INSTITUTO DE ESTUDOS SUPERIORES MILITARES

CURSO DE ESTADO-MAIOR CONJUNTO

2014/2015

TII

O PAPEL DA GNR NO CONTEXTO DA CIBERSEGURANÇA NACIONAL

O TEXTO CORRESPONDE A TRABALHO FEITO DURANTE A FREQUÊNCIA DO CURSO NO IESM SENDO DA RESPONSABILIDADE DOS SEUS AUTORES, NÃO CONSTITUINDO ASSIM DOUTRINA OFICIAL DAS FORÇAS ARMADAS PORTUGUESAS E DA GUARDA NACIONAL REPUBLICANA.

INSTITUTO DE ESTUDOS SUPERIORES MILITARES

O PAPEL DA GNR NO CONTEXTO DA CIBERSEGURANÇA NACIONAL

TCOR GNR/INF Paulo Daniel Duarte Machado

Trabalho de Investigação Individual do CEMC- 14/15

Pedrouços 2015

INSTITUTO DE ESTUDOS SUPERIORES MILITARES

O PAPEL DA GNR NO CONTEXTO DA CIBERSEGURANÇA NACIONAL

TCOR GNR/INF Paulo Daniel Duarte Machado

Trabalho de Investigação Individual do CEMC

Orientador: TCOR GNR/ADMIL Nuno Miguel Parreira da Silva

Pedrouços 2015

.

Agradecimentos

Este estudo foi realizado com o contributo de várias pessoas, sem o qual não teria sido possível a sua realização. Por esse motivo, manifesto a minha sentida gratidão e reconhecimento.

Na hora da sua conclusão, é em primeiro lugar, devida uma palavra de profundo agradecimento ao meu orientador - TCor ADMIL Nuno Miguel Parreira da Silva - a quem tenho que exprimir a minha gratidão pelo muito que aprendi como seu orientando, mas também por todas as suas qualidades profissionais e humanas, que o tornam um exemplo para mim e para todos nós. Este estudo não teria a mesma forma e conteúdo, sem os seus conselhos assertivos, permanente disponibilidade e pragmatismo dos seus ensinamentos.

Gostaria de deixar, de forma especial, o meu agradecimento a todos os docentes do Curso de Estado-Maior Conjunto, pela forma assumidamente competente e reconhecidamente douta com que transmitiram e partilharam conhecimentos sobre os temas da segurança e da defesa.

Um agradecimento também especial ao Coronel João Carlos Loureiro Magalhães, diretor do Curso de Estado -Maior Conjunto, pela sua permanente disponibilidade e apoio prestado para a realização do presente trabalho.

Não poderei deixar de dirigir um sincero e muito especial agradecimento a todos os entrevistados que, prontamente acederam a serem entrevistados, sem a sua colaboração este estudo não seria possível.

A todos os que me apoiaram de forma mais direta na concretização deste estudo, nomeadamente, aos camaradas Santos e Raposo, o meu obrigado pelo apoio e incentivo, assim como a todos os restantes, a quem por lapso não dirigi o meu agradecimento.

À minha esposa e filhas, pela jovialidade, boa disposição e alento que me transmitiram, e a quem dedico este trabalho.

Índice

Índice de Apêndices

Índice de Figuras

Índice de Tabelas

Resumo

A presente investigação tem como objetivo geral analisar como as forças e serviços de segurança, e em particular a GNR, poderão atuar no contexto da cibersegurança na sociedade portuguesa, procurando assim acrescentar conhecimento empírico que contribua para uma visão integradora dos esforços em curso neste domínio. Pela sua flexibilidade optamos por uma estratégia de investigação qualitativa e relativamente ao *design* da pesquisa optou-se pelo estudo de caso. Os métodos e técnicas utilizadas foram as entrevistas de aprofundamento- passíveis de tratamento através da análise de conteúdo, e a análise documental. Como resultado principal destacamos o diagnóstico de conjunto que fundamenta eventuais mudanças ou orientações que a GNR possa vir a prosseguir no âmbito da cibersegurança. E como conclusões mais importantes salientamos que deveria ser criado na estrutura da GNR um órgão autónomo e especializado em matérias de cibersegurança, a conceptualização relacionada com *cyberpolicing* e a criação de um CSIRT.

Palavras-chave

Ciberespaço, Cibersegurança, Atuação, *Cyberpolicing*

Abstract

This research has as main objective to analyze the forces and security services, and in particular the GNR, may act in the context of cybersecurity in Portuguese society, thus seeking to add empirical knowledge that contributes to an integrated view of ongoing efforts. For its flexibility we chose a qualitative research strategy and in relation to research design we chosen the case study. The methods and techniques used were depth interviews amenable to treatment through content analysis, and document analysis. The main result we highlight, was the diagnostic set that supports any changes or guidelines that GNR is likely to continue in cybersecurity. And as most important conclusions, that should be created in the structure of GNR an independent and specialized body for cyber security matters, the conceptualization related to cyberpolicing and the creation of a CSIRT.

Keywords

Cyberspace, Cybersecurity, Intervention, Cyberpolicing

Lista de Abreviaturas

C	
CCD	*Center Cyber Defense*
CEDN	Conceito Estratégico de Defesa Nacional
CEPOL	*European Police College*
CESEDEN	*Centro Superior de Estudios de la Defensa Nacional*
CESI	Conceito Estratégico de Segurança Interna
CERT	*Computer Emergency Response Team*
CERT.PT	*Computer Emergency Response Team* nacional
CNCSeg	Centro Nacional de Cibersegurança
CSIRT	*Computer Security Emergency Response Team*
D	
DoD	*Department of Defense*
E	
EC3	*European Cybercrime Center*
EDA	*European Defense Agency*
ENCT	Estratégia Nacional de Combate ao Terrorismo
ENCSeg	Estratégia Nacional de Cibersegurança
ENISA	*European Network and Information Security Agency*
EUROPOL	*European Union´s Law Enforcement Agency*
G	
GNR	Guarda Nacional Republicana
GRESI	Grupo de Reflexão Estratégica sobre a Segurança Interna
I	
IDN	Instituto de Defesa Nacional
IESM	Instituto de Estudos Superiores Militares
L	
LOIC	Lei da Organização e Investigação Criminal
LSI	Lei de Segurança Interna
N	
NATO	*North Atlantic Treaty Organization*
NCIRC	*NATO Cooperative Cyber Defense Centre of Excellence*
O	

OCDE	Organização para a Cooperação e Desenvolvimento Económico
OE	Objetivos Específicos
P	
PCSD	Política Comum de Segurança e Defesa
PJ	Polícia Judiciária
PSP	Polícia de Segurança Pública
Q	
QC	Questão Central
QD	Questão Derivada
R	
RASI	Relatório Anual de Segurança Interna
S	
SEF	Serviço de Estrangeiros e Fronteira
SIS	Sistema de Informações e Segurança
SGSSI	Secretário-Geral do Sistema de Segurança Interna
SRI	Segurança das Redes e de Informação
T	
TI	Tecnologias de Informação
TIC	Tecnologias de Informação e Comunicação
U	
UE	União Europeia
UIT	União Internacional de Comunicações

Introdução

O ciberespaço é uma realidade e um fenómeno muito mais complexo e abrangente do que a internet propriamente dita, compreendendo serviços, modelos de negócio, infraestruturas, diferentes dinâmicas sociais próprias, bem como diferentes tipos de atores.

O atual estado de desenvolvimento tecnológico é suscetível de criar ferramentas capazes de transformar ataques cibernéticos em verdadeiros atos de guerra, através de intrusões hostis como a manipulação ou sabotagem de infraestruturas críticas, sejam estas de comunicações, estruturas industriais sensíveis, sistemas de navegação e transportes, redes de energia, banca e serviços financeiros e outros sistemas determinantes.

É hoje inquestionável o aumento dos incidentes e ataques maliciosos, que têm como alvo infraestruturas de informação dos governos, instituições públicas e privadas, empresas e cidadãos. São raras as semanas em que não surgem notícias relacionadas com ataques cibernéticos. Acresce o facto de ser difícil reconstituir qualquer percurso criminal entre os diferentes agentes delituosos, em virtude dos atos serem praticados em diversos pontos do ciberespaço, sentindo-se os infratores protegidos pelo anonimato que este domínio lhes proporciona. Neste âmbito, as ameaças existentes no ciberespaço não devem ser encaradas numa perspetiva regional mas global, e também numa dimensão holística a qual compreende todas as áreas do conhecimento humano.

O ciberespaço é assim cada vez mais vulnerável a todo o género de práticas criminais, belicistas e subversivas. Algumas das razões para se verificar esta realidade estão relacionadas com o facto das comunicações se processarem a nível planetário entre uma rede infindável de dispositivos tecnológicos e interdependentes, em que se considera faltar o elemento territorialidade para se poder impor o direito nacional e internacional.

Por outro lado, a elevada acessibilidade ao ciberespaço, a sua falta de regulação, o seu enorme manancial de utilizadores, na maior parte das vezes mal informados acerca das ameaças provenientes do ciberespaço, bem como a forma extremamente fácil como se trocam dados, potencia ações delituosas neste meio. Por tudo isto, só asseguramos a plenitude das vantagens e oportunidades que o ciberespaço nos oferece se garantirmos a confiança da sua fiabilidade e resiliência a ameaças externas. Neste âmbito, assume especial importância a questão da proteção do ciberespaço ou cibersegurança, que envolve diversos atores intervenientes e responsáveis, onde se incluem as diversas entidades do Estado, o setor público-privado e principalmente os cidadãos. Sendo que, a partilha da informação e a cooperação no plano interno e externo entre diferentes entidades com

responsabilidades ligadas à cibersegurança torna-se decisiva na prevenção e no combate ao diferente espectro das ciberameaças.

Assim, e pelas razões expostas, justifica-se o presente tema na sua plenitude, mormente no nosso caso, em que iremos analisar a forma como as forças e serviços de segurança em Portugal poderão cooperar com as entidades intervenientes e responsáveis no domínio da cibersegurança, quer no plano nacional, quer no plano internacional.

Na nossa investigação definimos como âmbito de estudo e campo geral de investigação, a proteção do ciberespaço. Como se trata de um tema abrangente, por motivos de tempo e de amplitude do trabalho, procedemos à delimitação da nossa investigação à compreensão de qual o papel da Guarda Nacional Republicana (GNR), na cooperação com as entidades intervenientes e responsáveis no domínio da cibersegurança.

Assim, o objetivo geral desta investigação é analisar como as forças e serviços de segurança, e em particular a GNR, poderão atuar no contexto da cibersegurança na sociedade portuguesa, procurando assim acrescentar conhecimento empírico que contribua para uma visão integradora dos esforços em curso neste domínio e, consequentemente estimular e potenciar sinergias no âmbito nacional e internacional.

Para atingir este objetivo, definimos como objetivos específicos (OE), os seguintes:

- OE1. Compreender a importância estratégica da proteção do ciberespaço;
- OE2. Analisar o enquadramento normativo da cibersegurança;
- OE3. Definir o quadro de intervenção das forças e serviços de segurança no âmbito da cibersegurança;
- OE4. Apresentar um modelo de atuação da GNR no quadro da cibersegurança.

A necessidade de desenvolver uma estratégia integradora e mobilizadora de sinergias nacionais, capaz de reduzir o risco social e potenciar a utilização do ciberespaço deu origem à definição de uma proposta de Estratégia Nacional de Cibersegurança. Com esta estratégia procura-se proteger as áreas que materializam a Soberania Nacional, assegurando a autonomia política e estratégica da Nação, mas sobretudo impor a cibersegurança como uma prioridade nacional. No mesmo sentido, a Estratégia Nacional de Combate ao Terrorismo preconiza a implementação de um plano de ação nacional para a proteção contra as ciberameaças, integrado numa Estratégia Nacional de Cibersegurança. E o estudo "Segurança Interna Horizonte 2025 - Um Conceito Estratégico de Segurança Interna", do Grupo de Reflexão Estratégica sobre a Segurança Interna (GRESI), menciona explicitamente que a atividade de segurança interna também deverá ser exercida no

ciberespaço. Ora, é precisamente neste cenário onde se pretende edificar uma estrutura nacional lógica e coerente, que nos propomos refletir, emergindo naturalmente a seguinte Questão Central (QC): "Em que medida as forças e serviços de segurança, poderão cooperar com as entidades intervenientes e responsáveis no domínio da cibersegurança?"

Associadas à QC, foi possível formular as seguintes Questões Derivadas (QD):

- QD1: Qual a importância estratégica da proteção do ciberespaço?
- QD2: A cibersegurança tem um enquadramento normativo ajustado à realidade nacional?
- QD3: Qual o quadro de atuação das forças e serviços de segurança no domínio da cibersegurança?
- QD4: De que modo a GNR pode atuar e cooperar no quadro da cibersegurança?

O processo de investigação desenvolveu-se em função das questões levantadas, central e derivadas, que assumem, inevitavelmente, um papel orientador de todo o processo (Cfr. Modelo de análise em Apêndice B). Neste sentido, optamos por uma estratégia de investigação qualitativa, pois fundamentou-se no facto de existir um número reduzido de unidades de amostragem, mas também por se pretender a recolha de informação em profundidade e em continuidade, possibilitando a exploração de uma multiplicidade de facetas e dimensões, com o objetivo de compreender o fenómeno em estudo na sua totalidade.

Relativamente ao *design* da pesquisa adotada, optámos pelo estudo de caso, dado que elaboramos uma análise detalhada e intensiva de um único caso, ou seja, a atuação e cooperação da GNR no quadro da cibersegurança, possibilitando, assim, captar a complexidade e a natureza particular do caso em questão. Os métodos e instrumentos utilizados foram a entrevista individual semiestruturada - com base num guião com um conjunto de tópicos a colocar ao entrevistado - e a análise documental. Outro elemento essencial é a definição do principal método de amostragem, que nesta investigação será a amostragem intencional. Embora, seja um método não probabilístico, o que não permite a generalização dos resultados, garante que os casos sejam selecionados de forma estratégica (Cfr. Percurso metodológico e a definição da estratégia metodológica em Apêndice A).

O presente trabalho encontra-se estruturado em quatro capítulos, que procuram dar uma sequência lógica a toda a investigação, de forma a conseguir responder às questões de investigação levantadas anteriormente.

No primeiro capítulo abordamos a dimensão estratégica do ciberespaço, em que inicialmente identificamos os conceitos estruturantes da presente investigação de forma a apresentar um sucinto quadro conceptual e subsequentemente explicamos a importância deste novo domínio na vertente da segurança e defesa. No segundo capítulo caraterizamos o enquadramento normativo da cibersegurança, apresentando numa primeira fase no âmbito do quadro internacional, as principais organizações e normativos em vigor e subsequentemente no quadro nacional, expomos os normativos jurídicos mais relevantes e orientações estratégicas nesta área. De seguida, no terceiro capítulo, apresentamos o enquadramento geral de atuação das forças e serviços de segurança no âmbito da cibersegurança e analisamos particularmente a atuação da GNR neste domínio. E, no quarto capítulo efetuamos a análise e apresentação dos resultados, respondendo às questões de investigação e avaliando os contributos para o conhecimento. O trabalho de investigação individual termina com as conclusões obtidas, limitações do estudo, bem como com sugestões para investigações futuras.

1. Dimensão estratégica da proteção do ciberespaço

"A estruturação em rede das sociedades mais desenvolvidas e a criação do ciberespaço constituem caraterísticas fundamentais da conjuntura estratégica do século XXI, e neste âmbito, pensar o mundo em que vivemos passa por perspetivar uma sociedade em rede, em que a interação entre os homens deixa de estar influenciada por barreiras geográficas e passa a ser condicionada pela disponibilidade e pelo tempo de acesso aos recursos de informação" (IDN-CESEDEN, 2013, p. 8). Para a compreensão da dimensão do ciberespaço, iremos de seguida, apresentar um breve enquadramento dos conceitos teóricos que consideramos nucleares e abordar a importância da proteção do ciberespaço na vertente da segurança e defesa, e do seu papel crucial para o normal funcionamento das infraestruturas críticas.

a. Ancoragem conceptual

A nível internacional, quando abordamos os conceitos relacionados com o ciberespaço e a cibersegurança, os termos frequentemente usados são normalmente expressos em inglês, mas tendo geralmente o seu significado diferentes matrizes, dependendo do país de origem e de quem os usa. Verifica-se assim que nem sempre é possível encontrar concordância com a tradução direta dos termos anglo-saxónicos que os compõem (IDN-CESEDEN, 2013, p. 11). E quanto à cibersegurança ou proteção do ciberespaço importa mencionar, que não existe uma definição que seja consensual quer a nível nacional ou internacional. De facto, um relatório recente que comparou estratégias de cibersegurança nacionais de países, considerados de referência nesta área, destacou precisamente a inexistência de uma definição comum e harmonizada de cibersegurança, o que pode, por exemplo, causar confusão entre os diversos países quando do estudo de abordagens internacionais contra as ameaças globais do ciberespaço (Pierre Audoin Consultants , 2013, p. 14).

Admitida assim a ideia da multiplicidade de conceitos, revela-se conveniente construir e apresentar no âmbito da presente investigação, um sucinto - mas necessariamente enquadrador - quadro conceptual sobre a temática, recorrendo para isso à autoridade de peritos e entidades relevantes nesta matéria.

Partindo deste pressuposto, iniciamos pelo conceito de ciberespaço[1], sendo que este foi criado e popularizado por William Gibson (1984, p. 12) no seu romance intitulado

[1] Para uma análise mais aprofundada sobre o âmbito do ciberespaço ver Castells (2004), Murray (2007) e Mayer, et al. (2014).

"Neuromancer", onde previa que a crescente dependência da sociedade dos computadores e tecnologias de informação criaria um universo virtual eletrónico, que designou por ciberespaço. Conforme refere Fernandes (2014, p. 68), o ciberespaço "designa hoje a rede global de infraestruturas de tecnologias de informação interligadas entre si, especialmente as redes de telecomunicações e os sistemas de processamento dos computadores". Segundo Kuehl (2009, pp. 24-42) o ciberespaço é um domínio operacional cujo caráter distintivo e único, é enquadrado pela utilização da eletrónica e do espetro eletromagnético para criar, guardar, modificar, trocar e explorar informação através de sistemas baseados em tecnologias de comunicação da informação interligados e as suas infraestruturas associadas.

E segundo Caldas (2011, p. 94),

> "se entendermos o ciberespaço como todo o espaço ou território que integra as redes eletrónicas ou de comunicação que constituem a infraestrutura sobre a qual são criados, tratados, armazenados e distribuídos fluxos de informação, então a cibersegurança[2] deve ser de igual modo entendida como a segurança desse mesmo espaço cibernético."

Referindo ainda o mesmo autor (2011, p. 94), "que o conceito de cibersegurança numa visão alargada cobre todas as dimensões de segurança que afetam o designado ciberespaço ou espaço cibernético".

Conforme assinalado na estratégia da União Europeia (UE) para a cibersegurança (2013, p. 3), a cibersegurança refere-se, por norma, às precauções e ações que podem ser utilizadas para proteger o ciberespaço, tanto nos domínios civil como militar, contra as ameaças decorrentes da interdependência das suas redes e infraestruturas informáticas ou que as possam danificar, procurando-se assim manter a disponibilidade e a integridade das redes e infraestruturas e a confidencialidade das informações nelas contidas.

Relativamente ao termo cibercrime, segundo Ghernaoti (2013, p. 25) este pode ser definido como qualquer atividade criminosa realizada através do ciberespaço ou da internet. Inclui todas as formas de ações criminosas digitais levadas a efeito através de tecnologias digitais, dispositivos eletrónicos e redes de telecomunicações. O conceito de cibercrime refere-se, geralmente, a um amplo leque de diferentes atividades criminosas que

[2] Sobre os conceitos de cibersegurança ver ainda Thampi, et al. (2014), Fisher (2009) e Andreasson (2012).

envolvem os computadores e os sistemas informáticos, quer como instrumentos quer como alvos principais. A cibercriminalidade[3] inclui as infrações tradicionais, infrações relativas aos conteúdos (e.g., distribuição de material pedopornográfico) e crimes respeitantes exclusivamente a computadores e sistemas informáticos (Comissão Europeia, 2013, p. 3).

