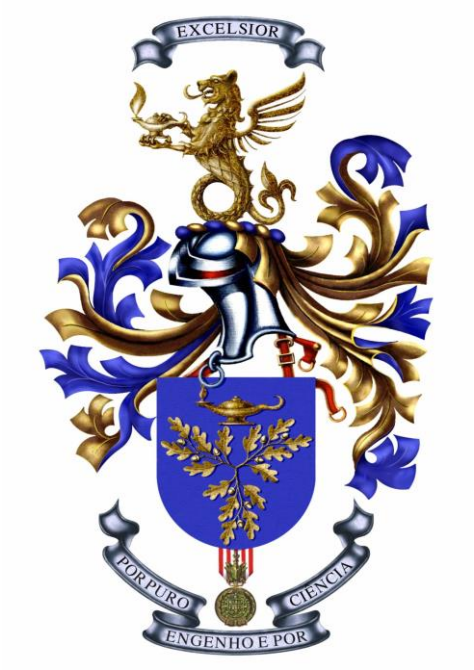
INSTITUTO UNIVERSITÁRIO MILITAR
DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS
CURSO DE ESTADO-MAIOR CONJUNTO
2018/2019



Trabalho de Investigação Individual

A INTERVENÇÃO DAS FORÇAS DE SEGURANÇA NA PROTEÇÃO DE INFRAESTRUTURAS CRÍTICAS E O PAPEL DAS FORÇAS ARMADAS

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.

Pedro Manuel Monteiro Fernandes
MAJ TM

INSTITUTO UNIVERSITÁRIO MILITAR

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

A INTERVENÇÃO DAS FORÇAS DE SEGURANÇA NA PROTEÇÃO DE INFRAESTRUTURAS CRÍTICAS E O PAPEL DAS FORÇAS ARMADAS

MAJ TM Pedro Manuel Monteiro Fernandes

Trabalho de Investigação Individual do CEMC 2018/2019

Pedrouços 2019

INSTITUTO UNIVERSITÁRIO MILITAR

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

A INTERVENÇÃO DAS FORÇAS DE SEGURANÇA NA PROTEÇÃO DE INFRAESTRUTURAS CRÍTICAS E O PAPEL DAS FORÇAS ARMADAS

MAJ TM Pedro Manuel Monteiro Fernandes

Trabalho de Investigação Individual do CEMC 2018/2019

Orientador: TCOR GNR/INF António Manuel Barradas Ludovino

Coorientador: TCOR GNR/CAV Marco Paulo A. de Rodrigues Gonçalves

Pedrouços 2019

Declaração de compromisso Antiplágio

Eu, **Pedro Manuel Monteiro Fernandes**, declaro por minha honra que o documento intitulado **"A Intervenção das Forças de Segurança na Proteção de Infraestruturas Críticas e o papel das Forças Armadas"** corresponde ao resultado da investigação por mim desenvolvida enquanto auditor do **CEMC 2018/2019** 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**, 13** de **maio** de **2019**

PEDRO MANUEL MONTEIRO FERNANDES

Assinado de forma digital por PEDRO MANUEL MONTEIRO FERNANDES
Dados: 2019.06.17 22:13:20 +01'00'

Pedro Manuel Monteiro Fernandes

Agradecimentos

O presente trabalho de investigação não poderia chegar a bom porto sem o precioso contributo e apoio de várias pessoas que me ajudaram a trilhar este caminho até ao fim.

Em primeiro lugar, não posso deixar de agradecer ao meu orientador, o Tenente-Coronel António Ludovino, pelo apoio, dedicação, conhecimento e atenção disponibilizada de forma permanente ao longo deste percurso. De igual forma agradeço também ao meu coorientador, o Tenente-Coronel Marco Gonçalves, que muito me ajudou, principalmente na fase de elaboração do projeto de investigação.

Em segundo lugar, agradeço a todos os entrevistados, nomeadamente ao Subintendente João Pestana, ao Major Pedro Ares, ao Tenente-Coronel Pedro Graça, ao Engenheiro Lino Santos e ao Capitão-de-mar-e-guerra Vizinha Mirones pela sua disponibilidade e apoio manifestado e pelos relevantes dados fornecidos nas entrevistas concedidas. Igualmente agradeço aos 15 Comandantes Territoriais da Guarda Nacional Republicana que de forma anónima muito contribuíram para este estudo.

