação de risco é caracterizada pela identificação, avaliação e controlo dos riscos para um nível compatível com o valor atribuído ao ativo. Neste passo a IC deve:
    i) Definir potenciais alternativas de contramedidas e consequentes estratégias de mitigação, estimando o investimento e respetivos custos de operação de cada operação;
    ii) Assumindo a aplicação de tais contramedidas alternativas e consequentes estratégias de mitigação, recalcular as consequências, probabilidade de ameaça e vulnerabilidades para cada opção;
    iii) Calcular o risco, dada a consequência da opção de mitigação e subtrair o risco sem a mesma (a opção de “não fazer nada”), para assim obter o benefício de cada opção;
    iv) Calcular a relação custo/beneficio através dos passos usados nos pontos i) e iii) obtendo assim uma estimativa da quantidade de redução do risco por cada unidade de custo;
    v) Selecionar as opções que apresentam uma melhor relação benefícios /custo. Alocar os recursos financeiros, humanos, etc. necessários para implementar e operar as opções selecionadas. Deverá também ser tido em consideração o custo de oportunidade, uma vez que por cada unidade monetária investida na redução do risco, a mesma não estará disponível para ser investida nos projetos que à missão ou operação da IC dizem diretamente respeito;
    vi) Gerir a implementação e operação das opções selecionadas, avaliar a sua efetividade e modificá-las com regularidade para obtenção da eficiência máxima. O processo de análise de risco deve ser repetido periodicamente ou sempre que necessário dada a existência de novas

informações resultantes do ambiente de operação ser tendencialmente dinâmico e por conseguinte se encontrar em constante mudança;

vii) Desenvolver um plano de comunicações detalhado que esteja em vigor e com o qual todos os indivíduos, que possam potencialmente vir a ser afetados por um incidente, estejam familiarizados. O plano de comunicações deve também sofrer atualizações regulares uma vez que as próprias tecnologias de comunicação também se encontram em constante evolução. Devem ser utilizados meios de comunicação *standard* bem como variados métodos de comunicação tais como internet, telemóvel, redes sociais etc;

viii) Deverão ser considerados os planos de evacuação, se necessários, como parte integrante da resolução do risco. Os mesmos devem considerar todos os tipos razoáveis de incidentes que poderiam afetar as próprias rotas de evacuação, as estratégias de evacuação bem como os seus tempos. Estes planos devem incluir estimativas do número de indivíduos e os meios de evacuação.

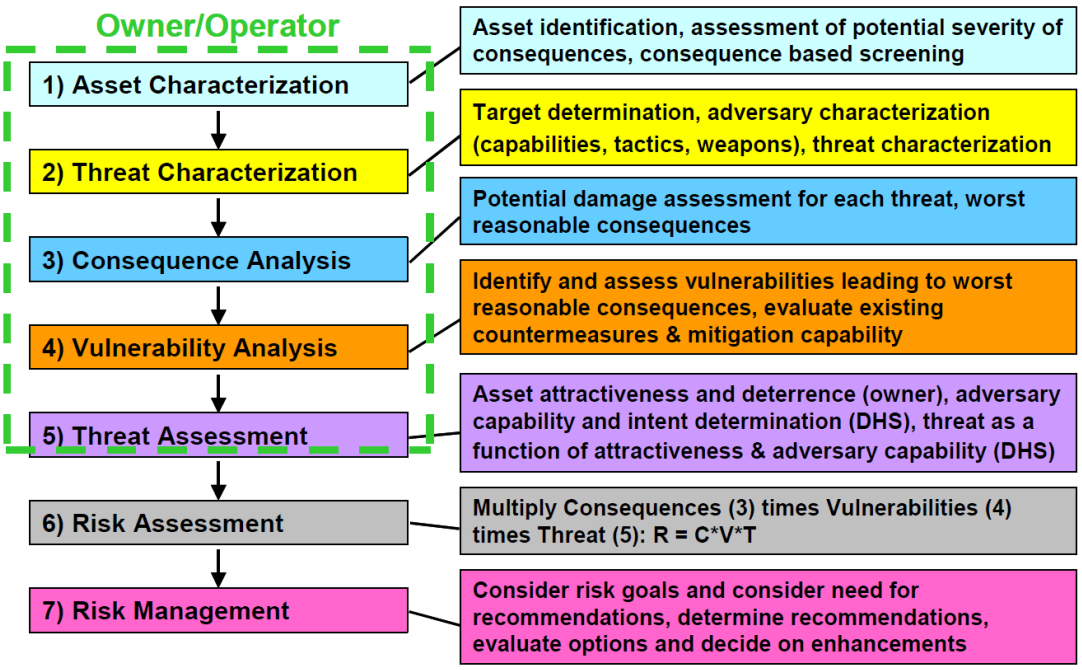

Figura 15 – Sete Passos da Metodologia RAMCAP

7 Análise

Após compilação de toda a informação contida nos capítulos anteriores, isto é, após o estudo individualizado das ICN, metodologias de proteção de ativos críticos (RAMCAP e ISO 31000) e, concretamente, dos conceitos e princípios relacionados com a ciberdefesa e cibersegurança em Portugal, existe agora a necessidade de cruzar a fundamentação teórica com a realidade. O que se pretende objetivamente é confrontar os princípios teóricos com a realidade do ambiente nacional e tirar daí conclusões com o objetivo de responder à pergunta de partida. Para tal, o capítulo de análise encontra-se dividido em duas seções, a primeira direcionada para as metodologias de proteção, ISO31000 e RAMCAP, e a segunda direcionada para a análise da cibersegurança e ciberdefesa, relacionando os dois conceitos com as duas metodologias anteriormente referidas.

7.1 Aplicação do Modelo de Análise

Tal como referido na introdução, no presente capítulo pretende-se o confronto entre a teoria recolhida e o ambiente operacional existente em Portugal verificado aquando das entrevistas. A análise é realizada de acordo com o modelo de análise inicialmente definido, com o objetivo de estudar as metodologias aplicadas na gestão de risco e proteção das ICN, analisando duas metodologias, uma para a gestão de risco, a ISO31000, e uma outra direcionada para a proteção e gestão de infraestruturas críticas, a RAMCAP. Do estudo destas duas metodologias pretende-se perceber quais os procedimentos e conceitos teóricos previstos pelas mesmas para, posteriormente, verificar se estes são, ou podem ser, aplicados pelos organismos e entidades responsáveis pela ciberdefesa e cibersegurança na proteção das ICN.

7.2 ICN, Politicas de Gestão de Risco

7.2.1 Planos de Emergência ICN

O presente trabalho de investigação tem como objeto central de estudo as ICN. Assim no capítulo 1, secção 1.1, estas são caracterizadas como instalações físicas, de tecnologia, serviços, redes ou bens que se forem interrompidos ou destruídos provocariam graves impactos em vários sectores da sociedade. Este facto justifica a necessária criação de planos de emergência e de uma abordagem de gestão do risco consentânea com a criticidade dessas infraestruturas.

Cada plano de emergência de acordo com o Decreto-Lei nº 62 de 9 de Maio de 2011 deve incluir uma análise de risco baseada em cenários de ameaça grave e tanto na vulnerabilidade de cada elemento como nos impactos potenciais. Esta análise deve ser igualmente feita à segurança dos sistemas de informação através da identificação, seleção e priorização das contramedidas e procedimentos de segurança permanentes e progressivos a ativar consoante o grau de ameaça aplicável. O objetivo da sua existência é minimizar os potenciais efeitos da perturbação ou destruição de uma IC.

Segundo o Programa Europeu de Proteção das Infraestruturas Criticas (COM 786,2006) para que, numa situação de emergência, se verifique maior eficiência e eficácia nos procedimentos de minimização e mitigação de danos e de reposição da normalidade as ICN devem permitir uma participação coordenada dos proprietários/operadores, das autoridades e entidades nacionais responsáveis, bem como o intercâmbio de informações entre países vizinhos.

7.2.2 Definição dos Critérios e Requisitos de Segurança

No quinto capítulo desenvolveu-se o estudo da ISO31000, a norma para a gestão do risco que incluí princípios e linhas de orientação recomendadas. A principal recomendação desta norma, expressa na secção 5.2 do presente trabalho, é que todas as organizações desenvolvam, implementem e mantenham em constante processo de melhoria uma estrutura cujo objetivo é integrar o processo de gestão de risco na governação, cultura, estratégia, planeamento e políticas da organização.

Na secção 5.7.3 ”Definição do Critérios de Risco” do mesmo capítulo, como parte integrante do processo de gestão do risco, é identificada a necessidade de definição dos critérios de risco em qualquer organização. Na definição dos critérios de risco deverá ser tido em consideração, entre outros, o nível de tolerância ao risco e a forma como este é definido bem como as orientações das partes interessadas. A teoria prevê ainda a existência de critérios que poderão não ser de carácter facultativo, isto é, poderão ser resultado de exigências legais ou de requisitos regulamentares subscritos pela organização.

Assim, com base na informação recolhida nas entrevistas, a entidade responsável pela elaboração dos requisitos de segurança, aos quais as ICN devem dar resposta durante a definição dos seus critérios de risco, é a ANPC, sendo que na área ciber a definição destes requisitos está prevista ser feita com o apoio do CNCS.

7.2.3 Custos Versus Medidas de Segurança

Uma vez que, de acordo com a ISO31000 e a RAMCAP, a qualquer medida de segurança ou proteção está associado um custo, devendo inclusive ser calculado a relação custo/beneficio com o objetivo de obter uma estimativa da quantidade de redução do risco por cada unidade de custo e, pressupondo que o principal objetivo do sector privado é a obtenção de lucro, sabendo que em Portugal, na generalidade, as ICN são propriedade do sector privado, foram identificadas duas abordagens cumulativas do problema.

- A autorregulação, isto é, a existência de um diálogo entre o sector público e o sector privado no sentido de encontrar o equilíbrio, onde o sector privado aceita que é para o seu interesse e para o interesse nacional os princípios e requisitos de segurança emanados pela ANPC e implementa-os.
- No caso em que o mecanismo de autorregulação não seja suficiente torna-se necessária a existência de um mecanismo que permita aplicar regras, produzir normas e garantir o seu cumprimento pelas entidades privadas.

Foi consentâneo, em todos os especialistas entrevistados, que deveria existir uma autoridade que regulasse e auditasse, relativamente ao domínio ciber, o cumprimento dos requisitos de segurança definidos, não tendo sido porém identificada a existência atual de tal entidade em Portugal, sendo ponto concordante

que essa regulação deveria ser feita pelas autoridades competentes na área tal como acontece noutros sectores mas nunca pelas FFAA.

Segundo a ISO31000 um dos passos do processo de gestão de risco é a compreensão do contexto externo das organizações. Isto inclui as relações das partes interessadas externas no que respeita aos seus valores e perceções. O objetivo desta compreensão é garantir que no momento do desenvolvimento dos critérios de risco os objetivos e preocupações de todas as partes são tidas em consideração. Pressupondo que, tanto a cibersegurança como a ciberdefesa são partes interessadas nas políticas de gestão de risco das ICN, a ciberdefesa também deverá apoiar na definição dos requisitos de segurança no domínio ciber, o que de acordo com a metodologia RAMCAP se concretiza no apoio à caracterização e avaliação da ameaça, análise de consequências e vulnerabilidades, avaliação do risco e sua gestão.

Atualmente, de acordo com o que foi apurado pelas entrevistas realizadas, o que está previsto acontecer é a ANPC elaborar os requisitos de segurança apenas com o apoio do CNCS não estando previso que as FFAA se pronunciem sobre esses mesmos requisitos.