E no que concerne à ciberguerra[4], o documento de terminologia conjunta dos Estados Unidos para as operações cibernéticas define-a como "um conflito armado conduzido somente ou em parte, por meios cibernéticos. As operações militares conduzidas para negar à força opositora a utilização eficaz dos sistemas de ciberespaço e de armas no conflito. Inclui ataques cibernéticos, ações de defesa e facilitação de cibernética" (U.S. Department of Defense, Joint Chiefs of Staff, 2011). Segundo Fernandes (2014, p. 153) a ciberguerra pode ser caraterizada como a utilização, ofensiva e defensiva, dos sistemas de informação e comunicação, para negar, corromper ou destruir a informação de um adversário atacando os seus sistemas e redes de computadores.

Profundamente relacionados com os conceitos anteriormente apresentados surgem-nos os conceitos de ciberterrorismo, hacktivismo e ciberespionagem Assim, entende-se por ciberterrorismo[5] a utilização da internet e das tecnologias de informação com motivações ideológicas, para organizar e executar ataques contra as redes de computadores, sistemas e infraestruturas de telecomunicações (Natário, 2013, p. 320). Por hacktivismo[6] entende-se a utilização de técnicas e software específico, tendo em vista explorar tecnologias de informação de forma pouco usual ou ilegal, para aumentar a visibilidade, influência e capacidade de intervenção para uma determinada causa, sendo esta técnica usada principalmente contra Estados e grandes empresas (Santos, et al., 2008, p. 81). E por ciberespionagem[7] entende-se o ato ou a prática de obtenção de informações classificadas ou sensíveis de indivíduos, governos ou inimigos, para obtenção de vantagens militares, políticas ou económicas, através da utilização de métodos de exploração ilegais na internet, redes, software ou computadores (ENISA, 2013, p. 1).

Estudando as relações entre estes conceitos no ciberespaço, Santos (2011, p. 18) considera que "o espectro de motivações observadas estende-se desde o gozo pessoal e o estatuto dentro de um grupo decorrentes da experimentação de técnicas de *hacking* numa

[3] Sobre os conceitos de cibercriminalidade ver ainda Kierkegaard (2008), Brenner (2010) e McQuade (2009).
[4] Para uma análise mais aprofundada sobre a ciberguerra *vide* Libicki (2009), Clarke & Knake (2010), Ventre (2011) e Rosenzweig (2013).
[5] Sobre o âmbito do ciberterrorismo ver ainda Last & Kandel (2005).
[6] Para uma melhor compreensão do *hacktivism vide* Jordan & Taylor (2004) e Donk, et al. (2004).
[7] Em relação aos conceitos de ciberespionagem ver ainda Ventre (2011).

das extremidades, até à obtenção de uma vantagem competitiva de um Estado relativamente a outro, na outra". O perfil dos autores pode ser caracterizado através do binómio composto pelo grau de conhecimentos técnicos e pelo nível de profissionalismo ou associação criminosa. A figura seguinte resume o pensamento deste autor:

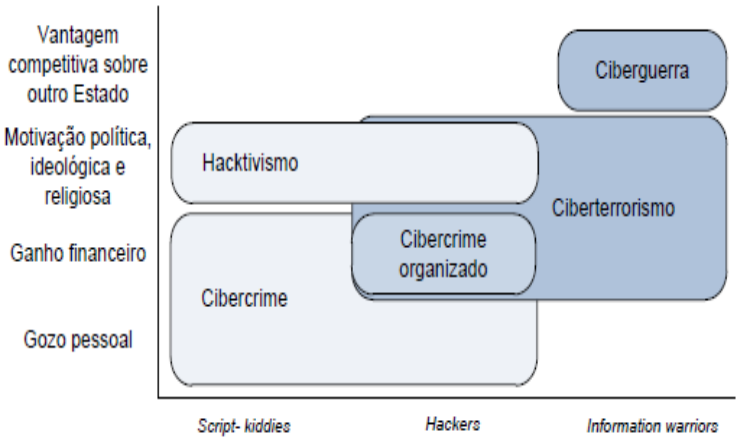


Figura 1-Espetro de ameaças
Fonte: (Santos, 2011, p. 17)

Por último, e no mesmo sentido Klimburg (2011, p. 41) refere que "cibercrime, ciberterrorismo e ciberguerra partilham uma base tecnológica comum, ferramentas, logística e instrumentos. Podem também partilhar as mesmas redes sociais e ter objetivos similares. As diferenças entre estas categorias de ciberatividades são frequentemente ténues, ou estão apenas nos olhos de quem as vê."

b. Um novo domínio

"As infraestruturas de informação e o ciberespaço são indispensáveis na nossa sociedade, e o seu correto funcionamento assume importância crucial para a livre circulação da informação e dos processos e serviços dependentes desse fluxo" (Nunes, 2010, p. 1194). Para se ter uma visão panorâmica desta rede procedemos à análise das estatísticas disponíveis referentes à internet. Segundo a *Internet World Stats*[8], o número de utilizadores da internet supera já os 3 mil milhões de utilizadores ativos em todo o mundo, distribuídos conforme a figura seguinte, encontrando-se o valor mais significativo (1,386 mil milhões) na Ásia, que é também o continente mais populoso e heterogéneo do planeta.

[8] Conforme sítio da *Internet World Stats*, em http://www.internetworldstats.com/stats.htm [acedido em 02/04/1015]. Os dados apresentados são referentes a 30 de junho de 2014.

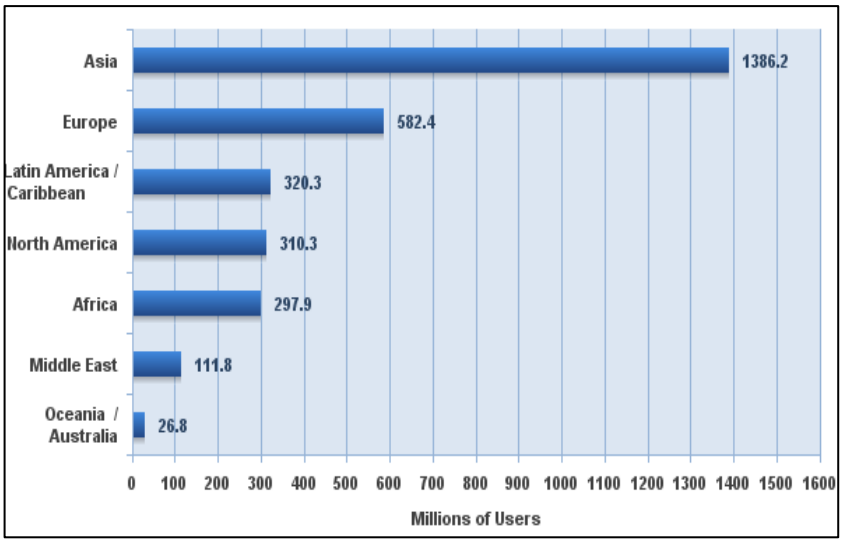


Figura 2- Utilizadores de internet por região geográfica
Fonte: *Internet World Stats*

Relativamente à taxa atual de penetração da internet (percentagem de utilizadores da internet na população total) a nível global esta é de 42,3%, enquanto na Europa, Oceânia/ Austrália, e na América do Norte, as taxas de penetração são muito superiores, respetivamente 70,5% na Europa, 72,9% na Oceânia/Austrália e 87,7% na América do Norte[9].

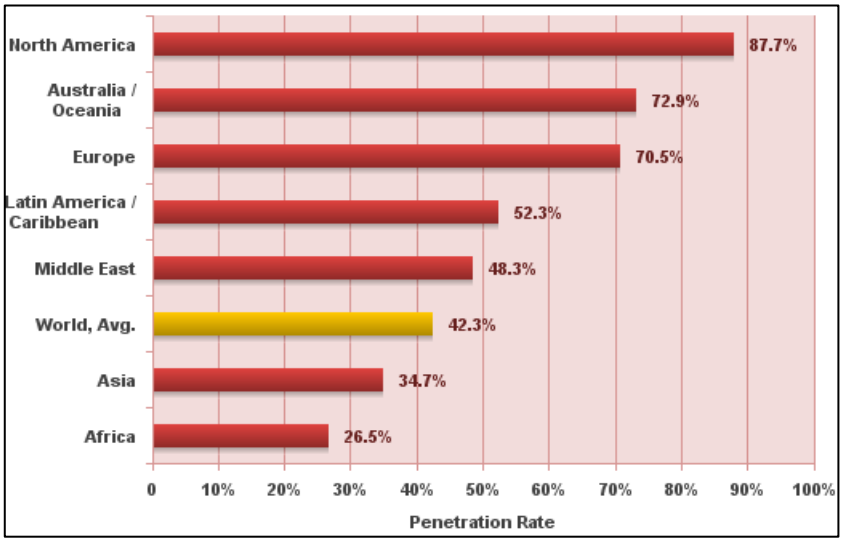


Figura 3- Taxa de penetração da internet por região geográfica
Fonte: *Internet World Stats*

Mas o "ciberespaço não se limita à internet, sendo uma experiência mais vasta, de imersão numa verdadeira plataforma de comunicação a nível global" (Natário, 2013, p. 826), da qual o Departamento de Defesa dos EUA (DoD) reconhece oficialmente a sua

[9] Os dados apresentados são também referentes a 30 de junho de 2014.

dependência para o funcionamento efetivo da sua estrutura, referindo que opera mais de 15 mil redes e 7 milhões de dispositivos de computação, distribuídos por centenas de países em todo o mundo (DoD, 2011, p. 1).

Neste âmbito, Fernandes (2014, p. 44) acrescenta ser inegável a existência de um processo que considera de globalização, sendo expectável que o número de utilizadores do ciberespaço aumente significativamente nas próximas décadas.

Assim, no mundo globalizado de hoje, em que se procura o acesso a grandes quantidades de informação em tempo útil, o ciberespaço constitui uma dimensão crítica do funcionamento normal da sociedade moderna, da sua segurança, da sua economia e dos seus negócios[10]. A necessidade de acesso e troca permanente de informação tem inerentemente associada critérios de segurança, uma vez que a informação deve ser protegida contra acessos ou modificações não autorizados (IDN-CESEDEN, 2013, p. 10). Pelo que, o ciberespaço e as redes de informação e de comunicações se tornaram indispensáveis para a sociedade. Sendo a sua proteção, resiliência e vulnerabilidades questões de vital importância[11].

E como alerta Viana (2012, p. 5), é neste espaço comum que assentam as redes de telecomunicações vitais, de transporte e de distribuição de energia das quais dependem o comércio global, a segurança energética e a prosperidade das sociedades modernas.

Ciente da importância do ciberespaço, a UE (2013, p. 20) no âmbito da sua estratégia para a cibersegurança – que será caraterizada no capítulo seguinte - alertou para a necessidade dos Estados-Membros disporem de "estruturas preparadas para garantir a resiliência do ciberespaço, combater a cibercriminalidade e prover à defesa" e serem capazes de atingir o nível de capacidade necessário para lidar com incidentes informáticos.

Também, a Organização do Tratado do Atlântico Norte (NATO) no seu conceito estratégico elegeu como uma das maiores ameaças atuais, a competição e a denegação do uso do ciberespaço, enquanto espaço comum, face à crescente sofisticação dos ataques cibernéticos e aos danos que podem infligir no funcionamento dos sistemas dos governos, na economia e infraestruturas críticas (Viana, 2012, p. 6).

E como identifica Cavelty (2008, p. xi) à medida que a rede de comunicações global se continua a desenvolver a um ritmo alucinante, impulsionada por desenvolvimentos inovadores em tecnologia, a capacidade dos Estados para garantir a segurança das redes é

[10] Relacionado com este âmbito ver ainda Grady & Parisi (2006).
[11] Para uma análise mais aprofundada *vide* Kremer & Muller (2014).

cada vez mais baseada na interdependência entre as agências e na cooperação com outros governos. Este autor alerta-nos também para a crescente dependência da internet que levanta sérias preocupações políticas de regulação, privacidade, direitos de autor e acesso.

Atento ao quanto fica exposto, Halpin (2006, p. 73) apresenta-nos o paradoxo atual no âmbito da cibersegurança quando observa que "para muitas aplicações, precisamos, de sistemas altamente disponíveis, confiáveis e seguros. Para muitas aplicações críticas, precisamos de força em profundidade. O que temos, na prática, é a fraqueza em profundidade. Os sistemas de informação e redes estão cheias de vulnerabilidades e de elos fracos."

No âmbito das ameaças[12], como sintetiza Magriço (2014, p. 9):

> "Para muitos utilizadores das novas tecnologias de informação, o ciberespaço proporciona acesso à informação e entretenimento, construção de coletivos inteligentes e oportunidade de estabelecimento de novos fluxos comunicacionais, facilitando o contacto entre pessoas espalhadas por diversas regiões do planeta. Para outros, no entanto este ambiente equivale a um território sem lei, o que justifica todo o tipo de condutas, já que é um espaço à parte, subtraído de qualquer ingerência ou censuras sociais, o que possibilita desde a prática de atos que não são realizados em contactos de face a face em razão das regras de boa conveniência, até ao estabelecimento de redes invisíveis de criminalidade."

Neste sentido, Cavelty (2008, p. 31) menciona que devido à natureza global das redes de informação, os ciberataques podem ser lançados a partir de qualquer lugar do mundo, e descobrir a sua origem, continua a ser uma grande dificuldade, podendo estes ser realizados de inúmeras maneiras por qualquer pessoa com um computador ligado à internet, e para fins que vão desde a pirataria juvenil, crime organizado, ativismo político à guerra estratégica.

Também a NATO refere no seu documento estratégico (2010) que "os ciberataques estão a tornar-se mais frequentes, mais organizados e mais custosos nos danos que infligem às administrações governamentais, (…) redes de transporte e fornecimento, bem como a

[12] Sobre as ameaças, para uma análise mais aprofundada, ver Norwood & Carwell (2009). O Relatório Anual de Segurança Interna (RASI) de 2014 destaca, entre outras ameaças, a "de natureza ciber que se manifesta no cibercrime organizado, no *hacktivismo*, na espionagem e no terrorismo" (2015, p. 10).

outras infraestruturas críticas; podem atingir um patamar que ameaça a prosperidade nacional e Euro-Atlântica, a segurança e a estabilidade."

A este respeito os autores Santos, Bravo e Nunes (2012, p. 164) referem a existência de três domínios de atuação face aos ciberataques, respetivamente o domínio da proteção simples, o domínio da prossecução criminal e o domínio da defesa do Estado, apresentando e caraterizando o âmbito de cada um destes domínios, cuja sistematização se encontra descrita na tabela seguinte:

Tabela 1- Domínios de atuação na proteção do ciberespaço
Fonte: (Santos, et al., 2012, p. 165)

	Proteção Simples	**Prossecução criminal**	**Defesa do Estado**
Caraterização	Os ciberataques são vistos como ameaças à disponibilidade, integridade e confidencialidade da informação e de outros ativos.	Os ciberataques são vistos como atos criminalmente relevantes.	Os ciberataques são vistos como um ato de Guerra, pondo em risco a existência do Estado.
Objetivos	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.
Aspetos legais e constitucionais	Salvaguarda dos direitos individuais e da privacidade dos cidadãos.	Atuação dentro do quadro da legislação aplicável e segundo as regras do sistema judicial.	Atuação sujeita à Constituição da República, Lei do Estado de Sítio e do Estado de Guerra, bem como ao Direito Internacional dos Conflitos Armados e dos Direitos Humanos.
Atores	Técnicos de sistemas de redes, Indústria TIC, autoridades reguladoras setoriais, CSIRT, utilizadores TIC.	Órgãos de polícia criminal, Ministério Público e Magistrados Judiciais	Forças Armadas e Serviços de Informações.

Estes autores referem ainda "que a resposta a ciberataques contra infraestruturas da informação críticas pressupõe sempre uma intervenção no domínio da proteção simples, podendo ainda, considerando a sua motivação e a extensão do seu impacto, implicar a ação nos domínios da prossecução criminal e da defesa do Estado" (Santos, et al., 2012, p. 172), sendo esta articulação entre os domínios retratada na seguinte figura:

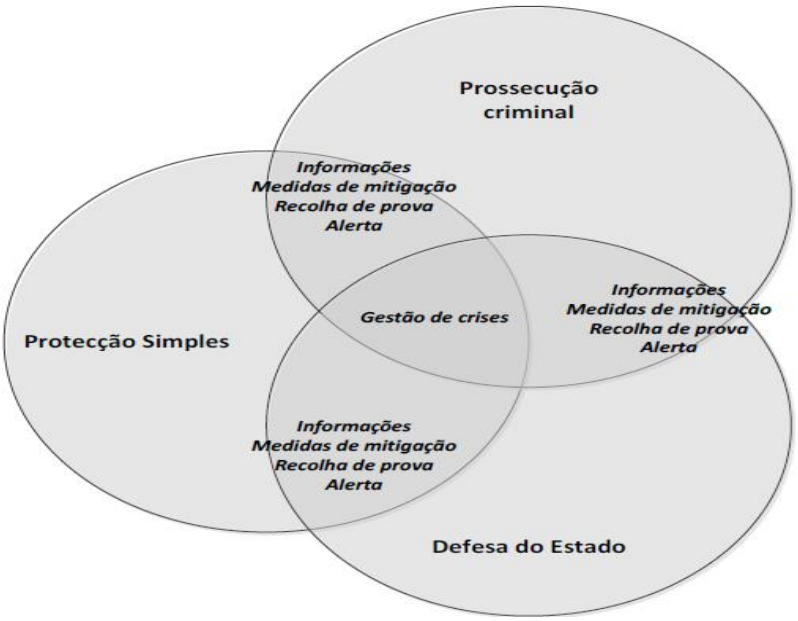


Figura 4- Articulação entre domínios de atuação
Fonte: (Santos, et al., 2012, p. 173)

No âmbito particular da defesa[13], a terra, o mar, o ar e o espaço têm constituído os domínios tradicionais de desenvolvimento das operações militares e, por conseguinte, é neles que se têm centrado os esforços relacionados com a obtenção de capacidades militares. No entanto, o ciberespaço já foi definido e aceite como o quinto domínio operacional, no qual se levam a cabo operações militares específicas e em relação ao qual as operações militares que se desenvolvem nos outros domínios dependem cada vez mais (IDN-CESEDEN, 2013, p. 11).

Esta interdependência entre todas as dimensões encontra-se bem expressa na seguinte figura que integra o *FM 3-38 Cyber Electromagnetic Activities*:

[13] Para uma análise mais aprofundada, no âmbito da defesa, ver Rosenzweig (2013), Ventre (2011) e Libicki (2009).

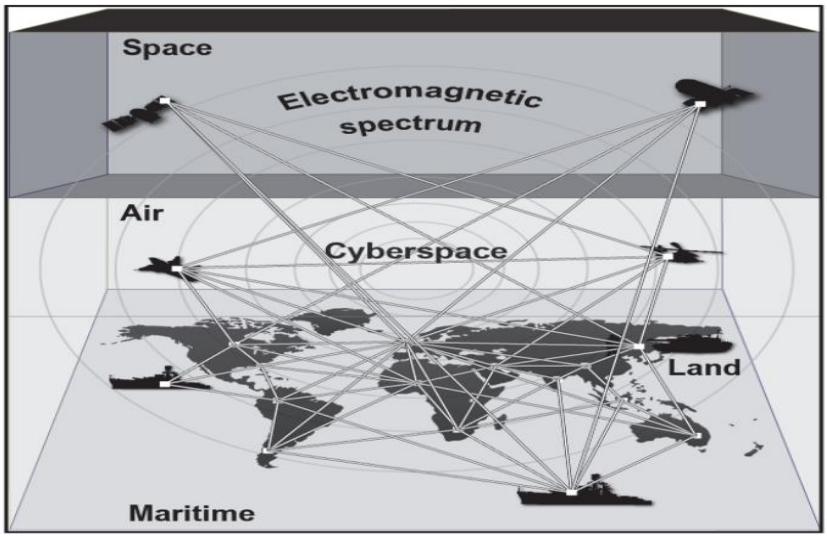


Figura 5- Relação entre os cinco domínios e o espetro eletromagnético
Fonte: *FM 3-38* (2014, pp. 1-4)

E como ensina Santos (2014, p. 20) o ciberespaço permite produzir efeitos pelo facto de constituir uma plataforma global de circulação da informação no âmbito do espaço de operações mediático, com a possibilidade de agir através das perceções da realidade que se podem produzir e difundir globalmente, e por constituir a base de sustentação das infraestruturas críticas em que se alicerça o funcionamento das sociedades modernas, cuja importância será de seguida abordada.

