INSTITUTO UNIVERSITÁRIO MILITAR

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

CURSO DE PROMOÇÃO A OFICIAL GENERAL

2022/2023

Trabalho de Investigação Individual

CONTRIBUTOS PARA UM MODELO DE ATUAÇÃO DA GUARDA NACIONAL REPUBLICANA NO CIBERESPAÇO

O TEXTO CORRESPONDE A TRABALHO FEITO DURANTE A FREQUÊNCIA DO CURSO NO IUM SENDO DA RESPONSABILIDADE DO SEU AUTOR, NÃO CONSTITUINDO ASSIM DOUTRINA OFICIAL DAS FORÇAS ARMADAS PORTUGUESAS OU DA GUARDA NACIONAL REPUBLICANA.

COR GNR Gonçalo Nuno Silva Gonçalves de Carvalho

INSTITUTO UNIVERSITÁRIO MILITAR

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

CONTRIBUTOS PARA UM MODELO DE ATUAÇÃO DA GUARDA NACIONAL REPUBLICANA NO CIBERESPAÇO

COR GNR Gonçalo Nuno Silva Gonçalves de Carvalho

Trabalho de Investigação Individual

Pedrouços 2023

INSTITUTO UNIVERSITÁRIO MILITAR
DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

CONTRIBUTOS PARA UM MODELO DE ATUAÇÃO DA GUARDA NACIONAL REPUBLICANA NO CIBERESPAÇO

COR GNR Gonçalo Nuno Silva Gonçalves de Carvalho

Trabalho de Investigação Individual

Orientador: COR ADMIL GNR TIR Nuno Miguel Parreira da Silva

Pedrouços 2023

Declaração de compromisso Antiplágio

Eu, **Gonçalo Nuno Silva Gonçalves de Carvalho**, declaro por minha honra que o documento intitulado **Contributos para um Modelo de Atuação da Guarda Nacional Republicana no Ciberespaço**, corresponde ao resultado da investigação por mim desenvolvida, enquanto auditor do **Curso de Promoção a Oficial General 2022/2023** no Instituto Universitário Militar, e que é um trabalho original, em que todos os contributos estão corretamente identificados em citações e nas respetivas referências bibliográficas.

Tenho consciência que a utilização de elementos alheios não identificados constitui grave falta ética, moral, legal e disciplinar.

Pedrouços, 31 de julho de 2023

Assinado por : **GONÇALO NUNO SILVA GONÇALVES DE CARVALHO**
Num. de Identificação: 10363860
Data: 2023.07.31 20:07:28+01'00'

CARTÃO DE CIDADÃO

Gonçalo Nuno Silva Gonçalves de Carvalho
COR GNR

Agradecimentos

Um trabalho de investigação é um processo cognitivo intenso de reflexão, partilha e estudo que promove o debate e a geração de ideias novas, com o fim último de compreender os fenómenos sociais. Nesta senda, foram várias as pessoas que contribuiram significativamente para o sucesso deste trabalho de investigação individual, às quais gostaria de manifestar a minha profunda gratidão e apreço.

Um agradecimento muito especial ao meu orientador, Coronel Nuno Parreira da Silva, pela sua permanente disponibilidade, incentivo, amizade e valiosos contributos e ensinamentos de ordem prática e científica, que tornaram este árduo percurso menos penoso.

A todos os especialistas nacionais e internacionais, da Procuradoria-geral da República, do Centro Nacional de Cibersegurança, da SIRESP, S.A., da Polícia Judicária, da GNR, da *Guardia Civil* de Espanha e da *Gendarmerie Nationale* de França, que tive o privilégio de entrevistar e a quem agradeço penhoradamente o precioso tempo cedido e a partilha da experência e conhecimento que valorizaram grandemente esta investigação.

Agradeço igualmente ao Diretor de Curso de Promoção a Oficial General 2022/2023, ao Corpo Docente do IUM e a todos os Auditores do Curso, o apoio, camaradagem e a partilha do saber.

Por fim, agradeço profundamente à minha família, a quem dedico este trabalho, pelo incondicional apoio, paciência e compreensão pela ausência nesta fase, em especial ao meu pai, a quem o destino não permitiu testemunhar este momento significativo da minha carreira.

Índice

Índice de Apêndices

Índice de Figuras

Índice de Quadros

Resumo

O ciberespaço tornou-se numa das dimensões fundamentais da vida em sociedade, na qual as atividades quotidianas foram transferidas ou duplicadas, sendo igualmente um espaço propício a atividades ilícitas. A Guarda Nacional Republicana (GNR) assumiu o desafio de ampliar a sua capacidade de atuação no ciberespaço, graças a uma resposta integrada ao fenómeno da cibercriminalidade no mundo real e virtual, através da afirmação da capacidade de ciberpolícia.

O objeto de estudo desta investigação focou-se no modelo de atuação policial da GNR, no ciberespaço. Para tal, o método de investigação usado foi o raciocínio indutivo, apoiado numa estratégia de investigação qualitativa, num estudo de caso, na análise documental e nos dados recolhidos, em entrevistas realizadas a especialistas nacionais e internacionais, ligados à cibersegurança e cibercriminalidade.

Os resultados obtidos demonstraram que a definição de um modelo de atuação policial da GNR passa pela atribuição de competências legais no âmbito da investigação dos crimes ciberinstrumentais, da melhoria da cooperação institucional, da criação de uma estrutura de coordenação das áreas da cibersegurança e da cibercriminalidade, com reforço de meios nas unidades territoriais e a projeção da atividade policial, nas suas diversas dimensões, nos distintos domínios do ciberespaço.

Palavras-chave:

Ciberespaço; Cibersegurança; Cibercriminalidade; Modelo de Atuação Policial

Abstract

Cyberspace has become one of the fundamental dimensions of life in society, in which daily activities have been transferred or duplicated, being also a space propitious to illicit activities. The Republican National Guard (GNR) has taken on the challenge of expanding its ability to operate in cyberspace, thanks to an integrated response to the phenomenon of cybercrime in the real and virtual world, through the establishment of cyberpolice capabilities.

The object of study of this research focused on the GNR police performance model in cyberspace. To this purpose, the research method was based on inductive reasoning, based on a qualitative research strategy, a case study approach, documental analysis and data collected from interviews conducted with national and international experts related to cybersecurity and cybercrime.

The obtained results demonstrated the definition of GNR police performance model includes the assignment of legal competences in the scope of the investigation of instrumental cybercrimes, the reinforcement of institutional cooperation, the establishment of a coordination structure in the areas of cybersecurity and cybercrime, with the reinforcement of resources in the territorial units and the projection of police activity, in its various dimensions, in the distinct domains of cyberspace.

Keywords:

Cyberspace; Cybersecurity; Cybercrime; Police Performance Model

Lista de abreviaturas, siglas e acrónimos

C

CCD	Centro de Ciberdefesa
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
CG	Comando-geral
CIRC	*Computer Incident Response Capability*
CNCS	Centro Nacional de Cibersegurança
CO	Comando Operacional
COMCYBERGEND	Comando do Ciberespaço da *Gendarmerie*
CRP	Constituição da República Portuguesa
CSIRT	*Computer Security Emergency Response Team*

D

DCRP	Divisão de Comunicação e Relações Públicas
DCSI	Direção de Comunicações e Sistemas de Informação
DI	Direção de Informações
DIC	Direção de Investigação Criminal
DO	Departamento de Operações

E

ECUE	Estratégia de Cibersegurança da União Europeia
EC3	*European Cybercrime Center*
ENCD	Estratégia Nacional de Ciberdefesa
ENCT	Estratégia Nacional de Combate ao Terrorismo
ENSC	Estratégia Nacional de Segurança do Ciberespaço
ENISA	*European Network and Information Security Agency*
EUROPOL	*European Union´s Law Enforcement Agency*

EG2025	Estratégia da Guarda Nacional Republicana
F	
FIEP	Associação Internacional de *Gendarmeries* e de Forças de Polícia com Estatuto Militar
FS	Forças de Segurança
FSS	Forças e Serviços de Segurança
G	
GNR	Guarda Nacional Republicana
GRESI	Grupo de Reflexão Estratégica sobre a Segurança Interna
I	
IA	Inteligência Artificial
IDN	Instituto de Defesa Nacional
IUM	Instituto Universitário Militar
L	
LC	Lei do Cibercrime
LOGNR	Lei Orgânica da Guarda Nacional Republicana
LOIC	Lei da Organização e Investigação Criminal
LSI	Lei de Segurança Interna
M	
MAI	Ministério da Administração Interna
N	
NATO	*North Atlantic Treaty Organization*
O	
OE	Objetivo Específico
OG	Objetivo Geral
OPC	Órgão de Polícia Criminal
OSINT	*Open Source Intelligence*

P

PJ	Polícia Judiciária
PSP	Polícia de Segurança Pública

Q

QC	Questão Central
QD	Questão Derivada

R

RASI	Relatório Anual de Segurança Interna
RCM	Resolução do Conselho de Ministros

S

SEPNA	Serviço de Proteção da Natureza e do Ambiente
SIRP	Sistema de Informações da Republicana Portuguesa
SIS	Sistema de Informações e Segurança
SSI	Sistema de Segurança Interna

T

TI	Tecnologias de Informação
TII	Trabalho de Investigação Individual
TIC	Tecnologias de Informação e Comunicação

U

UCCiber	*Unidad de Coordinación de la Ciberseguridad*
UE	União Europeia

1. Introdução

Com o desenvolvimento tecnológico e a utilização generalizada da internet surgiu uma nova dimensão virtual, o ciberespaço, para onde a atividade humana está a ser duplicada ou transferida. O ciberespaço é "um ambiente complexo, de valores e interesses, constituído por uma área de responsabilidade coletiva, resultante da interação entre pessoas, redes e sistemas de informação" (RCM, 2019) e representa um (novo) domínio sem fronteiras e em constante construção e expansão, no qual se esbate, cada vez mais, a linha entre o mundo real e o virtual.

Este contexto gera um vasto leque de novas oportunidades para a sociedade digital mas, por outro lado, cria um ambiente propício para a prática de atividades ilícitas e proporciona aos criminosos um amplo leque de ferramentas que atenta contra a segurança das pessoas e das instituições.

De acordo com o Relatório de Segurança Interna 2022 (SSI, 2022) registou-se um crescimento da cibercriminalidade de 48,3% face a 2021 e de 68,2% em relação a 2019. A subida não se deve a uma causa única, sendo transversal dentro das categorias do crime ciberinstrumental, cibercrime em sentido lato e do ciberdependente, cibercrime em sentido estrito, especialmente os crimes de acesso indevido ou ilegítimo, interceção ilegítima (+60,1%) e de falsidade informática (+54,3%). O Centro Nacional de Cibersegurança (CNCS) prevê, igualmente, uma tendência de subida do número de incidentes de cibersegurança e de cibercrimes no ciberespaço de interesse nacional, com um especial incremento dos crimes que utilizam a esfera digital de modo instrumental, como a burla informática. Genericamente, destacam-se quatro focos de insegurança: cibercriminalidade; ciberespionagem; desinformação e *hacktivismo*, entre as ameaças ao ciberespaço de interesse nacional.

O atual Governo Constitucional aprovou a Estratégia Nacional de Segurança do Ciberespaço (ENSC) (Resolução do Conselho de Ministros n.º 92/2019, de 5 de junho) com o objetivo de "incrementar a segurança das redes e sistemas de informação, de modo a garantir a proteção e defesa do ciberespaço de interesse nacional e assim potenciar sua utilização livre, segura e eficiente por parte de todos os seus utilizadores".

Estabelece ainda a ENSC (RCM, 2019, p. 2889) que os desafios colocados pela prevenção e investigação destas novas tipologias de crimes e de ameaças, bem como a prática de crimes antigos, com recursos a novos métodos, implicam uma oportuna evolução da legislação e que os sistemas de resposta às ameaças, nomeadamente o policial e judiciário,

em esforço coordenado, se adaptem e desenvolvam um esforço de "apetrechamento, que os habilite a cumprirem cabalmente as suas missões", ou seja, "proteger os bens jurídicos legalmente consagrados e os direitos dos cidadãos."

Pela natureza e missão, cabe às Forças de Segurança (FS), em particular à GNR, estar atenta a estes novos desafios e exigências da sociedade, considerando o seu "dispositivo e implantação territorial" e por ser uma força "especialmente vocacionada para atuar em todo o espetro de prevenção e conflitualidade" (EG2025, 2020, p. 25).

Segundo Alves (2013, p. 192), a GNR no cumprimento das missões deve equacionar o processo social da sociedade em rede, fruto do desenvolvimento tecnológico, da compressão do espaço e do tempo que o mesmo impõe e das mudanças sociais que provoca, com vastas implicações sociológicas. Ciente desta necessidade premente, a GNR no seu processo de planeamento estratégico materializado na "Estratégia da Guarda 2025" (EG2025), definiu como objetivo estratégico: "ampliar a capacidade de atuação no ciberespaço" e para tal "garantir uma resposta integrada da Instituição ao fenómeno da cibercriminalidade no mundo real e virtual, através da ampliação das capacidades de ciberpolícia, no âmbito da prevenção e alerta, divulgação e consciencialização e investigação".

Assim, a GNR, pelo seu conjunto diversificado de competências específicas e capacidades operacionais, deve definir e consolidar um modelo de atuação policial no ciberespaço, baseado no enquadramento estratégico, atribuições legais, na organização e afirmação das suas capacidades de ciberpolícia, em cooperação com os parceiros nacionais e internacionais, de modo a prevenir e a reprimir os comportamentos ilícitos ocorridos no ciberespaço e a garantir a segurança do mesmo.

Atendendo ao previsto na ENSC e ao estabelecido na EG2025, a presente investigação assume especial relevância e pertinência no quadro das entidades responsáveis pela segurança do ciberespaço e para a GNR, em particular.

O objeto da investigação deste trabalho é a atuação policial da GNR no ciberespaço, em Portugal, na sua área de responsabilidade.

Após a ponderação do contexto e da base conceptual onde a investigação se enquadra, importa delimitá-la nos domínios do tempo, do espaço e do conteúdo (Santos & Lima, 2019, p. 42). Relativamente ao domínio temporal, pretende-se desenvolver a investigação centrada no período correspondente à atualidade, ou seja, os anos de 2022 e 2023.

No que concerne à dimensão espacial, a mesma está contida à estrutura de Comando da GNR, em especial, o Comando Operacional (CO) e as Unidades, em Portugal, visto que esta Força de Segurança, de natureza militar, encontra-se apta a cobrir todo o espetro da conflitualidade, constituindo-se como uma instituição na primeira linha da resposta nacional em matéria de Segurança e Defesa.

No domínio do conteúdo, o estudo abrangerá, concretamente, a atuação da GNR no âmbito do cumprimento das suas atribuições, nos diferentes domínios do ciberespaço, em Portugal, em cooperação com os parceiros institucionais nacionais e estrangeiros. No final desta investigação, pretende-se propor contributos para a definição de um modelo de atuação policial da GNR no ciberespaço, em Portugal, na sua área de responsabilidade.

Face ao objeto de estudo, a problemática da investigação aplicada e a pertinência institucional, definiu-se o seguinte Objetivo Geral (OG): propor contributos para a definição de um modelo de atuação policial da GNR no ciberespaço em Portugal, na sua área de responsabilidade.

De modo a conseguir cumprir com o objetivo geral da investigação, torna-se necessário atingir os seguintes objetivos específicos (OE): OE1: Analisar o quadro de intervenção da GNR no ciberespaço em Portugal; OE2: Analisar as estruturas organizacionais das forças de segurança congéneres, a *Guardia Civil* espanhola e a *Gendarmerie Nationale* francesa que garantem a segurança do ciberespaço.

Este estudo é relevante para a GNR por responder à Questão Central (QC): Que contributos podem ser adotados na definição de um modelo de atuação policial da GNR no ciberespaço em Portugal, na sua área de responsabilidade? Com o propósito de responder a esta questão, foram definidas duas questões derivadas (QD), as quais estão diretamente relacionadas a cada um dos OE, designadamente: QD1: Qual o quadro de intervenção da GNR no ciberespaço em Portugal? QD2: Quais foram as estruturas organizacionais adotadas pelas forças de segurança congéneres, a *Guardia Civil* espanhola e a *Gendarmerie Nationale* francesa, de modo a garantirem a segurança do ciberespaço?

O presente trabalho escrito está estruturado em sete capítulos. Após a introdução, o segundo capítulo apresenta o enquadramento teórico e conceptual. O terceiro, explana a metodologia. Os capítulos quatro e cinco são autónomos, embora interligados, nos quais são apresentados os dados, discutidos os resultados e dadas respostas a cada uma das QD. No capítulo seis, são apresentados os contributos para um modelo de atuação policial da GNR no ciberespaço, como resposta à QC. Por fim, nas conclusões, está uma síntese do trabalho,

o resumo dos resultados obtidos, os contributos para o conhecimento e as limitações e recomendações para futuros estudos nesta área do conhecimento.

2. Enquadramento teórico e conceptual

Neste capítulo, pretende-se explanar um conjunto alargado de obras de referência, estudos nacionais e internacionais sobre os conceitos estruturantes considerados mais relevantes para o tema em estudo e identificados no modelo de análise, apresentado no Capítulo 3.4, de modo a ajudar a definir o contexto, o significado e a importância do problema (Freixo, 2011).

A presente investigação está contextualizada, fundamentalmente, na área dos Estudos de Segurança Interna e dos Fenómenos Criminais, especificamente, nas outras áreas da Prevenção e Investigação Criminal, Fenómenos Criminais, Modelos de Atuação e das "Técnicas e Tecnologias Militares", subáreas de "Ciberdefesa/Cibersegurança".

2.1 Quadro conceptual e conceitos estruturantes

Para melhor entendimento da relevância da dimensão do ciberespaço, apresentar-se-á um breve enquadramento dos conceitos nucleares desta investigação.

2.1.1 Ciberespaço, cibersegurança e ciberameaças

Ao longo dos últimos trinta anos, a *internet* teve um desenvolvimento exponencial, assumindo-se como motor do desenvolvimento tecnológico, ligando definitivamente toda a sociedade em rede, através de novos processos de interação (Nunes, 2015, pp. 200-201), dando origem à globalização da informação, do conhecimento e do saber (Gouveia & Santos, 2015, p. 62).

Ao estabelecer a ligação à *internet*, acedemos a uma rede de cobertura mundial, na qual a comunicação passa a ser dirigida pelo tempo de interação, num espaço virtual que designamos por ciberespaço (Nunes, 2016, pp. 200-201).

O conceito de ciberespaço foi criado e popularizado por William Gibson (1984, p. 12) no romance intitulado *"Neuromancer*", como representação de um universo virtual eletrónico e no qual a sociedade dependeria dos computadores e das Tecnologias de Informação e Comunicação (TIC). O ciberespaço é descrito na ENSC como um "ambiente complexo, de valores e interesses, materializado numa área de responsabilidade coletiva, que resulta da interação entre pessoas, redes e sistemas de informação". Contudo, considerando a multiplicidade de abordagens ao mesmo conceito, com o intuito da melhor compreensão do mesmo, elaborou-se um quadro resumo que constitui o Apêndice A.

De acordo com Santos (2015, p. 61), o ciberespaço do ponto de vista funcional disponibiliza um conjunto de aplicações ou dimensões, das quais destaca a rede global de comunicações eletrónicas (*internet*), o *media* global e o espaço de interação social (redes

sociais, os jogos *online* e a democracia eletrónica) e a biblioteca digital (*World Wide Web* e a *Cloud*). Refere, ainda, que apresenta algumas caraterísticas distintivas dos outros quatro domínios naturais (terra, mar, ar e espaço), como o anonimato e a "aterritorialidade". Contudo, independentemente da abordagem ao conceito, todas as definições modernas de ciberespaço reconhecem o seu carácter omnipresente e mais abrangente reconhecendo implicitamente as suas profundas ligações ao mundo físico e de suporte da sociedade (Nunes & Natário, 2014, p. 5).

Com a necessidade de manter o funcionamento de sistemas informáticos que constituem o ciberespaço e afetam todos os domínios da atividade humana, surge o conceito de cibersegurança, definido pela ENSC como:

> […] conjunto de medidas e ações de prevenção, monitorização, deteção, reação, análise e correção que visam manter o estado de segurança desejado e garantir a confidencialidade, integridade, disponibilidade e não repúdio da informação, das redes e sistemas de informação no ciberespaço, e das pessoas que nele interagem. (RCM, 2019, p. 2889).