7.3 Capacidade de Defesa e Segurança no Domínio Ciber

7.3.1 Caracterização da Capacidade

Uma capacidade do domínio militar, está tipicamente associada a uma materialização de meios, sejam eles: aeronaves, carros de combate ou navios. Ao domínio ciber falta esta componente de materialização o que coloca alguns entraves à sua verdadeira perceção, fato que foi apontado pelas entrevistas realizadas. Tal é igualmente comprovado pela teoria exposta no capítulo quatro na secção 4.1 que aos domínios de atuação na componente ciber diz respeito, uma vez que segundo o mesmo, uma das considerações a ter em conta é a necessidade de investimento público e privado, não só em tecnologia, mas também, em recursos humanos capazes de executar a monitorização, deteção, reação e gestão de segurança.

Também segundo a ISO31000, no que concerne à conceção da estrutura para gestão do risco, um dos primeiros passos é a compreensão da organização e do seu contexto o que, entre outros procedimentos, deve incluir uma avaliação dos

recursos e conhecimentos disponíveis. Refere ainda a mesma teoria que quando se fala em recursos será igualmente necessário mencionar a competência, experiência e aptidões dos recursos humanos disponíveis, sendo que no domínio ciber esta análise é particularmente importante uma vez que como já referido os recursos humanos representam um papel de particular importância.

De acordo com as entrevistas realizadas, foi também consentâneo entre os especialistas que o domínio ciber se trata de uma capacidade essencialmente de conhecimento onde a existência de um reduzido número de indivíduos altamente qualificados e especializados poderá fazer toda a diferença.

Assim quando se fala de capacidade no domínio ciber dever-se-á ter em consideração as condicionantes referidas e, apesar de os meios materiais, ou seja a tecnologia, se revelar importante tal como acontece nos outros domínios, neste, é o conhecimento uns dos fatores mais importantes.

7.3.2 Cibersegurança e Ciberdefesa

Segundo a ISO31000, outro passo da análise e gestão de risco consiste precisamente na análise e compreensão do contexto externo relativamente às relações das partes interessadas externas no que respeita aos seus valores e perceções e uma vez que, em Portugal, tanto a cibersegurança como a ciberdefesa são partes interessadas nas políticas de gestão de risco da ICN no domínio ciber, foram abordados no terceiro capítulo os dois conceitos com vista ao seu aprofundamento uma vez se tratarem de dois temas centrais da investigação e o seu estudo essencial para a correta resposta à pergunta de partida.

Segundo (HAYES,2011), no capítulo 4, a ciberdefesa depende apenas em parte do sector civil (cibersegurança), por outro lado a cibersegurança necessita de pesquisa e de capacidades da ciberdefesa. Os ataques e as ameaças internacionais poderão necessitar da intervenção de ambos, tendo em conta que tanto as ferramentas de proteção da informação como os treinos e exercícios são semelhantes e os especialistas de uma área podem cooperar com a outra. Outra ideia relevante retirada do quarto capítulo é a estreita relação verificada entre a segurança e a defesa nacional também no domínio ciber, isto é, a ciberdefesa e a cibersegurança revelam-se também indissociáveis, não se conseguindo garantir a capacidade de cibersegurança sem o levantamento de uma capacidade de

ciberdefesa e vice-versa, devendo por isso existir um ambiente cooperativo entre as duas entidades.

Segundo a opinião de alguns especialistas entrevistados a ciberdefesa inclui tudo o que a cibersegurança inclui no que à proteção dos sistemas diz respeito, adicionando a capacidade ofensiva, a CNA (Computer Network Atack) e CNE (Computer Network Exploitation) no contexto de operações militares. Faz parte da missão das FFAA proteger os seus sistemas de qualquer ameaça. A ciberdefesa não é apenas uma componente da cibersegurança, indo mais além que a proteção e segurança dos sistemas próprios. (MELO, 2015)

As FFAA para além de garantirem a cibersegurança dos seus sistemas, utilizam o ciberespaço como um novo domínio operacional, podendo nele combater, à semelhança do que já acontece nos restantes domínios operacionais: terra, mar, ar. Como tal a utilização da violência armada no ciberespaço no decorrer de operações militares é uma competência própria e exclusiva das FFAA e consequentemente da ciberdefesa. Estas intervirão no ciberespaço sempre que esteja em causa a defesa e proteção dos seus sistemas militares ou a soberania nacional.

Fora do âmbito estritamente militar, a intervenção das FFAA apenas pode ocorrer nos termos da lei, tal como acontece noutras situações, nos três estados de exceção previstos: estado de sítio, estado de guerra e estado de calamidade pública. (MELO, 2015) Significa assim, que na eventualidade de um ataque por parte de um inimigo externo, inimigo esse que segundo a opinião consentânea dos especialistas entrevistados é de difícil identificação (SANTOS, 2014) (MELO, 2015) (CCD, 2015), as consequências do mesmo podem ser divididas em três cenários generalistas:

- O comprometimento das capacidades das FFAA (causa bélica);
- Uma calamidade pública (as IC são atingidas);
- Uma situação de Estado de Sítio (em que o governo é atingido e o país torna-se ingovernável devido a um ciberataque).

Em qualquer uma destas situações a Constituição da República diz que o empenho das FFAA faz-se por ordem direta do poder político. (MELO, 2015)

As FFAA devem executar portanto uma monitorização constante de todo o ciberespaço com o principal objetivo de defenderem os seus próprios sistemas. Dessa monitorização, caso surjam dados indicadores de uma potencial ameaça a uma ICN a ciberdefesa deverá comunica-los uma vez que também tem um papel cooperante com a proteção das ICN. As FFAA detém ainda a responsabilidade de atuar nos três regimes de exceção e a exclusividade legal do uso da força no domínio ciber, isto é, executar operações de CNA e CNE.

7.3.3 Quatro Domínios de Atuação

Aquando da realização das entrevistas foi consensual a ideia de que a melhor forma de compreender as missões e responsabilidades da cibersegurança e da ciberdefesa seria pelo estabelecimento de uma relação com o que acontece atualmente com a segurança e com a defesa, estabelecendo igualmente um paralelismo com a ameaça terrorista uma vez que estas se tratam de ameaças maioritariamente assimétricas e provenientes de atores estatais e não estatais. Assim as funções de combate ao cibercrime, que correspondem no mundo real ao combate ao crime, são responsabilidade das forças de segurança, as missões, no mundo real, de defesa do estado contra ameaças externas e que são da responsabilidade das FFAA, também no ciberespaço lhe ficam atribuídas, ou seja, as FFAA, são responsáveis pela defesa militar do ciberespaço.

Em paralelo, tal como referido no quarto capítulo secção 4.1, para o combate aos ciberataques podem ser considerados três domínios de atuação: o domínio da proteção simples, da prossecução criminal e da defesa do estado.

No domínio da proteção simples os ataques são caraterizados como ameaças à disponibilidade, integridade e confidencialidade da informação e de outros ativos, assim os objetivos da proteção simples são os de proteger potenciais alvos contra ciberataques, em termos legais e constitucionais pretende-se a salvaguarda dos direitos individuais e da privacidade dos cidadãos sendo os principais atores deste domínio os técnicos de sistemas e de redes, a própria industria das TIC, as autoridades reguladoras sectoriais, os fórum CSIRT e os próprios utilizadores TIC.

Já no domínio da prossecução criminal, os ciberataques são vistos como atos criminalmente relevantes, sendo os objetivos deste domínio prevenir crimes e

identificar, julgar e condenar os seus responsáveis, a legislação aplicada são as regras normais do sistema judicial sendo os principais atores os órgãos de polícia criminal, o ministério público e os magistrados judiciais.

Do domínio da defesa do estado os ciberataques são vistos como um ato de guerra que poderá pôr em risco o funcionamento do mesmo, sendo objetivos deste domínio a eliminação da ameaça que coloca em causa a soberania nacional ou o ganho de superioridade também no domínio ciber relativamente a um dado inimigo. Para tal a atuação neste domínio está sujeita aos termos previstos na Constituição da República, na Lei do Estado de Sitio e do Estado de Guerra bem como no Direito Internacional dos Conflitos Armados e dos Direitos Humanos, os seus atores são as FFAA e os serviços de informação.

Adicionalmente foi sugerido um quarto domínio por alguns dos especialistas nacionais entrevistados: o domínio diplomático, onde se incluem a título exemplificativo as políticas de não proliferação de ciberarmas, diretivas europeias de cibersegurança, entre outros.

É o conjunto destes quatro domínios que deve constituir a capacidade de cibersegurança e ciberdefesa nacional, isto é, os quatro domínios devem funcionar de forma colaborativa e integrada para que todo o processo de segurança e defesa também no domínio ciber aconteça de forma eficiente e eficaz.

7.3.4 Formação e Qualificação no Domínio Ciber

Tal como referido na secção 5.3.1 referente à avaliação do contexto interno das organizações, a ISO 31000, refere que um dos fatores a ter em conta num processo gestão do risco são os recursos e conhecimento existentes. Sendo na secção 5.3.5 do mesmo capítulo, recursos, entendidos, não só mas também, como competência, experiência e as aptidões existentes nos recursos humanos disponíveis bem como apontada a necessidade de disponibilização de programas de formação.

Assim, em conformidade com a teoria anteriormente referida, todos os especialistas entrevistados apontaram também a formação como um elemento chave no domínio ciber tendo sido verificada uma escassez de recursos humanos qualificados a nível mundial dado este ser um domínio recente. A questão da falta de recursos humanos qualificados agrava-se, segundo a visão da ciberdefesa, uma

vez que, conforme referido, esta para além de ter de possuir todas as capacidades da cibersegurança necessita ainda de adquirir a capacidade de CNE e CNA. Com vista a que as FFAA adquiram este nível de capacidade existe a necessidade de qualificar mais recursos humanos com estas competências. Processo que poderá ser facilitado dada a futura instalação da escola de sistemas de comunicação e informações da NATO em Portugal transferida de Itália.

As FFAA têm recursos humanos, qualificados na área de sistemas de informação, comunicação e tecnologias. A partir do momento em que passam a existir operações militares também no domínio ciber, torna-se imperativo a existência de uma adaptação dos planos de formação dos recursos humanos, tal como acontece nos outros domínios. Desenvolver CNO é uma componente idêntica a operar um sistema de armas e por isso implica uma qualificação intensiva que, neste momento, não só em Portugal como nos restantes países, ainda se está a ser desenvolvida. Ainda não existe uma tipificação de um modelo que defina quais as qualificações mínimas para que seja possível operar eficazmente um sistema de armas ciber.

Sendo a formação apontada como um requisito chave do domínio ciber dada a importância que o conhecimento assume no referido domínio, as FFAA, apesar de possuírem alguns recursos humanos com a formação base em sistemas de informação, comunicação e tecnologias necessitam agora, dada a especificidade e exigência da condução de CNE e CNA, de adaptar, não só os planos de formação, como também as carreiras dos militares envolvidos para que estes possam atingir essa capacidade.

O presente capítulo de análise, encontrando-se dividido em duas seções, a primeira direcionada para as metodologias de proteção e gestão do risco, ISO31000 e RAMCAP, e a segunda direcionada para a análise da cibersegurança e ciberdefesa, permitiu a interligação destes quatro conceitos base de todo o trabalho. Desta interligação, isto é, ao cruzar as metodologias de gestão e proteção de ICN, que nos fornecem os procedimentos teóricos que devem ser seguidos, com a teoria abordada relativamente às ICN, bem como à ciberdefesa e cibersegurança e ainda com a informação retirada das entrevistas realizadas, permitiu a obtenção das conclusões necessárias para a resposta à pergunta de partida no capítulo seguinte.

8 Conclusão e Recomendações

Neste capítulo são apresentadas as conclusões resultantes de todo o levantamento teórico bem como do ambiente operacional no domínio ciber em Portugal. Pretende-se, com recurso à análise feita no capítulo anterior, dar resposta às questões e hipóteses colocadas aquando da introdução. Será ainda feito inicialmente um apanhado dos conceitos chave indispensáveis para a correta perceção desta dissertação de mestrado. Serão igualmente sistematizados os pressupostos assumidos para a realização da investigação bem como apresentadas algumas recomendações para trabalhos futuros.