Relativamente às infraestruturas críticas[14] estas são elementos-chave ao bem-estar social das comunidades em que se inserem. Embora a definição exata daquilo que é considerado crítico varie de país para país, há um fio condutor que liga todas as definições, que é a sua importância para o funcionamento normal da sociedade (Nunes & Natário, 2014, p. 249).

Outro elemento essencial, face ao funcionamento das sociedades modernas, deriva das infraestruturas críticas não serem um elemento isolado mas sim parte de um todo sistémico, interligado por relações de equilíbrio e interdependência, sendo que a falta de um dado elemento poderá colocar em causa todo o sistema. Desta forma, infraestruturas que se encontram dentro do território de determinado Estado poderão desempenhar funções vitais no funcionamento de infraestruturas situadas no território de um outro Estado, senão mesmo em vários outros Estados. No contexto das ameaças atuais o setor da informação e tecnologias de informação enfrenta desafios significativos, particularmente

[14] No âmbito das infraestruturas críticas *vide* ainda Grady & Parisi (2006) e Beggs (2010).

ao nível das infraestruturas das telecomunicações. Neste sector incluem-se sistemas de informação, sistemas de controlo, redes, internet, telecomunicações fixas, telecomunicações móveis, comunicações rádio, comunicações satélite e banda larga. A suspensão, mesmo que temporária, do funcionamento de serviços situados no sector da informação e tecnologias da informação além de desencadear resultados catastróficos imediatos colocaria em causa a coordenação e resposta a uma crise (Rocha, 2008, pp. 133-134). Esta interdependência encontra-se exemplificada na seguinte figura:

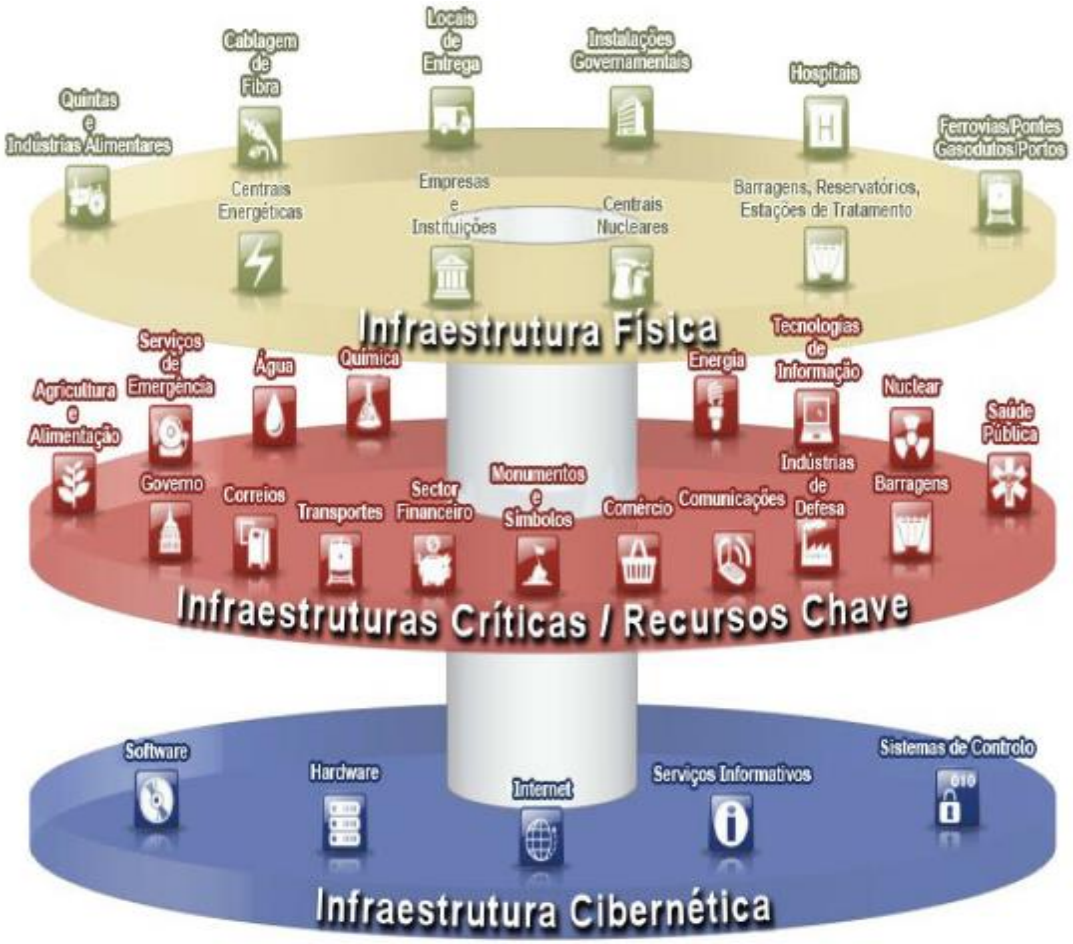


Figura 6 - A infraestrutura cibernética como base de todas as outras
Fonte: (Nunes & Natário, 2014, p. 256) adaptado de Beggs (2010)

E segundo Kowalik (2004, p. 60), torna-se necessário reconhecer que é impossível garantir totalmente a segurança de sistemas complexos, tais como as infraestruturas críticas. Portanto terão que ser desenvolvidas soluções sabendo que falhas de segurança ocorrerão. A questão não é desenvolver soluções que irão proteger um sistema para sempre, mas colocar em prática uma estratégia de adaptação a situações inesperadas.

Em suma e como síntese deste capítulo podemos afirmar que no mundo globalizado dos dias que correm, um dos desafios que mais prementemente se colocam aos Estados é o da cibersegurança. Nesta linha, revela-se crucial que quando falamos de ciberespaço, cibersegurança e dos outros conceitos neste âmbito associados, os mesmos se possam definir com clareza, não deixando ambiguidades ou incertezas na interpretação. Com efeito, e como refere Natário (2013, p. 313), o "ciberespaço envolve-nos de forma silenciosa e omnipresente. O crescimento explosivo da Internet trouxe consigo uma série de efeitos sociais e culturais que têm moldado todo o panorama mediático e cujos efeitos são cada vez mais visíveis (…)".

2. Enquadramento normativo da Cibersegurança

"A necessidade de edificar mecanismos de proteção e defesa, destinados a garantir a livre circulação da internet e do ciberespaço, tem encaminhado os Estados para o aprofundamento de uma cultura de cibersegurança e à tomada de consciência coletiva, relativamente à importância do desenvolvimento de políticas e estratégias cooperativas de combate a todas as formas de ataque cibernético" (IDN-CESEDEN, 2013, p. 51). Assim, a nível internacional[15] e nacional têm vindo a surgir normativos de cooperação, iniciativas legais e entidades "que definem normas e princípios destinados a garantir uma internet sustentável e um comportamento aceitável no ciberespaço" (IDN-CESEDEN, 2013, p. 51) sendo os mais relevantes, no âmbito da segurança e defesa[16], de seguida apresentados.

a. O quadro internacional

(1) Organização das Nações Unidas

A nível das Nações Unidas, destacamos o papel da União Internacional de Comunicações (UIT) que é a agência especializada nas tecnologias de informação e comunicação. Os seus objetivos estão definidos na Constituição e Convenção da UIT[17]. A Constituição contém não só as disposições gerais em matéria de obrigações e direitos para os Estados no que diz respeito às telecomunicações (e.g., as melhores práticas que devem ser aplicadas em relação à manutenção das linhas de comunicação) mas também as obrigações dos Estados da proteção e manutenção dos seus meios de telecomunicação, aplicando-se assim à internet (Alexander Klimburg , 2012, p. 154).

A nível de iniciativas salientamos o lançamento pela UIT em 2007 da *Global Security Agenda*, a nível de cooperação internacional visando aumentar a confiança e a segurança da sociedade da informação, e o lançamento em 2009 do *Draft Cybercrime Legislation Toolkit*, com o propósito de fornecer exemplos de normas e materiais de referência como meios auxiliares na criação de leis e procedimentos harmonizados (Natário, 2013, p. 845).

[15] Para aprofundar o âmbito das iniciativas normativas internacionais ver Portnoy & Goodman (2009).
[16] Pelo que, nesta ótica apesar de desempenharem um papel importante não abordaremos as organizações de normalização e gestão da internet, como por exemplo, a *Internet Corporation for Assigned Names and Numbers* (ICANN), a *Internet Governance Forum* (IGF) e a *Internet Society* (ISOC).
[17] Estes normativos estão disponíveis no sítio http://www.itu.int/pub/S-CONF-PLEN-2011 [acedido em 3 de abril de 2015].

(2) Conselho da Europa

No âmbito do Conselho da Europa é de relevar, a Convenção sobre o Cibercrime de 23 de novembro de 2001[18] que visa "proteger a sociedade da criminalidade no ciberespaço, nomeadamente através da adoção de legislação adequada e da melhoria da cooperação internacional" de modo a "tornar mais eficazes as investigações e os procedimentos criminais relativos a infrações relacionadas com sistemas e dados informáticos, bem como permitir a recolha de provas por meio eletrónico de uma infração penal" [19].

Sobre a Convenção torna-se importante referir que "sendo o primeiro tratado internacional sobre criminalidade contra sistemas de computadores, redes ou dados, pretendeu harmonizar as várias legislações nacionais sobre a matéria, propiciar e facilitar a cooperação internacional e facilitar as investigações de natureza criminal" (Verdelho, et al., 2003). Para atingir este desiderato a Convenção impõe aos Estados signatários que adequem a sua legislação penal interna às especificidades do cibercrime, visando assim a harmonização de legislações, incluindo os instrumentos processuais e de produção de prova adequados e simplificando a cooperação internacional de modo a facilitar e agilizar a deteção, a investigação e a recolha de prova (Dias, 2010, p. 31).

Visando a harmonização penal, a Convenção sobre o Cibercrime divide os crimes em três tipos de infrações:

- Infrações penais contra a confidencialidade, integridade e disponibilidade de dados e sistemas informáticos - que inclui no art. 2.º o acesso ilegítimo, no art. 3.º a interceção ilegítima, no art. 4.º a interferência em dados, no art. 5.º a interferência em sistemas e no art. 6.º o uso abusivo de dispositivos;
- Infrações penais relacionadas com computadores - que abrange no art. 7.º a falsidade informática e no art. 8.º a burla informática;
- Infrações penais relacionadas com o conteúdo e relacionadas com a violação do direito de autor e direitos conexos - que inclui no art. 9º as infrações penais relacionadas com a pornografia infantil e no art. 10º as infrações no âmbito do direito de autor e direitos conexos (Assembleia da República, 2009).

[18] Para uma análise mais aprofundada desta Convenção consultar Verdelho, et al. (2003) e Simas (2014).

[19] Conforme preâmbulo da Convenção sobre o Cibercrime, aprovada pela Resolução da Assembleia da República n.º 88/2009, de 15 de setembro. Tendo igualmente sido aprovado o protocolo adicional relativo à incriminação de atos de natureza racista e xenófoba praticados através de sistemas informáticos (Assembleia da República, 2009).

(3) União Europeia

Para a EU, o ciberespaço é uma "área de justiça" onde os direitos humanos, a liberdade de expressão, o direito à privacidade e a proteção de dados pessoais devem ser preservados e, através de um esforço cooperativo de todos os Estados membros, os criminosos devem ser identificados e responsabilizados (IDN-CESEDEN, 2013, p. 64).

A estratégia da UE para a cibersegurança também refere os valores que são do interesse dos cidadãos europeus: as leis[20] e normas, a proteção de direitos fundamentais, a liberdade de expressão, os dados pessoais e a privacidade, o acesso para todos, a governação multilateral, democrática e eficiente e a responsabilidade compartilhada para garantir a segurança (Comissão Europeia, 2013, p. 4). Esta estratégia articula-se e desenvolve-se em cinco prioridades estratégicas:

- Garantir a resiliência do ciberespaço;
- Reduzir drasticamente a cibercriminalidade[21];
- Desenvolver a política e as capacidades no domínio da ciberdefesa no quadro da política comum de segurança e defesa (PCSD);
- Desenvolver os recursos industriais e tecnológicos para a cibersegurança;
- Estabelecer uma política internacional coerente em matéria de ciberespaço para a União Europeia e promover os seus valores fundamentais (Comissão Europeia, 2013, p. 5)

Relativamente às entidades europeias relevantes nesta temática, destacamos como mais relevantes, a Agência Europeia para a Segurança das Redes e da informação (ENISA)[22], o Centro Europeu da Cibercriminalidade (EC3)[23] no quadro da EUROPOL, o *Computer Energency Response Team (CERT)* da UE[24], a Academia Europeia de Polícia (CEPOL)[25] e a Agência de Defesa Europeia (EDA)[26].

A figura seguinte sintetiza a visão da UE, da ligação das diversas entidades europeias às entidades nacionais, com diferentes funções e a sua articulação em torno de três pilares

[20] Sobre as iniciativas legislativas no âmbito da UE ver Murray (2007) e Marsden (2011).
[21] A questão da cibercriminalidade também é identificada como uma ameaça comum importante na Estratégia de segurança interna da UE (Conselho da Europa, 2010).
[22] Para mais informações sobre esta agência consultar o sítio https://www.enisa.europa.eu/.
[23] Consultar também o sítio https://www.europol.europa.eu/content/megamenu/european-cybercrime-centre-ec3. Importa destacar a estreita ligação com a INTERPOL nesta área, conforme referido no sítio http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime.
[24] Para mais informações consultar o sítio http://cert.europa.eu/cert/plainedition/en/cert_about.html.
[25] Sobre a CEPOL consultar o sítio https://www.cepol.europa.eu/.
[26] Ver também o sítio http://www.eda.europa.eu/.

fundamentais – (i) a segurança das redes e da informação (SRI), (ii) a repressão e (iii) a defesa – de forma a tentar resolver os problemas da cibersegurança de modo integrado:

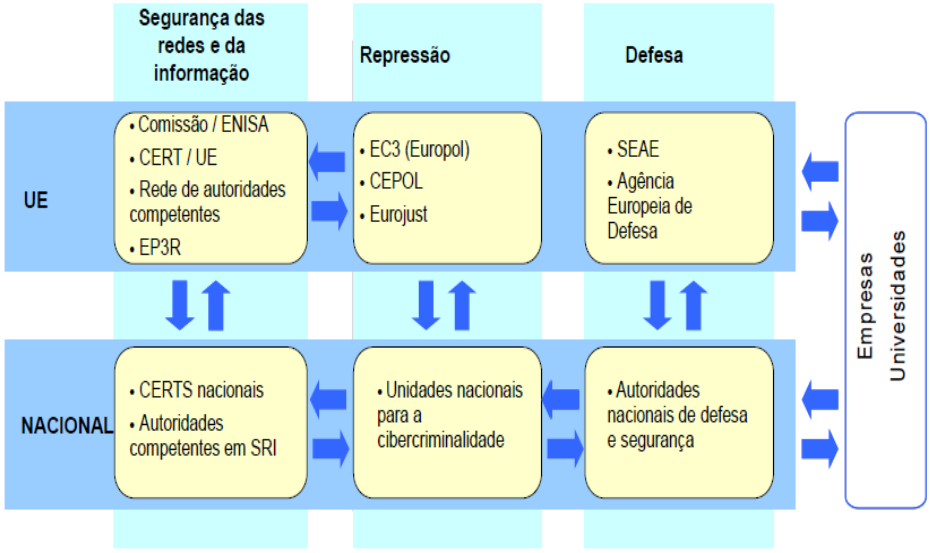


Figura 7- Entidades europeias no âmbito cibersegurança
Fonte: (Comissão Europeia, 2013, p. 20)

(4) Organização do Tratado do Atlântico Norte

Também a Organização do Tratado do Atlântico Norte (NATO) tem vindo a desenvolver atividades significativas nesta área. O seu conceito estratégico aprovado na Cimeira de Lisboa, que ocorreu em 18 e 19 de novembro de 2010, quanto às capacidades de defesa e dissuasão prevê que deve assegurar a totalidade das capacidades necessárias para dissuadir e defender contra qualquer ameaça à segurança das populações. Relativamente aos ciberataques[27] estabeleceu que deverá desenvolver mais a capacidade de prevenir, detetar e recuperar de ciberataques, acrescentando ainda que deverá reforçar e coordenar as capacidades de ciberdefesa nacionais, colocando todos os organismos da organização sob uma ciberproteção centralizada e integrando, melhor a ciberconsciencialização, aviso e resposta com os Estados-Membros (NATO, 2010).

Neste domínio, uma capacidade importante da NATO[28] é o apoio aos seus membros pelo *NATO Computer Incident Response Capability* (NCIRC) na proteção e resposta a

[27] Segundo Jens Stoltenberg, Secretário-Geral da NATO, foram registados em 2014 nos sistemas da NATO cerca de 3000 eventos de cibersegurança, conforme referido em http://www.nato.int/cps/en/natohq/opinions_116854.htm?selectedLocale=en [acedido em 4 de abril de 2015].

[28] Para mais informações ver http://www.nato.int/cps/en/natohq/topics_78170.htm?selectedLocale=en [acedido em 5 de abril de 2015].

ciberataques dentro das suas infraestruturas. Destacando-se também, o *NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE)*[29] cuja missão se centra no reforço da capacidade cooperativa da ciberdefesa, partilhando informação entre a NATO e os seus membros, bem como, com outras organizações neste âmbito, através do desenvolvimento de doutrina e conceitos, educação, investigação e desenvolvimento, lições aprendidas e consultadoria.

(5) Organização para a Cooperação e Desenvolvimento Económico

Desde 1992, que a Organização para a Cooperação e Desenvolvimento Económico (OCDE) [30] no âmbito da cibersegurança, tem vindo a desenvolver análise de políticas de segurança[31] e recomendações para governos e outros *stakeholders,* sobre como atuarem no ambiente digital.

Com efeito, os principais contributos da OCDE para a área da cibersegurança, parecem ser a sua capacidade para desenvolver recomendações com base em princípios de alto nível e políticas flexíveis capazes de gerar consensos e pontos de convergência, envolvendo as respetivas partes interessadas (IDN-CESEDEN, 2013, p. 71).

Em síntese, "enquanto a maior parte das estratégias nacionais aborda a cibersegurança na vertente da segurança e defesa dos Estados, a orientação da OCDE, tem sido essencialmente a de concertar iniciativas destinadas a aumentar o nível global de cibersegurança uma vez que só assim será possível aumentar as vantagens competitivas dos Estados na nova economia" (IDN-CESEDEN, 2013).

b. O ordenamento legislativo nacional

Na linha do que antecede, iremos de seguida apresentar a legislação nacional relevante neste domínio, bem como as principais orientações estratégicas – referindo neste âmbito algumas propostas de Estratégia Nacional de Cibersegurança - e entidades intervenientes.

[29] Para uma análise mais aprofundada consultar o sítio https://ccdcoe.org/index.html.
[30] Para uma informação mais detalhada sobre os vários normativos existentes ver o sítio http://oe.cd/security.
[31] Um exemplo disso foi a aprovação das diretivas de salvaguarda da privacidade em 1980 pela OCDE, considerado o primeiro instrumento político internacional no domínio da cibersegurança.