A cibersegurança também se refere à segurança dos indivíduos, relativamente à informação digital, dos dados pessoais, à privacidade e às liberdades e diretos individuais, no âmbito do ciberespaço. Considerando que a maioria das componentes do ciberespaço são da responsabilidade dos privados, a sua proteção não é exclusivamente da responsabilidade dos Estados (Santos, 2018, p. 26).

De acordo com Carvalho (2022, p. 76), a cibersegurança engloba os recursos técnicos, processuais e humanos que visam garantir primariamente a segurança da informação, visto ser a primeira barreira do ciberespaço. Segundo Marques (2020) pode afirmar-se que a cibersegurança possui quatro dimensões: defesa; segurança interna; económica e cidadania, conforme esquematizado na Figura 1:

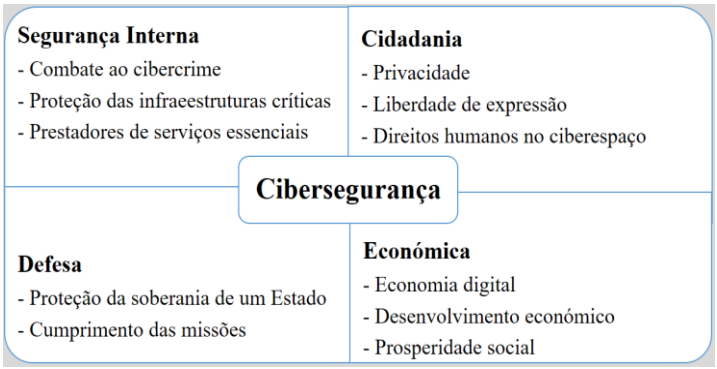

Figura 1 - Dimensões da cibersegurança
Fonte: Adaptado a partir de Carvalho (2022, p. 77).

A presente investigação irá centra-se, essencialmente, na dimensão da segurança interna.

Quanto às ciberameaças no ciberespaço podem ser agrupadas nas seguintes categorias: *hacktivismo*; cibercrime; cibercrime organizado; ciberespionagem; ciberterrorismo e ciberguerra (IDN-CESEDEN, 2013). As ciberameaças podem ter origem em indivíduos com diferentes motivações e nível de formação ou Estados, com objetivos distintos, nomeadamente, com vista à obtenção de fama ou vingança, benefícios económicos, vantagens táticas competitivas, dividendos e motivações políticas (Carvalho, 2022, p. 50), conforme se apresenta na Figura 2.

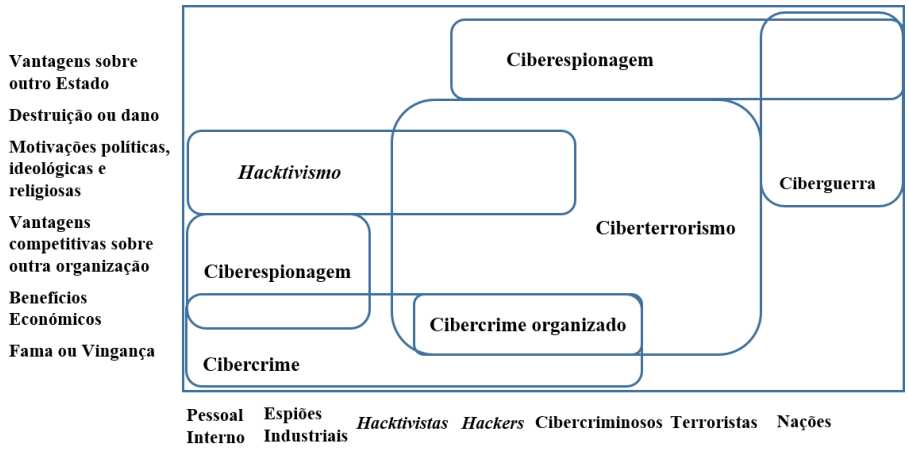

Figura 2 - Espetro de ameaças no ciberespaço

Fonte: Adaptado de Carvalho (2022, p. 50).

A principal diferença entre o domínio da cibersegurança e o domínio do combate ao cibercrime é que a primeira tem como objetivo a prevenção, enquanto no combate ao cibercrime, o foco assenta na reação a um ilícito, através da investigação criminal que procura identificar a autoria dos ciberataques e a condenação dos seus autores pelo sistema judicial. O combate ao cibercrime também contribui para a prevenção criminal, através da recolha de informações criminais. (Carvalho, 2022, pp. 80-81)

Por conseguinte, no domínio da prossecução criminal, segundo Santos (2015, pp. 63-65), "os ciberataques representam atos criminalmente relevantes, passíveis de ação penal, por serem direcionados contra as pessoas, ou contra interesses patrimoniais ou contra dados e informação. Este tipo de criminalidade é caraterizado pela transnacionalidade, atemporalidade, deslocalização e anonimato, o que torna o seu conhecimento e medição mais complexos. (Guedes, Moreira & Cardoso, 2021, p. 4).

Resumindo, os ciberataques são dirigidos, tendencialmente, contra pessoas, contra interesses patrimoniais ou contra a informação e dados (Santos, 2018, p. 27).

Relativamente ao conceito de cibercrime, a ENSC (RCM, 2019, p. 2889) define como os factos correspondentes a crimes previstos na Lei do Cibercrime (LC) (Lei n.º 109/2009, de 15 de setembro, alterada pela Lei n.º 79/2021, de 24 de novembro, da Assembleia da República) e ainda a outros ilícitos penais praticados com recurso a meios tecnológicos, nos quais estes meios sejam essenciais à prática do crime em causa.

Relativamente ao ordenamento jurídico português, para Venâncio (2022, pp. 21-25) podem distinguir-se duas grandes tipologias distintas, para enquadrar a cibercriminalidade, designadamente, a criminalidade informática em sentido amplo e em sentido estrito. Na criminalidade em sentido amplo inclui-se toda a atividade criminosa que pode ser realizada por meios informáticos, quer quando a informática é apenas o instrumento para a prática de atos acessórios ou preparatórios, quer quando integram os elementos de um determinado tipo legal de crime. A criminalidade informática em sentido estrito é aquela em que o elemento digital surge como parte integradora do tipo legal ou mesmo seu objeto de proteção.

A EUROPOL, a par dos países da União Europeia (UE), distingue as seguintes tipologias de cibercrime: "ciberdependentes", os designados crimes informáticos estritos e os "ciberinstrumentais", os crimes que utilizam os meios informáticos como instrumentos para a sua execução, contudo, poderiam utilizar outros meios (Bravo, 2022, pp. 64-68).

Os conceitos anteriormente explanados estão intrinsecamente ligados ao *hacktivismo*, ciberterrorismo e ciberespionagem. Assim, entende-se por *hacktivismo* a utilização de técnicas e *software* específico, com o objetivo de explorar as TIC de forma incomum ou ilícita, de modo a potenciar a capacidade de intervenção, influência e visibilidade em prol de uma causa, por norma usada contra os Estados e grandes organizações (Santos, et al., 2011). Quanto ao ciberterrorismo, resulta da convergência entre terrorismo e o ciberespaço consistindo na condução de ataques ou tentativas de ataques contra computadores, redes de comunicação e informação armazenada, com o objetivo de provocar medo ou persuadir um governo ou os cidadãos, a fim de concretizar objetivos de ordem política ou sociais (Carvalho, 2022). A ciberespionagem é entendida como o(s) ato(s) de obtenção de informações classificadas ou sensíveis de indivíduos ou governos, para ganho de vantagens políticas, económicas ou militares, com recurso à utilização de métodos de exploração ilegais na *internet* e nos sistemas de informação (ENISA, 2013, p. 1).

Relativamente o conceito de ciberguerra, Fernandes (2014, p. 153) define 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". Segundo Nunes (2020, p. 21), o ciberespaço transcende a "sua componente infraestrutural (física) e estende o seu impacto para o domínio virtual que, pela sua natureza, ultrapassa os limites geográficos do tradicional teatro de operações militares". Na figura 3, é descrita, graficamente, a extensão das áreas de responsabilidade do ciberespaço.

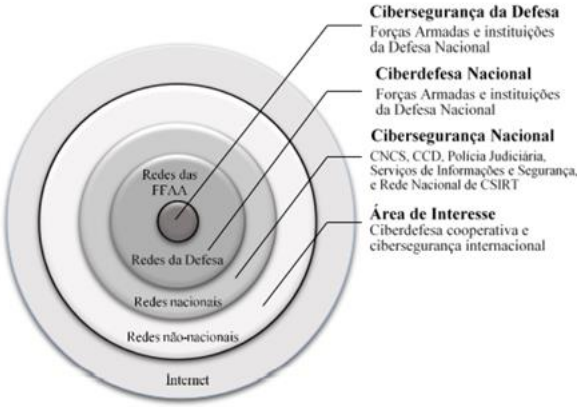

Figura 3 - Áreas de responsabilidade no ciberespaço

Fonte: Nunes (2020, p. 21).

Na Europa e em Portugal existem entidades responsáveis pela cibersegurança na área de interesse do ciberespaço europeu e nacional, conforme descrito no Apêndice B.

No seguimento da explanação dos conceitos de ciberespaço, cibersegurança e as diferentes tipologias de ciberameaças, torna-se pertinente entender a atuação policial no ciberespaço.

2.1.2 Atuação policial no ciberespaço

De acordo com Fernandes (2014, p. 92), tanto as forças armadas, como as forças e os serviços de segurança (FSS) estão a adaptar-se às ameaças e aos desafios do ciberespaço.

Ao longo dos tempos, foram definidos modelos de policiamento por força da necessidade das FS prevenirem a criminalidade, reforçarem a sua relação de confiança e proximidade com as comunidades e gerirem as expetativas da sociedade relativamente ao seu desempenho (Elias, 2018; Oliveira, 2006). Estes modelos, baseados em quadros teóricos e determinadas filosofias, foram testados e implementados do mais tradicional aos considerados mais atuais e modernos, os designados modelos preventivos (Moleirinho, 2018, p. 101). Sobre a existência de vários modelos, Fernandes (2014) elenca, designadamente o Policiamento Tradicional, Policiamento Comunitário, Policiamento Orientado para os Problemas e o Policiamento Orientado pelas Informações, conforme apresentado na Figura 4.

Figura 4 - Modelos de policiamento

Fonte: Moleirinho (2018, p. 102).

O exponencial uso das TIC por parte dos cidadãos e o consequente aumento e sofisticação da criminalidade no meio digital, exigiu melhores desempenhos nas diferentes áreas de atividade das FS, desde a prevenção e investigação criminal, às informações, à manutenção da ordem pública, à proteção e socorro e do ambiente (Moleirinho, 2018, p. 99).

À semelhança da sociedade em geral, as FS devem, igualmente, transpor a sua atividade para o ciberespaço, de forma a garantir a proximidade e o contacto permanente com o cidadão, de modo a proporcionar a todos o conhecimento, a consciência e a confiança necessários para a utilização livre e segura do ciberespaço, bem como prevenir os ilícitos criminais ocorridos neste domínio. Segundo Nunes (2012, p. 115) as FS devem ser "responsáveis por coordenar a resposta do Estado às atividades relacionadas com o cibercrime e o *hacktivismo*".

No âmbito do ciberespaço, os modelos de policiamento, baseados no uso dos instrumentos tecnológicos, são utilizados num racional de proatividade e preditividade, privilegiando igualmente os critérios de eficiência e de eficácia na gestão de recursos (Moleirinho, 2018, p. 99).

De acordo com a EUROPOL (2021, pp. 4-8), atualmente, a polícia é forçada a garantir a segurança das suas comunidades, no mundo real e no ciberespaço, numa convulsão tecnológica, onde o policiamento tradicional tem uma aplicabilidade cada vez menor, impondo-se soluções inovadoras e adaptáveis às novas exigências, mantendo ao mesmo tempo os princípios fundamentais de servir e proteger o cidadão.

A INTERPOL (2022, pp. 8-10) considera que a atividade policial necessita de novas abordagens, procedimentos e estruturas organizacionais, com vista a responder à crescente sofisticação, complexidade e transnacionalização do crime no ciberespaço. Assim, será importante proceder à transição de modelos reativos de policiamento para modelos pró-ativos, colaborativos, apoiados na inovação e nas novas tecnologias de informação, como a Inteligência Artificial (IA), e ajustados à mudança de expetativas sociais. Outro grande desafio, num futuro próximo, será expandir o âmbito do policiamento para ambientes virtuais, como o metaverso[1].

O policiamento dos ambientes digitais, como as redes sociais virtuais, começa a afirmar-se como uma estratégia/técnica de intervenção policial que tem permitido às FS projetar a sua atividade de forma transversal no ciberespaço. Esta vantagem advém das redes sociais permitirem a monitorização das interações sociais e da exposição e visibilidade públicas da atividade realizada na vida real (Trottier 2012; Andrejevic, 2009). Permite, deste modo, reforçar a comunicação e as políticas de segurança de proximidade entre as FS e a sociedade (Guedes, 2009). Atendendo às suas caraterísticas, as redes sociais, as aplicações e a *internet*, em geral, demonstram ser valiosas ferramentas de trabalho disponíveis para as FS, no cumprimento da sua missão, nos seus domínios de atuação, nomeadamente: na prevenção criminal; na investigação criminal; na ordem pública; nas informações, na proximidade e na comunicação com o cidadão.

Resumindo, segundo Moleirinho (2018, p. 101), os modelos de policiamento "pretendem representar as relações e as configurações que determinados Estados adotam relativamente a sua organização policial" e "aos estilos do exercício da função policial, os modelos de atuação policial". O conceito de modelo de atuação policial não se encontra definido e sustentado na literatura de referência nacional. Deste modo, considerando os conceitos apresentados, considerou-se como melhor definição de "modelo de atuação policial": a forma como uma força de segurança prossegue a sua missão, com base no enquadramento estratégico e legal, a organização e como gere a atividade policial, em cooperação com os parceiros nacionais e internacionais.

[1] De acordo com Ball (2022, p. 49), o metaverso é "uma rede interoperável e em grande escala de mundos virtuais 3D renderizados em tempo real que podem ser experimentados de forma síncrona e persistente por um número efetivamente ilimitado de utilizadores com um sentido individual de presença e com continuidade de dados, como a identidade, o histórico, as prerrogativas, os objetos, as comunicações e os pagamentos".

3. Metodologia

A presente pesquisa teve como referência os procedimentos recomendados relativamente às normas de autor do IUM (Fachada et al., 2020), bem como as Orientações Metodológicas para a Elaboração de Trabalhos de Investigação (Santos & Lima, 2019), para além da consulta de outras fontes primárias de referência, quando se justificou.

3.1. Estratégia de investigação e desenho de pesquisa

O método de investigação é baseado no raciocínio indutivo e optou-se por uma estratégia de investigação de natureza qualitativa, devidamente fundamentada na revisão de literatura nacional e internacional, assim como na interpretação dos normativos legais e institucionais que enquadram este estudo. Optou-se por uma abordagem do tipo qualitativo, dado que a análise incide em processos organizacionais, nos seus diferentes níveis e por existirem um número reduzido de unidades de amostragem. Pretendeu-se, deste modo, explorar as diversas dimensões, obter o máximo de conhecimento do fenómeno em estudo e explorar, sem o intuito de generalizar ou alcançar a representatividade estatística (Vilelas, 2009, pp. 105-109).

Relativamente ao desenho ou plano de pesquisa, optou-se pelo estudo de caso, dado que se "procura recolher informação detalhada sobre uma única unidade de estudo" e "descrever de forma rigorosa a unidade de observação" (Santos & Lima, 2019, p. 36), fundamentada teoricamente e com o rigor metodológico exigível (Bryman, 2012, p. 71), ou seja, a atuação da GNR nos diferentes domínios do ciberespaço, em Portugal, no âmbito do cumprimento das suas atribuições, em cooperação com os seus parceiros institucionais nacionais e estrangeiros. Nas subalíneas seguintes, pretende-se fundamentar as escolhas das diversas técnicas que constituem o método.

3.2. Técnicas de recolha, análise de dados e modelo de análise

Para Bisquera (1989), citado por (Coutinho, 2014. p. 24), os métodos de investigação "constituem o caminho para chegar ao conhecimento científico" e os procedimentos servem de "instrumentos para alcançar os fins de investigação", sendo as técnicas usadas, os "procedimentos de atuação" do método. Nas subalíneas seguintes é descrito o processo de seleção dos participantes na investigação, os instrumentos de recolha e as técnicas de análise dos dados, bem como, o modelo de análise com a descrição dos respetivos conceitos e dimensões.

3.2.1. Técnicas de recolha de dados

No que concerne aos instrumentos de recolha de dados, aplicaram-se as diversas técnicas adequadas a esta tipologia de investigação exploratória, de natureza qualitativa, através da análise documental das obras científicas, dos normativos legais e institucionais, de relatórios técnicos, assim como, as entrevistas. Considerou-se que a técnica de recolha e tratamento de dados mais apropriada para compreender o fenómeno em profundidade é a entrevista, elegeu-se o tipo semiestruturada para os três painéis de especialistas, de modo a conduzir a entrevista com a flexibilidade necessária (Quivy e Campenhoudt, 1992, pp. 193-194). Neste contexto, foram elaborados dois guiões de entrevista diferenciados, conforme Apêndice E.

Para Gonçalves, Gonçalves e Marques (2021, pp. 32-33) a seleção dos participantes numa investigação qualitativa, por norma, "não decorre de um processo de escolha aleatória de sujeitos que compõem uma determinada população". Deste modo, segundo Coutinho (2014, p. 245), "a amostra tem de ser apropriada, composta pelos participantes que melhor representam ou melhor conhecem o tópico sobre o qual incide a pesquisa". Com este intuito, elegeram-se como participantes desta investigação, os sujeitos que se enquadram nas seguintes categorias: os peritos reconhecidos no seio da GNR com competências relevantes na prevenção e segurança do ciberespaço; peritos com funções de relevo em instituições civis, cuja missão seja relacionada com a segurança do ciberespaço e peritos das forças congéneres, de Espanha e de França (*cfr.* Apêndice F).

Decorrente do processo de escolha dos participantes na investigação, obteve-se uma amostra qualitativa intencional, caraterizada pela homogeneidade fundamental das componentes, ou seja, todos os escolhidos pela caraterística de serem especialistas no âmbito do objeto de estudo (Gonçalves et al., 2021, p. 33). No que concerne ao processo de amostragem, dado o grau de detalhe, o mesmo encontra-se explanado no Apêndice D.

No que concerne aos instrumentos de recolha de dados, na fase exploratória recorreu-se à análise documental das obras académicas especializadas nesta área, dos normativos legislativos e institucionais, aos relatórios técnicos de instituições nacionais e estrangeiras e a entrevistas semiestruturadas de aprofundamento. A análise documental incidiu sobre os normativos legais e relatórios técnicos de interesse para a investigação. Esta análise permitiu uma sólida descrição e sistematização do objeto de estudo, decorrente da identificação, da seleção e da análise das fontes de informação (Gonçalves et al, 2021, p. 105).

3.2.2. Técnicas de análise de dados e modelo de análise

Na presente investigação utilizou-se técnicas próprias da investigação qualitativa, como é o caso da análise documental e de conteúdo, visto serem as mais adequadas para a análise do material textual obtido das entrevistas (Coutinho, 2014, pp. 216-228). Relativamente à análise de conteúdo aplicou-se um conjunto de técnicas que permitem analisar de forma sistemática um corpo de material textual, obtido através da realização das entrevistas aos comandantes/diretores/chefes com responsabilidades na área da segurança do ciberespaço e aos especialistas nacionais e internacionais descritos no Apêndice F. Deste modo, a análise de conteúdo ou dados foi efetuada através da categorização, a seleção com recurso à codificação e a redução dos dados que permitiu a consequente análise.

Por fim, apresenta-se o modelo de análise, conforme sistematizado na Figura 1.