8.1 Conclusão

A elaboração deste trabalho passou por várias fases cujo objetivo final era o de reunir informação pertinente e necessária com recurso à maior variedade possível de fontes de informação, o que incluiu o testemunho de especialistas no domínio da cibersegurança e ciberdefesa em Portugal.

A fim de proporcionar uma resposta objetiva e clara à pergunta de partida, primeiramente foram definidas as linhas orientadoras de toda a investigação, alguns conceitos introdutórios, bem como a já referida pergunta de partida e hipótese de trabalho. Foi ainda explicado o que motivou a realização deste trabalho e indicada a metodologia a ser seguida. Assim, foi assumida inicialmente a seguinte hipótese de trabalho;

"As Forças Armadas têm espaço para contribuir para a Cibersegurança das Infraestruturas Críticas Nacionais"

Foi igualmente definida a questão que definiu toda a linha condutora de desenvolvimento deste trabalho de investigação;

"As Forças Armadas têm espaço para contribuir para a Cibersegurança das Infraestruturas Críticas Nacionais?"

Posteriormente, com o âmbito e metodologia definidos iniciou-se um levantamento dos conceitos já existentes no âmbito da GI, a revisão da literatura, onde toda a temática relacionada com o tema foi contextualizada de acordo com o modelo de Quivy Campenhoudt. Desta forma foi adquirido conhecimento e teoria de base que permitiu o desenvolvimento de toda a restante investigação. Nesta fase foi abordado o conceito de GI, sendo o mesmo definido e interligado com as diversas áreas de ação transversais, tais como, *Intelligence*, Guerra Centrada em Rede, Guerra de Quarta Geração, *Information Assurance* e depois mais direcionadas para o tema em questão, Guerra Cibernética, Ciberataque, Ciberdefesa e Cibersegurança de forma a contextualizar o panorama atual.

Depois de todo o desenvolvimento onde, de acordo com a metodologia, foram abordadas as temáticas, ciberdefesa, cibersegurança, ICN e as metodologias ISO31000 e RAMCAP, é no capítulo 7, capítulo esse dedicado à análise, que são relacionados todos os conceitos, pretendendo-se nessa fase estabelecer um cruzamento de toda a teoria recolhida, compilada e tratada, com a realidade apurada aquando da realização das entrevistas. Nessa análise foi possível confrontar os princípios teóricos com ambiente nacional, isto é, tratou-se de um cruzamento de toda a informação com o objetivo de perceber em que medida as metodologias de proteção de ICN identificadas (ISO31000 e RAMCAP) interagem no contexto da ciberdefesa e da cibersegurança e vice-versa. Do cruzamento dos dados efetuados durante a análise retiram-se as seguintes conclusões intermédias:

- ✓ Cada IC é legalmente obrigada a deter um plano de emergência que dê resposta, entre outros, aos requisitos de segurança exigidos pela ANPC;
- ✓ Em matéria de cibersegurança está previsto esses mesmos requisitos serem definidos com o apoio do CNCS;
- ✓ As ICN devem permitir uma participação coordenada entre os seus proprietários/operadores e as autoridades nacionais responsáveis, bem como requisitarem o apoio do CNCS sempre que necessário;
- ✓ Sendo que, qualquer medida de segurança representa um custo e a maioria das ICN são operadas por entidades privadas cujo um dos principais objetivos se trata da obtenção de lucro, seria pertinente a existência de uma autoridade reguladora também no domínio ciber que auditasse o cumprimento dos requisitos definidos;

- ✓ A ciberdefesa, como parte interessada na defesa das ICN, deveria também, juntamente com a cibersegurança e com a ANPC, apoiar a definição dos requisitos de segurança a serem posteriormente cumpridos pelas ICN;
- ✓ A capacidade no domínio ciber é uma capacidade diferente das habituais, uma vez que não se consubstancia numa materialização de meios, sendo um dos fatores mais relevantes a existência de recursos humanos qualificados;
- ✓ Tal como acontece nos restantes domínios operacionais (ar, terra, mar e espaço) a cibersegurança e ciberdefesa são indissociáveis, sendo compaginável com o que acontece entre a segurança e a defesa;
- ✓ A ciberdefesa abrange todos os aspetos relacionados com cibersegurança e ainda cumulativamente a componente de CNA e CNE;
- ✓ A utilização de violência armada no ciberespaço, no decorrer de operações militares ou não, é uma competência própria e exclusiva das FFAA e consequentemente da ciberdefesa;
- ✓ Fora do âmbito estritamente militar a intervenção das FFAA apenas está prevista ocorrer nos termos da lei, nos três estados de exceção previstos, estado de sítio, estado de guerra e estado de calamidade pública;
- ✓ Verifica-se um número reduzido de recursos humanos qualificados na área ciber, situação que se agrava na área da ciberdefesa uma vez que os próprios Ramos ainda não possuem uma carreira especifica para a área da ciberdefesa, e os planos de formação ainda não estão elaborados nem mesmo ao nível NATO, não estando definidos os requisitos de formação necessários para certificar um operador de ciberdefesa.
- ✓ Atualmente a condução de CNA apenas está prevista no âmbito de uma operação militar de maior espetro sendo a ciberdefesa mais uma ferramenta ao dispor das chefias militares.

Estas conclusões têm como base os seguintes pressupostos, assumidos no início deste trabalho:

- Atualmente as sociedades mais desenvolvidas encontram-se tendencialmente estruturadas em rede, levando assim à construção do ciberespaço;

- O estado deve procurar garantir e aumentar a segurança das ICN, em colaboração direta com os operadores dessas mesmas infraestruturas.
- As ICN utilizam como referência a metodologia RAMCAP;
- Tanto a ciberdefesa como a cibersegurança são partes interessadas na proteção das ICN;

Podemos então, a partir das conclusões intermédias acima referidas, responder à pergunta de investigação definida inicialmente.

"As Forças Armadas têm espaço para contribuir para a Cibersegurança das Infraestruturas Críticas Nacionais?"

Dada a dificuldade existente em identificar a origem da ameaça no domínio ciber (secção 7.2.2) bem como os seus impactos face à sua natureza assimétrica e transversal, (secção 7.2.3) e uma vez que as FFAA serão chamadas a atuar contra uma ameaça externa ou contra qualquer outra que pelos seus impactos coloque em causa a Soberania Nacional (secção 7.2.2), as FFAA deverão também assegurar o desenvolvimento de capacidades e a criação de competências no domínio da ciberdefesa que tornem possível a proteção das infraestruturas de informação críticas e o governo eletrónico do Estado.

O ciberespaço constitui em si um novo domínio de interação social, onde, tal como se verifica nos restantes domínios de interação social, se torna necessário identificar o papel a desempenhar pelos diversos órgãos, públicos e privados, na garantia da sua proteção e utilização segura. Para tal é recomendada uma tentativa de avaliação do impacto dos diversos tipos de ataques cibernéticos, bem como o risco social associado a cada ameaça, separando os de motivação criminosa, que se enquadram essencialmente nas atribuições da cibersegurança, daqueles que, por apresentarem, entre outras, características como um maior poder disruptivo, alcance ou magnitude, possam colocar em risco a segurança e defesa do Estado e que como tal se enquadram na missão e atribuições da ciberdefesa, exigindo uma participação ativa das FFAA.

Assim, respondendo agora à pergunta de partida, resposta essa apoiada em dados objetivos e tratados no capítulo da análise e agora sintetizados e sistematizados na conclusão.

As FFAA participam na segurança das ICN no domínio ciber da mesma forma que o fazem no domínio aéreo, terrestre, naval e espacial. A defesa do ciberespaço deverá ser feita de forma colaborativa (secção 7.2.3), isto é, apesar da cibersegurança das ICN se encontrar mais enquadrada nas missões e atribuições do CNCS, que uma vez solicitado estará disponível para prestar o apoio necessário, e apoiará a ANPC na definição dos requisitos de segurança, as FFAA, como elemento que, com a missão primária da defesa dos seus próprios sistemas, monitoriza o ciberespaço, tendo conhecimento de uma ameaça às ICN deverá comunicar a referida informação às entidades competentes uma vez que faz parte das suas missões a cooperação com as entidades nacionais responsáveis pela cibersegurança, ciberespionagem, cibercrime e ciberterrorismo.

Assim, a defesa do Estado Português contra ameaças externas bem como a atuação nas três situações de exceção previstas (Calamidade Pública, Estado de Sitio ou Guerra) de forma a ser assegurado o regular funcionamento das instituições democráticas e o exercício das funções de soberania do Estado, são responsabilidades atribuídas pela Constituição da República Portuguesa às FFAA, sendo estas o único órgão legalmente capaz de executar CNA e CNE.

8.2 Recomendações e Futuras Contribuições

No seguimento da presente dissertação de mestrado, surgiram perspetivas de análise que poderão ser objeto de estudo no futuro, nomeadamente;

- No contexto da Força Aérea, perceber se um ataque à rede interna, RIGFA, rede não segura, teria ou não impacto na rede segura da Força Aérea.
- No contexto da cibersegurança nacional, estudar a obrigatoriedade ou não do cumprimento da norma ISO 27001*"Information Security Management"* por todas as ICN.

9 Referências Bibliográficas

ALBERTS, David S.; GARSTKA John J.; Stein Frederick P. - ***Network-Centric Warfare: Developing and Leveraging Information Superiority*.** CCRP Publication Series, 1999.

ALBERTS, David S.; GARSTKA John J.; HAYES, Richard E.; SIGNATORI and David T. – **Understanding Information Age Warfare**. Washington DC - EUA: CCRP Publication Series, 2001.

ASME- **A Risk Analysis Standard for Natural and Man-Made Hazards to Higher Education Institutions**, ISBN 9780791859636, 2005

ARQUILLA, RONEFELDT; John, David **– *Swarming and the Future of Conflict***. ISBN 0-8330-2885-5 RAND, 2000.

BATISTA, Gonçalo [et al] - **Ciberterrorismo: a nova forma de crime do sec. XXI, como combatê-lo?** Revista da Academia Militar Proelium, 2003.

BILLO, Charles; CHANG, Welton **– An Analysis of the Means and Motivations of Selected Nations States**. Institute for Security Technology Studies, Dartmouth College, 2004.

CARRIÇO, Alexandre, coord. – **Estratégia da Informação e Segurança da Informação: Investigação Conjunta IDN-CESEDEN**, Lisboa, 2013, ISBN 978-972-27-2272-8.

CEBROWSKI, Arthur K., US NAVY **– The Implementation of Network-Centric Warfare**. 2005.

CEDN- **Conceito Estratégico de Defesa Nacional**, Resolução do Conselho de Ministros Nº 19 de 2013, D.R. I Série B, 2013-04-05, 2013

COLEMAN, Kevin -.***Iranian Cyber Warfare Threat Assessment***. September, 2008.

CIVIL, A. N. (2012). *Infraestrutuas Criticas*. Obtido de Autoridade Nacional de Proteção Civil: http://www.prociv.pt/RiscosVulnerabilidades/Pages/InfraestruturasCriticas.aspx

COMISSÃO DAS COMUNIDADES EUROPEIAS: Comunicação da comissão ao conselho e ao parlamento europeu: **Proteção das infraestruturas criticas no âmbito da luta contra o terrorismo**, Bruxelas,2004

COMISSÃO DAS COMUNIDADES EUROPEIAS: Comunicação da Comissão **relativa a um Programa Europeu de Proteção das Infraestruturas Críticas**, Bruxelas, 2006

DECRETO-LEI N.º 49/2008. D.R. I Série. 89 (2008-09-19)

DECRETO-LEI N.º 62/2011. D.R. I Série. 89 (2011-05-09)

DECRETO-LEI N.º 69/2014. D.R. I Série. 89 (2014-05-09)

DECRETO-LEI N.º 289/2014. D.R. I Série. 250 (2014-12-29)

DEPARTMENT OF DEFENCE REPORT TO CONGRESS **– Network Centric Warfare**. 27 July, 2001.