Assim, no quadro jurídico português, identificamos com pertinência no âmbito da cibersegurança, os seguintes normativos[32] que iremos apresentar de forma sucinta, no seguinte quadro:

Tabela 2 - Legislação relevante no âmbito da cibersegurança
Fonte: Autor

LEGISLAÇÃO	
Lei de Segurança Interna (Lei n.º 53/2008 de 29 de agosto)	De particular importância para a cibersegurança, no âmbito das competências de controlo (art. 18º) do Secretário-Geral do Sistema de Segurança Interna (SG-SSI) das forças e serviço de segurança e da gestão de incidentes tático-policiais graves, onde se incluem os ataques contra infraestruturas críticas ou destinadas ao abastecimento e satisfação de necessidades vitais da população. Sendo também de destacar a elaboração do RASI e respetivas orientações estratégicas anuais.
Lei do Cibercrime (Lei n.º 109/2009 de 15 de setembro)	Que nos termos do seu art. 1.º, tem por objeto estabelecer "as disposições penais materiais e processuais, bem como as disposições relativas à cooperação internacional em matéria penal, relativas ao domínio do cibercrime e da recolha de prova em suporte eletrónico, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, e adaptando o direito interno à Convenção sobre Cibercrime do Conselho da Europa". Este normativo tipifica ainda cinco crimes, respetivamente: falsidade informática (art. 3º); dano relativo a programas ou outros dados informáticos (art. 4º); sabotagem informática (art. 5º); acesso ilegítimo (art. 6º); interceção ilegítima (art. 7º) e reprodução ilegítima de programa protegido (art. 8º).
Lei da Organização e Investigação Criminal (LOIC) (Lei n.º 49/2008 de 27 de agosto)	Que nos termos da alínea l), do n.º 3, do art. 7.º estipula ser da competência reservada da Policia Judiciária a investigação dos crimes informáticos e praticados com recurso a tecnologia informática, sem prejuízo da possibilidade de competência deferida a outro órgão de polícia criminal nos termos do seu art.º 8.
Lei n.º 32/2008 de 17 de julho	Que nos termos do seu art. 1.º, tem por objeto regular "a conservação e a transmissão dos dados de tráfego e de localização relativos a pessoas singulares e a pessoas coletivas, bem como dos dados conexos necessários para identificar o assinante ou o utilizador registado, para fins de investigação, deteção e repressão de crimes graves por parte das autoridades competentes".
Decreto-Lei n.º 62/2011 de 9 de maio	Que nos termos do seu art. 1.º tem por objeto estabelecer "os procedimentos de identificação e de proteção das infraestruturas essenciais para a saúde, a segurança e o bem-estar económico e social da sociedade nos setores da energia e transportes".

[32] Por limitações da presente investigação, não iremos detalhar os seguintes normativos legais diretamente relacionados, mas que poderão ser consultados para uma análise mais profunda: Código Penal, Lei da proteção de dados pessoais (Lei nº 67/98, de 26 de outubro); Lei da proteção jurídica de programas de computador (Decreto-Lei nº 252/94, de 20 de outubro); Código de direitos de autor e dos direitos conexos (Decreto-Lei nº 63/85, de 14 de março) e no Regime geral das Infrações tributárias (Lei nº 15/2001, de 05 de Junho).

Por seu turno, relativamente às orientações estratégicas nacionais identificamos como relevantes neste âmbito, o Conceito Estratégico de Defesa Nacional (CEDN)[33], a Estratégia Nacional de Combate ao Terrorismo (ENCT)[34], a proposta de Estratégia Nacional de Cibersegurança (ENCSeg)[35] e a proposta de Conceito Estratégico de Segurança Interna (CESI)[36].

No que concerne ao CEDN, este define os aspetos fundamentais da estratégia global a adotar pelo Estado para a consecução dos objetivos da política de segurança e defesa nacional, e antecipa uma elevada probabilidade de concretização de ameaças no ambiente de segurança global associadas a um potencial devastador relacionado com ataques cibernéticos.

Relativamente à ENCT, e conforme referido no seu preâmbulo "representa um compromisso de mobilização, coordenação e cooperação de todas as estruturas nacionais com responsabilidade direta e indireta no domínio do combate à ameaça terrorista", assentando este compromisso num conjunto de objetivos estratégicos concretizados por linhas de ação. Na tabela seguinte, apresentamos as suas linhas de ação relacionadas com a cibersegurança:

Tabela 3- Objetivos estratégicos e respetivas linhas de ação da ENCT
Fonte: Autor (síntese da ENCT)

ESTRATÉGIA NACIONAL DE COMBATE AO TERRORISMO	
OBJETIVOS ESTRATÉGICOS	**LINHAS DE AÇÃO**
DETETAR	➢ Intensificar a cooperação, no plano operacional, entre todas as entidades competentes, explorando em toda a plenitude o potencial das tecnologias de informação e de comunicação.
PREVENIR	➢ Consciencializar os operadores públicos e privados da natureza crítica da segurança informática; ➢ Intensificar a cooperação entre todos os setores da sociedade civil, por forma a responder aos desafios que a utilização da Internet coloca no domínio da radicalização e do recrutamento para o terrorismo;

[33] Resolução de Conselho de Ministros n.º 19/2013 de 21 de março. Para uma análise mais profunda sobre esta estratégia consultar Fontoura (2013) e Instituto de Defesa Nacional (2013).
[34] Resolução do Conselho de Ministros n.º 7-A/2015 de 19 de fevereiro de 2015.
[35] Proposta de Estratégia Nacional de Cibersegurança publicada pelo Gabinete Nacional de Segurança disponível em http://www.gns.gov.pt/NR/rdonlyres/ED57762F-3556-4C05-9644-888E35C790BB/0/PropostaEstratégiaNacionaldeCibersegurançaPortuguesa.pdf [acedido em 14 de novembro de 2014]
[36] Para uma análise mais aprofundada ver Lourenço, et al. (2015).

	➢ Defender a sociedade de conteúdos de apologia da violência e do terrorismo publicamente acessíveis pela Internet, promovendo a sua remoção e o seu bloqueio.
PROTEGER	➢ Desenvolver o Plano de Ação para a Proteção e Aumento da Resiliência das Infraestruturas Críticas, nacionais e europeias, com os respetivos planos de segurança da responsabilidade dos operadores e planos de segurança externos da responsabilidade das forças e serviços de segurança e da Autoridade Nacional de Proteção Civil; ➢ Implementar o Plano de Ação Nacional para a proteção contra as Ciberameaças, integrado numa estratégia nacional de cibersegurança; ➢ Avaliar as vulnerabilidades dos sistemas de informação críticos e manter e acompanhar a adoção das medidas de correção face a ciberataques.
PERSEGUIR	➢ Reforçar a colaboração e articulação entre os vários intervenientes e responsáveis nas áreas da cibersegurança, ciberespionagem, ciberdefesa e ciberterrorismo, nos termos da Constituição e da lei; ➢ Robustecer o Sistema Integrado de Informação Criminal, designadamente através do reforço da utilização da Plataforma para Intercâmbio de Informação Criminal e da clarificação do direito a ela aceder.
RESPONDER	➢ Executar ações que permitam exercitar os procedimentos e a articulação entre os diversos atores e desenvolver os mecanismos de interoperabilidade que permitam uma resposta pronta e eficaz a ocorrências terroristas, incluindo sistemas de informação críticos face a ciberataques.

Por sua vez, a proposta de ENCSeg surgiu na sequência dos trabalhos da edificação do Centro Nacional de Cibersegurança, definindo-se como um conjunto de iniciativas destinadas a potenciar a livre utilização do ciberespaço e garantir a sua segurança, promovendo a proteção de infraestruturas de informação críticas nacionais contra eventuais ataques cibernéticos ou a materialização de ciberameaças. Na tabela seguinte, são apresentados os seus objetivos e linhas de ação estratégicas:

Tabela 4 - Objetivos principais e respetivas linhas de ação estratégica da ENCSeg
Fonte: Autor (síntese da ENCSeg)

PROPOSTA DE ESTRATÉGIA NACIONAL DE CIBERSEGURANÇA	
OBJETIVOS PRINCIPAIS	**LINHAS DE AÇÃO ESTRATÉGICA**
Garantir a segurança no ciberespaço	➢ Analisar o ambiente de informação e antecipar eventuais ataques de forma a tomar as decisões apropriadas, acompanhando os últimos desenvolvimentos tecnológicos, analisando e antecipando ameaças a fim de estar na vanguarda; ➢ Detetar e bloquear ataques, alertar e apoiar as potenciais vítimas; ➢ Estimular e potenciar as capacidades científicas, técnicas, industriais e humanas do país de forma a manter a independência nacional neste domínio; ➢ Adaptar a legislação nacional de forma a incorporar os desenvolvimentos tecnológicos e novas práticas; ➢ Desenvolver iniciativas de cooperação internacional em áreas ligadas à segurança dos sistemas de informação, cibercrime, ciberdefesa e luta contra o terrorismo de forma a proteger melhor os sistemas de informação nacionais; ➢ Comunicar e informar de forma a influenciar e a aumentar a compreensão da população portuguesa relativamente à extensão dos desafios relacionados com a segurança dos sistemas de informação.
Fortalecer a Cibersegurança das Infraestruturas Críticas Nacionais	➢ Reforçar a Segurança das TIC nas Redes de Governo e da Administração Pública; ➢ Reforçar a Segurança dos sistemas de informação do Estado e dos operadores das infraestruturas críticas para assegurar uma maior resiliência (capacidade de sobrevivência) nacional.
Defender os Interesses Nacionais e a Liberdade de Ação no Ciberespaço	➢ Reforçar iniciativas nacionais estruturantes da "Sociedade de Informação e do Conhecimento"; ➢ Proteger e defender os mecanismos de Governação eletrónica do Estado; ➢ Levantar a Estrutura Nacional de Cibersegurança e Ciberdefesa; ➢ Estabelecer mecanismos de cooperação nacional e internacional, neste âmbito.

Ainda, no âmbito da teorização de estratégias nacionais de cibersegurança, dois autores nacionais têm produção teórica. O primeiro, Santos (2011) apresenta uma estrutura nacional para a cibersegurança organizada em 6 eixos de atuação – combate ao cibercrime, normalização e certificação, proteção de infraestruturas críticas, formação e consciencialização, alerta e resposta a incidentes e investigação e desenvolvimento – e três planos (político, estratégico e operacional), conforme descrito na figura seguinte:

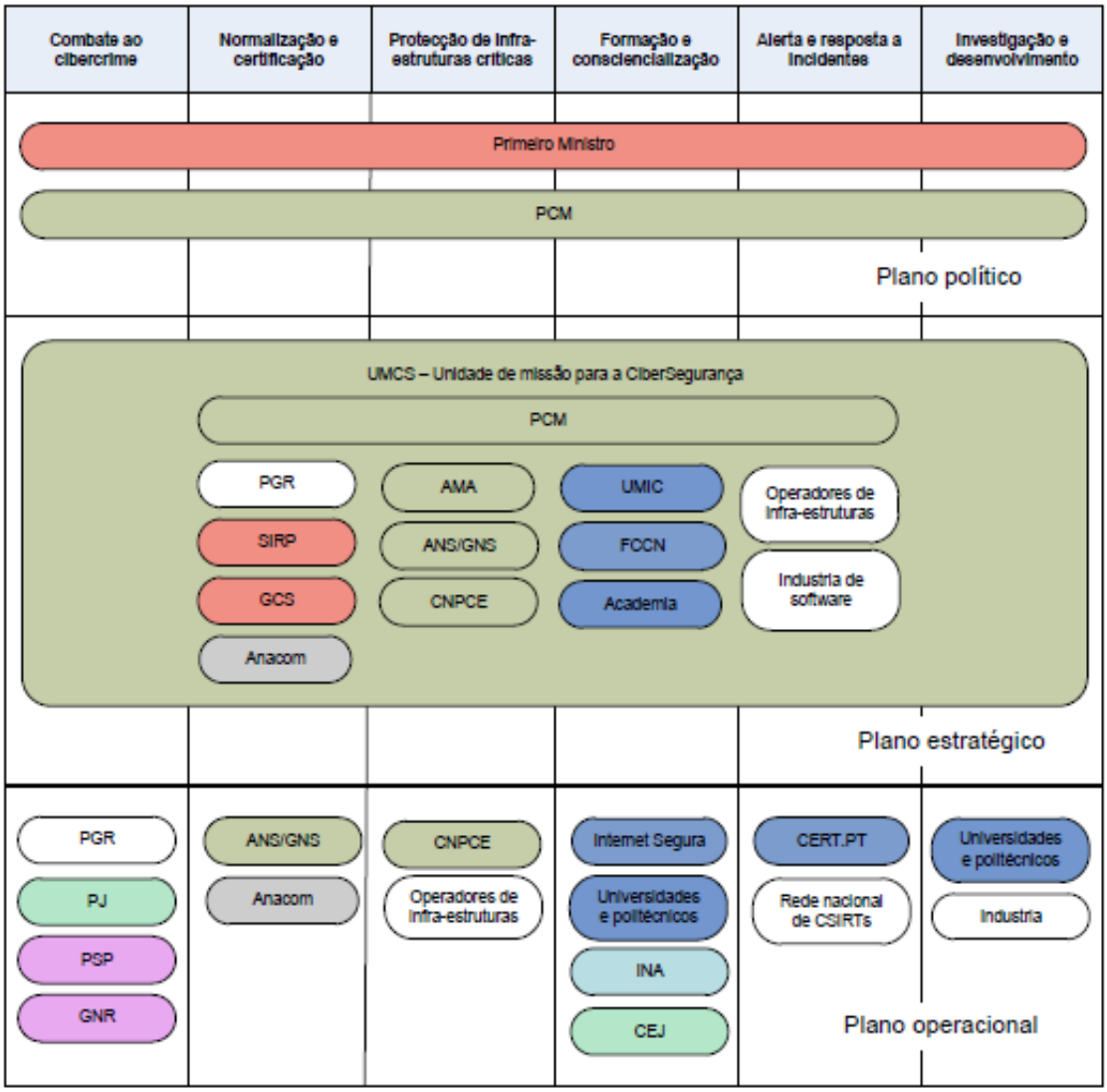


Figura 8 - Estrutura nacional para a cibersegurança
Fonte: (Santos, 2011, p. 103)

O segundo autor, Nunes (2012, p. 115) concebendo o ciberespaço como "uma área de responsabilidade coletiva" considera "necessário prever a existência de um órgão coordenador das áreas ligadas à Cibersegurança e Ciberdefesa do Estado (Conselho Nacional de Cibersegurança), facilitando a definição não só de uma orientação política e estratégica mais coordenada e sinérgica como também uma gestão de crises mais eficaz" [37], conforme retratado na figura seguinte:

[37] Para uma melhor compreensão da sua teorização *vide* Nunes (2012, pp. 113-127)

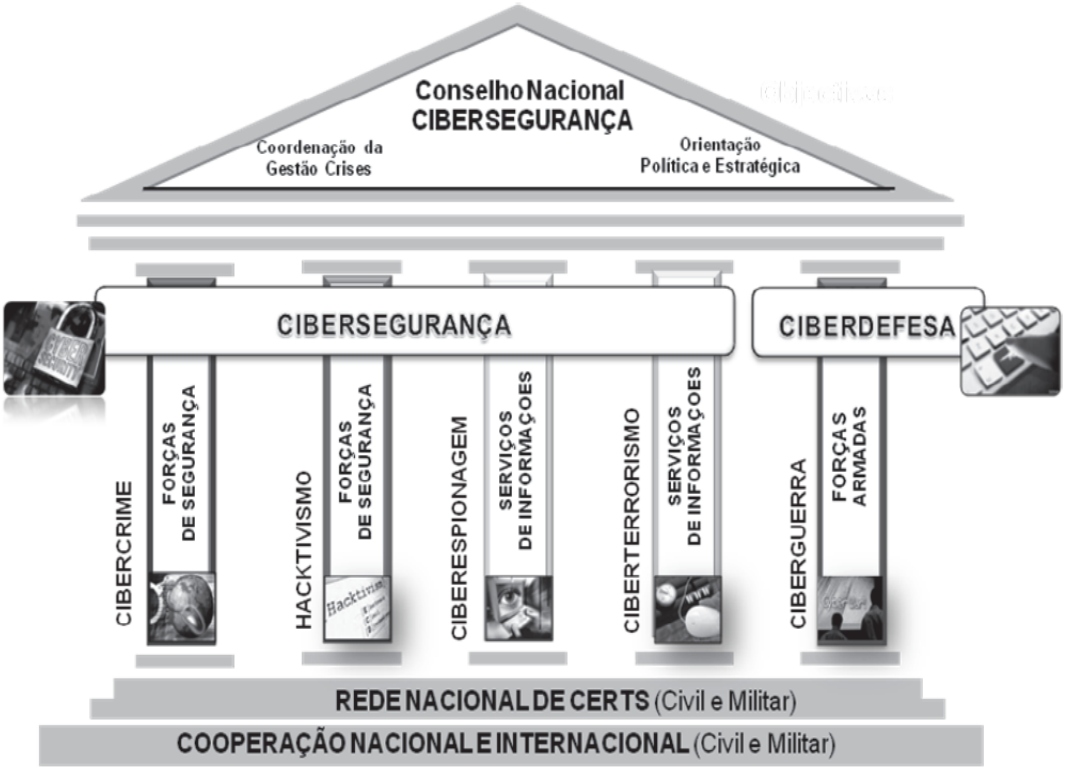


Figura 9- Cibersegurança nacional (um edifício, vários pilares)
Fonte: (Nunes, 2012, p. 116)

Este autor, ainda no plano das estratégias desenvolve toda uma lógica relativa à necessidade de articulação, alinhamento e criação de sinergias entre a cibersegurança e ciberdefesa, e as distintas estratégias, conforme a figura seguinte que ilustra esta sua conceção:

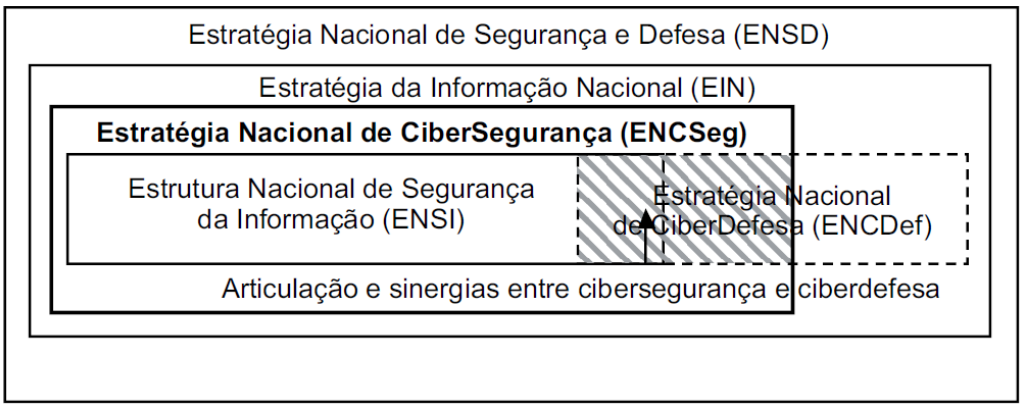


Figura 10- Enquadramento da Estratégia Nacional de Cibersegurança
Fonte: (Nunes, 2012, p. 119)

E finalmente, em relação à proposta de CESI, esta foi realizada pelo GRESI no estudo "Segurança Interna Horizonte 2025 - Um Conceito de Segurança Interna", que refere que a atividade de segurança interna também deverá ser exercida no ciberespaço. Este documento, entre outras orientações, no âmbito da cibersegurança estabelece uma linha de ação estratégica para o alargamento do sentimento de segurança à dimensão do ciberespaço (Lourenço, et al., 2015, p. 61), cuja síntese se apresenta na seguinte tabela:

Tabela 5 - Linha de ação estratégica n.º 5 e síntese da sua descrição
Fonte: Autor (síntese da CESI)

PROPOSTA DE CONCEITO ESTRATÉGICO DE SEGURANÇA INTERNA
LINHA DE AÇÃO ESTRATÉGICA N.º5 – Alargamento do sentimento de segurança à dimensão do ciberespaço
➢ Adequada prevenção e o combate das ciberameaças requerem a intervenção e cooperação de várias entidades do setor público e privado, no plano nacional e internacional, sendo relevante considerar as seguintes ações a desenvolver de forma concertada: melhorar a cooperação nacional e internacional, neste domínio; consciencializar a administração pública, cidadãos e sector empresarial; legislar sem prejuízo da privacidade; aproximar os peritos do setor privado; elaborar planos de contingência;
➢ Maior consciencialização das ameaças advenientes do ciberespaço seguramente que contribuirá para o reforço do sentimento de segurança e para a adoção de medidas preventivas que colaborarão para a diminuição objetiva da criminalidade;
➢ No domínio da cibersegurança a partilha da informação e a cooperação constituem elementos decisivos na prevenção e no "combate" ao diferente espectro das ciberameaças.