Figura 5 – Modelo de Análise

Objeto: A atuação policial da GNR no ciberespaço, em Portugal, na sua área de responsabilidade.					
Objetivo Geral	Propor contributos para a definição de um modelo de atuação policial da GNR no ciberespaço em Portugal, na sua área de responsabilidade.				
Questão Central	Que contributos podem ser adotados na definição de um modelo de atuação policial da GNR no ciberespaço em Portugal, na sua área de responsabilidade?				
Objetivos Específicos (OE)	**Questões Derivadas (QD)**	**Conceitos**	**Dimensões** (Código das entrevistas)	**Recolha de dados**	
				Instrumentos	**Técnicas de Análise**
OE1: Analisar o quadro de intervenção da GNR no ciberespaço em Portugal.	QD1: Qual o quadro de intervenção da GNR no ciberespaço em Portugal?	Ciberespaço Cibersegurança Ciberameaças	Enquadramento estratégico e legal da atuação policial no ciberespaço (A.01; A.02) Atuação policial da GNR no ciberespaço (B.01; B.02; B.03)	Entrevistas semiestruturadas (internamente e peritos externos)	Análise documental e análise de conteúdo (entrevistas)
OE2: Analisar as estruturas organizacionais das forças de segurança congéneres, a *Guardia Civil* e a *Gendarmerie Nationale*, que garantem a segurança do ciberespaço.	QD2: Quais foram as estruturas organizacionais adotadas pelas forças de segurança congéneres, a *Guardia Civil* espanhola e a *Gendarmerie Nationale* francesa, de modo a garantirem a segurança do ciberespaço?	Policiamento do Ciberespaço	Atuação policial da *Guardia Civil* e da *Gendarmerie Nationale* no ciberespaço (C.01; C.02; C.03; C.04)		

4. A atuação policial da GNR no ciberespaço

A polícia tem por função "defender a legalidade democrática e garantir a segurança interna e os direitos dos cidadãos", conforme previsto no n.º 1 do art.º 272.º da Constituição da República Portuguesa (CRP).

A atividade de segurança interna é um meio para realizar os fins do Estado de direito democrático, no respeito pelos cidadãos, face às ameaças e riscos diversos e "assenta em cinco pilares essenciais: prevenção da criminalidade, ordem pública, investigação criminal, informações e cooperação internacional (Fernandes, 2014; Elias, 2018).

Assim, estas são igualmente as quatro grandes áreas de enquadramento da atuação das FS, no mundo físico, pelo que deverão ser consideradas estruturantes na definição de um modelo de atuação da GNR no ciberespaço.

A GNR é uma das primeiras forças de segurança de natureza militar do mundo, designada de forças *gendármicas*, dado que a sua génese remonta ao ano 1801, com a criação da Guarda Real de Polícia. É uma instituição universal e polivalente, com um contexto e estrutura organizacional única em Portugal (Silva, 2015) que tem conseguido garantir em permanência, a proximidade aos cidadãos e a segurança das comunidades, na sua área de responsabilidade (Silva, 2022).

A missão geral da GNR visa "assegurar a legalidade democrática, garantir a segurança interna e os direitos dos cidadãos", no âmbito dos sistemas nacionais de segurança e proteção, "bem como colaborar na execução da política de defesa nacional, nos termos da Constituição e da Lei", conforme o n.º 2 do artigo 1.º da Lei Orgânica da GNR (LOGNR) (Lei n.º 63/2007, de 6 de novembro, retificada pela declaração de retificação n.º 1-A/2008).

O cumprimento da missão da GNR carateriza-se por uma sincronização perfeita entre a atividade operacional e as funções logísticas, visto que a manobra está dependente do princípio da unidade de comando. O posicionamento a GNR, a nível nacional, permite-lhe abarcar, em permanência, todo o espectro de prevenção e conflitualidade, em quaisquer das modalidades de intervenção das Forças Nacionais e nas mais diversas situações, desde o

tempo de paz ao tempo de guerra, a nível interno e externo (GNR, 2020, pp. 26-33), conforme esquematizado na Figura 6.

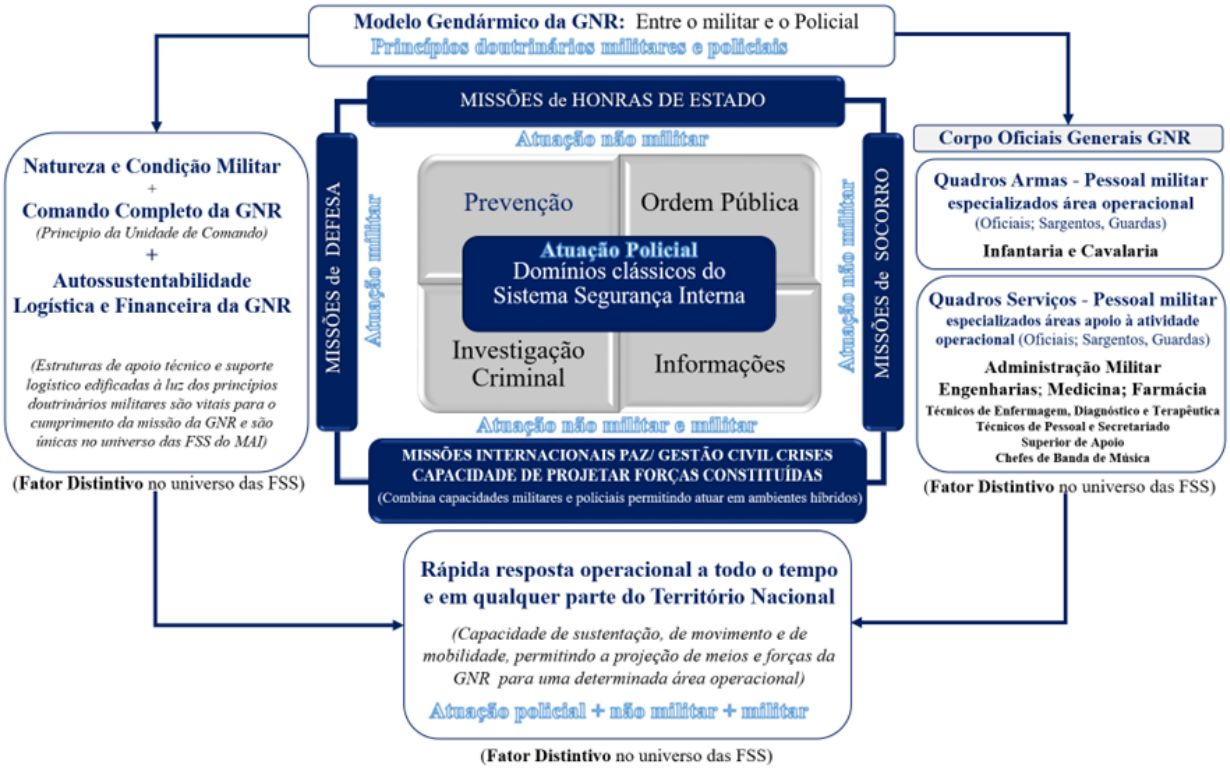

Figura 6 - O modelo gendármico da GNR e o espectro de missões

Fonte: Silva (2022).

De seguida importa analisar qual o quadro de intervenção da GNR no ciberespaço.

4.1. Quadro de intervenção da GNR no ciberespaço

A GNR no âmbito da investigação criminal e na qualidade de Órgão de Polícia Criminal (OPC), tem competência genérica para desenvolver um conjunto de ações que visam "prevenir a criminalidade em geral e efetuar diligências necessárias tendentes a investigar a existência de um crime e proceder à recolha de prova, determinar os seus agentes, a sua responsabilidade e efetuar as consequentes detenções" (Branco, 2010).

De referir ainda que a Lei da Organização da Investigação Criminal (LOIC) (Lei n.º 49/2008, de 27 de agosto), atribui, nos termos da alínea l), do n.º 3, do art.º 7, à PJ competência reservada da investigação dos crimes informáticos e praticados com recurso a tecnologia informática, sem prejuízo da possibilidade dessa competência ser delegada por autoridade judiciária noutro OPC, como a GNR ou a PSP.

Analisando as atribuições da GNR, previstas no artigo 3.º da LOGNR, identificou-se quais podem ser prosseguidas no âmbito da segurança do ciberespaço, descritas no Apêndice G, e quais os órgãos da estrutura orgânica da GNR que prosseguem a sua atividade neste

domínio, nomeadamente através das direções do CO e da Divisão de Comunicação e Relações Públicas (DCRP), conforme descrito no Apêndice H.

Da análise realizada, infere-se que as atribuições realizadas nos diferentes âmbitos de atuação, no mundo físico, estão a ser projetadas no mundo digital. Entre as mesmas, destacam-se igualmente as atribuições com referência expressa ao ciberespaço, cibercriminalidade e cibersegurança, introduzidas na sequência das alterações orgânicas materializadas pelo Despacho n.º 1292/2020 – Unidades orgânicas flexíveis, do Comandante-geral da GNR. Deste modo, a Direção de Comunicações e Sistemas de Informação (DCSI) assegura a direção, coordenação, controlo, gestão e execução das atividades da Guarda em matéria de cibersegurança. Neste âmbito, cabe a esta direção implementar a capacidade de cibersegurança, ainda em fase embrionária.

Destacam-se, igualmente, as atribuições da Direção de Informações de "realizar estudos normativos e pareceres técnicos no âmbito da cibersegurança e conduzir atividades de ciberinteligência, especialmente no domínio *open source intelligence* (OSINT), monitorizando, recolhendo e processando notícias existentes no ciberespaço". Esta atividade tem como finalidade a produção de relatórios de informações policiais e criminais. Os processos de pesquisa e de processamento da informação são orientados pelas áreas de interesse, visando o produto para apoiar a tomada de decisão, aos diferentes níveis (NEP/GNR – 2.01). Uma dessas áreas de interesse é a ciberinteligência que compreende a atividade de informações no ciberespaço, dividida pelos seguintes tópicos: consciência situacional (monitorização de eventos que permita a análise preditiva para orientar a atividade operacional), falsas notícias, criminalidade e delinquência no ciberespaço e *hacktivismo*. Esta atividade é realizada pelo Centro de Informações, responsável pela produção de informações a nível operacional e quando se justifica em apoio às operações correntes a nível tático.

Por último, as atribuições da Direção de Investigação Criminal (DIC) responsável pela realização de perícias criminalistas, nas quais se incluem a prova digital e o tratamento de informação criminal, recolhida no ciberespaço (Despacho n.º 1292/2020 – Unidades orgânicas flexíveis, do Comandante-geral da GNR).

É neste contexto, que importa analisar como a GNR pretende ampliar a capacidade de atuação no ciberespaço, garantindo uma resposta integrada da Instituição ao fenómeno da cibercriminalidade no mundo real e virtual, através do alargamento das capacidades de

ciberpolícia, no âmbito da prevenção e alerta, divulgação e consciencialização e investigação (GNR, 2020, p. 48).

Para melhor entendimento da forma como a GNR atua no ciberespaço, analisaram-se as perceções dos comandantes/diretores/chefes do CO e da DCRP e dos especialistas nacionais na área da cibersegurança e cibercriminalidade.

4.2. Perceções dos peritos sobre o quadro de intervenção da GNR no ciberespaço

Face ao descrito sobre a ENSC, procurou-se indagar junto dos comandantes/diretores/chefes da GNR e dos especialistas nacionais, com responsabilidades nesta área, se as linhas de ação previstas nos seis eixos de intervenção da referida estratégia são adequadas, face aos contributos que as FS podem oferecer neste esforço.

A ENSC (2019) "articula-se em enquadramento, objetivos e as linhas de ação do Estado em matéria de segurança do ciberespaço, de acordo com o interesse nacional". Analisadas as referidas linhas de ação constata-se que as FS são mencionadas no Eixo 1 - Estrutura de segurança do ciberespaço: "Reforçar a capacidade de cibersegurança nacional tendo em vista maximizar a resiliência das Forças e Serviços de Segurança" e no Eixo 4 - Resposta às ameaças e combate ao cibercrime: "Adequar, para efeitos de gestão de crises, as capacidades das Forças Armadas, das Forças e Serviços de Segurança (…) tendo em vista impulsionar uma abordagem integrada às ameaças e riscos em matéria de segurança do ciberespaço". Para melhor entendimento do enquadramento estratégico do ciberespaço, elaborou-se o Apêndice C.

Da análise realizada (Apêndice I), concluiu-se que a maioria dos entrevistados (9/13; 69%) considera que as atribuições das FS expressas na ENSC são insuficientes (*cfr*. Quadro 8 – Apd I).

Contudo, na linha de ação da prevenção, educação e sensibilização os entrevistados garantem que são suficientes (7/13; 54%), apresentando justificações para a mesma resposta (*cfr*. Quadro 8 – Apd I). A este respeito J. Nunes (entrevista por *email*, 4 de abril 2023) assegura que "internamente a GNR está a levar a cabo programas de sensibilização e produção de normativos, bem como conteúdos, recorrendo a portal interno e futuramente via plataforma NAU[2]". E externamente, a Instituição celebrou "[…] parcerias com a *Microsoft* e o projeto *Internet* Segura, difundidos através dos programas de proximidade, nomeadamente o Escola Segura". Ainda sobre esta linha de ação, R. Bravo (entrevista por

[2] "Ensino e Formação *Online* para Grandes Audiências" da Fundação para a Computação Científica Nacional.

videoconferência, 30 de março de 2023) releva que "a prevenção ganhava se fosse feita a cinco, a GNR, PSP, PJ, CNCS e o SIRP. Para tal, deve-se rever o plano de ação para coordenar as ações conjuntas, de modo a definir a mensagem e a quem difundi-la". Relativamente à linha de ação da proteção do ciberespaço, J. Nunes (*op. cit.*) refere que foi elaborado pelo CNCS o Projeto de Guia para Gestão de Riscos, "[…] contudo ainda não existe um modelo aprovado de gestão do risco pelas diversas estruturas nacionais a proteger, visto que ainda se encontram "[…] a construir uma mecânica de gestão das possíveis ameaças cibernéticas, carecendo de mais formação, boas práticas, *standards* e treino com auditoria de resultados para que se possa integrar a aprendizagem".

Recorda-se que o CNCS (2022, p. 4) tem registado uma tendência de crescimento do volume de incidentes e de cibercrimes, especialmente quanto aos crimes que utilizam a esfera digital de modo instrumental, como a burla informática cada vez mais frequente, ao contrário do crime estritamente informático, do âmbito da LC (Lei n.º 109/2009).

Do ponto de vista do enquadramento legal, procurou-se, igualmente, saber se as competências da GNR/PSP na investigação do cibercrime estão consentâneas com a tipologia e a incidência deste fenómeno criminal em Portugal.

Quanto à legislação no âmbito da cibercriminalidade em sentido estrito a maioria dos entrevistados (9/13; 69%) considera que a legislação está ajustada à tipologia de criminalidade praticada (*cfr.* Quadro 8 – Apd I). Ou seja, a criminalidade respeitante apenas àqueles crimes cujo tipo legal inclui, necessariamente, a prática do ato punível através de meios informáticos ou contra um bem informático (Venâncio, 2022, p. 167). Na classificação da UE/EUROPOL esta tipologia de criminalidade inclui os crimes ciberdependentes que se referem aos crimes previstos na LC (Lei n.º 109/2009), estendendo-se ao Código Penal e a outras fontes legais avulsas.

Quanto à legislação no âmbito da cibercriminalidade em sentido lato, a totalidade dos entrevistados (13/13; 100%) considera que a legislação deverá ser revista (*cfr.* Quadro 8 – Apd I). Segundo Venâncio (2022, p. 167), esta categoria "[…] abarca todos os atos ilícitos criminais praticados através das TIC, independentemente do seu tipo legal o prever". Refere ainda que esta é a face mais visível da criminalidade informática, em que "as TIC surgem apenas como um meio para a prática de um crime passível de ocorrer em meios que não digitais, embora o ciberespaço seja potencialmente muito mais danoso".

Segundo P. Verdelho (entrevista presencial, 22 de março de 2023), o quadro legal deve ser analisado em diferentes perspetivas. No que concerne à "[…] legislação penal substantiva

não necessita de ser revista, visto a tipologia de crimes previstos estar em linha com os documentos internacionais". Relativamente à legislação processual, "[…] existe espaço para evoluir […]", de modo a colmatar algumas lacunas relativas às ferramentas a atribuir à investigação criminal. Segundo R. Bravo (*op. cit.*) os estados membros da UE decidiram dividir os crimes em: "[…] crime comum, crime ciberdependente e crime ciberinstrumental […]". Acrescenta ainda que "[…] no crime ciberinstrumental a GNR e a PSP devem ter a relevância na LOIC e competências expressas relativamente ao crime ciberinstrumental".

A revisão da LOIC é defendida pela maioria dos inquiridos (8/13; 62%) que a consideram desajustada à realidade atual da cibercriminalidade (*cfr.* Quadro 8 – Apd I). P. Verdelho (*op. cit.*) entende que "[…] existe espaço para evoluir nas áreas da legislação processual penal e da cooperação policial e a LOIC deve ser revista, com vista a incrementar a eficácia e a especialização da investigação". Justifica que "hoje em dia, vivemos uma realidade diferente e, por isso, existe espaço para distribuir aos OPC genéricos os cibercrimes que, pela sua natureza, já são da sua competência, mas que utilizam meios mais complexos".

Face ao desafio imposto pela ENSC e pelos índices de cibercriminalidade, procurou-se indagar se a atual estrutura orgânica da GNR é adequada e se os meios humanos e materiais são suficientes no cumprimento da missão no ciberespaço.

Os inquiridos, com conhecimento da estrutura organizacional da GNR, defendem claramente que deverá ser criada uma estrutura de coordenação na dependência direta do CO (8/10; 80%) e que os meios humanos e tecnológicos devem ser reforçados (10/10; 100%), de modo a cumprir o cabal cumprimento da sua missão no ciberespaço (*cfr.* Quadro 9 – Apd I). A identificação desta necessidade está alinhada com a vontade expressa na EG2025 (2020, p. 44) da GNR "guiar-se pela premissa da constante abertura à mudança, ciente de que tanto ao nível da genética organizacional, como no campo estrutural e operacional, a ideia de transformação deve ser uma constante".

A este respeito, P. Oliveira (entrevista por *email*, 10 de março de 2023) defende igualmente esta necessidade visto que "as atividades relacionadas com a segurança no ciberespaço são distintas e complementares, existindo diferentes estruturas da Guarda (DO, DI, DIC e DCSI) a tratar as matérias relacionadas com esta área de intervenção". Afirma que "de modo a evitar sobreposição ou duplicação de esforços, seria pertinente desenvolver uma estrutura de coordenação de cibersegurança da Guarda, sob a direta dependência do Comandante Operacional (Direção de Cibersegurança)". Como vantagens defende que "[…] desta forma, potenciar-se-ia, não só a otimização dos recursos, a centralização e integração

das ações/funções desempenhadas, como também, a consolidação desta área de intervenção na Guarda, colocando a Instituição na vanguarda do desenvolvimento de modelos de policiamento modernos".

Relativamente à possibilidade da criação de uma estrutura de coordenação, D. Dores (entrevista por *email*, 16 de março de 2023) considera que a mesma "[…] não poderá existir sem haver um reforço das unidades territoriais com meios de combate ao cibercrime, com capacidade para desenvolver as ações necessárias para a investigação e combate ao cibercrime, mais associado à criminalidade comum". Esta opinião é também corroborada pela maioria dos entrevistados (6/10; 60%) (*cfr*. Quadro 9 – Apd I).

Para J. Nunes (*op. cit.*), em complemento, "deverá explorar-se os recursos que a tecnologia oferece para auxiliar no policiamento do ciberespaço, como por exemplo, "os sistemas de aprendizagem automática assistida por máquinas (*machine learning*) e mecanismos de apoio à predição na área de Inteligência Artificial" e "[…] as aplicações móveis, sobretudo aquelas que veiculam um serviço para os cidadãos". Da mesma forma, D. Dores (*op. cit.*) defende igualmente que a IA é uma mais-valia para o combate ao cibercrime "[…] dado o volume de dados informáticos dos quais se pode retirar informação (prova digital) e a complexidade para a sua análise".

Conforme referido anteriormente, o ciberespaço, do ponto de vista funcional, disponibiliza um conjunto de aplicações ou dimensões, das quais destaca a *internet*, as redes sociais e a biblioteca digital (Santos, 2015, p. 61). Face às dimensões referidas, os entrevistados consideram que as FS devem projetar a sua atividade operacional no ciberespaço, nos âmbitos da proximidade, prevenção criminal, investigação criminal, informações e ordem pública, nas seguintes dimensões do ciberespaço:

Quadro 1 - Projeção da atividade policial por dimensões do ciberespaço

Dimensões da atividade policial	Dimensões do ciberespaço
Proximidade	Redes sociais (10/10; 100%)
Prevenção criminal	*Internet* (8/10; 80%) Redes sociais (10/10; 100%) Jogos *online* e biblioteca digital (7/10: 70%)
Investigação criminal	*Internet* (8/10; 80%) Redes sociais (9/10; 90%) Biblioteca digital (8/10; 80%)
Informações	*Internet* (8/10; 80%) Redes sociais (8/10; 80%) Biblioteca digital (10/10; 100%)
Ordem pública	Redes sociais (9/10; 90%)

Face aos resultados obtidos, conclui-se que a atividade policial deverá ser projetada em todas as dimensões, em especial nas redes sociais, bem como na *internet*, biblioteca digital e jogos *online* (*cfr*. Quadro 9 – Apd I).