DESPACHO nº 136921/2013. D.R II Série. 208 (2013-09-28)

DESPACHO nº 13687/2013. D.R II Série. 208 (2013-09-28)

DINIS, José António Henriques **– A Guerra de Informação: Perspetivas de Segurança e Competitividade**. Revista Militar [Em linha]. 2009. [Consult. 20 Nov. 2015]. Disponível em WWW: <http://www.revistamilitar.pt/modules/articles/article.php?id=401>

ELLIS, Rod et al. "Implicit and Explicit Knowledge in Second Language Learning, Testing and Teaching. Grã-Bretanha: Short Run Press, 2009.

FM 100-6 – **Information Operations**. *August*, 1996.

HAMILL, Jonathan – **Modeling Information Assurance: A Value Focused Thinking Approach.** Wright-Patterson Air Force Base, Ohio, 2000.

HAYES, Richard E. - ***Cybersecurity and National Cyberdefense****:* ***Capability Development, Solutions, and Initiatives****,* ***Information Assurance:*** *Synergies and Integrated Efforts Between Cybersecurity and Cyberdefense*. 5 MAY, 2011 [Consult.1 Dez. 2014]. Disponível em www: http://www.ebrinc.com/files/hayes_information_assurance.pdf

ITU – ***ITU National Cyber Security Strategy Guide*****.** International Telecommunication Union, Switzerland, Geneva, 2012.

JAMISON, Edward **– Intelligence Strategiy for Fourth generation Warfare.** U.S. Army War College, Carlisle Barracks, Pennsylvania, 2006.

JOINT PUB 1-02 – ***Department of Defense Dictionary of Military and Associated Terms***. Estados Unidos da América: Joint Chiefs of Staff, 2001.

JP 2-0 – ***Joint Intellinge***. *USA: Chairman of the Join Chiefs of Staff (Joint Publication* 2-0, 22 *June* 2007), 2007.

JOINT PUB 3-13 **– Joint Doctrine for Information Operations**. USA: Joint Chiefs of Staff (Joint Publication 3-13, 9October1998), 1998.

JOINT PUB 3-24 **– Counterinsurgency Operations.** USA: Joint Chiefs of Staff (Joint Publication 3-24, 5October2009), 2009.

KHAN, Amos – **A Response to Fourth Generation Warfare.** S. Rajaratnam School of International Studies, Singapure, 2010.

KLIMBURG, Alexander (Ed.), **National Cyber Security Framework Manual**, NATO CCD COE Publication,Tallinn, 2012, ISBN 978-9949-9211-2-6

KUEHL, Dan - ***From Cyberspace to Cyberpower: Defining the Problem.*** Information Resources, Management College, National Defense University, 2009.

LEI ORGÂNICA N.º 1-A/2009. D.R. I Série, Suplemento. 129 (2009-07-07)

LIBICKI, Martin **– Cyberdeterrence and Cyberwar**. RAND Corporation, 2009. ISBN 978-0-8330-4734-2

LIND, William **– Understanding Fourth Generation War.** Military Review, September-October, 2004.

MOLANDER, Roger et al. "Strategic Information Warfare: A New Face of War". Santa Monica: Rand, 1996.

MOTEFF, John; PARFOMAK, Paul - ***Critical Infrastructure and Key Assets: Definition and Identification****. CRS Report for Congress*, 2004.

NP ISO 31000. 2013, Gestão do Risco: Principios e linhas de orientação; Monte de Caparica: IPQ.

PARK, C. Whan; JAWORSKI, Bernard J.; MACLNNIS, Deborah J. – ***Strategic Brand Concept – Image Management***. *In Journal of Marketing*, 1986. Vol. 50 p. 135-145

POLANYI, Michael. "The Tacit Dimension. Chicago: The University of Chicago Press, 1966.

QUIVY, Raymond e CAMPENHOUDT, Luc Van - **Manual de Investigação em Ciências Sociais**. 2ª Edição, Lisboa: Gradiva, 1998.

RFA 390-6 **– Política de Ciberdefesa da Força Aérea.** Fevereiro, 2011.

RIBEIRO, T. Cor. Carlos O. **– Guerra Centrada em Rede - Um conceito Operacional Emergente no século XXI. Proelium** - Revista da academia militar, 2008.

SANTOS, José **– Estratégia e Segurança Nacional na Era da Informação.** Revista Militar, 2005.

SANTOS, Lino; BRAVO, Rogério; NUNES, Paulo Viegas- **Proteção do Ciberespaço: Visão Analítica.** Lisboa: Edições Salamandra, 2012. ISBN 978-972-689-247-2

SANTOS, Lino. (2014). Centro Nacional de CIbersegurança. (E. Silva, Entrevistador)

WALTZ, Edward – ***Information warfare: principles and operations***. Boston, London: Artech House, Inc., 1998. ISBN 0-89006-511-X

10 Anexo A – Entrevistas

10.1 Entrevista a Sua Excelência Sr. Major General Pedro Melo

(Este texto, de propósitos académicos, não reflete de forma integral a referida entrevista, sendo apenas válido quando ao conteúdo e não quanto à forma)

P:Concorda com a afirmação de que, em matéria de ciberdefesa o papel das FFAA é proteger os seus próprios sistemas e estar preparada para atuar nos três regimes de exceção previstos (estado de sitio, emergência ou calamidade)?

R:A ciberdefesa, da forma como está definida, tem como alvo principal a defesa dos sistemas de informação das FFAA e da própria Defesa Nacional. Está definido que no Ministério da Defesa Nacional as infraestruturas de defesa são também alvo de proteção especial pelas FFAA. Estes são os alvos principais, mas como a ciberdefesa, para proteger as FFAA, tem que se possuir um conhecimento profundo do ciberespaço, não só das ameaças, mas também das principais e das melhores estratégias de defesa, as FFAA em casos normais poderão eventualmente antecipar um ataque muito antes de qualquer outra organização e deverão comunicar essa ameaça aos outros CIRCS nacionais que, de forma colaborativa, podem partilhar a informação entre si. Isto é, se for identificado um ataque pelas FFAA e se for percebido que o alvo desse ataque possa ser uma ICN é óbvio que as FFAA e o CCD não vão ficar parados à espera que o ataque se concretize, comunicará certamente essa informação ao CNCS ou à entidade que seja responsável pela sua segurança. É muito difícil no ciberespaço compartimentar se um ataque é apenas dirigido ao sistema A,B ou C. As FFAA ao protegerem os seus sistemas podem identificar ataques que outras entidades podem não detetar e vice-versa. É fácil compartimentar quando se fala de estruturas físicas mas no ciberespaço é mais complexo pois não há fronteiras físicas. As FFAA, segundo a lei, estão vocacionadas para responder a ataques externos. A questão que se coloca é se um ataque perpetrado a partir do outro lado do mundo é um ataque interno ou externo e

se neste caso quem teria que defender esse ataque seriam as FFAA. As coisas não são assim tão simples. Tudo está relacionado com a natureza, dimensão e tipo de ataque, ou seja: no domínio aéreo, terrestre e naval é relativamente fácil identificar qual a natureza do ataque e perceber se é interno ou externo e assim perceber qual o papel das FFAA. No domínio ciber não é bem assim, é muito difícil identificar o que está a acontecer, não fazendo sentido definir que no caso de um ataque a uma ICN quem responde é o CNCS e só no caso de a situação evoluir para uma das três situações previstas a responsabilidade passará para as FFAA. Não deverá ser um processo hierárquico, deverá sim ser uma malha, a defesa do ciberespaço é colaborativa, quem identificar primeiro o ataque deverá dar resposta, alertar e colaborar na respetiva defesa.

P2: Existe a opinião de que o que ditava a intervenção ou não das FFAA não seria tanto a dificuldade, nem a dimensão, nem o tipo de ataque, seriam sim as consequências do ataque. Se por força do ataque fosse decretado um dos três estados de exceção seriam acionadas as FFAA. Concorda?

R:Não concordo. Há coisas distintas. Quando é para defender podemos dizer que a ciberdefesa tem uma componente de proteção ou cibersegurança se assim lhe quisermos chamar. A ciberdefesa inclui tudo o que a cibersegurança tem no capítulo da proteção dos sistemas, adicionando mais a capacidade ofensiva, a CNA (Computer Network Atack) e CNE (Computer Network Exploitation) no contexto de operações militares. Faz parte da missão das FFAA proteger os seus sistemas de qualquer ameaça. A ciberdefesa não é uma componente da cibersegurança, indo mais além que a proteção e segurança dos sistemas da FFAA. As FFAA para além de fazerem a cibersegurança dos seus sistemas, utilizam o ciberespaço como um novo domínio operacional, podendo combater no ciberespaço, à semelhança do que já acontece nos outros domínios operacionais: terra, mar e ar. Como tal a utilização da violência armada no ciberespaço no decorrer de operações militares é uma competência própria e exclusiva das FFAA. As FFAA intervirão no ciberespaço sempre que em causa esteja a defesa e proteção dos seus sistemas. Nenhuma outra organização externa às FFAA tem a missão de proteger os sistemas militares. A intervenção das FFAA fora do âmbito militar apenas pode ocorrer nos termos da lei.

P:As FFAA terão capacidade de desenvolver CNO?

R:Começando por clarificar o conceito CNO (Computer Network Operations), e seguindo a doutrina americana, estas operações dividem-se em CND (Computer Network Defense),CNA (Computer Network Atack) e CNE (Computer Network Exploitation). A criação do CCD visa precisamente o desenvolvimento das CNO. Há já muito tempo que as FFAA praticam ações de cibersegurança,desde que usamos computadores. Os nossos sistemas são dos sistemas melhor protegidos em Portugal pois são sistemas relativamente mais fechados, em que muitos deles estão desligados da internet. Com a organização da ciberdefesa, nomeadamente a criação do CCD, iremos mais longe, teremos um conhecimento mais profundo, não só da defesa como também do ataque. Porque para saber defender bem temos de saber como o adversário pode conduzir o ataque. Será fundamental para as ações militares no futuro saber degradar a capacidade de comando e controlo do adversário. Podemos estar no princípio de um domínio novo tão importante que não admira que daqui a uns anos para termos sucesso num conflito, tal só será possível com a existência de supremacia no domínio do ciberespaço. O CCD não compete com o CNCS. A sua missão é distinta e não sobreponível com a missão do CNCS, Terá sim que existir um relacionamento institucional colaborativo entre ambos.

O ciberespaço é um novo domínio operacional em que quem lá combate não é a Força Aérea, não é a Marinha, não é o Exército, são outros militares, embora oriundos dos três Ramos. Para percebemos quem deveria ser o responsável pela ciberdefesa por um lado e da cibersegurança por outro, basta analisar o que acontece nos outros domínios operacionais relativamente a este assunto. À semelhança do que acontece com o domínio aéreo, marítimo e naval, quem manda na ciberdefesa é o comandante das FFAA. Se por outro lado, perguntarmos quem defende as ICN em termos das ameaças vindas do ciberespaço teremos que de ver o que a lei diz, no diz respeito aos restantes domínios operacionais, terra, mar e ar. Lembro que há uns anos atrás as FFAA tinham uma incumbência para defender as ICN e existiam planos para essa defesa que eram regularmente treinados. Era uma missão que estava atribuída as FFAA. Neste momento não está, as FFAA não têm como missão primeira defender as ICN, exceto se forem chamadas a intervir. Na ciberdefesa deve seguir-se o mesmo paradigma. Quando existe um acontecimento

no ciberespaço, que pela sua dimensão ou característica ultrapassa as capacidades de qualquer outra organização civil ou se simplesmente for necessário o apoio das FFAA, é dada ordem a estas para a atuar. O que as FFAA poderão ter, é a vantagem de estarem melhor preparadas e informadas e poderem antecipar se o ataque poderá ocorrer, uma vez que para nos defendermos de uma ameaça em qualquer domínio, temos que saber previamente quais são as ameaças, quem é o inimigo o tipo de armamento e nesse aspeto estaremos melhor preparados. Não devemos nunca cair na simplicidade de pensar que a cibersegurança é o mesmo que a ciberdefesa. A missão do CCD é diferente e não concorre com a missão do CNCS. Poderá colaborar, terá informação que poderá ser útil para a defesa dos sistemas nacionais e essa informação tem que fluir com o CNCS e vice-versa. Não deve existir qualquer tipo de competição entre cibersegurança e ciberdefesa sendo duas componentes do sistema de defesa de Portugal no domínio do ciberespaço.