Na linha do que antecede, importa agora elencar as principais entidades responsáveis pela cibersegurança em Portugal, respetivamente o Centro Nacional de Cibersegurança (CNCSeg)[38], o Centro de Ciberdefesa[39], o Gabinete do Cibercrime e o *Computer Emergence Response Team* nacional (CERT.PT).

Em relação ao CNCSeg, este tem uma natureza estratégica e operacional, tendo "por missão contribuir para que o país use o ciberespaço de uma forma livre, confiável e segura, através da promoção da melhoria contínua da cibersegurança nacional e da cooperação internacional(…)"[40]. Pelo papel nuclear deste Centro no contexto da cibersegurança

[38] Criado pelo Decreto-Lei n.º 69/2014 que republicou o Decreto-Lei n.º 3/2012 de 16 de janeiro.
[39] Despacho n.º 13692/2013, do Ministro da Defesa Nacional de 28 de outubro. De destacar a importância deste Centro no âmbito da ciberdefesa nacional, e a estreita articulação existente e interdependência com a área da cibersegurança nacional.
[40] Conforme n.º 2 do art. 2.º do diploma, em apreço.

nacional, apresentamos na tabela seguinte uma descrição das suas competências e atribuições:

Tabela 6 - Competências e atribuições do Centro Nacional de Cibersegurança
Fonte: Autor (síntese da CNCSeg)

CENTRO NACIONAL DE CIBERSEGURANÇA	
ÂMBITO	**DESCRIÇÃO**
Competências	➢ Analisar o ambiente de informação e antecipar eventuais ataques de forma a tomar as decisões apropriadas, acompanhando os últimos desenvolvimentos tecnológicos, analisando e antecipando ameaças a fim de estar na vanguarda; ➢ Desenvolver as capacidades nacionais de prevenção, monitorização, deteção, reação, análise e correção destinadas a fazer face a incidentes de cibersegurança e ciberataques; ➢ Promover a formação e a qualificação de recursos humanos na área da cibersegurança, com vista à formação de uma comunidade de conhecimento e de uma cultura nacional de cibersegurança; ➢ Exercer os poderes de autoridade nacional competente em matéria de cibersegurança, relativamente ao Estado e aos operadores de infraestruturas críticas nacionais: ➢ Contribuir para assegurar a segurança dos sistemas de informação e comunicação do Estado e das infraestruturas críticas nacionais; ➢ Promover e assegurar a articulação e a cooperação entre os vários intervenientes e responsáveis nacionais na área da cibersegurança; ➢ Assegurar a produção de referenciais normativos em matéria de cibersegurança; ➢ Apoiar o desenvolvimento das capacidades técnicas, científicas e industriais, promovendo projetos de inovação e desenvolvimento na área da cibersegurança; ➢ Assegurar o planeamento da utilização do ciberespaço em situação de crise e de guerra no âmbito do planeamento civil de emergência, no quadro definido pelo Decreto-Lei n.º 73/2013, de 31 de maio; ➢ Coordenar a cooperação internacional em matérias da cibersegurança, em articulação com o Ministério dos Negócios Estrangeiros.
Atribuições	➢ Atua em articulação e estreita cooperação com as estruturas nacionais responsáveis pela ciberespionagem, ciberdefesa, cibercrime e ciberterrorismo; ➢ As suas competências não prejudicam as atribuições e competências legalmente cometidas a outras entidades públicas, e coopera com entidades privadas nesta matéria.

No âmbito da política de ciberdefesa, o despacho ministerial que cria o Centro de Ciberdefesa, refere que fica na dependência do CEMGFA, e "constitui o órgão responsável pela condução de operações no ciberespaço e pela resposta a incidentes informáticos e ciberataques, com responsabilidades de coordenação, operacionais e técnicas".

Em relação ao Gabinete do Cibercrime, este foi criado por despacho de 7 de dezembro de 2011, do Procurador-Geral da República, sendo responsável pela coordenação do Ministério Público na área da cibercriminalidade.

E no que concerne ao CERT.PT este tem por objetivo melhorar a eficácia geral da reação a incidentes de cibersegurança em Portugal, facilitando a partilha de informação relevante e coordenando ações de mitigação e de resolução junto das diversas entidades implicadas.

Neste âmbito importa referir, que existe uma miríade de atores e entidades que por limitações inerentes ao presente trabalho não foi possível abordar, como ilustra a seguinte sistematização do autor Santos (2011), relativa às principais entidades e iniciativas contribuintes para a cibersegurança:

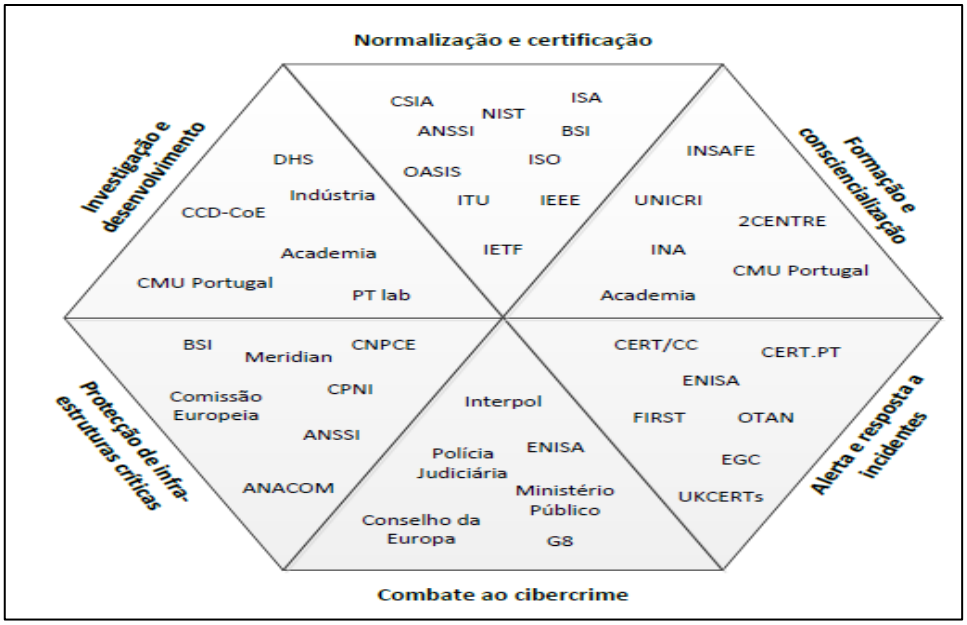


Figura 11 - Principais entidades e iniciativas na cibersegurança
Fonte: (Santos, 2011, p. 49)

Como síntese do presente capítulo, salientamos que a adequada prevenção e o combate às ciberameaças exige a intervenção e cooperação de várias entidades, no plano nacional e internacional, de forma a permitir a livre utilização do ciberespaço e garantir a sua segurança. Neste contexto, à medida que as nações e os respetivos sistemas de segurança e defesa se vão tornando cada mais dependentes do ciberespaço, mais exigente se torna a adoção e articulação de normativos e políticas no domínio da cibersegurança, de forma a promover a proteção de infraestruturas de informação críticas nacionais contra eventuais ataques cibernéticos ou a materialização de ciberameaças.

3. Atuação das forças e serviços de segurança no âmbito da cibersegurança

No mundo globalizado, um dos desafios que mais prementemente se colocam aos Estados é o da segurança, sendo a vertente da cibersegurança incontornável num mundo cada vez mais dependente do eficaz funcionamento de sistemas informáticos (Verdelho, 2005, p. 159). Neste quadro, e segundo Fernandes (2014, p. 92) a tendência para a afirmação da soberania nacional no ciberespaço está também a ter implicações a nível das forças armadas e forças e serviços de segurança que estão a adaptar-se aos desafios do ciberespaço e aos seus riscos. Assim, iremos de seguida analisar a intervenção das forças e serviços de segurança neste domínio, em termos gerais e em particular a GNR.

a. Enquadramento geral

Analisando a organização, as atribuições e as competências que constam das leis orgânicas das forças e serviços de segurança previstas no n.º 2 do art.º 25 da Lei de Segurança Interna (LSI)[41] não se identificam atribuições materiais e objetivas no âmbito da cibersegurança[42]. Todavia, como veremos as forças e serviços de segurança[43] atuam neste domínio concorrendo, em sentido lato, para garantir a segurança interna com o escopo de "garantir a ordem, a segurança e a tranquilidade públicas, proteger as pessoas e bens, prevenir e reprimir a criminalidade" e de "assegurar o normal funcionamento das instituições democráticas, o regular exercício dos direitos, liberdades e garantias fundamentais dos cidadãos e o respeito pela legalidade democrática", nos termos do n.º 1 do artigo 1.º da LSI.

Segundo Nunes (2012, p. 115) a atribuição de competências no ciberespaço deve obedecer à mesma lógica da segurança e defesa do Estado, assim considera "que as Forças de Segurança sejam responsáveis por coordenar a resposta do Estado às atividades

[41] Conforme a Lei n.º 63/2007 de 6 de novembro relativa à GNR; a Lei n.º53/2007 de 31 de agosto relativa à Polícia de Segurança Pública (PSP); Lei n.º 37/2008 de 6 de agosto relativo à Polícia Judiciária (PJ); o Decreto-Lei n.º 240/2012 de 6 de novembro relativo ao Serviço de Estrangeiros e Fronteiras (SEF) e a Lei n.º 9/2007 relativo ao Serviço de Informações de Segurança (SIS). Devido ao seu carater específico e limitações no âmbito das suas atribuições e competências, não analisamos os órgãos próprios da Autoridade Marítima Nacional e do Sistema de Autoridade Aeronáutica, previstos no n.º 3 do artigo 25.º da LSI.

[42] Com exceção da PJ no âmbito dos crimes informáticos (Lei n.º 49/2008 de 27 de agosto e Lei n.º 109/2009 de 15 de setembro), do SIS que no seu sítio apresenta as ciberameaças como uma das suas principais preocupações (vide http://www.sis.pt/ciberameaca.html) e da GNR no âmbito da "Estratégia da Guarda 2020", sendo esta última, analisada particularmente no capítulo seguinte.

[43] Para uma análise mais profunda sobre as forças e serviços de segurança ver Branco (2010), Raposo (2006) e Silva (2015).

relacionadas com o cibercrime e o *hacktivism*[44], que os Serviços de Informação da República atuem em caso de ciberespionagem e ciberterrorismo e que as Forças Armadas tenham que intervir para fazer face a ações de ciberguerra"[45].

No que concerne ao conceito de cibercrime, segundo Verdelho (2005, p. 164) "não está doutrinariamente definido o que se entende por cibercrime" e como refere Natário (2013, p. 833) "à semelhança do que ocorre com a definição do ciberespaço, o cibercrime também não parece ser fácil de definir com exatidão e esse facto é um dos grandes desafios que as autoridades do século XXI enfrentam no combate a esse fenómeno."[46]

A nível nacional, apresentamos na tabela seguinte, uma síntese da principal doutrina relativa à criminalidade relacionada com computadores:

Tabela 7 – Criminalidade relacionada com a utilização de computadores
Fonte: Autor adaptado de (Ascensão, 2001, pp. 286-287)

CRIMINALIDADE RELACIONADA COM A UTILIZAÇÃO DE COMPUTADORES	
Crimes que recorrem a meios informáticos	Não alterando o tipo legal comum, correspondem a uma especificação ou qualificação deste. Exemplo: o crime de burla informática e o crime de burla informática nas telecomunicações (art. 221º do Código Penal).
Crimes relativos à proteção de dados pessoais	Previstos na Lei n.º 67/98 de 16 de outubro, transposição da Diretiva n.º 95/46/CE e a Lei n.º 69/98 de 28 de outubro.
Crimes informáticos em sentido estrito	Sendo o bem ou meio informático o elemento próprio do tipo de crime. Neste grupo inserem-se os crimes previstos na Lei do Cibercrime.
Crimes relacionados com o conteúdo	Onde se destacam a violação do direito de autor, a difusão da pornografia infantil ou a discriminação racial ou religiosa.

Relativamente à criminalidade informática, a LOIC nos termos da alínea l), do n.º 3, do art. 7.º estipula ser da competência reservada[47] da Policia Judiciária[48] a investigação dos crimes informáticos e praticados com recurso a tecnologia informática, sem prejuízo da

[44] O conceito de *hacktivism*, caraterizado no capítulo 1, insere-se nas atribuições genéricas de prevenção e ordem pública da GNR e da PSP, bem como de recolha de informações do SIS.
[45] Neste âmbito ver ainda a teorização relativa aos domínios de atuação, em particular, o domínio da prossecução criminal em Santos, et al. (2012, pp. 168-170).
[46] De referir, que a própria Lei do Cibercrime não define o conceito de cibercrime.
[47] Para aprofundar o âmbito da competência reservada da PJ neste domínio *vide* Parecer da Procuradoria-Geral da República n.º 11/2011 disponível em http://www.dgsi.pt. No âmbito da investigação criminal ver as obras de Valente (2005) e (2006).
[48] A PJ assegura ainda o ponto de contato permanente no âmbito da Rede 24/7 da Convenção sobre o Cibercrime do Conselho da Europa.

possibilidade de competência deferida a outro órgão de polícia criminal nos termos do n.º 1 do art.º 8 quando "tal se afigure, em concreto, mais adequado ao bom andamento da investigação".[49]

Contudo, como referido no Relatório de Atividades de 2013 do Gabinete do Cibercrime da Procuradoria Geral da República, dá-se nota que a Polícia Judiciária não "tem desenvolvido diligências de inquérito nos casos de injúrias ou difamações através da Internet, devolvendo os respetivos processos sem investigação" (2013, p. 5), existindo assim dificuldades na interpretação da legislação em vigor[50].

Neste contexto e em síntese, o GRESI refere quanto à cibersegurança "a necessidade de dotar as Forças e Serviços de Segurança com competências específicas e capacidades próprias para prevenir e atuar de forma integrada e coordenada neste domínio" (2015, p. 63).

b. O caso da GNR

Analisando em particular a Guarda, esta conforme o n.º 2 do artigo 1.º da Lei n.º 63/2007, de 6 de novembro, retificada pela declaração de retificação n,º 1-A/2008 – "tem por missão, no âmbito dos sistemas nacionais de segurança e proteção, assegurar a legalidade democrática, garantir a segurança interna e os direitos dos cidadãos, bem como colaborar na execução da política de defesa nacional, nos termos da Constituição e da Lei"[51]. E a "missão confiada à GNR é extensa, multifacetada e exercida em todo o território nacional (continuidade temporal e territorial), no âmbito dos sistemas nacionais de segurança e proteção, bem como na execução da política de defesa nacional" Branco (2010, p. 244).

Assim, restringindo-nos ao nosso eixo de análise - a cibersegurança - identificamos na tabela seguinte, algumas das atribuições da Guarda previstas no artigo 3.º da Lei n.º 63/2007, de 6 de novembro, que podem ser prosseguidas no âmbito do ciberespaço:

[49] Designadamente nos termos do mesmo artigo, "quando existirem provas simples e evidentes", "estejam verificados os pressupostos das formas especiais de processo", "crime sobre o qual incidam orientações sobre a pequena criminalidade" e a "investigação não exija especial mobilidade de atuação ou meios de elevada especialidade técnica.

[50] Um dos motivos prendeu-se com o facto da expressão crimes informáticos ter sido substituída na lei pela expressão cibercrime.

[51] Para informação mais detalhada sobre a GNR, ver os diversos instrumentos de gestão disponíveis no seu sítio www.gnr.pt.

Tabela 8- Atribuições da GNR relevantes no ciberespaço
Fonte: Autor

ATRIBUIÇÕES DA GNR
➢ Garantir as condições de segurança que permitam o exercício dos direitos e liberdades e o respeito pelas garantias dos cidadãos, bem como o pleno funcionamento das instituições democráticas, no respeito pela legalidade e pelos princípios do Estado de direito;
➢ Garantir a ordem e a tranquilidade públicas e a segurança e a proteção das pessoas e dos bens;
➢ Prevenir a criminalidade em geral, em coordenação com as demais forças e serviços de segurança;
➢ Desenvolver as ações de investigação criminal e contraordenacional que lhe sejam atribuídas por lei, delegadas pelas autoridades judiciárias ou solicitadas pelas autoridades administrativas;
➢ Manter a vigilância e a proteção de pontos sensíveis, nomeadamente infraestruturas rodoviárias, ferroviárias, aeroportuárias e portuárias, edifícios públicos e outras instalações críticas;
➢ Prevenir e detetar situações de tráfico e consumo de estupefacientes ou outras substâncias proibidas, através da vigilância e do patrulhamento das zonas referenciadas como locais de tráfico ou de consumo;
➢ Contribuir para a formação e informação em matéria de segurança dos cidadãos;
➢ Assegurar o cumprimento das disposições legais e regulamentares referentes à proteção e conservação da natureza e do ambiente, bem como prevenir e investigar os respetivos ilícitos;
➢ Prevenir e investigar as infrações tributárias, fiscais e aduaneiras, bem como fiscalizar e controlar a circulação de mercadorias sujeitas à ação tributária, fiscal ou aduaneira.

De igual modo, analisando os órgãos superiores de comando e direção[52] da Guarda, identificamos nas direções do Comando Operacional um conjunto de competências que também podem ser prosseguidas no ciberespaço, conforme tabela seguinte:

[52] Conforme n.º 3 do art. 21º da Lei n.º 63/2007, de 6 de novembro e Decreto Regulamentar n.º 19/2008 de 27 de novembro.

Tabela 9 - Direções e respetivas competências relevantes no ciberespaço
Fonte: Autor

COMANDO OPERACIONAL	
DIREÇÕES	**COMPETÊNCIAS**
Direção de Operações	➢ Elaborar e difundir diretivas sobre prevenção criminal, policiamento comunitário e programas especiais, nomeadamente no âmbito da violência doméstica, do apoio e proteção de menores, idosos e outros grupos especialmente vulneráveis ou de risco.
Direção de Informações	➢ Proceder à pesquisa, análise e difusão de notícias e informações com interesse para a missão da Guarda; ➢ Proceder à identificação, análise e avaliação de riscos específicos associados ao cumprimento das missões da Guarda; ➢ Realizar as adequadas averiguações de segurança em caso de quebra ou comprometimento de segurança de informação, nos termos da legislação em vigor.
Direção de Investigação Criminal	➢ Proceder ao tratamento da informação criminal em coordenação com a direção de informações e assegurar a difusão de notícias e elementos de informação; ➢ Acompanhar a evolução da criminalidade e o surgimento de novas táticas e técnicas aplicáveis à investigação criminal;
Direção de Comunicações e Sistemas de Informações	➢ Assegurar a direção, coordenação, controlo, gestão e execução das atividades da Guarda em matéria de comunicações, eletrónica, sistemas e tecnologias da informação, segurança da informação e da simulação assistida por computador e da segurança e limpeza eletrónica e dos sistemas complementares de segurança física; ➢ Garantir a segurança da informação e das comunicações e das matérias classificadas, nomeadamente sub-registo e postos de controlo; ➢ Assegurar, em coordenação com as entidades nacionais responsáveis, o abastecimento, sustentação, operação e controlo das atividades da Guarda no domínio específico dos sistemas criptográficos e de segurança da informação.

A Diretiva Estratégica do Comandante-Geral da Guarda para o período compreendido entre 2015 e 2020, constitui-se como um documento enformador do planeamento e programação em termos de estratégia institucional, definindo como um dos objetivos estratégicos da Guarda para o horizonte 2015-2020, " incrementar a capacidade

de atuação no mundo ciber, garantindo uma resposta integrada da instituição ao fenómeno da cibercriminalidade no mundo real e virtual "[53].

No âmbito dos programas especiais que a Guarda desenvolve, designadamente o programa Escola Segura, importa salientar, entre outras iniciativas, o protocolo de cooperação com a *Microsoft* Portugal, celebrado em 2014[54] nos domínios da cidadania e segurança digitais, com especial enfoque sobre as redes sociais virtuais e o *ciberbullying*.

E finalmente no domínio da ciberdefesa, a Guarda participou no Exercício "Ciber Perseu – 2014" que decorreu de 10 a 13 de novembro, na qualidade de jogador[55].