Em complemento do referido, para P. Oliveira (*op. cit.*) é importante "[…] garantir a proximidade e a resposta ao cidadão, procurando a segurança e proteção da população na era digital, na medida em que é importante as funções policiais manterem-se operacionais no ciberespaço".

Destaca-se de igual modo, a referência, por parte de vários entrevistados, à necessidade da presença das FS no ambiente imersivo do metaverso.

Segundo R. Veloso (entrevista por *email*, 1 de abril de 2023) pelas "características do ambiente virtual criado pelo metaverso permite que as FS cheguem e interajam com demais utilizadores, potenciando a sensibilização e a prevenção criminal no domínio virtual à semelhança do que já acontece na vida real".

Questionados sobre as relações de cooperação entre a GNR e as outras instituições no âmbito da cibersegurança e da cibercriminalidade, a maioria dos inquiridos (7/10; 70%) refere que as mesmas são insuficientes ou mesmo inexistentes (*cfr*. Quadro 9 – Apd I). Sobre a cooperação, R. Raposo (entrevista por e-mail, 10 de abril de 2023) considera que "a cibersegurança não pode ser um espaço de competição, mas sim um espaço de cooperação entre a sociedade civil e as autoridades. Nenhuma entidade consegue, por si só, ser eficaz a agir de forma isolada".

De acordo com C. Costa (entrevista por email, 10 de abril de 2023), a criação do *Cyber Working Group* no âmbito do G4 (forças de cariz *gendármico* da França, Itália, Espanha e Portugal), no seio da Associação FIEP[3] é uma excelente oportunidade para incrementar a cooperação nos âmbitos da formação, proximidade digital e metaverso, mapeamento de capital humano no ambiente digital e cooperação operacional.

Após a análise das perceções dos entrevistados sobre o quadro de intervenção da GNR no ciberespaço, apresenta-se a síntese conclusiva das principais ideias e a resposta à QD1.

4.3. Síntese conclusiva e resposta à QD1

Em síntese e procurando responder à QD1: Qual o quadro de intervenção da GNR no ciberespaço? – Verificou-se que a ENSC, genericamente, não preconiza nas suas linhas de ação as atribuições que as FS prosseguem no âmbito da sua atuação em prol da segurança do ciberespaço. Embora, a GNR tenha vindo a realizar ações no âmbito da prevenção,

[3] Associação Internacional de *Gendarmeries* e de Forças de Polícia com Estatuto Militar.

educação e sensibilização dos grupos mais vulneráveis e nos âmbitos da proteção do ciberespaço e da resposta às ameaças e ao combate ao cibercrime, no seguimento da atividade policial que desenvolve diariamente.

Quanto à legislação no âmbito da criminalidade, conclui-se que a mesma poderá diferenciar os crimes ciberdependentes e os ciberinstrumentais, em alinhamento com os restantes países europeus e a EUROPOL. Tal classificação também facilitaria a atribuição de competências de investigação às FS, para além das cometidas à PJ. Concomitantemente, torna-se necessária a revisão da LOIC, nomeadamente a alínea l), do n.º 3, do art.º 7 da LOIC (Lei n.º 49/2008), que poderá prever a atribuição de competências de investigação do crime ciberinstrumental por parte das FS, ou seja, a face mais visível da criminalidade informática, representada pelos crimes tradicionais que agora são praticados com recurso ao meio digital (Venâncio, 2022, p. 167).

No respeitante à organização e aos meios que a GNR possui para cumprir a sua missão no ciberespaço, concluiu-se que a atual estrutura não está adequada às exigências da missão e que existe necessidade de criar um órgão na dependência do Comandante do Comando Operacional (CO) que coordene a atividade da GNR no ciberespaço, acompanhado do respetivo reforço das unidades territoriais com meios humanos especializados e meios técnicos apropriados. Esta alteração permitiria à GNR otimizar os recursos, centralizar e integrar o policiamento do ciberespaço. De realçar a importância de explorar os recursos que a tecnologia avançada oferece como a IA ou sistemas de *machine learning*, entre outros, como forma de potenciar o policiamento e maximizar o tratamento do elevado número de metadados existente no ciberespaço. Relativamente à projeção da atividade da GNR no ciberespaço, destaca-se a premência da Instituição prosseguir de forma planeada, coordenada e integrada a sua atividade no âmbito das dimensões da proximidade, prevenção criminal, informações, investigação criminal e ordem pública, nos diferentes domínios do ciberespaço, nomeadamente, as redes sociais, *internet*, jogos *online* e biblioteca digital, assim como, no metaverso que promete revolucionar o mundo digital.

No que concerne à cooperação com os parceiros nacionais e internacionais, concluiu-se que a mesma não é satisfatória, limitando o desenvolvimento do conhecimento nesta área. Destaca-se a referência à cooperação com as forças congéneres da GNR no âmbito do *Cyber Working Group* do G4 da Associação FIEP, como uma oportunidade para troca de experiências e partilha de boas práticas.

Com o intuito de compreender realidades distintas, considerou-se pertinente a análise das estruturas organizacionais que garantem a segurança do ciberespaço da *Guardia Civil*, de Espanha e *Gendarmerie Nationale*, de França, por serem forças congéneres, de natureza *gendármica*.

5. Estrutura organizacional das forças congéneres no âmbito da segurança do ciberespaço

O modelo de organização policial existente no sul da Europa é o chamado modelo napoleónico ou dualista, criado no séc. XIX pelo Império Napoleónico. Este modelo assenta na existência de duas polícias: uma de natureza militar, na dependência do Ministro da Defesa ou com uma dupla tutela, igualmente, com dependência do Ministro da Administração Interna (MAI) e outra polícia de natureza civil, depende do Ministro da Administração Interna. Quanto às competências legais das duas polícias, genericamente, as mesmas coincidem e são exercidas na sua área territorial respetiva. Este modelo é seguido em Portugal, Espanha, França e Itália (Gomes, 2001).

Neste capítulo, a análise restringe-se à estrutura organizacional adotada pelas forças congéneres da GNR, nomeadamente a *Guardia Civil* de Espanha e a *Gendarmerie Nationale* de França, responsável pela segurança no ciberespaço. Esta escolha assenta no facto destas FS integrarem, à semelhança da GNR, o modelo de organização napoleónico, ou *gendármico*, caraterizado por ser centralizado e dualista (Silva, 2015, p. 192) e essencialmente partilharem a mesma origem, natureza, organização e atribuições.

Por definição orgânica, a *Guardia Civil* é um Corpo de Segurança Pública de natureza militar e de âmbito nacional e integra as Forças e Corpos de Segurança do Estado espanhol (Guardia Civil, s.d.), enquanto a *Gendarmerie Nationale* é uma força armada responsável pelo policiamento, nomeadamente nas zonas rurais e suburbanas e na rede viária. Está sob a tutela do Ministério do Interior, mas é colocada sob a autoridade do Ministério das Forças Armadas para a execução das suas missões militares (*Gendarmerie*, s.d.).

Ambas as forças possuem competência de investigação de todas a tipologias de cibercrime, partilhando essa responsabilidade com as FS de natureza civil, aplicando-se o princípio da competência territorial.

5.1. Estrutura organizacional da *Guardia Civil* espanhola no âmbito da segurança do ciberespaço

Relativamente à perceção sobre os órgãos responsáveis pela segurança do ciberespaço da *Guardia Civil* não existe informação disponível em fontes primárias, pelo que se optou por entrevistar o responsável máximo da Unidade de Coordenação de Cibersegurança (UCCiber), criada ao abrigo do diploma legal *Orden* PCI/685/2019, de 18 de *junio*, aprovado pelo Governo de Espanha.

Em termos de enquadramento das missões que a *Guardia Civil* tem atribuídas no âmbito do ciberespaço, J. Solom (entrevista por *email*, 11 de abril de 2023) referiu que esta FS "possui unidades especializadas em cibercrime, ciberterrorismo, *hacktivismo* e cibersegurança". Estas missões estão distribuídas conforme Figura 7.

Figura 7 - Unidades especializadas da *Guardia Civil* no combate ao cibercrime

Fonte: Guardia Civil (2023).

Quanto aos pressupostos da reorganização da *Guardia Civil* para potenciar a sua atividade no ciberespaço, J. Solom (*op. cit.*), a mesma "[…] conta com várias unidades especializadas em diferentes áreas do ciberespaço que atuam para combater as ameaças *online*". Da análise da Figura 7, conclui-se que as estruturas responsáveis pelo combate ao cibercrime encontram-se distribuídas pela Direção, Órgãos Centrais e Unidades. Ao nível dos órgãos centrais, as responsabilidades operacionais estão distribuídas conforme a tipologia de cibercriminalidade ou a cibersegurança. O combate à cibercriminalidade é da responsabilidade da Chefia de Polícia Judicial, composta pelas unidades responsáveis pela investigação operativa, análise criminal e informática forense. O ciberterrorismo e o *hacktivismo* é responsabilidade da Chefia de Informação que realiza investigação operativa, análise criminal e informática forense. A cibersegurança da instituição é garantida pela Chefia de Serviços Técnicos, através da segurança da informação e o cumprimento normativo. Ao nível das unidades territoriais foram criadas as EDITE, equipas especializadas forenses e as *Equipos@* que garantem a proximidade com o cidadão. Segundo J. Solom (*op. cit.*) as *Equipos@* foram criadas "[…] face ao aumento do cibercrime durante a pandemia COVID-19" e as mesmas "[…] foram distribuídas por todo o território nacional,

integradas nas companhias territoriais e na dependência das Unidades Orgânicas da Polícia Judiciária de cada comando territorial, de modo a prestarem um apoio mais próximo ao cidadão". Estas equipas têm a seguintes tarefas: disseminação da cultura de cibersegurança aos cidadãos; receção e supervisão de queixas; investigação de cibercrimes menos complexos e assessoria interna.

Face ao número de estruturas responsáveis pelo combate à cibercriminalidade na *Guardia Civil*, em 2019, foi criada a UCCiber de modo a evitar a duplicação de atuações e o consequente aumento de esforços e recursos. J. Solom (*op. cit.*) refere que "a UCCiber estabelece certos procedimentos de harmonização relativamente à gestão de recursos humanos, materiais e financeiros e constitui-se como ponto de referência em matérias relacionadas com a cibersegurança, embora permanecendo à margem da investigação".

Considerando que a implementação de novas estruturas de coordenação, por norma, encontra resistências internas e externas, procurou-se indagar quais foram os constrangimentos identificados. Segundo J. Solom (*op. cit.*), "[…] existiu a necessidade de serem estabelecidos novos procedimentos de comunicação e coordenação com os diferentes organismos do Estado no domínio do ciberespaço" e assim o "[…] estreitamento das relações favoreceu o fluxo de informação, otimizando recursos e expandindo sinergias para melhorar a resposta conjunta às ciberameaças". Ao nível interno, considera que muitas das funções assumidas por esta unidade já estavam a ser desempenhadas individualmente pelos outros órgãos, "o que permitiu a centralização de recursos ou de tomada de decisões, de modo a contribuir para uma resposta conjunta da instituição, que seria mais firme e mais sólida face a um objetivo comum a todos: os cibercriminosos".

Com o intuito de compreender o processo de funcionamento de outra força congénere da GNR, decidiu-se, igualmente, analisar o Comando do Ciberespaço da *Gendarmerie Nationale* (COMCYBERGEND) de França.

5.2. Estrutura organizacional da *Gendarmerie Nationale* francesa no âmbito da segurança do ciberespaço.

Em 2021, foi criado[4] o COMCYBERGEND com o objetivo de incorporar um serviço dedicado ao combate contra o cibercrime da *Gendarmerie Nationale*. Com a sua criação, na dependência direta do Diretor-geral da *Gendarmerie Nationale*, pretendeu-se estabelecer uma coordenação eminentemente transversal das unidades dedicadas à cibercriminalidade,

[4] Despacho INTJ2124773A, de 25 de fevereiro de 2021, alterado pelo Despacho INTJ2106083A, de 25 de agosto de 2021, do Comandante da *Gendarmerie Nationale* de França.

com vista a obter a melhor operacionalidade, bem como uma identidade própria, a fim de facilitar parcerias, interações e uma verdadeira sinergia com os vários atores do meio digital (Boget, 2021, p. 124).

Segundo M. Boget (entrevista por *email*, 11 de abril de 2023) "o COMCYBERGEND concentra a sua ação no cibercrime, definido como todos os atos que violam tratados internacionais ou leis nacionais, utilizando redes ou sistemas de informação como meio de cometer uma infração ou um crime, ou visando-os".

A missão do COMCYBERGEND assenta em quatro dimensões: estratégica e de colaboração; prevenção e proximidade digital; investigações e apoio técnico nas operações digitais (Boget, 2021, p. 125). Para tal, foram criadas quatro divisões: estratégica, operações, proximidade digital e a técnica.

O COMCYBERGEND cobre todo o espectro do ciberespaço dentro das suas quatro divisões, articuladas conforme Figura 8.

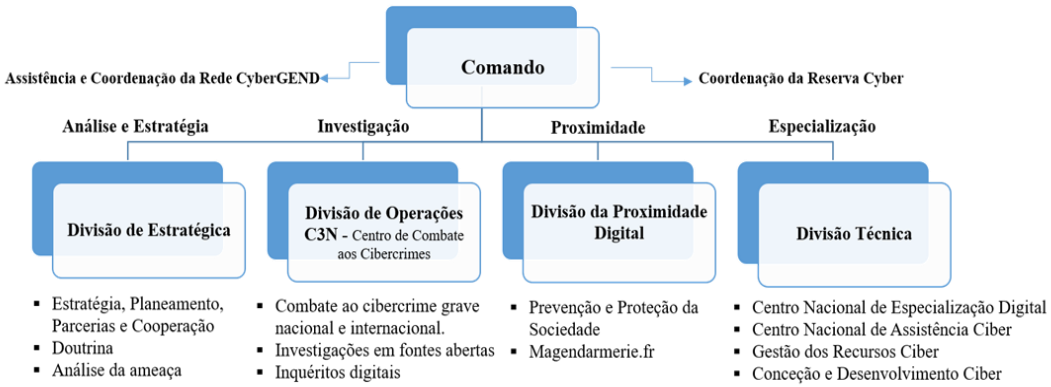

Figura 8 - Estrutura do COMCYBERGEND

Sobre a Divisão de Proximidade Digital, M. Boget (*op. cit.*) esclarece que a mesma "[…] intervém antes de mais numa base preventiva, a fim de acompanhar processo de digitalização da nossa sociedade e de alertar para os riscos a ela associados". Esta Divisão projeta a atividade no terreno através da Brigada Digital que gere o portal *magendarmerie.fr*. Este portal garante assistência aos cidadãos de forma permanente e interrupta. Segundo M. Boget (*op. cit.*), "[…] desde a sua criação, a Brigada já tratou de mais de 700.000 pedidos".

Relativamente à Divisão de Estratégia, M. Boget (*op. cit.*) referiu que a mesma "[…] acompanha os desenvolvimentos regulamentares e legislativos e desenvolve parcerias úteis a nível territorial, nacional e internacional com os sectores público e privado".

Quanto à Divisão de Operações é a unidade de polícia judiciária responsável pela luta contra a cibercriminalidade a nível nacional e internacional. De acordo com M. Boget (*op. cit.*) a sua ação centra-se principalmente na "[…] criminalidade grave: terrorismo, abuso

sexual de menores, vendas ilegais *online*, ataques aos sistemas automatizados de processamento de dados, fraude (plataforma PERCEV@L) ou a distribuição de conteúdos ilegais *online* e pelas infrações contra menores".

No que concerne à Divisão Técnica, M. Boget (*op. cit.*) esclarece que "[…] fornece apoio técnico à componente operacional através de laboratórios especializados para a extração e análise de provas, através do seu balcão único, apoio de peritos em processamento digital de provas e a conceção de ferramentas digitais para investigação". O COMCYBERGEND está presente em todos os níveis de atuação da instituição: local, departamental e nacional, conforme esquematizado na Figura 9.

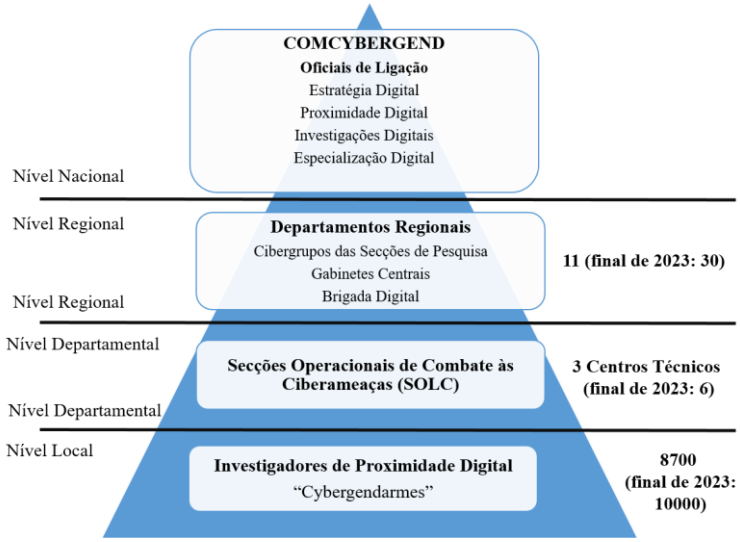

Figura 9 - Estrutura do COMCYBERGEND por níveis

Relativamente aos constrangimentos, destaca a dificuldade de recrutamento e a necessidade de meios tecnologicamente avançados em permanência.

Sobre a cooperação e a colaboração, M. Boget (*op. cit.*) afirma que "[…] baseiam-se no princípio do intercâmbio, quer seja de boas práticas, informação técnica ou operacional, formação ou partilha de ferramentas". No entanto alerta que "uma fraca cooperação por parte de um parceiro pode minar a relação de intercâmbio, visto que o principal objetivo de uma parceria é uma contribuição recíproca e equilibrada".

5.3. Síntese conclusiva e resposta à QD2

Em síntese e procurando responder à QD2 "Quais foram as estruturas organizacionais adotadas pelas forças de segurança congéneres, a *Guardia Civil* espanhola e a *Gendarmerie Nationale* francesa, de modo a garantirem a segurança do ciberespaço?" – verificou-se que estas FS optaram por estruturas e formas de organização distintas, embora com áreas de ação semelhantes. No caso da congénere espanhola, em 2019, foi criada a UCCiber com a missão de estabelecer procedimentos de harmonização, de forma a evitar a duplicação de atuações

no ciberespaço e o consequente desaproveitamento de recursos, embora sem competências operacionais. Quanto à congénere francesa, em 2021, criou o COMCYBERGEND, na dependência direta do seu diretor-nacional, com a missão de estabelecer uma coordenação eminentemente transversal, com uma identidade própria, de forma a potenciar as sinergias com todas estruturas internas e entidades externas. Releva-se a criação da Divisão de Estratégia, dedicada à análise, estratégia e produção de doutrina e a Divisão de Proximidade Digital, dedicada à prevenção e proteção dos utilizadores do ciberespaço. Relativamente à articulação da estrutura dedicada ao combate à cibercriminalidade, as duas FS dispõem de órgãos distribuídos pelos diferentes níveis hierárquicos, dedicados à proximidade com o cidadão, ao nível regional, através das *Equipos@*, da *Guardia Civil* e das Brigadas Digitais, da *Gendarmerie Nationale*. Destaca-se a projeção dos meios até ao nível local, no caso da congénere francesa, através dos chamados "cibergendarmes", que garantem o contacto permanente com o cidadão através da aplicação *magendarmerie.fr*. Relativamente aos constrangimentos verificados aquando da criação das estruturas referidas, a *Guardia Civil* identificou a necessidade de estabelecer novos canais de comunicação com as entidades externas e algumas resistências internas na fluidez da informação e na colaboração entre órgãos que prejudicou a eficácia das ações a desenvolver. Quanto à *Gendarmerie Nationale*, defende que a cooperação deve ser recíproca e equilibrada, de modo a não comprometer a estratégia internacional do COMCYBERGEND e o fio condutor das suas ações. Outro constrangimento prende-se com a necessidade permanente do incremento de recursos humanos qualificados e de meios materiais e financeiros face ao crescente número dos cibercrimes e da sua complexidade.