P:Sendo a maior parte das ICN operadas por entidades privadas cujo principal objetivo é a obtenção de lucro, e uma vez que as soluções de segurança estão sempre associadas a um custo, entende que deveria existir uma entidade externa que auditasse e regulasse o cumprimento dos requisitos de cibersegurança ou dos planos de segurança em termos gerais?

R:A regulamentação tem que existir, tal como existe noutros sectores. Na área da cibersegurança também deverão existir requisitos que deveriam ser cumpridos pelas ICN. Em termos de fiscalização desses requisitos esta deveria ser feita pelas entidades fiscalizadoras e nunca pelas FFAA. A analogia tem de ser feita da mesma forma como é feita para as outras áreas da vida em sociedade.

P:Qual a sua opinião sobre a eventual criação de um novo Ramo para o domínio ciber?

R:Em termos conceptuais, no futuro, a área ciber poderá vir a ser autonomizada pela importância que tem. O facto de falarmos em novo Ramo é exagerado. Cada vez mais temos de deixar cair a palavra Ramo e passar a ver as FFAA como um corpo único com várias componentes, a componente naval, terrestre, aérea e uma componente ciberespaço. As FFAA podem funcionar bem sem uma divisão

estanque dos Ramos, dai que na área da ciberdefesa os militares que trabalham neste domínio são recrutados e formados pelos Ramos, sendo a sua carreira regulada pelo ramo exercendo os militares funções no CCD. A criação de um ramo que tivesse necessidade de fazer recrutamento, formação, etc. é absurdo, não há dimensão.

P:O CCD reúne as capacidades humanas e técnicas necessárias para ser o último reduto da defesa do estado?

R:O CCD não é a última barreira, é a primeira. E terá essa capacidade, teremos um grande suporte de tecnologia para o conseguirmos fazer.

P:Concorda com afirmação de que capacidade do domínio ciber é uma capacidade diferente das habituais, isto é, por norma é comum, quando se pensa em capacidade, associar-se uma materialização direta de meios sejam eles aeronaves, carros de combate ou navios, o que não é o caso da capacidade ciber pois esta trata-se de uma capacidade de conhecimento intensivo onde a existência de um reduzido número de indivíduos altamente qualificados poderá fazer toda a diferença.

R:Concordo, não é ter muitos recursos financeiros para se adquirir toda a tecnologia que existe disponível que per-si fará a capacidade. O que é necessário é a existência de especialistas. O conhecimento é o mais importante. Temos de recorrer a sensores e tecnologia que nos permitam ter uma *"picture"* do ciberespaço e depois sim, ter recursos humanos que nos permitam interpretar essa mesma *"picture"* e tomar decisões no ciberespaço. São áreas em que a formação demora muitos anos e está em constante mudança e evolução.

P:É possível falar numa única autoridade nacional esta área?

R:Autoridade única no país há uma, o Sr. Presidente da República. No que respeita à ciberdefesa, se tivermos dúvidas, ela deve ser organizada como o que acontece nos outros domínios operacionais, terra, mar e ar. A legislação em vigor é clara na organização das responsabilidades atribuídas às FFAA e quem a chefia. No caso da

ciberdefesa é o CEMGFA que tem a competência sobre a utilização deste domínio operacional no decurso de operações militares... No caso da cibersegurança, a legislação entretanto publicada atribui responsabilidades ao CNCS no ciberespaço, assim como, lembrando que existem outras áreas cujas entidades terá responsabilidades na defesa do ciberespaço, como referências ao cibercrime e ciberespionagem, entre outras. Não vejo razão para não se utilizarem as estruturas nacionais já existentes a nível de direção, para também tratarem dos assuntos neste domínio do ciberespaço, a nível da organização civil facilitando a sua organização defensiva. Por outro lado, e seguindo o paradigma da Defesa e Segurança, também seria outra forma inteligente de organizar o ciberespaço.

P:Assumindo agora um cenário com uma ICN, a EDP, que pressupomos que possui neste momento capitais e gestão estrageiros, existindo um conflito externo e os gestores da EDP entendiam fazer um boicote de energia ao país com recurso ao domínio ciber. As FFAA teriam a capacidade, técnica, humana e legal para dar resposta, em termos práticos?

R: Em termos legais as FFAA apenas podem intervir se para isso forem solicitadas pelas entidades competentes, ou se tiver sido acionado e declarado um estado de exceção. Nessas condições as FFAA podem intervir em qualquer área. Nessas situações extremas, o general CEMGFA assume o comando das operações militares, a lei dá-lhe esse poder. Portanto as FFAA, têm de estar preparadas para intervir em qualquer área, as FFAA teriam de ajudar a recuperar o controlo, mas é óbvio que os especialistas em gestão de infraestruturas como a EDP não são as FFAA. O que aconteceria numa situação extrema é que as FFAA iriam ajudar a repor uma estrutura amiga nos postos de decisão. Neste caso, em que a EDP estaria controlada por pessoas da nação invasora, estas iriam ser afastadas da direção, forçadas a sair, se necessário com recurso à força e o país assumia o controlo da IC. As FFAA terão de ter a capacidade militar de tomar, fisicamente, o controlo da instalação. Sobre o controlo e administração dos sistemas, como temos técnicos portugueses a trabalhar nessas empresas, essa questão não se coloca uma vez que esses colaboradores voltariam as ter as condições para operar os sistemas normalmente obedecendo a ordens nacionais. Repor a normalidade de sistemas complexos poderia demorar vários dias ou meses sem o apoio dos

técnicos conhecedores dos próprios sistemas. Concluindo, à semelhança do que acontece nos domínios aéreo, naval ou terrestre as operações militares no ciberespaço na defesa de uma IC não serão certamente dissociadas da utilização dos restantes domínios operacionais.

10.2 Entrevista ao Sr. Major Valente – EMFA DCSI

(Este texto, de propósitos académicos, não reflete de forma integral a referida entrevista, sendo apenas válido quando ao conteúdo e não quanto à forma)

P: Existe a Capacidade de Ciberdefesa na Força Aérea?

R: Interpretando a capacidade de ciberdefesa como tendo 3 vetores, defensivo, exploração e ataque, não a Força Aérea não tem a capacidade de ciberdefesa, apenas possui sistemas que protegem os seus próprios sistemas. Não tendo também as FFAA a capacidade de atualmente defender Portugal e as consequentemente as suas infraestruturas críticas (ICN) no ciberespaço.

P:Como está organizada a capacidade de ciberdefesa na Força Aérea?

R: A DCSI (ver missão da DCSI), tem como missão a segurança dos sistemas informáticos Força Aérea, contudo alguns sistemas de comando e controlo do comando aérea são administrados pelo comando aéreo. A entidade que tem papel na segurança, DIVCSI na componente de doutrina, politicas estratégia uma vez que é uma divisão de estado-maior. Sendo que mais uma vez o comando aéreo pronuncia-se sobre os sistemas de comando e controlo sendo contudo a fronteira ténue, havendo permuta de conhecimento e apoio entre a direção e a divisão.

P: Para além do RFA 390-6 " Politica de ciberdefesa da Força Aérea" existe mais algum documento doutrinário ou legislação nacional /internacional que regule/oriente a ciberdefesa na Força Aérea?

R: A Força Aérea está comprometida com a legislação nacional, lei do cibercrime (mais relacionada com o cibercrime).Em termos de doutrina não, provavelmente o RFA 390-6 segue a doutrina NATO. Por definição a ciberdefesa devia proteger o país e nada do que existe escrito neste momento reflete esse objetivo.

P: A Capacidade de Ciberdefesa da Força Aérea é articulada com a capacidade de ciberdefesa dos restantes Ramos das FFAA?

R:Sim, existe a partilha de conhecimento, através de uma comissão coordenadora dos CIRC (*Computer Incidente Response Center ou Capability*) e existe também um órgão do EMGFA a CCCRISI (Comissão Coordenadora da Capacidade Resposta Incidentes de Segurança Informática e um GRISI (Grupo de Resposta a Incidentes de Segurança Informática) esta é nossa capacidade de segurança instalada. Existem reuniões sobre este fórum, com as entidades responsáveis pela segurança dos Ramos falam e coordenam com base nessa comissão coordenadora estratégias capacidades que são depois postas em pratica em exercícios NATO ou exercícios nacionais. O mundo da ciberdefesa é relativamente pequeno sendo muito importante "conhecermos as caras" dos elementos de ciberdefesa dos vários Ramos. Agora que está a nascer o CCD que ainda não tem "*initial operation capability"* (IOC) provavelmente a filosofia irá mudar, isto é, a Força Aérea que neste momento tem uma capacidade autónoma provavelmente irá ficar mais dependente funcionalmente do CCD. O CCD neste momento tem 7 elementos em permanência, 3 oficiais superiores 2 tenentes e 2 sargentos ajudantes. O CCD nascerá com 3 enclaves (extensões/filiais) um na marinha, um no exército e outro na Força Aérea.

P: Se existir um ataque ao CA, por exemplo ao radar, a Força Aérea está preparada?

R: Não, temos apenas capacidade de resposta. A DCSI esta mais sensível á RIGFA (rede interna geral da Força Aérea) para efeitos administrativos e logísticos (aceso á internet grupo *wise* pastas de rede- não classificada. No caso do radar como entra numa rede de comando e controlo é o CA que tem a primeira palavra a dizer, a primeira capacidade de resposta é do CA das suas equipas de segurança (não estão constituídas como equipas de ciberdefesa) que provavelmente estarão preparadas para dar uma resposta. Mas sem dúvida que existiram contactos em caso desse tipo de incidente entre as duas entidades.

P: A Força Aérea tem participação nas *computer emergence team* CERT?

R: Tem, a Força Aérea participa como membro das FFAA participa no fórum CSIRT nacional (Computer Security Incidente Response Teams),onde os representantes das equipas de resposta a incidentes de segurança informática se reúnem para discutirem a temática. Nesse fórum estão representadas algumas ICN, as FFAA, FCT (Fundação de Ciências e Tecnologia a FCCN (Fundação para a Computação Cientifica Nacional) sendo que foram estes dois últimos que criaram o site CERT.PT dado a inexistência de outro tipo de capacidade CERT. É um fórum que permite a discussão e conhecer as pessoas. Sendo um fórum sem nenhum tipo de formalização legal. Provavelmente esta capacidade irá agora para o CNCS agora sim fundamentada por enquadramento legal o que permitirá uma melhor coordenação de reposta a um ataque ciber a um ICN. Atualmente se algum elemento das FFAA chegar por exemplo junto da EDP para defender a EDP de um ataque externo provavelmente a própria EDP não dará acesso ao seu firewall uma vez que legalmente nada a obriga a faze-lo. Logo se o CEO da EDP disser que nenhum responsável de segurança da EDP participa no fórum, uma vez que a participação é voluntaria, nada o obriga.

P: De que forma as FFAA intervém na ciberdefesa das ICN?

R: Não intervém. Apenas no fórum de discussão CSIRT.

P: Tem conhecimento se o atual programa de proteção ICN engloba as FFAA?