Como síntese do presente capítulo, podemos afirmar que os fenómenos criminais ligados ao ciberespaço estão a evoluir e a crescer exponencialmente, sendo os seus efeitos pouco compreendidos ou percecionados pelas diversas entidades públicas ou privadas e pelos próprios cidadãos. No âmbito da atuação das forças e serviços de segurança "a partilha da informação e a cooperação constituem elementos decisivos na prevenção e no "combate" ao diferente espectro das ciberameaças" (Lourenço, et al., 2015, p. 61). E o grau de ameaça subjacente e a necessidade urgente de prevenir e reprimir os seus efeitos implica um correto dimensionamento, a geração e a reorganização de competências e valências de entidades que têm responsabilidades na área da segurança, como é o caso da Guarda.

[53] Conforme Estratégia da Guarda 2020 – Uma Estratégia de Futuro, disponível em http://www.gnr.pt/portal/internet/dcrp/EG2020/eg2020.swf [acedido em 9 de abril de 2015]. Neste contexto várias congéneres da GNR têm vindo a criar valências de prevenção (*Cyberpolicing*), tendo constituídas unidades policiais especializadas neste domínio (ex: *Grupo Delitos Telemáticos* em Espanha, *Département Cybercriminalité* em França, ou o *Reparto Indagini Techniche* em Itália).

[54] Segundo informação recolhida junto do Comando Operacional da GNR.

[55] O cenário geopolítico criado para o exercício, permitiu o desenvolvimento do plano de treino interno da Guarda e também possibilitou o treino sincronizado com todas as entidades intervenientes.

4. Apresentação e análise dos resultados

Neste capítulo, na primeira parte procedemos à apresentação e análise dos resultados. Para tal, respondemos a cada uma das questões derivadas, tendo por base a análise que realizámos anteriormente bem como a análise de conteúdo que realizámos às entrevistas. No caso das entrevistas, com base em grelhas de análise temática, procuramos, colocar em evidência as regularidades, ou seja, aquilo que se evidenciou como comum. Neste percurso analítico procurámos não eliminar as contradições e heterogeneidades presentes nos discursos, mas sim identificar os seus elementos mais recorrentes e estruturadores. Além disso, procurámos o necessário distanciamento analítico, interpretando esses discursos criticamente e confrontando-os, sempre que possível, com outras fontes. A segunda parte deste capítulo foi dedicada à avaliação das descobertas e contributos para o conhecimento, onde expomos e detalhamos uma análise SWOT relativa à cibersegurança na GNR e apresentamos alguns contributos.

a. Análise dos resultados

No âmbito da nossa investigação, realizamos dez entrevistas semiestruturadas, sendo seis a peritos reconhecidos no universo das forças armadas e de segurança, e quatro a peritos com funções académicas e de relevo em instituições civis (Cfr. Sinopses das entrevistas em Apêndice C). Orientados pelo pragmaticismo imposto pelas próprias condições da investigação, a partir do momento em que, reiteradamente, as entrevistas não traziam informação adicional, optámos por finalizar os respetivos procedimentos. Foi a partir do critério de redundância ou saturação que se definiram os limites da amostragem teórica. Aos entrevistados foi garantido que a utilização das informações e opiniões recolhidas apenas serviria para fins exclusivamente académicos, cuja identificação e função constam da tabela seguinte:

Tabela 10- Identificação dos entrevistados

Fonte: Autor

	Entrevistados	Função	Local
E1	Eng. José Carlos Martins	Coordenador CNCSeg	Lisboa
E2	Professor Vera-Cruz Pinto	Professor Universitário	Lisboa
E3	Tenente-Coronel Viegas Nunes	Exército / DCSI	Lisboa
E4	Inspetor-Chefe Rogério Bravo	Polícia Judiciária	Lisboa
E5	Dr. Pedro Verdelho	Gabinete Cibercrime da Procuradoria-Geral da República	Lisboa

E6	Prof. Dr José Tribolet	Instituto Superior Técnico	Lisboa
E7	Coronel João Barbas	IDN	Lisboa
E8	Major-General Agostinho Costa	2.º Comandante-Geral da GNR	Lisboa
E9	Major-General Botelho Miguel	Comandante do Comando Operacional da GNR	Lisboa
E10	Tenente-Coronel Santos	GNR/DCSI	Lisboa

Assim, em relação aos resultados da primeira questão de investigação, "Qual a importância estratégica da proteção do ciberespaço":

Tabela 11- Análise temática da primeira questão
Fonte: Autor

TEMÁTICA	DESCRIÇÃO	FREQUÊNCIA
Extensão do mundo real	Entendida principalmente como uma extensão das competências que as entidades já dispõem no mundo não virtual.	E3, E5
Domínio essencial	Entendida com um valor crucial para o funcionamento da sociedade.	E1, E2, E7, E8, E9,
Domínio abrangente	Assume um carater abrangente, planetário e integra todos os domínios económicos, políticos, etc.	E4, E6, E10

Na procura de resposta à primeira questão, importa salientar que todos os entrevistados referiram ser importante a proteção do ciberespaço, podendo-se agrupar as suas opiniões em três grandes áreas temáticas.

Na primeira, os entrevistados (Entrevistas n.º 3 e 5) vêm a proteção do ciberespaço como uma continuação do mundo real, em que os órgãos competentes no mundo real deverão prosseguir essas competências no ciberespaço de forma a evitar-se ruturas do suporte legal. Igualmente importante identificaram, a clarificação efetuada entre o que é cibersegurança e ciberdefesa, que é a origem de muitas confusões conceptuais (Entrevista n.º 3) e a referência ao conceito de ciberespaço como uma dimensão da segurança interna (Entrevista n.º 5). Na segunda área temática, os entrevistados apresentam a importância do ciberespaço para a sociedade referindo, em síntese, que nos encontramos "a viver em pleno a geração de informação e do conhecimento sobre a qual temos que procurar deter o seu domínio e controlo sob pena de ficarmos irremediavelmente distantes das oportunidades e vantagens estratégicas" (Entrevista n.º 9). E na última área temática, destacamos a forma como o ciberespaço, à escala planetária, "revoluciona e integra de forma cinética e

ininterrupta todos os processos económicos, políticos, culturais através do uso intensivo de tecnologias de informação" (Entrevista n.º 10).

Em relação à segunda questão de investigação, "A cibersegurança tem um enquadramento normativo ajustado à realidade nacional?":

Tabela 12 - Análise temática da segunda questão
Fonte: Autor

TEMÁTICA	DESCRIÇÃO	FREQUÊNCIA
Enquadramento normativo atualizado	Enquadramento normativo é recente e responde às atuais exigências no âmbito da cibersegurança.	E5, E7
Enquadramento normativo em consolidação	Enquadramento normativo encontra-se em fase de elaboração ou em fase de consolidação.	E1, E3, E9
Enquadramento normativo desajustado	Enquadramento normativo não acompanha dinâmica evolutiva deste domínio.	E2, E4, E6, E8, E10

Em relação a esta segunda questão de investigação, as opiniões dividiram-se em três áreas temáticas. Na primeira, os entrevistados consideram que o enquadramento normativo é recente e responde às atuais exigências, designadamente a atual Lei do Cibercrime, que "é uma lei moderna, que enquadra as coisas como têm que ser e dá ferramentas suficientes para investigar…" (Entrevista n.º 5).

Na segunda, os entrevistados consideram que se está numa fase embrionária de elaboração da legislação, existindo algum trabalho ainda a fazer nesta matéria, embora se considere também que "essa legislação não existindo de facto existe no espírito da lei e *de jure*" (Entrevista n.º 3). E está-se neste momento a trabalhar na Estratégia Nacional para a Segurança do Ciberespaço ou Cibersegurança, e futuramente nas vertentes legísticas e de boas práticas (Entrevista n.º 1). E na última área temática, os entrevistados consideram que o enquadramento normativo não está ajustado à realidade nacional e internacional por erros de transposição acrítica do legislador ou existência de "entidades administrativas a quem são conferidas poderes de polícia (Entrevista n.º 4), e por motivo "da velocidade das decisões ao nível das normas não acompanhar a dinâmica evolutiva que este domínio tem tido nos tempos mais recentes (Entrevista n.º 8).

No que concerne à terceira questão de investigação, "Qual o quadro de atuação das forças e serviços de segurança no domínio da cibersegurança"?:

Tabela 13 - Análise temática da terceira questão
Fonte: Autor

TEMÁTICA	DESCRIÇÃO	FREQUÊNCIA
No âmbito das respetivas competências	A atuação insere-se no respetivo quadro de competências ou atividades que desenvolve.	E1, E3, E6, E7
Repensar atual quadro de atuação	A atuação neste domínio deverá ser reconsiderada atendendo à evolução da cibersegurança.	E2, E4, E5, E8, E9, E10

Da análise desta questão releva-se duas áreas temáticas. Na primeira, os entrevistados consideram que o quadro de atuação das forças e serviços de segurança no âmbito da cibersegurança "é uma continuação da vida real, terá de ser sempre visto dessa forma, como uma extensão das suas competências" (Entrevista n.º 3) e num quadro de atuação total e abrangente, onde numa lógica de segurança interna não é possível dissociar a realidade física da realidade virtual.

Na segunda área temática, os entrevistados consideram que as forças e serviços de segurança deverão atuar em algumas das "áreas mais relevantes da cibersegurança, nomeadamente as relacionadas com o *security* e com o *safety*" (Entrevista n.º 9), existindo ainda a opinião de um entrevistado que a investigação "devia estar centralizada e não espalhada por várias entidades" (Entrevista n.º 4). Uma outra área de atuação prende-se com a questão do cibercrime, que "tradicionalmente a GNR e PSP não tem intervenção" (Entrevista n.º 5), porque a cibercriminalidade é entendida como sendo de competência reservada da Polícia Judiciária em termos de investigação criminal, embora existam dúvidas relativamente à sua competência reservada no que respeita à investigação do cibercrime porque, o "termo criminalidade informática já não se encontra positivado na atual lei do Cibercrime" (Entrevista n.º 10).

E finalmente, no que concerne à quarta questão de investigação "De que modo a GNR pode atuar e cooperar no quadro da cibersegurança?":

Tabela 14 - Análise temática da quarta questão
Fonte: Autor

TEMÁTICA	DESCRIÇÃO	FREQUÊNCIA
Âmbito das suas atribuições legais	A atuação deve ser vista como uma extensão das suas atribuições no mundo não virtual.	E3, E5, E7, E2
Âmbito de prevenção geral	A atuação e cooperação deve inserir-se num quadro de prevenção nacional.	E4, E6
Âmbito dos seus programas específicos	A atuação e cooperação insere-se no âmbito dos seus programas especiais e órgãos.	E1, E8, E9, E10

Na procura de resposta à última questão, importa salientar que todos os entrevistados referiram que a Guarda pode atuar e cooperar no ciberespaço, podendo-se agrupar as suas opiniões em três grandes áreas temáticas.

Na primeira área, vista como uma extensão das suas atribuições no mundo não virtual, a GNR tem que evoluir no sentido de ficar responsável pela investigação de "uma boa parte da criminalidade praticada com o auxílio de meios informáticos sem ter nada a ver com crimes informáticos" (Entrevista n.º 5), sendo estes uma continuação dos crimes da sua competência mas praticados noutro espaço, como por exemplo, as burlas e injúrias. Mas para isso precisa de ter "departamentos especializados, não se pode viver de voluntarismos, tem de se ter uma estrutura" (Entrevista n.º 5).

Uma segunda área de atuação prende-se com a participação no âmbito da prevenção e sensibilização em termos gerais (Entrevista n.º 1) ou "integrado com os outros dois órgãos de polícia criminal num plano nacional de prevenção" (Entrevista n.º 4).

E a última área de atuação, insere-se no âmbito dos seus programas especiais e órgãos, sendo que "a Guarda tem que estar presente nos dois mundos e as políticas públicas de segurança que o Estado implementa e que a Guarda operacionaliza, têm que ser efetivas nas duas dimensões" (Entrevista n.º 8). Para isso, deveria ser criado na sua estrutura um órgão autónomo e especializado em matérias de cibersegurança "que tenha capacidade de promover a prevenção e o combate aos diferentes tipos de ciberameaças" (Entrevista n.º 10). E também o desenvolvimento de capacidades de "análise e acompanhamento de redes, de medidas complementares de segurança quer ativas como passivas, e desenvolvimento de ferramentas de monitorização e rastreabilidade de sistemas" (Entrevista n.º 9).

b. Avaliação das descobertas e contributos para o conhecimento

Analisadas as respostas às questões de investigação iremos, de seguida, proceder a uma avaliação do posicionamento da Guarda no âmbito da cibersegurança. Entre as diversas técnicas disponíveis ou ferramentas optamos pela análise SWOT[56], porque a mesma permite uma delimitação que se afigura útil neste estudo, pois o seu objetivo é identificar os assuntos chave e facilitar uma abordagem estratégica, centrando-se nas

[56] A análise SWOT é uma técnica analítica do tipo check-list, cujo autor foi Weihrich (1982), e que consiste em analisar o ambiente externo e interno da organização através de uma série de parâmetros relativos às oportunidades, ameaças, forças e fraquezas da organização (Tavares, 2006, p. 120).

questões com maior impacto potencial (Carapeto & Fonseca, 2014, p. 169). Antes de apresentar a análise convém ressalvar, que esta análise é primária, considerando que o tema se encontra em permanente debate, sofrendo os seus vetores constantes adaptações.

Tabela 15 - Análise SWOT - cibersegurança na GNR
Fonte: Autor

Pontos fortes (**S**trenghts)	**Pontos fracos (W**eaknesses**)**
✓ Cultura institucional de cumprimento da missão; ✓ Desempenho reconhecido como excelente nas áreas de informação, investigação criminal e sistemas de informação; ✓ Conhecimento interno e experiência na produção de aplicações informáticas; ✓ Existência de militares com formação em sistemas de informação e engenharia informática; ✓ Capacidade de cibersegurança; ✓ Dimensão estratégica da sua área de responsabilidade territorial.	✓ Resistência à mudança; ✓ Falta de formação e consciencialização sobre questões ligadas à cibersegurança; ✓ Deficiente regulamentação interna no domínio da segurança da informação na vertente das TIC; ✓ Fraco enquadramento da missão da Guarda na área da cibersegurança nacional; ✓ Inexistência de um órgão com competências na área da cibersegurança; ✓ Visão institucional sobre competência reservada da PJ no âmbito do cibercrime.
Oportunidades (**O**pportunities)	**Ameaças** (**T**hreats)
✓ Crescente importância da qualificação em segurança digital na sociedade civil; ✓ Estado embrionário da cibersegurança noutros órgãos de polícia criminal de competência genérica; ✓ Implementação de nova sala técnica na DCSI/GNR; ✓ Aumento da cibercriminalidade poderá originar alterações da LOIC, a nível da competência reservada da PJ nesta área; ✓ Existência de organismos, no setor público e privado, ligados diretamente ou indiretamente à cibersegurança; ✓ Projetos de financiamento a nível nacional e internacional.	✓ Espetro de ciberameaças maior e mais complexo; ✓ Política de austeridade orçamental; ✓ Dispersão de competências por várias entidades responsáveis pela cibersegurança; ✓ Assimetrias tecnológicas relativas a outros organismos; ✓ Insuficientes parcerias com entidades públicas e privadas; ✓ Colapso dos sistemas informáticos do MAI por ciberataque.

Importa agora passar a um diagnóstico de conjunto que fundamente eventuais mudanças e orientações que a GNR possa vir a prosseguir no âmbito da cibersegurança. Assim cruzando ameaças/oportunidades e forças/fraquezas podemos chegar a quatro orientações estratégicas.

A primeira estratégia, denominada de agressiva (S-O/ Maxi-Maxi), vai procurar relacionar as oportunidades acima identificadas com os pontos fortes da GNR, conforme se ilustra na tabela 16:

Tabela 16 - Estratégias agressivas
Fonte: Autor

Estratégias agressivas
✓ Criar no sítio oficial da GNR, uma área de excelência no âmbito do alerta, informação e prevenção a nível das ciberameaças;
✓ Definir um novo modelo policial a nível de prevenção nesta área *(Cyberpolicing)*[57]*;*
✓ Realizar, a nível nacional, ações de sensibilização nas escolas e autarquias sobre segurança digital, através dos programas especiais da GNR, em articulação com restantes entidades;
✓ Promover ações de sensibilização, junto de dirigentes do Estado e organismos públicos e privados, organizando seminários, conferências e palestras;
✓ Candidaturas a programas de financiamento nacionais e internacionais;
✓ Estabelecer ligações e trocas de saberes e experiências com forças congéneres;
✓ Prover maior formação a militares da GNR na área da segurança digital, no âmbito da CEPOL.

A segunda estratégia, designada de reestruturação (W-O/ Mini-Maxi), vai procurar relacionar as oportunidades anteriormente identificadas com os pontos fracos da GNR, conforme se pode visualizar na tabela 17:

Tabela 17- Estratégias de reestruturação
Fonte: Autor

Estratégias de reestruturação
✓ Sensibilizar os vários escalões hierárquicos relativamente à importância das questões ligadas à cibersegurança;
✓ Promover ações de formação internas na área da cibersegurança. Os formadores poderão ser da GNR com experiência adquirida;
✓ Analisar todo o acervo legislativo nacional e internacional no sentido de inventariar e caracterizar possíveis competências ou formas de intervenção no âmbito da cibersegurança;
✓ Criar doutrina e referenciais nestas áreas;
✓ Assegurar a partilha e tratamento de informação policial ou criminal à escala global de toda a GNR;
✓ Implementar ações de auditoria;
✓ Implementar programas de "Gestão da Mudança" organizacional, subordinadas às TI em geral;

[57] Conceito de prevenção policial aplicado ao ciberespaço, consistindo na monitorização e acompanhamento de eventos ou fenómenos com relevância policial, no âmbito das atribuições legais da GNR e em respeito pelos princípios da legalidade e proporcionalidade.

A terceira estratégia, denominada de diversificada (S-T/ Maxi-Mini), vai procurar relacionar as ameaças anteriormente identificadas com os pontos fortes da GNR, conforme se ilustra na tabela 18.

Tabela 18 - Estratégias diversificadas
Fonte: Autor

Estratégias diversificadas
✓ Estabelecer parcerias ao nível tecnológico e de informação com entidades públicas e privadas com vista ao desenvolvimento das TI na GNR;
✓ Criar um Gabinete de Cibersegurança;
✓ Divulgar a GNR a nível nacional, as suas inúmeras valências, vantagens para o país em termos económicos: eficiência, economia e eficácia;
✓ Assegurar a presença e atuação progressiva no mundo ciber, afirmando a Guarda como determinante no mundo real e no mundo virtual.

E a quarta estratégia, designada de defensiva (W-T/ Mini-Mini), vai procurar relacionar as ameaças anteriormente identificadas com os pontos fracos da GNR, conforme se ilustra na tabela 19.

Tabela 19 - Estratégias defensivas
Fonte: Autor

Estratégias defensivas
✓ Criar um *Computer Security Incident Response Team* (CSIRT) na GNR que tenha a capacidade de prestar um conjunto de serviços de segurança no âmbito da formação, consciencialização e resposta interna a ciberacidentes;
✓ Afirmar a GNR, no âmbito das medidas cautelares de polícia, na manutenção da custódia da prova digital no "local do crime" (instalações, residências, entre outras);
✓ Incentivar e estabelecer protocolos com outras entidades com responsabilidades na área da segurança da informação no domínio da cibersegurança;
✓ Estreitar a ligação com Centro Nacional de Cibersegurança e Centro de Ciberdefesa para colmatar assimetrias tecnológicas e fazer face a colapso dos sistemas informáticos;
✓ Sensibilizar os vários decisores para o retorno que o investimento na área da cibersegurança na GNR irá representar a nível do funcionamento interno, e ao nível dos encargos sociais e económicos relacionados com as ameaças advenientes do Ciberespaço;
✓ Estabelecer protocolos de colaboração com academias e universidades.

Da análise efetuada, entendemos destacar pela sua relevância, a criação de um Gabinete de Cibersegurança na GNR, o conceito relacionado com a ciberprevenção (*cyberpolicing*) e a criação dum CSIRT.