6. Contributos para um modelo de atuação policial da GNR no ciberespaço

Face aos argumentos anteriormente expostos, salienta-se que não se considerou relevante a divergência de opiniões entre os comandantes/diretores/chefes da GNR e os peritos entrevistados das áreas da cibersegurança e da cibercriminalidade e dos comandantes/chefes das forças congéneres, visto que foram entendidas como perceções diferentes, que podem ser explicadas pelo conhecimento e experiência diferenciados dos conceitos e/ou visões distintas sobre o papel a desempenhar pelas instituições no âmbito da presente investigação.

Importa relembrar que a ENSC é o instrumento estratégico nacional no âmbito da segurança do ciberespaço. Nas suas linhas de ação faz referências explicitas às FS, nomeadamente, a necessidade de "maximizar a resiliência das Forças e Serviços de Segurança", no âmbito da cibersegurança e de "adequar, para efeitos de gestão de crises, as capacidades (…) das Forças e Serviços de Segurança (…) tendo em vista impulsionar uma abordagem integrada às ameaças e riscos em matéria de segurança do ciberespaço" (RCM, 2019). Contudo, consultadas as atividades desenvolvidas no âmbito da ENSC, inscritas no Plano de Ação de 2019[5], constata-se que apenas uma está registada no âmbito do MAI e no Relatório de Avaliação de Execução de 2020, apenas constam três, correspondente a 1% de total das atividades realizadas pelo conjunto das entidades. Sobre o número de atividades do MAI inscritas e executadas no Plano de Ação da ENSC, L. Santos (entrevista por email, 30 de março de 2023) refere que "[…] após a aprovação da ENSC foram solicitados contributos a todos os ministérios e restantes entidades, incluindo o MAI, com o objetivo de serem inscritas as atividades a incluir no plano de ação". Depreende-se, portanto, que deverá existir maior proatividade por parte do MAI e das FS na definição e execução das atividades a realizar no âmbito da ENSC, em coordenação com o CNCS e restantes entidades públicas e privadas. De acordo com P. Verdelho (*op. cit.*) "a GNR e PSP deveriam ter mais referências expressas na ENSC porque aquilo que conhecíamos por cibercrime, já não é cibercrime" e por estas FS "[…] serem polícias de proximidade e terem conhecimento do terreno e da tipologia das queixas apresentadas, o que permite identificar mais rapidamente os fenómenos criminais que estão a ocorrer e contrariar os mesmos".

Relativamente à legislação que enquadra o combate à cibercriminalidade, identificou-se a necessidade de revisão da classificação dos cibercrimes em alinhamento com os restantes países da Europa, o que facilitaria a distribuição das competências de investigação

[5] *Cfr*. www.cncs.gov.pt/docs/ensc2019-2023-pa-2019-2020-2021-execucao2020-mai21.pdf.

atribuídas às FSS, especialmente, dos chamados crimes ciberinstrumentais. Sobre este assunto, L. Santos (*op. cit.*), defende que "[…] no contexto desta revisão, a competência da investigação dos crimes tradicionais, praticados através do uso do meio digital (cibercrime instrumental) deve ser igualmente da competência das FS". De modo a materializar este constrangimento, ficou evidente a necessidade de revisão da LOIC, de forma a potenciar a atuação da GNR no ciberespaço.

No que concerne à estrutura organizacional da GNR destinada a garantir a segurança no ciberespaço, identificou-se a necessidade de criação de um órgão na dependência do comandante do CO, visto que as atribuições neste domínio não abrangem toda a atividade prosseguida pela instituição e não são devidamente planeadas e coordenadas de forma centralizada. Da análise às estruturas das congéneres, considera-se relevante a diferença de tipologia de estruturas adotadas, nomeadamente uma estrutura de coordenação e um comando funcional, pela *Guardia Civil* e pela *Gendarmerie Nationale*, respetivamente. Igualmente de referir a existência de órgãos com a responsabilidade da análise estratégica, planeamento, cooperação, doutrina e avaliação das ameaças, bem como, as destinadas a garantir a proximidade com o cidadão, de forma a garantir a sensibilização e proteção como utilizadores do ciberespaço. Em ambas as forças, a atividade no ciberespaço é garantida por todos os níveis da estrutura hierárquica. Recorde-se que na GNR o DO, a DCSI, a DIC e a DI possuem atribuições no domínio do ciberespaço e não existe uma estrutura de coordenação da atividade destes órgãos neste âmbito.

Considerando que a atividade das FS é desenvolvida nas dimensões da proximidade, prevenção criminal, informações, investigação criminal, ordem pública, em cooperação com os seus parceiros, tal desiderato só será possível se for prosseguida nas diferentes dimensões do ciberespaço, nomeadamente, nos ambientes de interação social, aplicações, *internet* e potenciado os recursos que a tecnologia oferece. Dada a complexidade e a evolução constante da cibercriminalidade, impõe-se assim às instituições com responsabilidades no ciberespaço, uma estreita cooperação com seus parceiros nacionais e internacionais.

6.1. Síntese conclusiva e resposta à QC

Em síntese e procurando responder à QC "Que contributos podem ser adotados na definição de um modelo de atuação policial da GNR no ciberespaço em Portugal, na sua área de responsabilidade?" – em alinhamento com a definição adotada de modelo de atuação policial – "a forma como uma força de segurança prossegue a sua missão, com base no seu enquadramento estratégico e quadro legal de intervenção, a sua natureza e organização e

como gere a sua atividade policial, em cooperação com os parceiros nacionais e internacionais", apresenta-se a sistematização dos principais contributos identificados, designadamente:

a. No âmbito da ENSC, apresenta-se um conjunto de 16 medidas a realizar pela GNR, alinhadas com 22 linhas de ação, distribuídas pelos seis eixos de intervenção, com vista a reforçar a segurança do ciberespaço, conforme descrito no Apêndice J. Com vista a ser elaborado um plano de implementação, apresentam-se as medidas propostas, avaliadas e priorizadas por ordem de primazia, no Apêndice K, baseada na análise adaptada da matriz de qualidade de decisão de Kepner & Tregoe (1981, 2013);
b. Em sede de revisão da Estratégia da GNR, deverá ser considerado no processo de formulação estratégica a ampliação e consolidação a sua capacidade de atuação no ciberespaço, materializada numa estratégia parcelar que preconize a implementação das capacidades de cibersegurança e de combate à cibercriminalidade, nos diferentes âmbitos da sua atividade policial;
c. Relativamente ao enquadramento legal, a GNR deverá desenvolver as diligências necessárias, junto das autoridades competentes, com vista à elaboração de uma proposta de alteração da LOIC e consequente atribuição de competências de investigação dos crimes ciberinstrumentais;
d. No que concerne à estrutura organizacional, constituir um grupo de trabalho com vista à criação e implementação de um Centro de Coordenação de Cibersegurança e Cibercriminalidade (CentroCiber), na dependência do Comandante do CO, baseado na experiência das forças congéneres, com atribuições nas seguintes áreas:
    1) Ponto de contacto em matéria de segurança no ciberespaço;
    2) Planeamento e coordenação da atividade operacional da GNR no âmbito da cibersegurança e combate à cibercriminalidade;
    3) Elaboração e difusão de estudos, procedimentos e normas no âmbito da cibersegurança e da cibercriminalidade;
    4) Gestão de projetos de financiamento, inovação e desenvolvimento no âmbito da segurança do ciberespaço;
    5) Avaliação das necessidades de revisão e atualização da legislação no âmbito da cibersegurança e cibercriminalidade;
    6) Promoção da capacidade do conhecimento e análise das ameaças à segurança do ciberespaço;

7) Coordenação e cooperação com as diversas entidades nacionais e internacionais com responsabilidades na segurança do ciberespaço;
8) Planeamento das atividades de formação e especialização do efetivo e das ações de prevenção, educação e sensibilização a ministrar ao público-alvo;
9) Colaboração no planeamento da aquisição e gestão dos meios técnicos necessários à condução da atividade operacional no ciberespaço;
10) Apoio às unidades territoriais no âmbito da cibersegurança e da cibercriminalidade.

e. Ainda no âmbito da estrutura organizacional, equacionar a criação de um núcleo de "ciberguardas", na dependência das Secções de Informações e Investigação Criminal, das Unidades Territoriais;
f. Na área da capacitação e afetação dos recursos humanos, equacionar a criação da especialização de cibersegurança e cibercriminalidade;
g. No âmbito da gestão da atividade operacional, elaborar um plano de atuação no ciberespaço nas dimensões de: proximidade, prevenção criminal, informações, investigação criminal e ordem pública, nos diferentes domínios do ciberespaço;
h. Conceber um plano de cooperação e colaboração com as entidades públicas e privadas nacionais, organismos internacionais e forças congéneres, com relevância nas diferentes áreas da segurança do ciberespaço, com vista à criação de sinergias, partilha de informação e conhecimento e promoção de colaboração mútua.

7. Conclusões

O ciberespaço tornou-se uma das dimensões fundamentais da vida em sociedade, com ligações ao mundo físico e no qual as atividades quotidianas foram transferidas ou duplicadas. Para além das vantagens e oportunidades evidentes para a sociedade, este ambiente é igualmente propício à prática de atividades ilícitas, cometidas através de um meio informático e de tecnologia eletrónica digital que põe em causa a segurança da informação, dos equipamentos e sistemas de rede e dos direitos e liberdades dos cidadãos, assim como das organizações públicas e privadas.

As entidades nacionais têm registado, em Portugal, uma tendência de incremento do número de incidentes de cibersegurança e de cibercrimes no ciberespaço de interesse nacional, com um especial incremento dos crimes que utilizam a esfera digital de modo instrumental e de forma transversal nos crimes ciberdependentes. São igualmente destacados como focos de insegurança: a ciberespionagem, a desinformação e o *hacktivismo*. Face a estas ciberameaças, compete ao Estado a promoção das medidas de segurança necessárias à proteção do ciberespaço, no domínio da proteção simples, da prossecução criminal, da guerra e da diplomacia.

A ENSC é o instrumento estruturante, aprovado pelo Estado, para a capacitação nacional em matéria de segurança do ciberespaço, de acordo com o interesse nacional. A ENSC prevê que os desafios colocados pela prevenção e investigação destas novas tipologias de crimes e de ameaças, exigem uma oportuna evolução da legislação e que os sistemas de resposta às ameaças, nomeadamente, o policial e judiciário, devem adaptar-se e desenvolver capacidades que lhes permita proteger os bens jurídicos legalmente consagrados e os direitos dos cidadãos.

A GNR ciente da necessidade de adaptação a estas novas exigências impostas pela transformação da sociedade, definiu na EG2025 como objetivo estratégico - ampliar a capacidade de atuação no ciberespaço: garantir uma resposta integrada ao fenómeno da cibercriminalidade no mundo real e virtual, através da ampliação das capacidades de ciberpolícia. De modo a cumprir este desígnio, a GNR deverá definir e implementar um modelo de atuação policial no ciberespaço, baseado no seu enquadramento estratégico, atribuições legais, na sua organização e afirmação das suas capacidades de ciberpolícia, de modo a prevenir e a combater os comportamentos ilícitos ocorridos no ciberespaço, em cooperação com os seus parceiros nacionais e internacionais.

O método de investigação deste estudo, fundamentou-se essencialmente, no raciocínio indutivo e optou-se por uma estratégia de investigação numa abordagem de natureza qualitativa, apoiada na revisão de literatura nacional e internacional, bem como na interpretação dos normativos legais que enquadram esta pesquisa e nas perceções dos dirigentes do CO e DCRP da GNR e dos painéis de especialistas nacionais e internacionais. O desenho de pesquisa baseou-se num estudo de caso, visto que foram recolhidos dados sobre uma única unidade de estudo.

Relativamente ao OE1 - Analisar o quadro de intervenção da GNR no ciberespaço em Portugal, correspondente à QD1, concluiu-se que as atividades prosseguidas pela GNR no âmbito do ciberespaço são diminutas face à sua dimensão e capacidade de intervenção neste domínio. Como justificação, verificou-se um reduzido envolvimento nas ações realizadas ao abrigo da ENSC e a falta de previsão legal das atribuições e das competências de investigação das diferentes tipologias de cibercrime. Apesar do referido anteriormente, a GNR tem projetado a sua atividade policial, em todas as suas dimensões operacionais, justificando-se a criação de uma estrutura de coordenação das mesmas na dependência do comandante do CO e o reforço de meios humanos e tecnológicos, de modo a permitir a afirmação da sua capacidade de ciberpolícia e contribuir decisivamente para a segurança do ciberespaço de interesse nacional.

No que concerne ao OE2 - Analisar as estruturas organizacionais das forças de segurança congéneres, a *Guardia Civil* e a *Gendarmerie Nationale*, que garantem a segurança do ciberespaço, correspondente à QD2, concluiu-se que estas forças congéneres da GNR possuem estruturas próprias dedicadas a todo o espectro das ciberameaças, embora com configurações distintas. Enquanto a *Guardia Civil* espanhola adotou uma Unidade de Coordenação de Cibersegurança, de forma a coordenar a atividade das outras Chefias e harmonizar os procedimentos internos relativos à cibercriminalidade e cibersegurança, a *Gendarmerie Nationale* francesa criou o Comando do Ciberespaço na dependência direta do diretor-geral, com vista a uma coordenação eminentemente transversal das unidades dedicadas à cibercriminalidade e cibersegurança e desta forma incrementar a sua capacidade operacional nesta área e facilitar parcerias, interações e uma verdadeira sinergia com os vários atores do meio digital. Ambas as forças projetam as suas valências, neste âmbito, em toda a estrutura organizacional, com especial enfoque na proximidade com o cidadão e a investigação do cibercrime ao nível das unidades territoriais.

Por fim, quanto ao OG - Propor contributos para a definição de um modelo de atuação policial da GNR no ciberespaço em Portugal, na sua área de responsabilidade, diretamente relacionado com a QC, concluiu-se que a GNR para ampliar a sua capacidade de atuação nos distintos domínios do ciberespaço e a sua afirmação no domínio da capacidade de ciberpolícia, torna-se necessário um ajuste do enquadramento estratégico e legal das suas atribuições e competências de investigação do cibercrime e proceder a uma mudança da genética organizacional, de forma a projetar e gerir a sua atividade policial, nas diferentes dimensões da sua atuação, baseado num modelo de atuação policial dedicado ao ciberespaço.

Como contributos para o conhecimento, no seguimento dos estudos científicos realizados na área da cibersegurança e da cibercriminalidade, respeitantes ao papel das FS na segurança do ciberespaço, na presente investigação foi igualmente possível apurar o seguinte: a formulação e execução estratégica da segurança do ciberespaço não contempla as potencialidades das FS neste domínio e as mesmas não tem realizado atividades ao abrigo do Plano de Ação da ENSC; a necessidade de revisão do quadro legal vigente no âmbito do combate ao cibercrime, visto não atribuir as devidas competências legais de investigação do cibercrime às FS, face ao crescimento exponencial e a abrangência dos fenómenos criminais registados; a exigência e urgência da criação de uma estrutura orgânica de coordenação, no seio da GNR, que planeie e coordene toda a atividade policial nos diferentes domínios do ciberespaço e permita a cooperação com os seus parceiros nacionais e internacionais relevantes na segurança do ciberespaço; e a necessidade de definir o conceito de modelo de atuação policial no ciberespaço.

Quanto às limitações da investigação, destaca-se o facto de não ter sido possível entrevistar um maior número de académicos no domínio da cibersegurança e do direito do cibercrime e não ter sido possível estudar outras forças congéneres da GNR.

Considerando os resultados obtidos nesta investigação propõe-se que em estudos futuros sejam incluídas outras forças de segurança congéneres da GNR, bem como, seja estudada a edificação da capacidade de cibersegurança e de ciberpolícia na GNR.

Conclui-se esta investigação lembrando que a GNR, pela sua natureza e polivalência, é uma força especialmente apta a cobrir, em permanência, todo o espetro da conflitualidade, e tem demonstrado, ao longo dos tempos saber adaptar-se e fazer face à complexidade de novos ambientes e exigências da sociedade, guiando-se pela premissa da constante da mudança e transformação, tanto ao nível da genética organizacional, como na sua capacidade operacional. Deste modo, a definição de um modelo de atuação policial no ciberespaço será

determinante para a afirmação da GNR, como entidade nacional relevante na segurança do ciberespaço.

Referências bibliográficas

Alves, A. C. (2013). *Emergência de uma Sociologia da Polícia*. Lisboa: Revista da GNR.

Andrade, J., Lobo, V., Morgado, J., Santos, L. & Silva, N. (2017). *O reconhecimento formal da área científica das ciências miliares: um imperativo e uma inevitabilidade?* Revista Militar, n. º 2583, 2-20.

Andrejevic, M. (2009). *Privacy, Exploitation, and the Digital Enclosure*. Amsterdam Law Forum. 1(4), 47–62.

Assembleia da República (2005). *Constituição da República Portuguesa. Sétima Revisão*. Lisboa: Assembleia da República – Divisão de Edições.

Ball, M. (2022). *Metaverso*. Alma do Livros.

Barrinha, A. & Carrapiço, H. Cibersegurança. (2016). Em: Duque, R., Noivo, D., & Silva, T. A. *Segurança Contemporânea* (pp. 245-262). Lisboa: Pactor.

Beaufre, A. (1965). *Introduction a la Stratégie*. Paris: Librarie Armand Colin.

Boget, M. (2021). Le Comcybergend tout seul ne sera rien. *Revue de la Gendarmerie Nationale*. Dezembro 20121 – N.º 270 (pp. 124-128).

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

Bravo, R. (2023, 13 de fevereiro). Da Segurança da Informação à CiberDefesa: contributos para um alinhamento de conceitos [Página *online*]. Retirado de https://www.academia.edu/40494857/Segurança_da_informação_e_cibersegurança_aspetos_práticos_e_legislação

Bryman, A. (2012). *Social Research Methods (*4.ª Ed.) Oxford: Oxford University Press.

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

Carvalho, A. R. (2022). *As Informações na Segurança do Ciberespaço. Uma Abordagem Holística à Segurança neste Domínio.* Lisboa: *Lisbon International Press.*

Centro Nacional de Cibersegurança (2021). *Relatório Cibersegurança em Portugal. Políticas Públicas*. Lisboa: Nozzle, Lda.

Centro Nacional de Cibersegurança (2022). *Relatório Cibersegurança em Portugal. Riscos & Conflitos*. 3.ª Edição. Lisboa: Autor.

Comissão Europeia (2020, 16 de dezembro). Nova estratégia de cibersegurança da UE e novas regras para aumentar a resiliência das entidades críticas físicas e digitais.

Perguntas e respostas [Página *online*]. Retirado de https://ec.europa.eu/commission/presscorner/detail/pt/qanda_20_2392

Coutinho, C. P. (2016). *Metodologia de Investigação em Ciências Sociais e Humanas: Teoria e Prática*. Coimbra: Almedina.

Couto, A. C. (2020). *Elementos de Estratégia – apontamentos para um curso*. Alfragide: Leya.

Decreto-Lei n.º 249/2015, de 28 de outubro (2015). *Aprova a orgânica do ensino superior militar, consagrando as suas especificidades no contexto do ensino superior, e aprova o Estatuto do Instituto Universitário Militar*. Diário da República, I Série, 211. Lisboa: Conselho de Ministros.

Decreto-Lei n.º 65/2021, de 30 de julho (2015). *Aprova o Regime Jurídico da Segurança do Ciberespaço*. Diário da República, I Série, 147. 8-21. Lisboa: Conselho de Ministros.

Elias, L. (2018). *Ciências Policiais e Segurança Interna. Desafios e Prospetiva*. Lisboa: ICPOL-ISCPSI.

ENISA (2013). *Cybersecurity cooperation - Defending the digital frontline*. Heraklion, Grécia.

EUROPOL (2021), *The Cyber Blue Line. Europol Spotlight.* Report series. Luxembourg: Publications Office of the European Union.

Fachada, C. P. A., Ranhola, N. M. B., & Santos, L. A. B. (2019). *Regras e Normas de Autor no IUM* (2.ª ed., revista e atualizada). IUM Atualidade, 7. Lisboa: Instituto Universitário Militar.

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

Fernandes, L. F. (2014). *Intelligence e Segurança Interna*. Lisboa: Sersislito.

Freixo, M. J. V. (2011). *Metodologia Científica: Fundamentos, Métodos e Técnicas*. 3.ª ed. Lisboa: Instituto Piaget.

Gendarmerie Nationale (s.d.). *Notre institution* [Página *online*]. Retirado de https://www.gendarmerie.interieur.gouv.fr/notre-institution

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

Giroux, Henry A. (2006). *Para Além do Espectáculo do Terrorismo. A Incerteza e o Desafio dos Novos Media*. Mangualde. Edições Pedago.