R: Não tenho conhecimento. Desconheço a existência de um Plano Nacional de Proteção de ICN. Como chefe da secção de ciberdefesa na DCSI não conheço o plano de emergência de cibersegurança de proteção da infraestruturas crítica que é a Força Aérea. Sendo que na parte do comando aéreo – parte classificada, os sistemas de comando e controlo pode estar previsto pela NATO. Deverá ser analisado se a parte dos sistemas não classificados que são responsabilidade da DCSI uma vez afetada põem em causa ou não os sistemas informáticos classificados do comando aéreo. Mas ainda não foi estudado.

P: Face ao impacto disruptivo das ciberameaças e à necessidade de garantir o comando integrado das operações a desenvolver no ciberespaço, os Estados

Unidos da América, em 2009, anunciaram a criação do *US Cyber Command*, assumindo de forma clara o ciberespaço como um novo domínio operacional, onde podem ser conduzidas operações militares. Seguindo a iniciativa norte-americana, a Alemanha anunciou pouco tempo depois o levantamento da sua estrutura nacional de cibersegurança e ciberdefesa, no âmbito da qual previa o levantamento e ativação de um comando militar para o ciberespaço. Mais recentemente, cerca de 30 países assumiram igualmente iniciativas neste Domínio tem conhecimento se Portugal se integra nesse grupo?

R: Tenho conhecimento, Portugal não integra esse grupo. Podemos chegar ao ponto de Portugal evoluir para um quinto ramo. Neste momento temos as forças terrestres no vetor terrestre, as forças navais no vetor marítimo e as forças aéreas nos vetor aéreo mas nasceu um vetor novo, o ciberespaço. Por isso defendo que nos Força Aérea não devemos cultivar a capacidade de podermos ter a capacidade de ataque, não deverá nascer na Força Aérea. Por tal como quando não existia a preocupação de uma guerra aérea antes de existirem aviões, também não se previa a capacidade de existir uma guerra no Ciber espaço antes de existir Ciber espaço, mas agora já há essa potencialidade.

P: Se existir hoje um ataque a uma central da EDP que mande abaixo a rede elétrica, sabe se as FFAA são mobilizadas, se algo esta previsto?

R:Sei, as FFAA não são mobilizadas a não ser que a EDP o peça.

P2: E temos capacidade para apoiar, está algo previsto?

R: Não está nada previsto mas sim temos essa capacidade de apoiar e dar um tipo de informação. Num cenário caótico, dependendo sempre da vontade da EDP, pediria ajuda ao fórum CSIRT, e provavelmente ao CNCS a curto prazo, no caso do fórum CSIRT a FFAA serão apenas mais um elemento a apoiar da resolução do problema. E essa capacidade de resposta cria-se de forma informal. É um novo tipo de ameaça por isso muito pouco ainda está escrito, muito pouco está previsto e planeado para lhe dar resposta.

P:Qual a sua opinião relativamente ao fato de sendo as FFAA o último reduto na defesa do Estado, estas deverem ter mais impacto e contributo na defesa das IC desse mesmo estado nomeadamente um papel regulado e auditor?

R:Não, as FFAA não devem ser a entidade reguladora nem auditora. Devem sim ser precisamente o último reduto, ou seja deveríamos ter uma forma de conseguir garantir a segurança do ciberespaço. Não conseguindo concretizar como seria isso feito. As mesmas regras com que a Força Aérea ou as FFAA se defendem das ciber ameaças são as mesmas que qualquer outra entidade ou infraestrutura. As FFAA deveriam ter mais equipamento e mais capacidade de defesa que por exemplo as restantes infraestruturas criticas e isso não acontece, na verdade por exemplo a EDP tem mais capacidade de ciberdefesa que a própria Força Aérea e esse fato deve-se às restrições orçamentais. Mais uma vez falando da área não classificada. Sim as FFAA deveriam ter a capacidade de proteger e defender as nossas infraestruturas críticas mas essa capacidade ainda não está criada. Assim como deveria ser criada a parte legislativa que permita as FFAA intervir em caso de um incidente informático que ponha em causa a infraestrutura critica.

10.3 Entrevista ao Centro de Ciberdefesa

(Este texto, de propósitos académicos, não reflete de forma integral a referida entrevista, sendo apenas válido quando ao conteúdo e não quanto à forma)

P:Concorda com a ideia de que, em termos de ciberdefesa, o papel das FFAA é proteger os seus próprios sistemas e estar preparada para atuar nos três regimes de exceção previstos (estado de sitio, emergência ou calamidade)?

R:Não, o conceito de ciberdefesa é muito mais vasto, isso é apenas aquilo que é transcrito do genérico que está na constituição, que as FFAA em todos os ambientes, incluindo o ambiente de guerra cibernética, podem ser chamadas em caso de conflito externo para atuar diretamente sob as ordens do CEMGFA. O CCD tem por missão, e vai ser aprovado por decreto lei uma vez que já foi regulamentado na lei orgânica do EMGFA, proteger as redes das FFAA em conjunto com os CIRCS dos Ramos, porque cada ramo tem um CIRC, e esses é que são responsáveis por proteger cada segmento de rede e sistemas, o CCD terá um papel de coordenação, monitorização e apoio a todos esses CIRCS e no fundo será a entidade responsável por gerir os conflitos do ponto de vista não cinético, como suporte às CNO (defesa, exploração e ataque). O CCD não tem ainda um quadro orgânico, que, do ponto de vista da atuação, possa ser utilizado do ponto de vista operacional tal como são conduzidas as operações no domínio terrestre, naval ou aéreo. Os CIRCS dos Ramos serão os braços armados da ciberdefesa sendo que também existe um CIRC no EMGFA, mas o CCD não é apenas uma entidade que será chamada em situações de conflito extremo, estaremos em operação no dia-a-dia e atuaremos de acordo com as indicações do CEMGFA e numa perspetiva muito de proteção e depois eventualmente de ataque e exploração.

P:Sendo a maior parte das ICN são operadas por entidades privadas cujo principal objetivo é a obtenção de lucro, e uma vez que as soluções de segurança estão sempre associadas a um custo, entende que deveria existir

uma entidade externa que auditasse e regulasse o cumprimento dos requisitos de cibersegurança ou dos planos de segurança em termos gerais?

R:Infraestruturas críticas são tradicionalmente infraestruturas que são importantes para a condução de um estado nação (redes de transporte de energia, água, telecomunicações), o problema hoje é que é muito difícil, em Portugal, definir o que é uma infraestrutura crítica, mas também não é da nossa responsabilidade essa definição, será do CNCS uma vez que essas entidades são civis e não militares. Se deve ou não existir uma entidade externa, também não nos compete propor isso.

P:Qual a sua opinião sobre a eventual criação de um novo ramo para o domínio ciber?

R:Não creio que tenha sido sequer veiculada a criação de um novo ramo. Neste momento a intenção existente é a da criação de um centro agregado ao EMGFA, não está pensado ser expandido para a criação de um novo ramo. Nesta fase todo o domínio ciber, é um domínio onde estamos todos a aprender, quer os operadores das ICN que estão cada vez mais dependentes do domínio ciber e dos sistemas de informação, quer a componente da defesa que ainda está a perceber como integrar o domínio ciber nas operações militares, e convém ter ciente que quando falamos de CNO na componente ofensiva estamos a falar, nesta fase, numa operação militar conduzida no âmbito de uma operação militar de maior espetro, ou seja, ninguém irá fazer um ciberataque isoladamente, fará parte de uma estratégia de emprego de forças em que há um objetivo militar a atingir e nós seremos mais uma ferramenta ao dispor das chefias militares para atingir um objetivo, que por sua vez corresponderá a um objetivo estratégico fixado. Assim a questão de autonomizar e criar um ramo independente é prematuro constituir preocupação.

P:Entende que o CCD deve ser a entidade com maior capacidade no domínio ciber uma vez que é a entidade que para além dos aspetos normais da cibersegurança tem ainda a missão de atuar em momentos de exceção e ainda desenvolver CNO?

R:Como militares devemos sempre ser os melhores naquilo que fazemos na nossa área. Se a pergunta é uma tentativa de comparação das capacidades de CCD com

o CNCS, são coisas diferentes, o CCD existe dentro da defesa e que em caso de exceção, os CIRCS de cada ramo passam para o controlo operacional do CEMGFA deixando de estar dependentes de cada ramo e portanto nesse sentido o CCD tem de conseguir ser o melhor no controlo e gestão das atividades produzidas pelos CIRCS, não devemos olhar para o CCD como se este trabalhasse sozinho, o CCD trabalha pelo menos com mais quatro entidades, os CIRCS dos Ramos e do EMGFA diariamente para dar resposta aos problemas. O nosso objetivo é criar uma equipa macro que depois conduzirá as CNO de acordo com a vontade estratégica e operacional das chefias miliares. Quando se fala de quem tem as melhores capacidades no domínio ciber é algo tão genérico como perguntar quem tem as melhores capacidades no domínio do transporte aéreo, depende, provavelmente uma transportadora aérea terá um sistema muito mais otimizado para realizar um transporte de passageiros de longo curso agora se falarmos da missão de conduzir operações militares com aeronaves claramente a Força Aérea terá maior capacidade, no domínio ciber também existem vários domínios e existe uma missão muito especifica no CCD que é a condução de operações ofensivas que ai sim, termos de ser referência, na parte defensiva temos de estar no mínimio ao nível das ameaças para podermos defender as operações de comando e controlo das FFAA.

P:Existem ou existirão nas FFAA as capacidades quer técnicas, quer humanas, quer legais, para intervir junto dos sistemas de uma ICN mesmo contra a sua vontade?

R:Penso que na verdade isso seja mais uma questão legal. Nas situações previstas na constituição, por indicação do Sr. Presidente da República as FFAA podem atuar junto de qualquer entidade civil. Existe uma lei de 1995 que é a Lei da Mobilização e Requisição no Interesse à Defesa Nacional, que define que, em Estado Sitio e Estado de Guerra existe a mobilização de recursos humanos e de recursos materiais, os que forem necessários para atingir os objetivos permanentes da Política Defesa Nacional, por isso se estiver na esfera da política nacional assegurar o fornecimento de energia elétrica, sim, existe um mecanismo legal que autoriza a mobilização. Se uma ICN, por motivos alheios à sua vontade sofrer um ataque e os seus sistemas ficarem inoperacionais, o CNCS avança em primeiro lugar e caso a situação evolua para uma das três situações de exceção é que entra o CCD.

P:É possível falar de uma autoridade nacional do domínio ciber em Portugal?

R:Se é possível, ou não, existirão pessoas mais qualificadas que eu para responder a essa pergunta. Comparando com outro tipo de autoridades não é possível colocar as FFAA "debaixo de um chapéu" em que têm de trabalhar com outras entidades em que depois existe uma outra entidade a coordenar todas as operações, tal como também não acontece em outros domínios operacionais. Ter uma autoridade nacional que tem autoridade sobre o CNCS, CCD e outras entidades não me parece plausível.

P2:Quem garante se os privados cumprem os requisitos que entendemos como sendo os requisitos mínimos de segurança para as nossas ICN?

R:Exato, quem é que garante que as ICN estão, por exemplo, certificadas com a ISO27001, que basicamente é uma norma que determina ao nível da segurança de informação como deve ser feita a certificação para o sistema ser considerado seguro. Mas não é CCD que deve responder a essa pergunta uma vez que estamos a focar entidades civis. Não relacionado com a área ciber o GNS tem responsabilidade em certificar espaços físicos, existindo inclusivamente espaços militares que têm de ser também certificados pelo GNS em termos de segurança física de acordo com os parâmetros NATO, UE e nacionais.

P3:Tem conhecimento se existe ou não essa autoridade?