Numa lógica de racionalização e de organização, o Gabinete de Cibersegurança poderia ter sob a sua alçada o CSIRT, assim como um núcleo dedicado à ciberprevenção[58], entre outros órgãos técnicos especializados. Nesta lógica, o CSIRT da Guarda entre outras atribuições, teria por responsabilidade responder internamente a ciberincidentes, validar aspetos de arquitetura organizacional ou aplicacional dos sistemas informáticos e realizar ações de investigação e desenvolvimento na área das novas tecnologias que podem ou poderão vir a ser utilizados no âmbito de fenómenos criminais ligados ao ciberespaço.

E por fim, o núcleo dedicado à ciberprevenção, teria entre outras atribuições, a responsabilidade de planear e operacionalizar ações e campanhas de prevenção e de sensibilização, internas e externas no domínio do *cyberpolicing* especialmente com recurso às novas tecnologias de comunicações e de conhecimento (Cfr. *Draf* da estrutura do Gabinete de Cibersegurança da GNR em Apêndice E)

Finalizada esta análise, e na linha do que antecede, iremos de seguida apresentar uma interpretação do nosso contributo em relação aos modelos teóricos anteriormente abordados. Assim, em relação ao modelo teórico de Santos, Bravo e Nunes (2012, p. 164):

Tabela 20 - Interpretação do modelo de atuação na proteção do ciberespaço
Fonte: Adaptação do autor de (Santos, et al., 2012)

	Proteção Simples	Prossecução Criminal	Defesa do Estado
Atores	GNR atua através do CSIRT	GNR atua como órgão de polícia criminal	GNR colabora nos termos legais

De igual forma, se efetuarmos a comparação em relação ao modelo de Santos (2011) de estrutura nacional para a cibersegurança, constituída por seis eixos de atuação, temos:

[58] A exemplo do que já acontece com os programas especiais na GNR que são uma repartição da Direção de Operações do Comando Operacional da GNR.

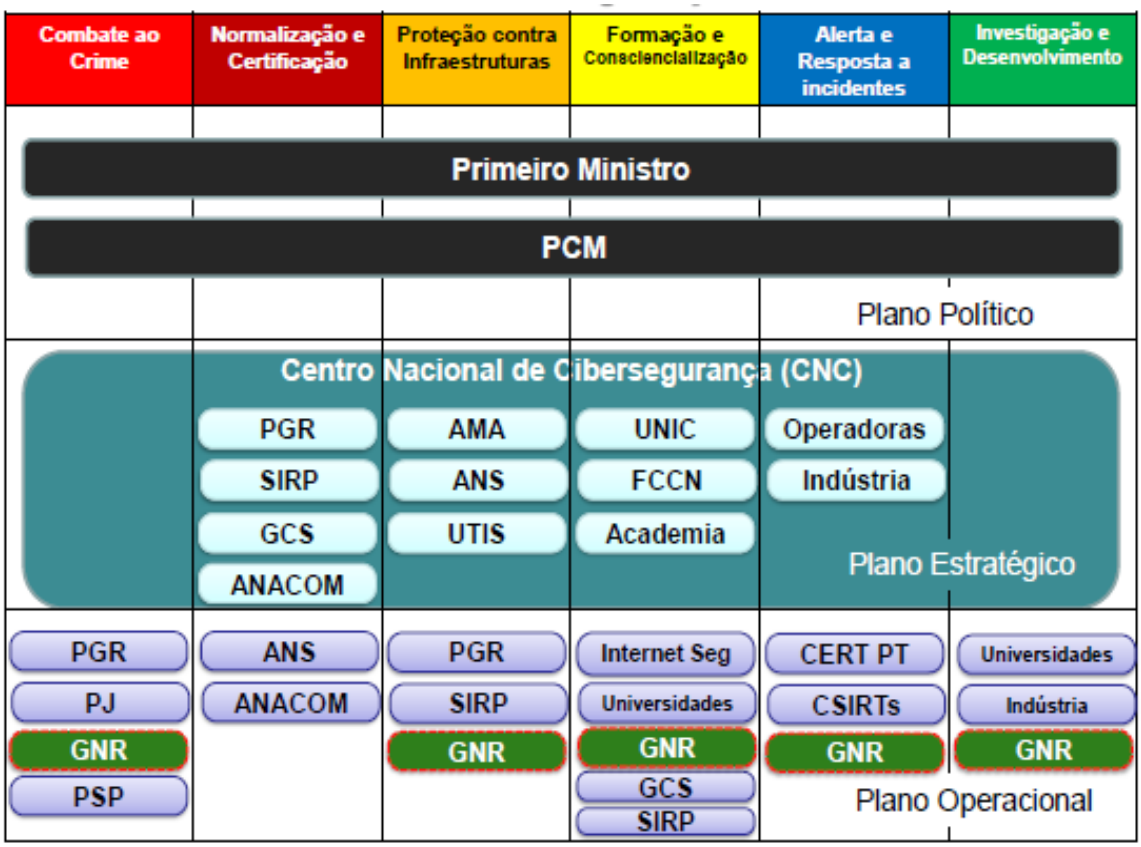


Figura 12 – Interpretação da estrutura nacional para a cibersegurança
Fonte: Autor adaptado de (Santos, 2011)

Com síntese deste capítulo, podemos afirmar que o ciberespaço tem uma importância estratégica para as sociedades modernas e, consequentemente também um domínio onde as forças e serviços de segurança não podem deixar de fazer a sua atuação. No atual e futuro enquadramento legislativo, não só têm que estar aptas a dar uma resposta eficaz aos novos tipos de criminalidade, como também deverão aí garantir a segurança e tranquilidade dos cidadãos. Para atingir este desiderato, a Guarda deverá gerar capacidades prioritárias neste domínio de forma a assumir uma presença relevante e prestigiante, tal como definido na sua Estratégia 2020.

Conclusões

A realização da presente investigação teve como principal objetivo analisar como as forças e serviços de segurança poderiam atuar no contexto da cibersegurança nacional, e em particular a GNR, num momento em que a definição de uma Estratégia Nacional de Cibersegurança - que se define como um conjunto de iniciativas destinadas a potenciar a livre utilização do ciberespaço e garantir a sua segurança, promovendo a proteção de infraestruturas de informação críticas nacionais contra eventuais ataques cibernéticos ou a materialização de ciberameaças - assume uma importância crescente e peso inegável no âmbito da autonomia política e estratégica de Portugal.

É preciso recordarmos que o ciberespaço se apresenta, cada vez mais, como uma realidade para a concretização de práticas criminais, belicistas ou de índole subversiva e que, por outro lado, a sua elevada acessibilidade, a sua dificuldade de regulação, aliado ao seu enorme manancial de utilizadores, na generalidade mal informados e raramente preparados para as questões de segurança, potenciam inúmeras ameaças provenientes do ciberespaço, permitindo que de forma extremamente fácil se troquem dados e informações potenciadores de ações delituosas.

E no âmbito da Defesa Nacional e Segurança nas dimensões cognitiva, informativa e física, o ciberespaço constitui-se na atualidade como um elemento distinto e equiparável aos domínios terrestre, aéreo e naval das áreas de interesse e dos teatros de operações, relevando o seu controlo como um fator acrescido e decisivo nas componentes de negócio, na velocidade de acesso a dados, na geração de informação e conhecimento, e na obtenção de vantagem operacional para alcançar objetivos militares e civis.

Neste contexto, considerando a abrangência do tema e por motivos de tempo e amplitude do trabalho, procedemos à delimitação da nossa investigação à compreensão de qual o papel da GNR na cooperação com as entidades intervenientes e responsáveis no domínio da cibersegurança. Definimos como QC para o lançamento inicial da pesquisa "Em que medida as forças e serviços de segurança, poderão cooperar com as entidades intervenientes e responsáveis no domínio da cibersegurança?", e associadas a esta QC formulamos as respetivas QD.

O processo de investigação desenvolveu-se em função das questões levantadas, central e derivadas que assumiram, inevitavelmente, um papel orientador de todo o processo, tendo sido percorridas todas as fases da metodologia científica em harmonia com

as Orientações Metodológicas para a Elaboração de Trabalhos de Investigação do IESM (Cfr. Percurso metodológico e a definição da estratégia metodológica em Apêndice A).

Avança-se agora com as principais conclusões desta investigação. Em primeiro lugar sistematizou-se a revisão da literatura mais relevante sobre as temáticas da cibersegurança, enquadramento normativo e quadro de atuação das forças e serviços de segurança, respetivamente nos capítulos 1, 2 e 3. No capítulo 1, numa primeira parte analisou-se e relacionou-se os conceitos teóricos relacionados com o ciberespaço e a cibersegurança procurando apresentar-se um sucinto quadro conceptual. Observou-se uma multiplicidade de conceitos, em que os termos usados são normalmente expressos em inglês, mas existindo diferentes significados, dependendo do país de origem e de quem os usa. Em relação ao conceito de cibersegurança, concluiu-se pela inexistência de uma sua definição que seja comum e harmonizada quer a nível nacional ou internacional, o que dificulta o estudo de abordagens internacionais contra as ameaças globais do ciberespaço. Na segunda parte deste capítulo abordou-se a dimensão estratégica do ciberespaço, concluindo-se pela sua dimensão crítica para o normal funcionamento das sociedades modernas, sendo neste domínio que assentam as principais infraestruturas críticas de telecomunicações, de transporte e de distribuição de energia.

No capítulo 2, sistematizou-se no âmbito da segurança e defesa, o quadro normativo internacional e nacional da cibersegurança, apresentando os normativos, iniciativas legais e entidades mais relevantes. No quadro internacional, analisou-se a UIT, a Convenção sobre o Cibercrime do Conselho da Europa, a estratégia da UE para a cibersegurança e principais entidades europeias, as capacidades da NATO e os contributos da OCDE, concluindo-se pela existência de um quadro internacional de intervenção e cooperação de várias entidades de forma a permitir a livre circulação no ciberespaço e garantir a sua segurança.

No quadro nacional, analisou-se e estruturou-se a legislação nacional relevante neste domínio, apresentando-se as principais orientações e propostas estratégicas existentes, assim como as entidades intervenientes. Em relação à legislação nacional, efetuamos apenas uma síntese remetendo a sua análise crítica para a componente analítica desta investigação, e em relação às orientações estratégicas nacionais, concluímos pela existência de uma quadro nacional em processo de consolidação, constituído pelo atual CEDN e ENCT e propostas de ENCSeg e CESI. Pela sua relevância, efetuamos a síntese destas orientações estratégicas e no âmbito da teorização de estratégias nacionais de

cibersegurança, concluímos pela existência de dois autores nacionais que têm apresentado produção teórica, respetivamente Nunes (2012) e Santos (2011).

O capítulo 3 permitiu que de forma breve se observasse a intervenção das forças e serviços de segurança neste domínio, em termos gerais e em particular a GNR. Inicialmente, efetuamos uma síntese da principal doutrina relativa à criminalidade relacionada com a utilização dos computadores e concluímos com um quadro conceptual de dúvidas existentes sobre o conceito de cibercrime e sua competência reservada à PJ. Em relação à GNR apresentamos um quadro de atribuições e competências dos seus órgãos, que podem ser prosseguidas no ciberespaço, concluindo-se com a apresentação de um dos objetivos estratégicos da GNR para o horizonte 2015-2020, no âmbito da cibersegurança.

A segunda parte desta investigação, de natureza mais analítica, constituída pelo capítulo 4, dirigiu-se exclusivamente à apresentação e análise dos resultados. Numa primeira parte, respondemos a cada uma das questões derivadas, tendo por base a análise teórica que realizámos anteriormente, bem como a análise de conteúdo que realizámos às entrevistas. A segunda parte deste capítulo foi dedicada à avaliação das descobertas e contributos para o conhecimento, onde expomos e detalhamos uma análise SWOT relativa à cibersegurança na GNR e apresentamos alguns contributos.

Em relação às conclusões das entrevistas, salientamos que todos os entrevistados consideraram ser importante a proteção do ciberespaço, vendo este domínio ou como uma continuação do mundo real ou como uma dimensão crítica para a sociedade e com abrangência planetária. No que concerne ao enquadramento legislativo sobre a cibersegurança concluiu-se que este ainda está numa fase embrionária de elaboração ou se encontra desajustado, não acompanhando assim a dinâmica evolutiva do sector. Relativamente ao quadro de atuação das forças e serviços de segurança neste âmbito, concluiu-se que este se insere no respetivo quadro de competências de atividades que desenvolvem no mundo não virtual ou que deverá ser reconsiderado atendendo à evolução da cibersegurança. E em relação à atuação da Guarda, esta pode ser vista como: uma extensão das suas atribuições; no âmbito dum quadro de prevenção nacional ou no âmbito dos seus programas especiais e órgãos próprios.

A análise SWOT efetuada permitiu identificar um conjunto de estratégias agressivas, de reestruturação, diversificadas e defensivas, de forma a apresentar alguns contributos, destacando-se a criação de um Gabinete de Cibersegurança na GNR, a conceptualização relacionada com a ciberprevenção (*cyberpolicing*) e a criação dum

CSIRT. Terminamos este capítulo com a interpretação de dois modelos teóricos anteriormente abordados, perante as descobertas efetuadas.

Como principal contributo para o conhecimento, destacamos que a adequada prevenção e o combate às ciberameaças exige a intervenção e a cooperação de várias entidades, no plano nacional e internacional, pelo que, a GNR, enquanto força de segurança de natureza militar deverá criar capacidades no sentido de poder contribuir para a sua prevenção e combate, na esfera das suas competências, no sentido de se preparar para fazer face aos novos desafios da cibersegurança.

A aplicação prática do nosso trabalho poderá passar pela implementação de um modelo de segurança de *cyberpolicing* na GNR, tendo em vista prevenir o atual espetro de ciberameaças, sendo necessário também criar um órgão especializado que promova a coordenação técnica com outros órgãos da GNR, de forma a potenciar as suas valências nesta área altamente especializada (Cfr. *Draf* da estrutura do Gabinete de Cibersegurança da GNR em Apêndice E).

Por último, como todas as investigações empíricas, também esta tem as suas limitações, no entanto, a que se considerou como principal foi sem dúvida a de natureza metodológica, designadamente o facto de se ter utilizado uma amostra reduzida, que compromete a generalização extensiva.

Como recomendação para futuras linhas de investigação sugerimos a análise de como a GNR poderá atuar perante o fenómeno do hacktivismo, a intervenção da GNR no quadro da nova ENCT e a cooperação com o Centro de Ciberdefesa, em virtude do seu estatuto militar.

Bibliografia

Alexander Klimburg , 2012. *National Cyber Security Framework Manual.* Tallinn: NATO CCD COE Publication.

Andreasson, K., 2012. *Cybersecurity - Public Sector Threats and Responses.* Boca Raton: Taylor & Francis Group, LLC.

Ascensão, O., 2001. Criminalidade Informática. In: *Estudos sobre Direito da Internet e da Sociedade da Informação.* Coimbra: Editora Almedina.

Assembleia da República, 2009. *Aprova a Convenção do Cibercrime (Resolução da Assembleia da República n.º 88/2009).* Lisboa: Diário da República.

Assembleia da República, 2009. *Protocolo adicional relativo à incriminação de atos de natureza racista e xenófoba praticados através de sistemas informáticos (aprovado pela Resolução da Assembleia da República n.º 91/2009, de 15 de setembro)..* Lisboa: Diário da República.

Beggs, P., 2010. *Securing the Nation´s Critical Cyber Infrastructure.* California: Department of Homeland Security.

Branco, C., 2010. *Guarda Nacional Republicana - Contradições e ambiguidades.* Lisboa: Edições Sílabo.

Brenner, S. W., 2010. *Cybercrime : criminal threats from cyberspace.* Santa Barbara, California: Praeger.

Caldas, A., 2011. Uma Estratégia Nacional de Cibersegurança. In: P. Noguês, ed. *Segurança&Defesa.* Loures: Diário de Bordo, Lda, pp. 94-98.

Carapeto, C. & Fonseca, F., 2014. *Administração Pública - Modernização, Qualidade e Inovação.* 3.ª ed. Lisboa: Edições Sílabo, Lda.

Castells, M., 2004. *A Galáxia Internet: Reflexões sobre Internet, Negócios e Sociedade.* Lisboa: Fundação Calouste Gulbenkian.

Cavelty, M. D., Mauer, V. & Krishna-Hensel, S. F., 2008. *Power and Security in the Information Age - Investigating the Role of the Sate in the Cyberspace.* Hampshire: Ashgate Publishing Limited.

Clarke, R. A. & Knake, R. K., 2010. *Cyber War: The Next Threat To National Security And What To Do About It.* 1 ed. New York: HarperCollins Publishers.

Comissão Europeia, 2013. *Estratégia da União Europeia para a cibersegurança: Um ciberespaço aberto, seguro e protegido.* Bruxelas: s.n.

Conselho da Europa, 2010. *Estratégia de segurança interna da União Europeia - Rumo a uma modelo europeu de segurança*, Bruxelas: União Europeia.

Dias, V. E., 2010. *A problemática da investigação do cibercrime,* Lisboa: Faculdade de Direito da Universidade de Lisboa.

DoD, 2011. *Department of Defense Stategy for Operating in Cyberspace.* s.l.:s.n.

Donk, W., Loader, B. D., Nixon, P. G. & Rucht, D., 2004. *Cyberprotest: New media, citizens and social movements.* London: Routledge.

ENISA, 2013. *Cybersecurity cooperation - Defending the digital frontline.* Heraklion, Grécia: s.n.

Fernandes, J. P., 2014. *Ciberguerra: Quando a Utopia se Transforma em Realidade.* Vila do Conde: Verso da História.

Fisher, E. A., 2009. *Creating a national framework for cybersecurity: an analysis and options.* New Rork: Nova Science Publishers, Inc..

Fontoura, L., 2013. *Segurança e Defesa Nacional - Um Conceito Estratégico.* Coimbra: Edições Almedina, S.A..

Ghernaouti, S., 2013. *Cyber Power - Crime, Conflict and Security in Cyberspace.* Lausanne, Switzerland: EPFL Press.

Gibson, W., 1984. *Neuromancer.* New York: The Berkley Publishing Group.

Grady, M. F. & Parisi, F., 2006. *The Law and Economics of Cibersecurity.* Cambridge: Cambridge University Press.

Guerra, I. C., 2006. *Pesquisa Qualitativa e Análise de Conteúdo.* Cascais: Princípia Editora.

Halpin, E., Trevorrow, P., Webb, D. & Wright, S., 2006. *Cyberwar, Netwar and the Revolution in Military Affairs.* Hampshire: Palgrave Macmillian.

Headquarters, Department of the Army, 2014. *FM 3-38 Cyber Electromagnetic Activities.* [em linha] Disponível em: https://armypubs.us.army.mil/doctrine/index.html [Consult. 16 janeiro 2015].

IDN-CESEDEN, 2013. *Estratégia da Informação e Segurança no Ciberespaço.* Lisboa: Instituto da Defesa Nacional.

Instituto da Defesa Nacional, 2013. *Conceito Estratégico de Defesa Nacional: Contributos e Debate Público,* Lisboa: Imprensa Nacional Casa da Moeda.

Instituto de Estudos Superiores Militares, 2014. *NEP/ACA-010- Trabalhos de investigação,* Lisboa: IESM.

Instituto de Estudos Superiores Militares, 2014. *NEP/ACA-18 - Regras de apresentação e referenciação para os trabalhos escritos a realizar no IESM,* Lisboa: IESM.

Jordan, T. & Taylor, P. A., 2004. *Hacktivism and Cyberwars: Rebels with a cause?.* Routledge: London.

Kierkegaard, S. M., 2008. *International Cybercrime,* Denmark: International Association of IT Lawyers (IAITL).

Klimburg, A., 2011. Mobilizing Cyber Power. *Survival: Global Politics and Strategy, vol.53, n.º1,* fevereiro-março, pp. 41-60.

Kowalik, J. S., Gorski, J. & Sachenko, A., 2004. *Cyberspace Security and Defense: Research Issues.* Gdansk: Springer.

Kremer, J.-F. & Muller, B., 2014. *Cyberspace and International Relations - Theory, Prospets and Challenges.* Bonn, Germany: Springer.

Kuehl, D., 2009. *Cyberspace & Cyberpower: Defining the Problem.* s.l.:Cyberpower & National Security.

Last, M. & Kandel, A., 2005. *Fighting Terror in Cyberspace.* Tuck Link, Singapore: World Scientific.