Gomes, P., Dias, M., Leitão, J., Mendes, M. & Oliveira, J. (2001). Modelos de Policiamento. *Revista Polícia Portuguesa*, Separata da Revista Polícia Portuguesa nº 128, março/abril, (1-27).

Gonçalves S., Gonçalves, J. & Marques, C. (2021). *Manual de Investigação Qualitativa. Conceção, Análise e Aplicações*. Lisboa: Pactor.

Gouveia, J.B. & Santos, S. (Coord.) (2015). *Enciclopédia de Direito e Segurança*. Coimbra: Edições Almedina.

Guarda Nacional Republicana. (2020). *A Estratégia da Guarda 2025 (EG2025), Uma Estratégia centrada nas Pessoas*. Lisboa: Autor.

Guarda Nacional Republicana. (2020b). *Despacho n.º 1292/2020 – Unidades orgânicas flexíveis, do Comandante-geral da GNR*. Série II. N.º 20 (pp. 20-105). Lisboa.

Guardia Civil (s.d.). Información Institucional [Página *online*]. Retirado de https://www.guardiacivil.es/es/institucional/Conocenos/index.html

Guedes. A. M. (2009). *As "redes sociais" digitais, a participação política e a segurança*. Em Pessoas & Territórios. Lisboa: Revista do Governo Civil de Lisboa.

Guedes, I. S., Moreira, S., & Cardoso, C. (2021). Cibercrime: Conceptualização, Desafios e Perceções Públicas. Em Guedes, I. S. & Gomes, M. A. M. (Coords.), *Cibercriminalidade. Novos Desafios, Ofensas e Soluções*. (pp. 3-23). Pactor.

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 Universitário Militar (2020a). NEP/INV-001(A1). *Procedimentos relativos à elaboração de trabalhos de Investigação realizados no âmbito de cursos que não atribuem grau académico*. Lisboa: Instituto Universitário Militar.

Instituto Universitário Militar (2020b). NEP/INV-003(A3). *Estrutura e regras de citação e referenciação de trabalhos escritos a realizar no IUM*. Lisboa: Instituto Universitário Militar.

INTERPOL (2022). *Scanning for the Future(s) of Policing: First steps towards a new global paradigma*. INTERPOL Innovation Centre.

Kepner, C. H., & Tregoe, B. B. (2013). *The New Rational Manager: An updated edition for the new world*. Princeton: Kepner-Tregoe.

Kuehl, D. (2009). *Cyberspace & Cyberpower: Defining the Problem*. *Cyberpower & National Security*.

Lei n.º 27/2021 de 17 de maio (2021). *Aprova a Carta Portuguesa de Direitos Humanos na Era Digital*. Diário da República, Série I, 5 - 10. Lisboa: Assembleia da República.

Lei n.º 49/2008, de 27 de agosto (2008). *Aprova a Lei da Organização e Investigação Criminal*. Série I. Lisboa: Assembleia da República.

Lei n.º 53/2007, de 31 de agosto. (2007). *Aprova a orgânica da Polícia de Segurança Pública*. Diário da República. 1ª Série, n.º 168, Assembleia da República.

Lei n.º 53/2008, de 29 de agosto (2008). *Lei de Segurança. Interna*. *Diário da República*, I Série, 167, 6135-6141. Lisboa: Assembleia da República.

Lei n.º 63/2007, de 6 de novembro (2007). *Aprova a orgânica da Guarda Nacional Republicana. Diário da República*, 1.ª Série, 213. 8043 a 8051. Lisboa: Assembleia da República.

Lei n.º 109/2009 de 15 de semtbro (2009). *Aprova a Lei do Cibercrime*, Série I. Lisboa: Assembleia da República.

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

Marques, A. (2020). Cibersegurança no Setor Marítimo. *CyberLaw by CIJIC*, (pp. 12-25). Retirado de http://www.cijic.org/publicacao/ge

Ministerio de la Presidencia, Relaciones con las Cortes e Igualdad (2019). *Orden* PCI/685/2019, de 18 de *junio, por la que se modifica la Orden* PRE/422/2013, de 15 *de marzo, por la que se desarrolla la estructura orgánica de los Servicios Centrales de la Dirección General de la Guardia Civil.* BOE n.º 150 (pp. 66756-66757)

Moleirinho, P. (2018). A importância dos modelos preditivos na área da segurança. Entre riscos e equilíbrios instáveis. Em: T. Rodrigues & M. Painho (Coord.), *Modelos Preditivos e Segurança Pública* (99-130). Porto: Fronteira do Caos.

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

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

NEP/GNR – 2.01 (2021). *Áreas de Interesse*. Lisboa: Guarda Nacional Republicana – Comando Operacional

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

Nunes, P. N. (2015). *Sociedade em Rede, Ciberespaço e Guerra de Informação. Contributos para o Enquadramento e Construção de uma Estratégia da Informação*. Lisboa: IDN.

Nunes, P. V. (2016). Ciberameaças e Quadro Legal dos Conflitos no Ciberespaço. Em Borges, J. & Rodrigues (Coord.), *Ameaças e Riscos Transnacionais no Novo Mundo Global* (pp. 199-215). Porto: Fronteira do Caos Editores, Lda.

Nunes, P. V. (Coord.). (2018). *Contributos para uma Estratégia Nacional de Ciberdefesa*. IDN Cadernos, 28. Lisboa: Instituto da Defesa Nacional.

Nunes, P. V. (2019). Conflitos da era da informação: Guerras cibernéticas. Catástrofes *Antrópicas. Uma Aproximação Integral*. Setembro 201), pp. 471-490. doi: https://doi.org/10.14195/978-989-26-1867-8.

Nunes, P. V. (2020). *A edificação da capacidade de ciberdefesa nacional*. (Trabalho de Investigação Individual em Curso de Promoção a Oficial General). Instituto Universitário Militar. Pedrouços.

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

Oliveira, J. F. (2006). *As Políticas de Segurança e os Modelos de Policiamento*. Coimbra: Almedina.

Procuradoria-Geral da República (2022). *Cibercrime: Denúncias Recebidas 2021*. Nota Informativa. Gabinete do Cibercrime, Lisboa: PGR.

Quivy, R., & Campenhoudt, L. V. (1992, 2005). *Manual de Investigação em Ciências Sociais* (1ª ed. e 4ª ed.). Lisboa: Gradiva

Resolução da Assembleia da República n.º 88/2009, de 15 de setembro. (2009). *Aprova a Convenção sobre Cibercrime*, adoptada em Budapeste em 23 de Novembro de 2001. Diário da República, 1.ª Série, 179, 6354-6380. Lisboa: Assembleia da República.

Resolução do Conselho de Ministros n.º 19/2013, de 21 de março. (2013). *Aprova o Conceito Estratégico de Defesa Nacional*. Diário da República, 1.ª Série, 67, 1981–1995. Lisboa: Presidência do Conselho de Ministros.

Resolução do Conselho de Ministros n.º 40/2023, de 3 de maio de 2023. (2023). *Aprova a Estratégia Nacional de Combate ao Terrorismo*. Diário da República, 1.ª Série, 85, 19-24. Lisboa: Presidência do Conselho de Ministros.

Resolução do Conselho de Ministros n.º 92/2019, 5 de junho (2019). *Aprova a Estratégia Nacional de Segurança do Ciberespaço 2019-2023*. Diário da República, 1.ª série, 108, 2888-2895. Lisboa: Presidência do Conselho de Ministros.

Resolução do Conselho de Ministros n.º 106/2022, de 2 de novembro. (2022). *Aprova a Estratégia Nacional de Ciberdefesa*. Diário da República, 1ª Série, 211, 13-22. Lisboa: Presidência do Conselho de Ministros.

Resolução do Conselho de Ministros n.º 115/2017, de 13 de julho de 2017. (2017). *Cria o grupo de projeto denominado "Conselho Superior de Segurança do Ciberespaço"*. Diário da República, 1.ª Série, 163/2017, 5035 – 5037. Lisboa: Presidência do Conselho de Ministros.

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

Santos, L. (2015). Ciberespaço e Cibersegurança. Em Gouveia & Santos (Coord.). *Enciclopédia de Direito e Segurança* (pp. 60-68). Coimbra: Almedina.

Santos, L. A. B., & Lima, J. M. M. (Coord.) (2019). *Orientações metodológicas para a elaboração de trabalhos de investigação* (2.ª ed., revista e atualizada). Cadernos do IUM, 8. Lisboa: Instituto Universitário Militar.

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

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

Silva, N. P. (2022). Cidadania e Segurança: Dinâmicas de Mobilização e Participação dos Cidadãos na Segurança Nacional (Trabalho de Investigação Individual em Curso de Promoção a Oficial General). Instituto Universitário Militar. Pedrouços.

Santos, L. (2018). Segurança do Ciberespaço. Em: P. Nunes (Coord.), *Contributos para uma Estratégia Nacional de Ciberdefesa* (pp. 25-31). Lisboa: IDN Cadernos.

Sistema de Segurança Interna (2022). *Relatório Anual de Segurança Interna 2022*. Lisboa.

Strate, L. (1999). *The varieties of cyberspace: Problems in definition and delimitation*. Wertern Journal of Communication. 382-412.

Trottier, D. (2012). *Policing Social Media. Canadian Review of sociology*. 49 (4), 411-425.

US Department of Defense (2006). *National Military Strategy for Cyberspace Operation*. Washington, D.C.: Chairman of the Joint Chiefs of Staff.

Venâncio, P. D. (2022). *Lições de Direito do Cibercrime. E da tutela penal de dados pessoais*. Coimbra: Editora d'Ideias.

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*. Volume I. Lisboa: Centro Atlântico, Lda.

Vilelas, J. (2009). *Investigação: o Processo de Construção do Conhecimento*. Lisboa: Edições Sílabo.

Apêndice A — Conceito de ciberespaço

Quadro 2 - Definição do conceito de ciberespaço por autor

Definição de ciberespaço	Autor
"Rede global de infraestruturas de tecnologias de informação interligadas entre si, especialmente as redes de telecomunicações e os sistemas de processamento dos computadores".	Fernandes (2014, p. 68)
"Um domínio caraterizado pelo uso de aparelhos eletrónicos e do espectro eletromagnético para salvaguardar, modificar e enviar dados através de sistemas de rede e estruturas físicas associadas".	US Department of Defense (2006)
"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".	Kuehl (2009, pp. 24-42)
"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"	Caldas (2011, p. 94)
"Conjunto das diferentes vivências do espaço associadas às tecnologias e à computação".	Strate (1999)
"Ambiente complexo, de valores e interesses, materializado numa área de responsabilidade coletiva, que resulta da interação entre pessoas, redes e sistemas de informação".	ENSC (2019)

Apêndice B — Entidades responsáveis pela cibersegurança

Na EU existem diversos organismos que garantem a segurança do ciberespaço. A ENISA é a agência europeia especializada em cibersegurança que tem por missão "contribuir para a realização dos objetivos consistentes em assegurar um elevado nível de segurança das redes e da informação na União e desenvolver uma cultura de segurança das redes e da informação em benefício" dos seus utilizadores. (ENISA, 2013, p. 42). Criado em 2011, o CERT-EU[6], sediado na Direção-geral da Informática da Comissão Europeia, contribui para a segurança das infraestruturas TIC de mais de 80 organismos da UE, ajudando-os a prevenir, detetar, atenuar e responder a ciberataques, e atuando como centro de intercâmbio de informações sobre cibersegurança e de coordenação da resposta a incidentes. O Centro Europeu de Competências em Cibersegurança[7] (*European Cybersecurity Competence Centre*) tem como missão aumentar as capacidades e a competitividade da Europa em matéria de cibersegurança, trabalhando em conjunto com uma rede de centros nacionais de coordenação para construir uma forte comunidade de cibersegurança.

No seio da Europol, o EC3 (*European CyberCrime Centre*) foi criado em 2013 e tem como objetivos o fortalecimento da resposta da aplicação da lei da criminalidade informática na União Europeia e ajuda na proteção dos governos, empresas e cidadãos europeus.

Em Portugal, existe o Centro Nacional de Cibersegurança, inserido no Gabinete Nacional de Segurança, que tem por missão: "contribuir para uma utilização livre, confiável e segura do ciberespaço de interesse nacional" e atua como "coordenador operacional e autoridade nacional em matéria de cibersegurança junto das entidades do Estado, operadores de infraestruturas críticas nacionais, operadores de serviços essenciais e prestadores de serviços digitais" e a sociedade em geral. No âmbito da resposta às ameaças e incidentes no ciberespaço existem os CERT (*Computer Emergency Response Team*) cuja função é identificar e responder a riscos cibernéticos e limitar o seu impacto e o CSIRT (*Computer Security Incident Response Team*) que tem por missão responder a incidentes relacionados com a segurança informática.

A PJ possui competência reservada de investigação do cibercrime, através da Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica (UNC3T), que é a unidade operacional especializada que dá resposta preventiva e repressiva ao fenómeno do cibercrime[8].No âmbito da ciberdefesa, o Centro de Ciberdefesa[9] (CCD) funciona como o braço das Forças Armadas no ciberespaço, como órgão conjunto, inserido no EMGFA e constituído por militares dos três ramos das Forças Armadas. A sua missão é garantir a integridade, confidencialidade e disponibilidade da informação e dos sistemas de informação da Defesa Nacional, essenciais ao exercício da nossa soberania, levando a cabo ações de defesa e, eventualmente, a criação de efeitos no, e através do, ciberespaço. O CCD privilegia a articulação e a partilha de informação com o CNCS e os *Computer Incident Response Capability* (CIRC) nacionais e internacionais, e outras entidades com responsabilidades no ciberespaço de modo a consolidar a estratégia de resposta nacional às ciberameaças.

[6] *Cfr*. https://cert.europa.eu/about-us
[7] *Cfr* https://cybersecurity-centre.europa.eu/index_en
[8] *Cfr*. https://www.policiajudiciaria.pt/unc3t/
[9] *Cfr*. https://www.defesa.gov.pt/pt/pdefesa/ciberdefesa/centro/Paginas/default.aspx

Apêndice C — Enquadramento estratégico do ciberespaço

De acordo com Couto (2020, pp. 76, 239), a política comanda a estratégia, sendo a primeira um fim e a segunda, como atividade, um meio para atingir esse fim, cujos objetivos são a segurança e o progresso e bem-estar social.

A estratégia é única pelo seu objeto e pelo seu método e na sua aplicação ela divide-se necessariamente em estratégias especializadas (Beaufre, 1965, pp. 24-26). Segundo o mesmo autor, no topo das estratégias encontra-se a estratégia total, imediatamente subordinada à política, cujo papel é definir a missão própria e a combinação das diversas estratégias gerais, subdivididas pelas áreas de aplicação, nomeadamente, política, económica, diplomática e militar.

Segundo Couto (2020, p. 248), que valida o modelo teórico de Beaufre, cada uma das estratégias gerais, articulam-se em estratégias particulares, conforme a natureza dos meios que empregam ou dos setores a que se dirigem. Entre a conceção e a execução da estratégia, podemos desenvolver as estratégias operacional estrutural e a genética. A estratégia operacional trata da "conceção e execução da manobra estratégica ao nível dos grandes subordinados" e a estratégia genética (ou logística) coloca à sua disposição os novos meios, no momento adequado e que sirvam o conceito estratégico adotado. A estratégia estrutural tem por objetivo a deteção e análise das vulnerabilidades e das potencialidades das estruturas existentes (Couto, 2020, pp. 248-251). Em resumo, de modo a materializar a estratégia, torna-se necessário distinguir os seus "aspetos operacionais (ligados à utilização dos meios), genéticos (associados à geração e sustentação de meios) e os aspetos estruturais (correspondentes à composição, organização ou articulação dos meios) (Couto, 2020, p. 249).

Considerando a missão e as atribuições das FSS conferidas pela CRP e pela Lei de Segurança Interna (LSI) (Lei n.º 53/2008, de 29 de agosto) e as suas leis orgânicas, conjugado com o Conceito Estratégico de Defesa Nacional (CEDN) (Resolução de Conselho de Ministros n.º 19/2013, de 21 de março), como a estratégia global a adotar pelo Estado, no âmbito da política e defesa nacional, e a ENSC, enquanto instrumento estruturante para a capacitação nacional em matéria de segurança do ciberespaço, interessa compreender o enquadramento estratégico da UE e nacional.

Neste sentido, importa analisar a Estratégia de Cibersegurança da União Europeia (ECEU) e as orientações estratégicas nacionais relevantes no âmbito da cibersegurança e proteção do ciberespaço, nomeadamente: o Conceito Estratégico de Defesa Nacional (CEDN), a Estratégia Nacional de Ciberdefesa (ENCD) (Resolução do Conselho de Ministros n.º 106/2022, de 2 de novembro), a Estratégia Nacional de Combate ao Terrorismo (ENCT) (Resolução do Conselho de Ministros n.º 40/2023 de 3 de maio de 2023), a proposta de Conceito Estratégico de Segurança Interna (CESI), considera-se relevante apresentar este estudo por não existir instrumento estratégico aprovado no âmbito da Segurança Interna (Lourenço, 2015), e ENSC.

No final de 2020, a União Europeia (UE) aprovou a "Estratégia de cibersegurança da UE para a década digital" que tem por objetivo "preservar uma *internet* global e aberta, mediante a utilização e o reforço de todos os instrumentos e recursos disponíveis, a fim de garantir a segurança e proteger os valores europeus e os direitos fundamentais de cada um de nós". Este documento apresenta novas iniciativas estratégicas que incluem: um ciberescudo à escala da UE; uma ciberunidade conjunta que permitirá reagir coletivamente; soluções europeias com vista a reforçar a segurança da *internet* à escala mundial; um regulamento relativo a uma *internet* das coisas segura; um conjunto mais sólido de instrumentos de ciberdiplomacia a nível da EU; uma cooperação

reforçada em matéria de cibersegurança; um programa de ação das Nações Unidas para gerir a segurança internacional no ciberespaço e cooperação com países terceiros e as organizações regionais e internacionais, incluindo a NATO e mecanismos de reforço das cibercapacidades da UE[10].

Relativamente 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 prevê uma elevada probabilidade de concretização de ameaças associadas a um potencial destruidor relativo aos ataques cibernéticos.

Quanto à ENCD, a mesma vem estabelecer uma visão que visa densificar conceitos e promover o desenvolvimento das capacidades de ciberdefesa nacional, no âmbito das Forças Armadas, devidamente articulada com as estruturas civis da defesa nacional, assim como com outras áreas de governação e entidades com responsabilidade pela segurança do ciberespaço, contribuindo para uma maior resiliência e soberania nacional no ciberespaço. (ENCD, p. 16)

Refere ainda que no ciberespaço "operam indivíduos, entidades e Estados com agendas desestabilizadoras, realizando ações de natureza encoberta, assimétrica e híbrida". Estas atividades constituem um forte impacto "no normal funcionamento dos Estados, das economias e das sociedades, comprometem a segurança, a confiança e a liberdade do uso - justo, equilibrado, partilhado e global - desse espaço coletivo da humanidade".

No que concerne à ENCT e conforme plasmado no seu preâmbulo "assume como compromisso combater a ameaça terrorista, no pleno respeito pelos direitos humanos e liberdades fundamentais e em estrita observância dos instrumentos legais internacionais e nacionais em vigor neste domínio". No domínio da segurança do ciberespaço, prevês as seguintes linhas de ação: "Garantir os meios apropriados para perseguir a utilização do ciberespaço para apoiar e financiar o terrorismo e promover o recrutamento, radicalização e disseminação de propaganda violenta"; "Coordenar todas as capacidades necessárias para combater os discursos de ódio e a desinformação no ciberespaço, bem como noutros espaços comunicacionais comuns globais"; "Coordenar todas as capacidades necessárias para combater os discursos de ódio e a desinformação no ciberespaço, bem como noutros espaços comunicacionais comuns globais" e "Garantir os meios apropriados para perseguir a utilização do ciberespaço para apoiar e financiar o terrorismo e promover o recrutamento, radicalização e disseminação de propaganda violenta".

Torna-se, igualmente, relevante revisitar a proposta de Conceito Estratégico de Segurança Interna CESI, apresentada pelo GRESI, no âmbito do estudo "Segurança Interna Horizonte 2025 - Um Conceito de Segurança Interna", embora não aprovado, que enfatiza a necessidade de a atividade de segurança interna ser igualmente exercida no ciberespaço. No referido documento, é proposta uma linha de ação estratégica com vista ao "alargamento do sentimento de segurança à dimensão do ciberespaço", com as seguintes ações:

- 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;

[10] *Cfr*. https://ec.europa.eu/commission/presscorner/detail/pt/qanda_20_2392

- 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 (Lourenço, 2015, p. 61).