R:Da informação que disponho não existe essa autoridade. Se alguém decidir, que isso é um aspeto crítico para o país existem mecanismos legais para o fazer, tal como acontece noutras áreas (ex. área da construção, área alimentar),isto é, podem existir mecanismos legais que obriguem as ICN a cumprir determinados requisitos para poderem fornecer um dado serviço (telecomunicações, águas, etc.), depois quem vai fiscalizar já é uma função que não nos compete. Mas realmente a falha de um desses sistemas pode comprometer do ponto de vista genérico uma dada área das FFAA. Provavelmente do ponto de vista legal ainda muito terá que ser definido, mas não é da nossa responsabilidade.

P:Está prevista a articulação do CCD com o CNCS?

R:Sim está previsto, não só a coordenação com o CNCS como também uma coordenação estreita com o CIRC da NATO e dos Ramos e com uma entidade, que foi neste momento absorvida pelo CNCS, era o CERT.pt. Tudo isso está previsto e o CCD tem ligações de trabalho com as entidades, não podemos trabalhar de "costas voltadas" numa área que acaba por ser global. Em termos de lei orgânica o CCD é a entidade responsável pela cibersegurança do sector defesa, por isso o CNCS, que tem de coordenar com todos sectores, no âmbito da defesa o CCD é o representante para o CNCS.

P:São realizados treinos de uma situação no domínio ciber que implique a mobilização das FFAA junto das ICN?

R:Sim, o ano passado foram realizados dois exercícios nesta área, o "Lusitano" que é um exercício do EMGFA que envolve a participação de todos os Ramos onde o CCD já esteve a participar especificamente na área ciber e um exercício da NATO, o "*cyber coalition*" que muitos países da NATO e parceiros participam e trabalham precisamente esta área da ciber.

P:Concorda com afirmação de que capacidade do domínio ciber é uma capacidade diferente das habituais, isto é, por norma é comum, quando se pensa em capacidade, associar-se uma materialização direta de meios sejam eles aeronaves, carros de combate ou navios, o que não é o caso da capacidade ciber pois esta trata-se de uma capacidade de conhecimento intensivo onde a existência de um reduzido número de indivíduos altamente qualificados poderá fazer toda a diferença.

R:Sim, mas também necessitamos de ter meios técnicos. Contudo também é necessário saber operar esta área e bem. As FFAA tem recursos humanos, em cada ramo, qualificado nesta área, área de sistemas de informação, comunicação e tecnologias. É essencial um conhecimento de base, uma vez que é um conhecimento muito técnico que abrange muitas áreas, o que implica um conhecimento elevado. Irá obrigar a uma adaptação dos planos de formação dos

recursos humanos para trabalharem nesta área. A partir do momento que passam a existir operações na área ciber, tal como acontece nos outros domínios, também terão que existir nesta área. Operar um sistema de informação qualquer engenheiro consegue, a componente ciber é uma componente idêntica a operar um sistema de armas e por isso implica uma qualificação intensiva que neste momento, não só em Portugal como nos restantes países, ainda estão a pensar como se irá criar essa componente de qualificação que permita " transformar" um engenheiro num operador de ciberdefesa, um elemento capaz de operar o sistema de armas ciber defesa, a própria NATO ainda não tem um modelo de qualificação e formação na aérea ciber, ainda está um projeto em estudo para dizer quais são as qualificações mínimas necessárias para uma pessoa operar o nosso sistemas de armas ciber.

10.4 Entrevista ao Sr. Engenheiro Lino Santos - Centro Nacional de Cibersegurança

(Este texto, não reflete de forma integral a referida entrevista, sendo apenas válida quando ao conteúdo e não quanto à forma e apenas para efeitos académicos)

P: Dado não ser um termo consensual, qual a sua definição de ciberdefesa e de cibersegurança?

R: Só não é consensual se "tentarmos inventar muito", segurança e defesa embora sejam dois termos não completamente disjuntos são mais ou menos consensuais. A defesa está relacionada com a proteção de fronteiras relativamente a um inimigo externo. Hoje em dia existem outras ameaças externas para além dos atores estatais e a fronteira entre segurança e defesa é difusa, em vários domínios, mesmo no ciber. Quando falamos em terrorismo a ameaça também é externa e se repararmos quem trata o terrorismo ou pelo menos coordena o combate ao terrorismo em Portugal é o sistema de segurança interna e não a defesa. O ciber pode ser comparado ao terrorismo uma vez que são ameaças assimétricas, atores estatais e não estatais.

Posto isto, o que é normalmente aceite é definir a ciberdefesa como as capacidades de proteção dos sistemas próprios das FFAA – assegurar o funcionamento em missão, proteção do perímetro das FFAA e depois a segunda via, a exploração do ciberespaço - CNO que só as FFAA o podem fazer – ações ofensivas.

Para mim a Cibersegurança é um conjunto de capacidades nos vários domínios de atuação com vista a melhorar a insegurança das redes e inclui as medidas de proteção simples nos Ramos civil e militar, inclui a prossecução criminal (combate ao cibercrime) e a defesa. Se perante uma situação qualquer chegarmos a uma das três situações previstas na Constituição (Estado de Sítio, Calamidade ou Guerra) as FFAA assumem o controlo a partir daí e têm de estar preparadas para isso.

Mais uma vez comparando com o terrorismo qualquer estado tem ao seu dispor 4 domínios disponíveis, proteção simples (treino das pessoas para se protegerem e

identificarem eventuais terroristas, proteção de instalações e sistemas), depois como o terrorismo é crime, o sistema judicial deve identificar os terroristas e levá-los à justiça para serem punidos, por outro lado, a defesa também tem um papel muito ativo no combate contra o terrorismo, depois ainda existe o campo diplomático. E este é o esforço conjunto contra o terrorismo, mais uma vez a cibersegurança também tem estes 4 domínios, proteção simples (CNCS, as autoridades reguladoras sectoriais, as iniciativas de consciencialização de utilização segura da internet, os CERT), depois temos o domínio da prossecução criminal, a maior parte dos atos praticados por *hackers* configuram um crime (policia judiciaria e tribunais) e depois temos a defesa que tem a necessidade de proteção dos seus próprios sistemas e depois tem a capacidade ofensiva ("tal como a Força Aérea tem os aviões prontos, não quer dizer que ande sempre aos tiros a alguém, é necessário é estar pronto para quando for necessário") e depois as FFAA tem uma responsabilidade maior em situações de emergência e de guerra. Temos ainda campo diplomático (politicas de não proliferação de ciberarmas, diretivas europeias de cibersegurança).Na minha opinião cibersegurança é tudo isto. Estas são as competências que contribuem para uma melhor cibersegurança nacional.

P: Como está organizada a capacidade de cibersegurança em Portugal?

R: Não temos uma estrutura de cibersegurança em Portugal, é algo que venho a defender há muitos anos. O decreto lei 62 de 2011 prevê a identificação das ICN e a criação de planos de segurança aprovados pelo Secretário-Geral da Administração e Segurança Interna, este é um trabalho que acontece em coordenação com a ANPC (elaboração dos planos), esse trabalho está a ser feito com uma metodologia que prevê uma análise de risco, na sequência da análise de risco são propostas um conjunto de medidas, para ser feita uma análise de risco é necessário desenhar um conjunto de cenários, os cenários em Portugal identificados como prioritários são a ameaça terrorista, sísmica e a ameaça ciber. Na questão da ameaça ciber estamos atrasados, uma vez que nos últimos anos as relações institucionais não foram muito favoráveis.

O CNCS no seu corpo de atuação tem as ICN como um eixo prioritário, os serviços de reação que estão a ser desenhados têm duas áreas de atuação, os organismos do estado e as ICN. Também é cometida ao CNCS a responsabilidade do

planeamento civil de emergência do ciberespaço que também vai tocar nos planos que estão a ser preparados pela ANPC, por isso, quando se diz que a responsabilidade é de A ou de B eu não tenho tantas certezas assim. Para mim a proteção de ICN é uma responsabilidade vinda do DL 62/2011 da ANPC e do sistema de segurança interna o que não quer dizer que o CNCS não trabalhe para as IC e não tenha as IC como uma prioridade.

P: O CNCS não deveria ser a entidade com mais capacidade (conhecimento) na área ciber e o responsável nesse domínio?

R: Isso seria o cenário ideal. Não convém também dividir os planos isto é, a ANPC trata da ameaça terrorista e o CNCS trata da ameaça ciber, uma vez que um plano de segurança deve responder a todas as áreas de forma holística o que não quer dizer, e é o que vai ser feito, o CNCS vai ajudar a ANPC a elaborar os requisitos para os planos de segurança de cada IC, porque quem apresenta os planos é cada IC mas quem define os requisitos e a ANPC com o apoio do CNCS.

P: Tem informação se CNCS é considerado uma IC?

Pela definição não, uma vez que se o CNCS, por algum motivo, interrompesse a sua atividade o país não parava, as pessoas não eram afetadas a curto médio prazo.

P: A que tipo de problemas dá resposta/incidentes da resposta o CNCS?

Às ameaças Ciber, com 3 grupos de entidades servidas, os organismos do estado, as ICN e o ciberespaço funcional em geral.

P: O CNCS já adquiriu a IOC?

Ainda não.

P: O CNCS terá capacidade técnica e humana para dar resposta a um incidente de Cibersegurança?

Terá de ter. Neste momento se acontecesse algum incidente grave é óbvio que respondemos ao problema mas estruturalmente não estamos preparados (final de janeiro)

P: Qual a relação das ICN com os CNCS, tem papel regulador ou auditor?

Prefiro não responder a essa pergunta.

As IC pertencem a um sector de atividade e cada sector tem um regulador. E também para a área ciber deverá ser assim. Deverá ser uma abordagem em rede. E não hierárquica. O CNCS não vai combater cibercrime, nem vai atuar em caso de emergência ou de guerra com responsabilidade de coordenação nacional, isso é responsabilidade da defesa.

P:Entende que deveria existir um organismo/entidade que devesse "obrigar" as ICN a cumprir determinados requisitos nacionais em matéria de cibersegurança?

A maior parte das ICN são operadas por privados. Uma forte disrupção ou uma falha prolongada de uma dessas ICN vai alterar o estado normal, vai provocar tumultos, logo o bom funcionamento das ICN é do interesse nacional. Há duas abordagens cumulativas do problema. Uma a autorregulação, diálogo entre o sector público e o privado no sentido de encontrar o equilíbrio, isto é, o sector privado aceita que é para o seu interesse e para o interesse nacional os princípios e requisitos de segurança. Mas como qualquer medida de segurança tem um custo há sempre o lado de quem paga. Logo pode não ser suficiente o mecanismo de auto regulação e aí é necessário aplicar regras "*top down"*, produzir norma e obrigar o privado a executá-la. E depois há uma terceira abordagem que é a" auto regulação se possível regulação se necessário".

Adicionalmente alguns sectores têm uma tradição muito forte na autorregulação, sector bancário, nesta área ciber há muito que produzem normas internacionais que têm que ser adotadas por cada banco de forma a estes poderem estar "em jogo".

Respondendo à sua pergunta, eu diria que é necessário uma entidade centralizada que emitisse norma, mas que se deve primeiro procurar um entendimento entre o

sector público e privado em mecanismo de auto regulação. Ainda não estamos nesta fase porque não há um diálogo público-privado. A autorregulação que existe é privado-privado.

P: Entende que em última circunstância devia ser permitido a uma entidade ou organismo estatal intervir nos sistemas de uma dada IC, mesmo sem a necessidade do seu consentimento, no sentido de dar resposta a um incidente nacional?

R: O estado não pode entrar dentro de uma empresa, nunca uma autoridade do estado vai configurar uma *firewall* de uma empresa privada. O estado não pode sequer ter essa responsabilidade. A teoria aponta para 3 tipos de autoridade, a autoridade total (existe a possibilidade de conduzir operação na comunidade servida, na prática só existe quando o CERT pertence à entidade o CERT da EDP faz uma analise e executa), autoridade partilhada (o CNCS aponta um conjunto de medidas de mitigação e a decisão é conjunta entre o centro e as IC, nós só temos uma parte da informação mas a IC tem outra) e depois uma situação em que a autoridade é praticamente nula, a decisão é só tomada pela IC. Estes são os tipos de autoridades teóricas existentes para uma ação das equipas de reação a incidentes.