Libicki, M. C., 2009. *Cyberdeterrence and Cyberwar.* Santa Monica: RAND Corporation.

Loureiro dos Santos, J. A., 2014. *O Futuro da Guerra.* 1.ª ed. Lisboa: Nova Vega.

Lourenço, N. et al., 2015. *Segurança Horizonte 2025. Um Conceito de Segurança Interna.* Lisboa: Ediçoes Colibri.

Magriço, M. A., 2014. *A Exploração Sexual de Crianças no Ciberespaço.* Lisboa: Alêtheia Editores.

Marsden, C. T., 2011. *Internet Co-Regulation - European Law, Regulatory Governance and Legitimacy in Cyberspace.* 1.ª ed. New York: Cambridge University Press.

Mayer, M., Martino, . L., Mazurier, P. & Tzvetkova, G., 2014. *How would you define Cyberspace?.* Pisa: Scuola Superiore Sant'Anna.

McQuade, S. C., 2009. *Encyclopedia of cybercrime.* Westport, Connecticut: Greenwood Press.

Murray, A. D., 2007. *The Regulation of Cyberspace - control in the online environment.* 1.ª ed. Abingdon: Routledge-Cavendish.

Natário, R. M., 2013. O Carácter Trinitário da Guerra no Ciberespaço. In: *Revista Militar n.º 4.* Lisboa: Empresa da Revista Militar, pp. 301-323.

Natário, R. M., 2013. O Combate ao Cibercrime: Anarquia e Ordem no ciberespaço. In: *Revista Militar n.º 10.* Lisboa: Empresa da Revista Militar, pp. 823-858.

NATO, 2010. *Strategic Concept For the Defence and Security of The Members of the North Atlantic Treaty Organisation.* [em linha] Disponível em: http://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf [Consult. 15 fevereiro 2015].

Norwood, K. T. & Catwell, S. P., 2009. *Cybersecurity, cyberanalysis and warning.* New York: Nova Science Publishers, Inc..

Nunes, P. F., 2010. Mundos Virtuais, Riscos Reais: Fundamentos para a definição de uma Estratégia de Informação Nacional. In: *Revista Militar.* Lisboa: Empresa da Revista Militar, pp. 1169-1198.

Nunes, P. F., 2012. A definição de uma Estratégia Nacional de Cibersegurança. In: *Nação e Defesa - Revista Quadrimestral n,º 133.* Lisboa: Insituto da Defesa Nacional, pp. 113-127.

Nunes, P. V. & Natário, R. M., 2014. Risco Social no Ciberespaço. A Vulnerabilidade das Infraestruturas Críticas. In: *Revista Militar.* Lisboa: Empresa da Revista Militar, pp. 249-286.

Pierre Audoin Consultants , 2013. *Competitive analysis of the UK cyber security sector.* Version 1 ed. London: s.n.

Portnoy, M. & Goodman, S., 2009. *Global Initiatives to Secure Cyberspace - An Emerging Landscape.* Fairfax: Springer.

Procuradoria-Geral da República, 2013. *Relatório de Atividades de 2013 do Gabinete do Cibercrime,* Lisboa: PGR.

Raposo, J., 2006. *Direito Policial - Tomo I.* Coimbra: Edições Almedina, SA.

Rocha, M. T., 2008. Protecção de Infraestruturas Críticas. In: *Segurança&Defesa.* Loures: Diário de Bordo, pp. 133-143.

Rosenzweig, P., 2013. *Cyber Warfare - How Conflits in Cyberspace are Challenging America and Changing The world.* Santa Barbara, California: Praeger.

Santos, J. L. A. d., 2011. *Contributos para uma melhor governação da cibersegurança em Portugal,* Lisboa: Universidade Nova de Lisboa.

Santos, L. A. & Lima, J. M., 2014. *Orientações Metodológicas para a Elaboração de Trabalhos de Investigação.* Lisboa: IESM.

Santos, L., Bravo, R. & Nunes, P. V., 2012. Proteção do ciberespaço: visão analítica. In: *Riscos, Segurança e Sustentabilidade.* Lisboa: Editora Salamandra, pp. 163-176.

Santos, P., Bessa, R. & Pimentel, C., 2008. *CYBERWAR - O fenómeno, as tecnologias e os atores.* Lisboa: FCA- Editora de Informática, Lda.

Secretário-Geral do Sistema de Segurança Interna, 2015. *Relatório Anual de Segurança Interna 2014,* Lisboa: s.n.

Silva, N. P., 2015. *Entre o Militar e o Policial - As Reformas da Administração Pública.* 1.ª ed. Lisboa: Diário de Bordo.

Simas, D. V., 2014. *O Cibercrime. Tese de Mestrado em Ciências Jurídico-Forenses,* Lisboa: Universidade Lusófina de Humanidades e Tecnologias.

Tavares, M. M., 2006. *Estratégia e gestão por objetivos: duas metodologias de gestão para as organizações atuais.* 3.ª ed. Lisboa: Universidade Lusíada Editora.

Thampi, S. M., Bhargava, B. & Atrey, P. K., 2014. *Managing Trust in Cyberspace.* Boca Raton: CRC Press Taylor & Francis Group, LLC.

U.S. Department of Defense, Joint Chiefs of Staff, 2011. *Joint Terminology for Cyberspace Operations.* [Em linha] Disponível em : http://www.nsci-va.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20Cyberspace%20Operations.pdf [Consult. 2014 dezembro 1].

Valente, M. M., 2005. *Teoria Geral do Direito Policial - Tomo I.* Coimbra: Edições Almedina, SA.

Valente, M. M., 2006. *Regime Jurídico da Investigação Criminal - Comentado e Anotado.* Coimbra: Edições Almedina, Lda.

Ventre, D., 2011. *Cyberwar and Information Warfare.* London: ISTE, Lda John Wiley & Sons, Inc..

Verdelho, P., 2005. Cibercrime e Segurança Informática. In: *Polícia e Justiça - Revista do Instituto Superior de Polícia Judiciária e Ciências Criminais N.º 6.* Coimbra: Coimbra Editora, pp. 159-175.

Verdelho, P., Bravo, R. & Rocha, M. L., 2003. *Leis do Cibercrime - vol. I.* Lisboa: Centro Atlântico, Lda.

Viana, V. R., 2012. Editorial. In: *Nação e Defesa n.º 133 - Revista Quadrimestral.* n.º 133 ed. Lisboa: Instituto da Defesa Nacional, pp. 5-7.

Apêndice A- Percurso metodológico e a definição da estratégia metodológica

Como referido por Santos e Lima (2014, p. 30), " todas as orientações empíricas se processam por estádios que passam da ignorância à descoberta, depois à representação mental dos processos sociais e ao seu confronto com os factos e observações e, só por fim, à exposição oral ou escrita dessa representação, com a finalidade de difusão do conhecimento". Assim, nesta nossa pesquisa percorremos as três fases, respetivamente a exploratória, analítica e conclusiva.

O objetivo geral desta investigação é analisar como as forças e serviços de segurança, e em particular a GNR, poderão atuar no contexto da cibersegurança na sociedade portuguesa, procurando assim acrescentar conhecimento empírico que contribua para uma visão integradora dos esforços em curso neste domínio e, consequentemente estimular e potenciar sinergias no âmbito nacional e internacional.

Para atingir este objetivo, definimos como objetivos específicos (OE), os seguintes:

- OE1. Compreender a importância estratégica da proteção do ciberespaço;
- OE2. Analisar o enquadramento normativo da cibersegurança;
- OE3. Definir o quadro de intervenção das forças e serviços de segurança no âmbito da cibersegurança;
- OE4. Apresentar um modelo de atuação da GNR no quadro da cibersegurança.

E como Questão Central (QC): "Em que medida as forças e serviços de segurança, poderão cooperar com as entidades intervenientes e responsáveis no domínio da cibersegurança?"

Associadas à QC, foi possível formular as seguintes Questões Derivadas (QD):

- QD1: Qual a importância estratégica da proteção do ciberespaço?
- QD2: A cibersegurança tem um enquadramento normativo ajustado à realidade nacional?
- QD3: Qual o quadro de atuação das forças e serviços de segurança no domínio da cibersegurança?
- QD4: De que modo a GNR pode atuar e cooperar no quadro da cibersegurança?

O processo de investigação desenvolveu-se em função das questões levantadas, central e derivadas, que assumem, inevitavelmente, um papel orientador de todo o processo.

Neste contexto, pela sua flexibilidade, optamos por uma estratégia de investigação qualitativa, dado que a análise incide em processos organizacionais, nas suas várias

componentes, onde se incluem também as relações informais. Esta opção fundamentou-se na existência de um número reduzido de unidades de amostragem, mas também por se pretender recolher informação em profundidade e em continuidade, possibilitando a exploração de uma multiplicidade de facetas e dimensões, com o objetivo de compreender o fenómeno em estudo na sua totalidade.

Relativamente ao *design* da pesquisa adotada, optámos pelo estudo de caso, dado que elaboramos uma análise detalhada e intensiva de um único caso, ou seja, a atuação e cooperação da GNR no quadro da cibersegurança, possibilitando, assim, captar a complexidade e a natureza particular do caso em questão.

Os métodos e instrumentos utilizados foram as entrevistas de aprofundamento - passíveis de tratamento através da análise de conteúdo, e a análise documental.

Todas as entrevistas de aprofundamento realizadas foram do tipo semiestruturadas e foram conduzidas pelo próprio investigador, o que por um lado, concedeu uma certa flexibilidade e liberdade às respostas dos entrevistados, mas por outro lado, também foram condicionadas por fatores de ordem cultural, cognitiva, motivacional e até conjuntural. Para o efeito, utilizou-se um guião constituído por um conjunto de tópicos ou questões articulados entre si que tornaram possível, por um lado, a compreensão do tema em análise, nas suas diferentes dimensões e níveis e por outro lado, permitiu que os entrevistados não abordassem temas dispersos (Cfr. Apêndice C). Ainda neste âmbito, importa salientar que foi solicitado intencionalmente a todos os entrevistados que interpretassem e se posicionassem face aos tópicos do guião, concedendo-lhes o tempo necessário para organizarem a sua opinião e evidenciando os significados atribuídos, permitindo que o entrevistador percecionasse a forma como estes sentem e interpretam as problemáticas em questão.

Para cada uma das entrevistas realizadas foram elaboradas análises detalhadas, posteriormente, a informação foi objeto de análise de conteúdo, utilizando para o efeito as grelhas de análise temáticas. A informação obtida revelou um teor muito rico, possibilitando, de facto, uma análise de conteúdo produtiva, através da qual sistematizamos e interpretamos toda a informação transmitida e complementamos algumas das conclusões retiradas da análise documental.

O outro método utilizado nesta investigação foi a análise documental, que se desenvolveu com recurso à bibliografia nacional e internacional existente sobre a cibersegurança, com o cuidado de recolher referências, para a constituição de uma base documental alargada sobre o tema. Embora estes documentos, contrariamente aos dados

obtidos no método anterior, não tenham sido produzidos pelo investigador, foram igualmente relevantes para esta investigação.

Outro momento crucial no nosso percurso metodológico foi a definição do principal método de amostragem, onde não se constituiu uma amostra no sentido estatístico do termo, mas uma amostra de conveniência ou intencional de forma a garantir os objetivos da investigação. Embora, seja um método não probabilístico, o que não permite a generalização dos resultados, garante que os casos sejam selecionados de forma estratégica. Todavia, temos consciência que esta impossibilidade de generalizar os resultados, para além do contexto criado, constitui uma limitação da nossa investigação.

No entanto, importa reiterar o que já referimos no Capítulo 4, ou seja, orientados pelo pragmaticismo imposto pelas próprias condições de uma investigação com estas caraterísticas, procurou-se, alguma heterogeneidade no processo de seleção dos entrevistados selecionados. Assim, mais do que entrevistar (ou inquirir) grande parte da população sobre o tema em questão, optou-se por entrevistar em profundidade as pessoas que reunissem cumulativamente os seguintes requisitos essenciais:

a) Tivessem conhecimentos teóricos e/ou competências técnicas sobre o ciberespaço, com reconhecimento académico e profissional na esfera das Forças Armadas e de Segurança;
b) Já tivessem atualmente ou pudessem vir a ter, a curto prazo, responsabilidades nos processos de cibersegurança nacional.

Como seria previsível, a utilização destes critérios recaiu sobre um número muito restrito de especialistas e profissionais. Desta forma foram realizadas 10 entrevistas semiestruturadas, sendo seis a peritos reconhecidos no universo das forças armadas e de segurança, e quatro a peritos com funções académicas e de relevo em instituições civis. Com este procedimento procurou-se esclarecer e compreender as perceções dos entrevistados sobre o fenómeno do ciberespaço e em particular da cibersegurança, aprofundando-se, algumas singularidades e regularidades. No entanto, por razões de estritamente de operacionalização da pesquisa e não por pressupostos teóricos de não interferência das esferas de vivência pessoal dos entrevistados, o enfoque analítico visou apenas as conceções e perceções sobre a proteção do ciberespaço, excluindo, outras dimensões da vida dos entrevistados.

Todavia, a partir do momento em que, reiteradamente, as entrevistas não traziam informação adicional, optou-se por finalizar os respetivos procedimentos, recorrendo ao

critério de redundância ou saturação e consequentemente tomou-se a decisão de não realizar mais entrevistas.

Por último, cumpre ainda referir que o presente Trabalho de Investigação Individual seguiu todas as normas e procedimentos definidos nas NEP/ ACA - 010 e ACA-018 bem como as "Orientações Metodológicas para a Elaboração de Trabalhos de Investigação" (Santos & Lima, 2014).

Apêndice B- Modelo de análise

Tabela 21 - Modelo de Análise
Fonte: Autor

Objetivos	Questões	Enquadramento conceptual	Análise de resultados
Geral: Analisar como as forças e serviços de segurança, poderão cooperar com as restantes entidades responsáveis no domínio da cibersegurança.	**Central:** *"Em que medida as forças e serviços de segurança, poderão cooperar com as restantes entidades responsáveis no domínio da cibersegurança?"*		**Cap. 4.** Apresentação e análise dos resultados
Específico: Compreender a importância estratégica da proteção do ciberespaço.	**QD1:** Qual a importância estratégica da proteção do ciberespaço?	**Cap. 1.** Dimensão Estratégica da proteção do ciberespaço.	Apresentação e análise temática de dez entrevistas semiestruturadas a peritos reconhecidos no universo das forças armadas e de segurança e no seio da sociedade civil.
Específico: Comparar o enquadramento normativo da cibersegurança.	**QD2:** A cibersegurança tem um enquadramento normativo ajustado à realidade nacional?	**Cap. 2**. Enquadramento normativo da cibersegurança.	
Específico: Definir o quadro de intervenção das forças e serviços de segurança no âmbito da cibersegurança.	**QD3:** Qual o quadro de atuação das forças e serviços de segurança no domínio da cibersegurança?	**Cap. 3.** Atuação das forças e serviços de segurança no âmbito da cibersegurança a. Enquadramento Geral	Aplicação de Análise SWOT – cibersegurança na GNR.
Específico: Apresentar um modelo de atuação da GNR no quadro da cibersegurança.	**QD4:** De que modo a GNR pode atuar e cooperar no quadro da cibersegurança?	**Cap. 3.** Atuação das forças e serviços de segurança no âmbito da cibersegurança b. O caso da GNR	Interpretação das descobertas face a modelos teóricos anteriormente apresentados.

Apêndice C – Guião da entrevista

Apresentação e objetivos da entrevista

Estamos a contactá-lo no sentido de nos facultar uma entrevista no âmbito de um trabalho de investigação individual do Curso de Estado-Maior Conjunto do Instituto de Estudos Superiores Militares, respeitante ao tema *" O papel da GNR no contexto da cibersegurança nacional"*, e cujo objetivo geral de investigação é analisar como as forças e serviços de segurança nacionais poderão cooperar com as restantes entidades responsáveis no domínio da cibersegurança nacional, procurando assim acrescentar conhecimento empírico que contribua para uma visão integradora dos esforços em curso neste domínio e, consequentemente estimular e potenciar sinergias no âmbito nacional e internacional. Neste contexto, assumimos como de especial relevância para a nossa investigação a auscultação da sua opinião.

Entrevista

1. O ciberespaço é uma realidade e um fenómeno muito mais complexo e abrangente do que a internet propriamente dita, compreendendo serviços, modelos de negócios, infraestruturas, dinâmicas sociais próprias, bem como diferentes tipos de atores. Qual a importância estratégica da proteção do ciberespaço?

2. Considera que a cibersegurança tem um enquadramento normativo ajustado à realidade nacional?

3. Qual o quadro de atuação das forças e serviços de segurança no domínio da cibersegurança?

4. Em particular, de que modo a GNR pode atuar e cooperar no quadro da cibersegurança?

Muito obrigado pela sua colaboração, que foi de extrema importância.

Paulo Daniel Duarte Machado

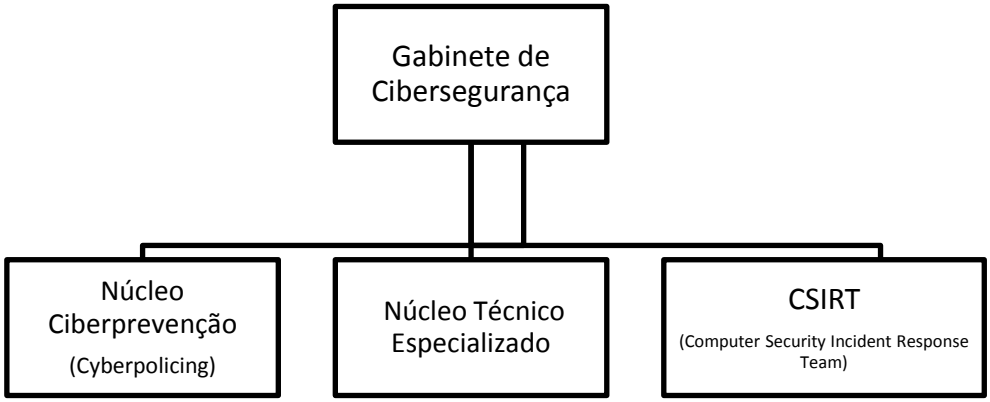
TCOR GNR/Inf

Apêndice D – Sinopse das entrevistas gravadas em suporte digital (DVD)

Nota: Não estão autorizadas cópias do suporte digital, nem a divulgação dos conteúdos, para fins diferentes daquele que é o âmbito do presente Trabalho de Investigação Individual.

Apêndice E – *Draft* estrutura do Gabinete de Cibersegurança da GNR

Apresentamos de seguida, um *draft* de organograma e algumas das atribuições dum possível Gabinete de Cibersegurança da GNR.



O Núcleo de Ciberprevenção (*Cyberpolicing)* teria por atribuições:

- Coordenar ações de cooperação com instituições públicas e privadas, em matéria de cibersegurança e ciberdefesa;
- Articular e coordenar, no plano técnico, outros órgãos da GNR, com atribuições na área da investigação e forense, bem como no domínio das informações em matérias ligadas com o ciberespaço;
- Planear e operacionalizar ações e campanhas de prevenção e de sensibilização no domínio do *cyberpolicing* especialmente com recurso às novas tecnologias de comunicação.

O Núcleo Técnico Especializado teria por atribuições:

- Realizar estudos ou pareceres técnicos no âmbito da cibersegurança;
- Analisar e difundir legislação nacional e internacional ligada com a cibersegurança;
- Difundir orientações de atuação no âmbito do *cyberpolicing*;
- Elaborar normativos internos, que incidam nos termos de utilização, limites e responsabilidades na utilização dos recursos tecnológicos;
- Recolher lições aprendidas e colaborar na produção de doutrina na área da prevenção e da repressão criminal no domínio do ciberespaço;

E o Computer Security Emergency Response Team (CSIRT) teria como atribuições:

- Validar aspetos de segurança da arquitetura informacional ou aplicacional dos sistemas informáticos que se encontrem em produção ou em fase de implementação na GNR;
- Contribuir, internamente, à resposta a ciberincidentes;
- Difundir informações relacionadas com a segurança;
- Dar suporte técnico especializado a outros órgãos com responsabilidade na área da investigação e forense digital;