Importa agora analisar o instrumento estruturante, aprovado pelo Estado, para a capacitação nacional em matéria de segurança do ciberespaço, de acordo com o interesse nacional, a ENSC.

A atual ENSC surge no seguimento da anteriormente aprovada pela Resolução do Conselho de Ministros n.º 36/2015, de 12 de junho, que visava "aprofundar a segurança das redes e dos sistemas de informação e potenciar uma utilização livre, segura e eficiente do ciberespaço, por parte de todos os cidadãos e das entidades públicas e privadas".

Em 2017, o Governo constituiu, ao abrigo da Resolução do Conselho de Ministros n.º 115/2017, de 24 de agosto, um grupo de projeto, denominado Conselho Superior de Segurança do Ciberespaço, que teve como um dos seus objetivos propor a revisão e elaborar a atual ENSC. Por seu turno, a Lei n.º 46/2018, de 13 de agosto, veio estabelecer o regime jurídico da segurança do ciberespaço, transpondo a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e dos sistemas de informação em toda a União. Através dessa lei, foi instituído o Conselho Superior de Segurança do Ciberespaço, enquanto órgão específico de consulta do Primeiro-Ministro para os assuntos relativos à segurança do ciberespaço. Destaca-se igualmente a aprovação, no ano de 2021, do Regime Jurídico da Segurança do Ciberespaço, aprovado pelo Decreto-Lei n.º 65/2021, de 30 de julho, que transpõe para o ordenamento jurídico nacional a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e dos sistemas de informação em toda a União.

No ano de 2019, foi aprovada a Estratégia Nacional de Segurança do Ciberespaço 2019-2023, aprovada pela Resolução do Conselho de Ministros n.º 92/2019, de 5 de junho que por definição:

> […] funda-se no compromisso de aprofundar a segurança das redes e sistemas de informação, como forma de garantir a proteção e defesa do ciberespaço de interesse nacional e potenciar uma utilização livre, segura e eficiente do mesmo por parte de todos os cidadãos, das empresas e das demais entidades públicas e privadas. (RCM, 2019).

A consecução da ENSC 2019-2023 "permitirá tornar Portugal um país mais seguro e próspero […] que preserve os valores fundamentais do Estado de Direito democrático e garanta o regular funcionamento das instituições face à evolução digital da sociedade."

A ENSC (2019) "articula-se em enquadramento, objetivos e as linhas de ação do Estado em matéria de segurança do ciberespaço, de acordo com o interesse nacional". A mesma estabelece três objetivos estratégicos: maximizar a resiliência, promover a inovação e gerar e garantir recursos. Cada um destes objetivos estratégicos têm associadas implicações e necessidades que permitem definir uma orientação geral e específica, "traduzida em seis eixos de intervenção, que enformam linhas de ação concretas destinadas a reforçar o potencial estratégico nacional no ciberespaço", conforme descrito na figura 5.

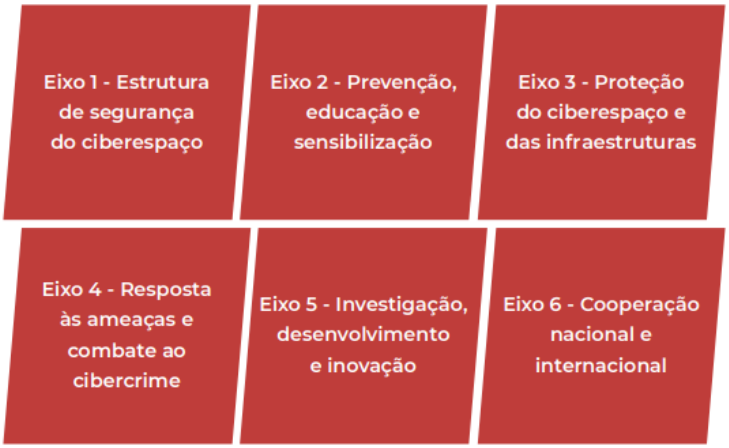

Figura 10 - Eixos de intervenção da ENSC 2019/2023

Fonte: CNCS (2021, p. 30)

Analisadas as linhas de ação de cada um dos eixos de intervenção, constata-se que as FS são referidas como atores intervenientes, na concretização da ENSC 2019-2023, nomeadamente no Eixo 1 - Estrutura de segurança do ciberespaço, na linha de ação: "Reforçar a capacidade de cibersegurança nacional tendo em vista maximizar a resiliência das Forças e Serviços de Segurança" e no Eixo 4 - Resposta às ameaças e combate ao cibercrime, na linha de ação: "Adequar, para efeitos de gestão de crises, as capacidades das Forças Armadas, das Forças e Serviços de Segurança e de outras entidades públicas e privadas, tendo em vista impulsionar uma abordagem integrada às ameaças e riscos em matéria de segurança do ciberespaço".

Relativamente à GNR, na "Estratégia da Guarda 2025" definiu como objetivo estratégico:

> Ampliar a capacidade de atuação no ciberespaço. Garantir uma resposta integrada da Instituição ao fenómeno da cibercriminalidade no mundo real e virtual, através da ampliação das capacidades de ciberpolícia, no âmbito da prevenção e alerta, divulgação e consciencialização e investigação. (GNR, 2020).

Apêndice D — Processo de amostragem

Com o objetivo de se conseguir um nível de representatividade que fosse adequado à investigação e que seja constituída pelos participantes que melhor conhecessem o tema da investigação (Coutinho, 2014, p. 245), definiu-se um conjunto de requisitos a preencher cumulativamente pelos participantes, nomeadamente: que desempenhassem atualmente funções de direção/chefia de órgãos do Comando-geral da GNR, com responsabilidades na segurança do ciberespaço; que tivessem mais de 20 anos de serviço; que tivessem conhecimento teórico-prático do tema da investigação.

Face à aplicação dos critérios, elegeu-se os nove comandantes, diretores e chefes do Comando Operacional e da Divisão de Comunicação e Relações Públicas do Comando-geral da GNR (*cfr.* Quadro 3 - Apd F). Assim, procurou-se obter uma amostra qualitativa intencional, num sentido não probabilístico, por caso múltiplos e por homogeneização, por se pretender analisar um conjunto homogéneo de participantes, no qual o controlo de diversidade é realizado face aos elementos internos do grupo selecionado (Coutinho, 2014). Ou seja, pretendeu-se obter a diversidade dentro do grupo dos dirigentes do Comando-geral da GNR, com funções relevantes no âmbito do domínio da segurança do ciberespaço, aplicando-se o "princípio da diversidade interna, procurando-se as variáveis pertinentes face a este objeto, isto é, aquelas que façam variar a posição do ator face ao objeto" (Guerra, 2006, pp. 46-47).

Para além dos participantes acima referidos, pretendeu-se complementar a informação recolhida com os contributos de especialistas com experiência no quadro conceptual e legal, pelo que foram definidos dois painéis de especialistas, nomeadamente: um painel com quatro peritos no âmbito no âmbito da segurança do ciberespaço e da cibercriminalidade: o Coordenador do Centro Nacional de Cibersegurança; o Chefe do Gabinete do Cibercrime da Procuradoria-geral da República; o Presidente da SIRESP, S.A. e o Coordenador de Investigação Criminal da Polícia Judiciária; Outro painel, constituído por responsáveis da *Guardia Civil* e *Gendarmerie Nationale* francesa com responsabilidades no âmbito da segurança do ciberespaço: o Comandante Comando do Ciberespaço da *Gendarmerie Nationale* francesa e o Chefe da Unidade Coordenação de Cibersegurança, da *Guardia Civil* espanhola (*cfr*. Quadro 4 e 5 - Apd F).

Apêndice E — Guiões das entrevistas

Guião da Entrevista

1. A Estratégia Nacional de Segurança do Ciberespaço 2019-2023 (ENSC) é o instrumento estruturante para a capacitação nacional, definindo o seu enquadramento, os seus objetivos e as linhas de ação do Estado em matéria de segurança do ciberespaço, de acordo com o interesse nacional. A ENSC traduz-se em seis eixos de intervenção, que enformam linhas de ação concretas com vista a reforçar o potencial estratégico nacional no ciberespaço. Considera que as linhas de ação previstas nos seis eixos de intervenção da ENSC são adequadas face aos contributos que as forças de segurança (GNR/PSP), no âmbito das suas atuais atribuições, podem oferecer em matéria de segurança do ciberespaço? Por favor, assinale na tabela a sua resposta (insuficientes/suficientes/excessivas).

Eixo	Ambito	Insuficientes	Suficientes	Excessivas
1	Estrutura de segurança do ciberespaço			
2	Prevenção, educação e sensibilização			
3	Proteção do ciberespaço e das infraestruturas			
4	Resposta às ameaças e combate ao cibercrime			
5	Investigação, desenvolvimento e inovação			
6	Cooperação nacional e internacional			

2. A ENSC destaca a necessidade de coordenação entre instituições com responsabilidade de garantir a segurança do ciberespaço e que as mesmas "desenvolvam um permanente esforço de apetrechamento, que as habilite a cumprirem cabalmente as suas missões" e que os sistemas, o policial e judiciário, "se adaptem às formas de responder às ameaças e investigar os crimes que recorrem às novas tecnologias". Face ao desafio imposto pela ENSC importa que as forças de segurança (GNR/PSP) considerem qual a melhor estrutura e os meios humanos e materiais necessários de modo a cumprir o desígnio acima referido.

   2.1 Na tabela assinale as opções que considera mais adequadas.

Natureza	Ambito	Sim	Não
Estrutura	A atual estrutura		
	Reforço das unidades territoriais com meios combate ao cibercrime		
	Uma estrutura de coordenação na dependência direta do Comandante Operacional		
	Um comando funcional responsável pela segurança do ciberespaço		
Meios	Aumento de efetivo especializado		
	Reforço de meios tecnológicos		

   2.2 Deseja acrescentar outras opções?

3. Segundo o Gabinete do Cibercrime da Procuradoria-Geral da República as denúncias de cibercrimes em sentido alargado aumentam persistentemente, de forma consistente, de ano para ano, desde 2016. Em 2022, registou-se um aumento de 73,58%. Destacam-se como ciberameaças particularmente significativas as ações que utilizam a engenharia social para a captura de informação, a fraude e a burla online, concretizadas pelas técnicas de manipulação do fator humano e a prática de crimes que utilizam a esfera digital de modo instrumental, entre outras. Considera que o enquadramento normativo das competências das forças de segurança (GNR/PSP) na investigação do cibercrime está consentâneo com a tipologia e a incidência deste fenómeno criminal em Portugal? Nomeadamente, nos seguintes tipos:

   3.1 Criminalidade informática em sentido estrito?

   (Crimes em que informática é o elemento integrador do tipo legal ou do bem protegido)

   3.2 Criminalidade informática em sentido lato?

   (Crimes em que informática é apenas um novo meio para a prática de um crime não especificamente previsto para o ambiente digital?

4. O ciberespaço, segundo Santos (2015), do ponto de vista funcional, disponibiliza um conjunto de aplicações ou dimensões, das quais destaca a rede global de comunicações eletrónicas (*internet*), o media global e o espaço de interação social (redes sociais, os jogos *online* e a democracia eletrónica) e a biblioteca digital (*World Wide Web* e a *Cloud*). Face às dimensões referidas, considera que as forças de segurança (GNR/PSP) devem projetar a sua atividade operacional no ciberespaço, nos âmbitos da proximidade, prevenção criminal, investigação criminal, informações e ordem pública?

   4.1 Na tabela assinale as opções que considera mais adequadas para cada dimensão (sim/não).

Natureza	Âmbito	Internet	Aplicações	Redes sociais	Jogos online	Biblioteca digital
Dimensão	Proximidade					
	Prevenção criminal					
	Investigação criminal					
	Informações					
	Ordem Pública					

   4.2 Pretende acrescentar alguma dimensão ou âmbito de atuação?

5. Considerando o enquadramento institucional nacional e internacional, como classifica as relações de cooperação da GNR com as outras instituições no âmbito da cibersegurança e da cibercriminalidade?

Ambito	Insuficientes	Ajustadas	A melhorar
Com as entidades nacionais responsáveis pela cibersegurança			
Com o Ministério Público			
Com a Polícia Judiciária			
Com as forças e serviços de segurança nacionais			
Com as forças congéneres estrangeiras			
Com a EUROPOL/INTERPOL			
Outras. Enumere quais.			

6. Antes de finalizar a entrevista, deseja fazer alguma sugestão ou comentário relativamente a algum assunto que não tenha sido abordado durante a entrevista?

Muito obrigado pela sua valiosa colaboração.

Gonçalo Nuno Silva Gonçalves de Carvalho

Coronel da GNR

Apresentação e objetivos da entrevista

No âmbito do Curso de Promoção a Oficial General (2022-2023), encontro-me a realizar um Trabalho de Investigação Individual (TII) subordinado ao tema: "**Contributos para um Modelo de Atuação da Guarda Nacional Republicana no Ciberespaço**".

Em Portugal, a GNR no seu instrumento de gestão estratégica materializado na "Estratégia da Guarda 2025" definiu como objetivo estratégico "ampliar a capacidade de atuação no ciberespaço", através de uma "resposta integrada da Instituição ao fenómeno da cibercriminalidade no mundo real e virtual, através da ampliação das capacidades de ciberpolícia, no âmbito da prevenção e alerta, divulgação e consciencialização e investigação". Com base neste pressuposto estratégico, importa analisar de que forma a GNR prossegue a sua atividade policial no ciberespaço nas dimensões da proximidade, prevenção criminal, informações, ordem pública, investigação criminal e cooperação institucional.

Assim, esta força de segurança, pelo seu conjunto diversificado de competências específicas e capacidades operacionais deve avaliar as suas capacidades de ciberpolícia, reorganizar-se e funcionar de forma integrada, de modo a policiar o ciberespaço e combater as condutas antissociais e os comportamentos ilícitos ocorridos no ciberespaço.

Destaca-se, o esforço realizado pelas congéneres da GNR, nomeadamente a *Guardia Civil* espanhola e a *Gendarmerie Nationale* francesa, na adaptação e reorganização do seu dispositivo, através do desenvolvimento de novas capacidades e criação de órgãos superiores de comando ou estruturas de coordenação específica, no sentido de incrementar da sua presença e a capacidade de intervenção no ciberespaço.

Face ao exposto, releva-se a importância desta entrevista, com vista à concretização do objetivo geral desta investigação de propor contributos que possam ser adotados na definição de um modelo de atuação policial da GNR no ciberespaço em Portugal, na sua área de responsabilidade.

Neste contexto, assumimos como de especial relevância para a nossa investigação a auscultação da sua opinião.

Gonçalo Nuno Silva Gonçalves de Carvalho

Coronel da GNR

Guião da Entrevista

1. Quais são as missões que a *Guardia Civil/Gendarmerie Nationale* tem atribuídas no âmbito do ciberespaço?
   (Missões no âmbito da cibersegurança, cibercrime, ciberterrorismo e hacktivismo).

2. Quais foram os pressupostos da reorganização da *Guardia Civil/Gendarmerie Nationale* para potenciar a sua atividade no ciberespaço?
   (Contexto nacional de ciberameaças e cibercriminalidade e exigências internas de resposta ao fenómeno descrito que justificaram a criação de estruturas específicas com a finalidade de garantir a segurança do ciberespaço).

3. Como se articula organicamente a *Guardia Civil/Gendarmerie Nationale* para cobrir todo o espectro da sua atividade no ciberespaço? Nomeadamente:
   Quais são as estruturas responsáveis pela cibersegurança, cibercriminalidade ciberterrorismo e hacktivismo (nível central e das unidades)? Quais são as suas missões e capacidades?

4. Que constrangimentos têm sido identificados, a nível interno e externo, face à operacionalização dos novos órgãos responsáveis pela segurança no ciberespaço (Unidade de Coordenação de Cibersegurança da *Guardia Civil* - Espanha/ComCyberGend da *Gendarmerie Nationale* – França)?
   4.1 Ao nível externo, quais os constrangimentos na cooperação com entidades nacionais e internacionais?
   4.2 Ao nível interno, quais as dificuldades sentidas na implementação e funcionamento da Unidade de Coordenação de Cibersegurança da *Guardia Civil* - Espanha/ComCyberGend da *Gendarmerie Nationale* – França?

5. Antes de finalizar a entrevista, deseja fazer alguma sugestão ou comentário relativamente a algum assunto que não tenha sido abordado durante a entrevista?

Muito obrigado pela sua valiosa colaboração.

Apêndice F — Lista dos entrevistados

Quadro 3 - Painel de comandantes, diretores e chefes da GNR

	Identificação dos entrevistados				
Código	**Posto**	**Nome**	**Unidade**	**Função**	**Data**
E1	Major-General	Rui Alberto Ribeiro Veloso	CG	Comandante do Comando Operacional	01BAR23
E2	Brigadeiro-General	Pedro Emílio da Silva Oliveira	CG	Diretor do Departamento Operações	10MAR23
E3	Coronel	Jorge Manuel Henriques Amado	CG	Diretor da Direção SEPNA	15MAR23
E4	Coronel	João Carlos Nascimento Nunes	CG	Diretor Direção de Comunicações e Sistemas de Informação	04ABR23
E5	Tenente-coronel	Diogo Almeida E. Brito Moreira Dores	CG	Diretor da Direção de Investigação Criminal	16MAR23
E6	Tenente-coronel	Hélder Romeu Serra Oliveira	CG	Diretor do Centro Integrado Nacional de Gestão Operacional	13MAR23
E7	Major	Mafalda de Jesus Gomes de Almeida	CG	Chefe da Divisão de Comunicação e Relações Públicas	12MAR23
E8	Coronel	Carlos João Soares Costa	CG	Diretor da Direção de Informações	10ABR23
E9	Tenente-coronel	Rogério Gil Raposo	CG	Especialista em Cibersegurança	10ABR23

Quadro 4 - Painel de especialistas nacionais

	Identificação dos entrevistados			
Código	**Categoria/Posto**	**Nome**	**Função/Entidade**	**Data**
E10	Eng.º	Lino Santos	Coordenador do Centro Nacional de Cibersegurança	30MAR23
E11	Procurador-geral Adjunto	Pedro Verdelho	Chefe do Gabinete do Cibercrime da Procuradoria-geral da República	22MAR23
E12	Brigadeiro-general	Paulo Viegas Nunes	Presidente da SIRESP, S.A.	08MAR23
E13	Inspetor-chefe	Rogério Bravo	Coordenador de Investigação Criminal – Polícia Judiciária	30MAR23

Quadro 5 - Painel de especialistas da *Guardia Civil* e *Gendarmerie Nationale* francesa

	Identificação dos entrevistados				
Código	**Posto**	**Nome**	**Organização**	**Função**	**Data**
E14	General de Divisão	Marc Boget	*Gendarmerie Nationale* francesa	Comandante do Comando do Ciberespaço	15MAR23
E15	Coronel	Juan Solom Clotet	*Guardia Civil* espanhola	Chefe da Unidade Coordenação de Cibersegurança	11ABR23

Apêndice G — Atribuições da GNR projetadas no ciberespaço

Quadro 6 - Atribuições da GNR projetadas no ciberespaço

ATRIBUIÇÕES DA GNR	Artigo 3.º LOGNR
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;	Alínea a), n.º 1
Garantir a ordem e a tranquilidade públicas e a segurança e a proteção das pessoas e dos bens;	Alínea b), n.º 1
Prevenir a criminalidade em geral, em coordenação com as demais forças e serviços de segurança;	Alínea c), n.º 1
Desenvolver as ações de investigação criminal e contraordenacional que lhe sejam atribuídas por lei, delegadas pelas autoridades judiciárias ou solicitadas pelas autoridades administrativas;	Alínea e), n.º 1
Manter a vigilância e a proteção de pontos sensíveis, nomeadamente infraestruturas rodoviárias, ferroviárias, aeroportuárias e portuárias, edifícios públicos e outras instalações críticas;	Alínea j), n.º 1
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;	Alínea m), n.º 1
Participar, nos termos da lei e dos compromissos decorrentes de acordos, tratados e convenções internacionais, (…) bem como em missões de cooperação policial internacional e no âmbito da União Europeia e na representação do País em organismos e instituições internacionais;	Alínea o), n.º1
Contribuir para a formação e informação em matéria de segurança dos cidadãos;	Alínea p), n.º 1
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;	Alínea a), n.º 2
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.	Alínea d), n.º 2

Apêndice H — Atribuições das Direções/Divisões prosseguidas no ciberespaço

Quadro 7 - Atribuições das Direções/Divisões prosseguidas no ciberespaço

Divisão de Comunicação e Relações Públicas	
– Planear, coordenar e executar as atividades de informação pública, assegurando a ligação do Comando da Guarda com a Comunicação Social.	
Comando Operacional	
Direções	**Competências**
Direção de Operações	– Assegurar a coordenação e controlo das atividades da Guarda no domínio do cumprimento das missões de natureza operacional, garantindo o apoio à direção operacional das unidades e dispositivo territorial, de acordo com as orientações estratégicas, os planos e as diretivas superiores. – Coordenar com o Centro Integrado Nacional de Gestão Operacional a monitorização e condução das operações correntes. – Elaborar, difundir e assegurar a coordenação do cumprimento das diretivas e orientações relativas às missões de segurança (…) atribuídas à Guarda, designadamente em matéria de policiamento e segurança de pessoas e bens e 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	– Realizar estudos normativos e pareceres técnicos no âmbito da cibersegurança e conduzir atividades de ciberinteligência, especialmente no domínio «open source intelligence» (OSINT), monitorizando, recolhendo e processando notícias existentes no ciberespaço. – Proceder à pesquisa e processamento de notícias para produção de informações em apoio ao nível estratégico, operacional e tático. – Elaborar estudos sobre a realidade sociológica e criminológica e relatórios temáticos de informações sobre criminalidade e delinquência. – Realizar as adequadas averiguações de segurança em caso de quebra ou comprometimento de segurança de informação. – Garantir o intercâmbio regular de informações com as outras FSS, com o Ponto Único de Contacto para a Cooperação Policial Internacional (PUC -CPI), com a estrutura de informações das Forças Armadas e/ou outras entidades com interesse geral para a missão da Guarda ou específico em razão da matéria.
Direção de Investigação Criminal	– Proceder ao tratamento da informação criminal em coordenação com a direção de informações e assegurar a difusão de notícias e informação. – Coordenar o funcionamento das atividades da Guarda em matéria de investigação criminal, nas vertentes operativa e de análise de informação criminal. – Acompanhar a evolução da criminalidade e o surgimento de novas táticas e técnicas aplicáveis à investigação criminal. – Realizar perícias criminalísticas e garantir o apoio às unidades nas atividades de polícia técnico-científica e do uso de meios centralizados.
Direção de Comunicações e Sistemas de Informações	– Assegurar a direção, coordenação, controlo, gestão e execução das atividades da Guarda em matéria de Cibersegurança. – 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.