P:Uma vez que as FAA são, à luz da Constituição e da Lei, o último reduto na defesa do estado, entende que estas deverão ser o organismo com maiores capacidades técnicas e humanas no domínio ciber?

R: A escalada para a defesa está mais relacionada com o impacto do que com a dificuldade. A questão não é uma questão de ter mais capacidade é uma questão legal da constituição. Em termos de dificuldade, se o problema é difícil há uma coordenação internacional.

10.5 Entrevista ao Sr. Tenente-Coronel Viegas Nunes

(Este texto, de propósitos académicos, não reflete de forma integral a referida entrevista, sendo apenas válido quando ao conteúdo e não quanto à forma)

P:Existe a capacidade de ciberdefesa nas FFAA?

R:Em primeiro lugar é necessário " clarificar as águas" entre ciberdefesa e cibersegurança. A melhor forma para isso é perceber, no mundo real, quais são as missões de segurança e quais são as missões de defesa e estabelecer um paralelo com o mundo virtual que não é diferente, isto é, o que é chamado de segurança e de defesa no mundo real tem também uma extensão virtual, o que significa que as funções de combate ao cibercrime, que são no mundo real o combate ao crime, a responsabilidade é das forças de segurança, missões de defesa (de guerra) são da responsabilidade das FFAA, são aliás inalienáveis das FFAA (missão das FFAA defesa do estado contra ameaças externas segundo a constituição da república) e tal tem repercussão no ciberespaço, isto é as FFAA são responsáveis pela defesa militar do ciberespaço.

Daqui podemos retirar que uma coisa é falar de segurança (cibersegurança) outra coisa é falar de defesa (ciberdefesa). Na sua essência as duas não são absolutamente distintas nem diferenciáveis para lá do facto de a ciberdefesa ter de ter tudo o que a cibersegurança tem em termos de capacidades mais as *computer network operations* (CNO com três componentes, ataque defesa e exploração). À luz da ordem jurídica só as FFAA podem desenvolver CNO. Em termos simplistas as FFAA têm de fazer tudo aquilo que todas as entidades que trabalham em cibersegurança fazem mais CNO, isto é, as capacidades e qualificações necessárias à cibersegurança têm de existir nas FFAA de forma mais exigente para que seja possível conduzir operações no ciberespaço.

As FFAA devem ter a capacidade de ciberdefesa mas esta ainda não está operacional, existe um mandato para levantar a capacidade para ser atingida a IOC (*initial operational capability*) no final do ano de 2014, logo não existe no momento da entrevista uma capacidade estruturada e operacional de ciberdefesa nas FFAA.

Quando alguém disser que está pronto, é o primeiro passo para deixar de estar pronto, porque isto é uma capacidade que se vai construindo e adaptando no tempo porque o desenvolvimento tecnológico é muito rápido e não se coaduna com soluções consolidadas, antes pelo contrário, isso é uma perversão de ter capacidade.

P:Como está organizada a capacidade de ciberdefesa? Já existe algo organizado ou pensado uma vez que ainda não existe a capacidade?

R:Esta capacidade de ciberdefesa como já foi referido encontra-se em fase de levantamento. Estamos numa fase intermédia desse desenvolvimento, estamos na IOC. Ainda não é possível falar de uma organização da capacidade de ciberdefesa, deverá existir até 2020. É prematuro dizer que as FFAA possuem uma capacidade efetiva.

P:O Despacho 13691 de 2013 prevê a criação de um CCD no âmbito do estado maior general das FFAA em simultâneo com a criação de um único serviço que coordene as comunicações e os sistemas de informação em articulação com os Ramos procurando-se uma lógica de centralização e especialização dos recursos existentes. Em conhecimento desta diretiva?

R: Não é uma diretiva. É uma orientação política para a ciberdefesa dimanada do Sr. Ministro da Defesa, é uma diretiva orientadora, como em qualquer área militar antes de ser levantada a capacidade é necessário uma diretiva orientadora que é o que esse documento constitui, é por isso, uma orientação para o levantamento. Nesse documento vinha a indicação de que deveria ser o EMGFA a fazer o estudo e a submeter um plano de levantamento da capacidade que foi aprovado no início deste ano. Existe por isso um plano de implementação mas que como o próprio nome indica ainda está em implementação.

P:Tem conhecimento se essa capacidade de ciberdefesa estará articulada com o CNCS?

R:Sim, em princípio tudo indica que estará articulada, aliás se formos ver o despacho que cria o CNCS há um conjunto de competências que são cruzadas e que são integradas, logo essa integração existe e está definida na lei, mas nem o próprio CNCS está completamente operacional, ainda está em levantamento também. Por isso Portugal, neste momento, tem duas estruturas de cibersegurança e ciberdefesa em levantamento.

P:Tem conhecimento se no domínio da ciberdefesa, Portugal está a seguir alguma metodologia, isto é, se está a seguir alguma orientação da UE, NATO, USAF?

R:A metodologia que está a ser seguida é a do plano e a implementação do plano, plano esse que foi desenvolvido em devido tempo pelo EMGFA, que posteriormente foi submetido ao Sr. Ministro que despachou favoravelmente e neste momento está a ser implementado. O plano tem que dar resposta à diretiva orientadora do Sr. Ministro.

P:Tem conhecimento se as FFAA em geral e cada ramo em particular, como constituintes de uma ICN, possuem um plano de emergência que contemple os aspetos ciber tal como obriga o DL 62/2011. Cada ICN deve ter um plano de emergência elaborado num período de um ano após ter sido classificada com ICN.

R:A visão de que as FFAA são um IC decorre da sua função fundamental para a soberania e segurança do estado, mas para efeito de gestão não são compagináveis com as restantes IC. Ou seja, as FFAA não são geridas por entidades externas, as ICN e o plano de desenvolvimento e articulação das IC neste momento esta residente na autoridade nacional de proteção civil, e essa autoridade nacional de proteção civil não tem jurisdição sobre a instituição militar, é um ministério diferente, e o ministério da administração interna não tem jurisdição sobre as FFAA. As FFAA têm, obviamente, planos de contingência, quando atacadas as

suas IC, há inclusivamente normativos, regras e diretivas orientadoras para esse efeito, para os vários Ramos e de forma conjunta. Mas não há nenhuma jurisdição direta da aplicação dessa orientação geral. As FFAA tem consciência que são uma IC porque garantem a soberania do estado, não são geridas da mesma forma que as outras ICN. E não estão sujeitas à obrigatoriedade referida. As FFAA obedecem em termos gerais às orientações que foram definidas para as ICN, mas têm os seus regulamentos e estruturas próprias.

P:Tem conhecimentos se as FFAA têm capacidade técnica para serem o último reduto em matéria de cibersegurança e de ciberdefesa, isto é, terão as próprias ICN mais capacidades técnicas que as FFAA?

R:O ciberespaço é algo novo, a quantidade de técnicos qualificados tanto nas FFAA como fora delas, no país é muito limitada e este não é um problema nacional é um problema global. Tanto que é, que os grandes estados estão a "capturar as cabeças" aos vários países para integrarem as suas próprias estruturas e constituírem as suas próprias capacidades. Existe por isso muita procura e pouca oferta.

Havendo esta atribuição às FFAA, estas só têm uma solução, que é a de tornar possível e para isso necessitam de um plano de implementação da capacidade que vai passar inevitavelmente por formar e qualificar mais gente nessas capacidades e competências.

Esta é uma capacidade muito especial, estamos habituados a lidar com capacidades que têm uma materialização direta de meios, aeronaves, carros de combate, navios, o que não é o caso desta capacidade, esta é uma capacidade de conhecimento intensivo, significa que podem existir 3 ou 4 pessoas qualificadíssimas e essas pessoas fazem toda a diferença. Aliás um F16 ou um carro de combate ou navio permite pagar uma capacidade, logo este é um desafio de conhecimento intensivo, significa com isto que nós ou percebemos a curva de desenvolvimento da capacidade e a necessidade de ter de desenvolver conhecimento e nos adaptamos para acompanhar a dinâmica da ameaça ou ficaremos muito desajustados da ameaça.

P:Considera que deve ser uma área em que Portugal deve investir?

R:Tem obrigação disso. É uma das áreas em que os pequenos países devem e podem investir dada a assimetria dos meios, o único fator substantivo é o conhecimento. O país reconhecido como estando mais à frente, é um pequeno país que foi atacado em 2007 – Estónia (possui uma grande capacidade técnica neste domínio). Portugal esta a liderar no âmbito da UE um projeto internacional de educação e treino para a ciberdefesa e participa num semelhante no âmbito da NATO.

P:As FFAA têm autoridade legal para intervir no caso de um ciberataque?

R:O funcionamento é por coroas sucessivas. As FFAA à luz da Constituição devem intervir em três situações, Estado de Sítio, Estado de Calamidade Pública e Estado de Guerra, mais uma vez todas estas três situações são compagináveis com o ciberespaço. Significa que se formos atacados por um país externo, estamos em Estado de Guerra (a dificuldade é saber quem nos ataca), as consequências desse ataque podem ser o comprometimento das capacidades das FFAA (causa bélica), podem ser uma calamidade pública (as IC são atingidas) ou uma situação de Estado de Sítio (em que o governo é atingido) e o país torna-se ingovernável devido a um ciberataque e é necessário repor essa situação. Em qualquer uma destas situações a CR diz que o empenho das FFAA faz-se por ordem direta do poder político, o Sr. Presidente da República necessita de assinar um decreto a autorizar o emprego das FFAA, o mesmo há-de acontecer no caso de um ciberataque de larga escala que coloque o país nessa situação. Portanto tudo funciona numa sequencia natural, por exemplo a EDP é atacada a primeira responsabilidade é dos técnicos da EDP que colocam os sistemas em continuidade do serviço, se estes não conseguirem escala para o CNCS, se este não conseguir repor, como a EDP poem em causa o abastecimento de energia elétrica a toda a população e população fica dependente desse abastecimento, são acionadas de forma complementar as FFAA. Estas terão de ter melhores meios que os restantes e neste momento duvido que alguém tenha meios para resistir a um ciberataque de grande escala. Enquanto o plano não for implementado é precoce falar em capacidade estruturada da forma que se pretende. Se existir hoje um ataque existem procedimentos a serem seguidos, podem é ainda não estar ao nível do que se pretende mas também para isso há resposta, significa que se por acaso não for encontrada resposta nacional há

ao nível das alianças capacidade de pedir ajuda internacional, aliás, qualquer ataque de larga escala tem sempre um impacto internacional portanto a cooperação internacional é tão ou mais importante que as sinergias nacionais. Agora se as FFAA têm a obrigação institucional de dar resposta.

P:Concorda com a criação de um novo ramo apenas dedicado ao ciberespaço seguindo o exemplo dos EUA que anunciaram a criação do *cyber comand*?

R:No nosso país, dificilmente. Agora é necessário uma carreira para quem estiver direcionado para o domínio ciber, seguramente que sim uma vez que é uma área extremamente específica e dedicada para haver grandes alterações na carreira dos envolvidos, o estatuto da parte ciber vai crescer como nos outros países como um comando de componente, será mais um vetor de poder da força em termos práticos, o que julgo que será exequível a curto prazo é ter um CCD, e a longo prazo um comando de ciberdefesa que não será um comando como o das forças aéreas ou terrestes ou navais mas há-de ser um comando pelo menos ao nível das forças especiais dependente do EMGFA.

P:As FFAA deverão ter um papel regulador ou auditor na ciberdefesa das ICN, isto é, de garantir que EDP, por exemplo, cumpre os mínimos de segurança?

R:Nem pensar. As FFAA têm um mandato muito específico à luz da Constituição da República.