Apêndice I — Análise das entrevistas

Quadro 8 - Perceções sobre o enquadramento estratégico e legal da atuação policial no ciberespaço

Enquadramento estratégico e legal da atuação policial no ciberespaço (Código A)																		
Cód. Questão	**Seg. Código**	**Segmento Identificado**	**E1**	**E2**	**E3**	**E4**	**E5**	**E6**	**E7**	**E8**	**E9**	**E10**	**E11**	**E12**	**E13**	**Total**	**Resultados**	**Resultados**
A.01	A.01.S01	As atribuições da GNR/PSP na ENSC são insuficientes	1	1		1	1		1	1		1	1	1		9	9/13	**69%**
	A.01.S02	Atribuições da FS na Prevenção, educação e sensibilização suficientes			1	1		1	1			1		1	1	7	7/13	**54%**
A.02	A.02.S01	Legislação no âmbito da cibercriminalidade em sentido restrito suficiente	1	1		1	1		1			1	1	1	1	9	9/13	**69%**
	A.02.S02	Legislação no âmbito da cibercriminalidade em sentido lato insuficiente	1	1	1	1	1	1	1	1	1	1	1	1	1	13	13/13	**100%**
	A.02.S03	Necessidade de revisão da LOIC	1	1		1	1	1		1			1		1	8	8/13	**62%**

Quadro 9 - Perceções sobre a atuação policial da GNR no ciberespaço

Atuação policial da GNR no ciberespaço (Código B)																
Cód. Questão	**Seg. Código**	**Segmento Identificado**	**E1**	**E2**	**E3**	**E4**	**E5**	**E6**	**E7**	**E8**	**E9**	**E12**	**Total**		**Resultados**
B.01	**B.01.S01**	Estrutura de coordenação na dependência direta do Comandante Operacional	1	1	1	1	1		1		1	1	8	8/10	**80%**
	B.01.S02	Reforço das unidades territoriais com meios de combate ao cibercrime	1	1			1	1	1	1			6	6/10	**60%**
	B.01.S03	Reforço de meios humanos e tecnológicos	1	1	1	1	1	1	1	1	1	1	10	10/10	**100%**
B.02	**B.02.S01**	Projeção da atividade policial na dimensão proximidade - *Internet*	1	1	1				1		1	1	6	6/10	**60%**
	B.02.S02	Projeção da atividade policial na dimensão proximidade - Aplicações	1			1	1	1	1		1		6	6/10	**60%**
	B.02.S03	Projeção da atividade policial na dimensão proximidade - Redes Sociais	1	1	1	1	1	1	1	1	1	1	10	10/10	**100%**
	B.02.S04	Projeção da atividade policial na dimensão proximidade - Jogos *online*	1			1	1		1		1		5	5/10	**50%**
	B.02.S05	Projeção da atividade policial na dimensão proximidade - Biblioteca digital	1			1	1	1	1		1		6	6/10	**60%**

	B.02.S06	Projeção da atividade policial na dimensão prevenção criminal - *internet*	1	1	1	1	1	1			1	1	8	8/10	**80%**
	B.02.S07	Projeção da atividade policial na dimensão prevenção criminal - Aplicações	1				1	1			1		4	4/10	**40%**
	B.02.S08	Projeção da atividade policial na dimensão prevenção criminal - redes sociais	1	1	1	1	1	1	1	1	1	1	10	10/10	**100%**
	B.02.S09	Projeção da atividade policial na dimensão prevenção criminal jogos *online*		1		1	1		1	1	1	1	7	7/10	**70%**
	B.02.S10	Projeção da atividade policial na dimensão prevenção criminal - Biblioteca digital	1		1		1	1	1		1	1	7	7/10	**70%**
	B.02.S11	Projeção da atividade policial na dimensão investigação criminal - *internet*	1		1	1	1	1	1	1		1	8	8/10	**80%**
	B.02.S12	Projeção da atividade policial na dimensão investigação criminal - aplicações	1				1	1	1	1			5	5/10	**50%**
	B.02.S13	Projeção da atividade policial na dimensão investigação criminal - redes sociais	1	1		1	1	1	1	1	1	1	9	9/10	**90%**
	B.02.S14	Projeção da atividade policial na dimensão investigação criminal - jogos *online*		1			1	1	1		1	1	6	6/10	**60%**
	B.02.S15	Projeção da atividade policial na dimensão investigação criminal - biblioteca digital	1		1	1	1	1	1		1	1	8	8/10	**80%**
	B.02.S16	Projeção da atividade policial na dimensão informações - *internet*	1	1			1	1	1	1	1	1	8	8/10	**80%**
	B.02.S17	Projeção da atividade policial na dimensão informações - aplicações	1	1			1			1	1	1	6	6/10	**60%**
	B.02.S18	Projeção da atividade policial na dimensão informações - Redes sociais	1	1		1	1	1		1	1	1	8	8/10	**80%**
	B.02.S19	Projeção da atividade policial na dimensão informações - jogos *online*					1				1		2	2/10	**20%**
	B.02.S20	Projeção da atividade policial na dimensão informações - biblioteca digital	1	1	1	1	1	1	1	1	1	1	10	10/10	**100%**
	B.02.S21	Projeção da atividade policial na dimensão ordem pública - *internet*	1	1			1		1	1		1	6	6/10	**60%**
	B.02.S22	Projeção da atividade policial na dimensão ordem pública - aplicações	1					1				1	3	3/10	**30%**
	B.02.S23	Projeção da atividade policial na dimensão ordem pública - redes sociais	1	1	1	1	1	1	1	1		1	9	9/10	**90%**
	B.02.S24	Projeção da atividade policial na dimensão ordem pública - jogos *online*											0	0/10	**0%**
	B.02.S25	Projeção da atividade policial na dimensão ordem pública - biblioteca digital				1	1	1				1	4	0/10	**40%**
B.03	**B.03.S01**	Relações de cooperação entre a GNR e outras instituições insuficientes		1	1		1		1	1	1	1	7	07/10	**70%**

Apêndice J — Proposta das medidas a desenvolver pela GNR

Quadro 10 – Proposta de medidas a desenvolver pela GNR no âmbito da ENSC

Eixos	Linhas de ação da ENSC	Proposta de medidas a desenvolver pela GNR
Eixo 1 - Estrutura de segurança do ciberespaço	– Reforçar a capacidade de cibersegurança nacional tendo em vista maximizar a resiliência das Forças e Serviços de Segurança (…).	– A criação de um Centro de Coordenação de Cibersegurança e Cibercriminalidade (CentroCiber) e do reforço da capacidade de cibersegurança e das competências no âmbito da segurança do ciberespaço das Direções do CO e das Unidades Territoriais contribuirá para o reforço da capacidade de cibersegurança nacional.
	– Promover uma maior articulação e coordenação das entidades relevantes nas áreas da segurança do ciberespaço, nomeadamente, através da criação de sinergias com as entidades que integram o Sistema de Segurança Interna (…).	– A criação do CentroCiber permitirá estabelecer um ponto de contacto único, com vista a uma maior articulação e coordenação com todas as entidades relevantes nas áreas da segurança do ciberespaço e potenciar as sinergias no seio do SSI.
Eixo 2 - Prevenção, educação e sensibilização	– Reforçar os meios de recolha e processamento de informação e as capacidades de análise. – Conhecer os agentes de ameaça, as suas intenções e capacidades e avaliar os potenciais impactos gerados pela sua atividade. – Antecipar a emergência, evolução e mutação das ameaças, possibilitando a adoção atempada de ações que acrescentem resiliência.	– Reforçar a capacidade de análise do Centro de Informações, através do investimento nos meios de recolha e processamento de informação, nomeadamente através de *software* adequado, sistemas de aprendizagem automática assistia por máquinas, mecanismos de apoio à predição na área de IA e desenvolvimento de aplicações móveis.
	– Valorizar os profissionais no âmbito da segurança do ciberespaço, ampliando o número de especialistas, qualificando profissionais e envolvendo os diversos atores de toda a sociedade. – Tirar proveito das estruturas de ensino e formação militares e policiais nacionais e internacionais, (…) para o aprofundamento do conhecimento relacionado com o ciberespaço e contribuindo para a sensibilização e prevenção na sua utilização.	– Estabelecer protocolos de cooperação com estabelecimentos de ensino superior e de ensino de formação profissional, com vista à formação de especialistas, nas diferentes categorias, no âmbito das áreas da cibersegurança e cibercriminalidade. – Promover a cooperação com as forças congéneres e organizações internacionais no âmbito da formação e qualificação dos seus militares nas áreas da cibersegurança e cibercriminalidade. – Introduzir nos planos de curso de formação inicial e de qualificação matérias de cibersegurança e cibercriminalidade.

	– Criar uma sociedade mais resiliente, estimulando nos cidadãos o desenvolvimento de competências digitais (…). – Criar instrumentos e reforçar as medidas de sensibilização da sociedade civil para o uso seguro e responsável das tecnologias digitais, dando particular importância à capacitação e conhecimento obtidos por crianças, adolescentes, população sénior e outros grupos de risco. – Reforçar as competências e conhecimentos em segurança do ciberespaço na educação (…). – Promover a educação e literacia digital enquanto condição basilar para a confiança e utilização dos recursos digitais de uma forma consciente, informada e responsável das novas tecnologias pelas novas gerações e os grupos especialmente vulneráveis. – Organizar e realizar exercícios que permitam avaliar o grau de preparação e a maturidade das diversas entidades para lidar com incidentes com impacto relevante, potenciando sinergias. Adicionalmente participar em exercícios de âmbito internacional; – Promover programas de sensibilização específicos junto das instituições públicas e privadas, que robusteçam a vertente comportamental de segurança em ambiente digital, com base na partilha de conhecimento especializado sobre os agentes da ameaça e seus modos de atuação.	– Elaborar e difundir conteúdos de formação, através do Departamento de Operações, em articulação com o CNCS e os parceiros institucionais, de sensibilização e reforço das competências e conhecimentos em segurança do ciberespaço dirigido às novas gerações e aos grupos especialmente vulneráveis. – Planear e coordenar as ações de formação e sensibilização a ministrar pelas unidades territoriais junto das crianças, adolescentes, professores, população sénior e outros grupos de risco.
Eixo 3 - Proteção do ciberespaço	– Promover o contínuo desenvolvimento das capacidades e maturidade das entidades nacionais na prevenção, deteção, resposta e recuperação perante cenários adversos à segurança do ciberespaço que possam produzir impactos nas suas redes e sistemas de informação e ecossistema que as caracteriza, consolidando a confiança mútua, a partilha de informação e conhecimento, e a cooperação célere e eficaz.	– Através da implementação e desenvolvimento da capacidade de cibersegurança na DCSI contribuir para o desenvolvimento das capacidades e maturidade das entidades nacionais na prevenção, deteção, resposta e recuperação perante cenários adversos à segurança do ciberespaço.
	– Promover estruturas de cooperação nacional e setorial de proteção do ciberespaço, inclusive do setor público ao nível central, regional e local, e também do setor privado, incluindo as pequenas e médias empresas, para a partilha de informação e de promoção da colaboração mútua na proteção de interesses comuns.	– Estreitar e promover a cooperação entre a GNR, através do CentroCiber, e as instituições públicas e privadas para a partilha de informação e de promoção da colaboração mútua na proteção de interesses comuns.
Eixo 4 - Resposta às ameaças e combate ao cibercrime	– Adequar, para efeitos de gestão de crises, as capacidades das Forças Armadas, das Forças e Serviços de Segurança e de outras entidades públicas e privadas, tendo em vista impulsionar uma abordagem integrada às ameaças e riscos em matéria de segurança do ciberespaço.	– Desenvolver internamente a capacidade de atuar em situações de gestão de crises no ciberespaço. – Participar em exercícios de gestão de crises no ciberespaço em conjunto com o CNCS, as FSS e as Forças Armadas.

	– Proceder à avaliação das necessidades de revisão e atualização da legislação. – Avaliar no âmbito da cibercriminalidade a necessidade de ajustamento das normas processuais penais aos desafios globais que a mesma coloca e, em particular quanto a eventual acesso transfronteiriço a dados (prova digital), a eventual cooperação com operadores de comunicações estrangeiros e a agilização de ações de investigação online, incluindo as que possam enquadrar-se no contexto de ações encobertas, nos termos da lei.	– Participar ativamente na revisão e atualização a legislação relevante no âmbito da cibersegurança e cibercriminalidade.
	– Consolidar e promover a capacidade nacional de conhecimento das ameaças à segurança do ciberespaço, de forma colaborativa entre as autoridades nacionais com responsabilidade nesta área e com a participação ativa das entidades do setor público e privado.	– Promover a partilha de informação, entre a GNR e as autoridades nacionais com responsabilidade nesta área, entidades do setor público e privado, no âmbito conhecimento das ameaças à segurança do ciberespaço.
Eixo 5 - Investigação, desenvolvimento e inovação	– Promover a inovação aliada à cibersegurança no Estado através das tecnologias de informação e comunicação mais eficazes, de acordo com outras estratégias nacionais pertinentes.	– Estabelecer protocolos de cooperação com centros de inovação e desenvolvimento do Estado para desenvolvimento de projetos de inovação na área das tecnologias de informação.
Eixo 6 - Cooperação nacional e internacional	– Integrar organismos internacionais de cibersegurança e de ciberdefesa tendo em vista a cooperação internacional e a afirmação de Portugal neste domínio. – Aprofundar a coordenação e cooperação entre as diversas entidades nacionais com responsabilidades na segurança do ciberespaço, tendo em vista uma melhor capacidade de alerta e resposta para fazer face às ameaças.	– Fomentar a cooperação nacional e internacional entre a GNR e as diversas entidades nacionais com responsabilidades na segurança do ciberespaço, tendo em vista uma melhor capacidade de alerta e resposta para fazer face às ameaças.

Apêndice K — Análise das medidas propostas

Quadro 11 - Análise da ordem estratégica e primazia das medidas propostas

Medidas propostas	IMP	DIF	NEC	TOTAL	PRI
M1-Criar um Centro de Coordenação de Cibersegurança e Cibercriminalidade (CentroCiber) e reforçar a capacidade de cibersegurança e das competências no âmbito da segurança do ciberespaço das Direções do CO e das Unidades Territoriais contribuirá para o reforço da capacidade de cibersegurança nacional.	3	3	3	27	**1**
M2-Estabelecer um ponto de contacto único, através do CentroCiber, com vista a uma maior articulação e coordenação com todas as entidades relevantes nas áreas da segurança do ciberespaço e potenciar as sinergias no seio do SSI.	3	3	3	27	**1**
M3-Reforçar a capacidade de análise do Centro de Informações, através do investimento nos meios de recolha e processamento de informação, nomeadamente através de *software* adequado, sistemas de aprendizagem automática assistia por máquinas, mecanismos de apoio à predição na área de IA e desenvolvimento de aplicações móveis.	3	2	3	18	**2**
M4-Estabelecer protocolos de cooperação com estabelecimentos de ensino superior e de ensino de formação profissional, com vista à formação de especialistas, nas diferentes categorias, no âmbito das áreas da cibersegurança e cibercriminalidade.	3	2	2	12	**2**
M5-Promover a cooperação com as forças congéneres e organizações internacionais no âmbito da formação e qualificação dos seus militares nas áreas da cibersegurança e cibercriminalidade.	2	3	2	12	**2**
M6-Introduzir nos planos de curso de formação inicial e de qualificação matérias de cibersegurança e cibercriminalidade.	2	2	2	8	**3**
M7-Elaborar e difundir conteúdos de formação, através do Departamento de Operações, em articulação com o CNCS e os parceiros institucionais, de sensibilização e reforço das competências e conhecimentos em segurança do ciberespaço dirigido às novas gerações e aos grupos especialmente vulneráveis.	2	3	1	6	**3**
M8-Planear e coordenar as ações de formação e sensibilização a ministrar pelas unidades territoriais junto das crianças, adolescentes, professores, população sénior e outros grupos de risco.	2	3	2	12	**2**
M9-Implementação e desenvolvimento da capacidade de cibersegurança na DCSI contribuir para o desenvolvimento das capacidades e maturidade das entidades nacionais na prevenção, deteção, resposta e recuperação perante cenários adversos à segurança do ciberespaço.	3	1	2	6	**3**
M10- Estreitar e promover a cooperação entre a GNR, através do CentroCiber, e as instituições públicas e privadas para a partilha de informação e de promoção da colaboração mútua na proteção de interesses comuns.	2	1	2	4	**3**
M11-Desenvolver internamente a capacidade de atuar em situações de gestão de crises no ciberespaço.	3	2	2	12	**2**

M12- Participar em exercícios de gestão de crises no ciberespaço em conjunto com o CNCS, as FSS e as Forças Armadas.	1	2	2	4	**3**
M13-Participar ativamente na revisão e atualização a legislação relevante no âmbito da cibersegurança e cibercriminalidade.	2	2	2	8	**3**
M14-Promover a partilha de informação, entre a GNR e as autoridades nacionais com responsabilidade nesta área, entidades do setor público e privado, no âmbito conhecimento das ameaças à segurança do ciberespaço.	2	2	2	8	**3**
M15-Estabelecer protocolos de cooperação com centros de inovação e desenvolvimento do Estado para desenvolvimento de projetos de inovação na área das tecnologias de informação.	3	1	2	6	**3**
M16-Fomentar a cooperação nacional e internacional entre a GNR e as diversas entidades nacionais com responsabilidades na segurança do ciberespaço, tendo em vista uma melhor capacidade de alerta e resposta para fazer face às ameaças.	2	2	2	8	**3**

Legenda:
IMP – Importância - Avalia a pertinência da medida determinando a intensidade do retorno da sua implementação.
Muito importante: 3; Importante: 2; Pouco importante: 1.
DIF - Dificuldade - Qualifica a complexidade em implementar a medida.
Simples: 3; Acessível: 2; Difícil: 1.
NEC – Necessidade - Caracteriza a urgência da implementação, face às consequências negativas na ausência da ação.
Muito urgente: 3; Urgente: 2; Pouco urgente: 1
PRI – Prioridade de implementação da medida.
Baixa: 3-10 (3); Intermédia: 11-19 (2); Máxima: 20-27 (1)