Em terceiro lugar, agradeço a todos quantos, direta e indiretamente, me apoiaram neste trabalho, aos quais deixo uma palavra de apreço e gratidão, especialmente aos meus amigos e camaradas do Curso de Estado-Maior Conjunto 2018/2019.

Por fim, o meu profundo e sentido agradecimento vai para as mulheres da minha vida, a Marisa, a Mafalda e a pequena Corolina nascida no decorrer deste trabalho, pelo tempo que lhes roubei para poder “levar esta carta a Garcia”.

A todos, muito obrigado.

Índice

Índice de Apêndices

Índice de Figuras

Índice de Quadros

Resumo

Tomando como objeto de estudo as infraestruturas críticas, este trabalho de investigação tem como objetivo analisar a intervenção das forças de segurança na proteção dessas infraestruturas e identificar situações em que as Forças Armadas possam ser utilizadas nesta área. Pretende-se assim, perceber qual o estado atual desta temática em Portugal com vista a propor melhorias ao respetivo sistema.

Assim, seguindo um raciocínio dedutivo, a partir dos conceitos legalmente definidos, percorre-se uma metodologia baseada numa estratégia qualitativa, usando o estudo de caso da Guarda Nacional Republicana, para caracterizar a intervenção das forças de segurança na proteção das infraestruturas críticas. Deste modo, recorrendo a entrevistas a diferentes intervenientes e especialistas no assunto, e a um inquérito por questionário, para além cuidada análise documental, chega-se um conjunto de conclusões que retratam o atual estado de desenvolvimento destas matérias.

Dos principais resultados obtidos, destaca-se o facto de ser necessário conferir uma melhor coerência ao atual quadro legal, de garantir uma maior coordenação, harmonização de procedimentos e racionalização de meios e de tempo entre os diferentes intervenientes na proteção das infraestruturas críticas. Desta forma conseguir-se-á melhor preparar a intervenção nessas infraestruturas para fazer face a eventuais ameaças que se possam vir a concretizar, garantindo a sua continuidade e integridade que é essencial para manutenção de funções vitais para a sociedade.

Palavras-chave: Proteção de Infraestruturas Críticas, Forças de Segurança, Forças Armadas

Abstract

Concerning the critical infrastructures, this research aims to analyze the intervention of the security forces in the protection of these infrastructures and to identify situations in which the Armed Forces can be used in this area. The goal is to understand the current state of this issue in Portugal and propose some improvements to the respective system.

Thus, following a deductive approach, from the concepts legally defined, a methodology based on a qualitative strategy, using the case study of the National Republican Guard, is traced to characterize the intervention of the security forces in the protection of critical infrastructures. Therefore, through interviews with different actors and subject matter experts, and a questionnaire survey, in addition to careful documentary analysis, comes a set of conclusions that portray the current state of development of these matters.

As main results, we conclude that it is necessary to give a better coherence to the current legal framework, to ensure greater coordination, harmonization of procedures and rationalization of means and time between the different actors in the protection of critical infrastructures. In this way it will be better to prepare the intervention in these infrastructures to face possible threats that may come to fruition, guaranteeing their continuity and integrity that is essential for the maintenance of vital functions for society.

Keywords: *Critical Infrastructures Protection, Security Forces, Armed Forces*

Lista de abreviaturas, siglas e acrónimos

A

ANEPC	Autoridade Nacional de Emergência e Proteção Civil
ANPC	Autoridade Nacional de Proteção Civil
AR	Assembleia da República

C

CEDN	Conceito Estratégico de Defesa Nacional
CEMGFA	Chefe do Estado-Maior-General das Forças Armadas
CMG	Capitão-de-mar-e-guerra
CNCS	Centro Nacional de Cibersegurança
CNPCE	Conselho Nacional de Planeamento Civil de Emergência
CRP	Constituição da República Portuguesa
CSSI	Conselho Superior de Segurança Interna

D

DL	Decreto-Lei

E

EMGFA	Estado-Maior-General das Forças Armadas
ENCT	Estratégia Nacional de Combate ao Terrorismo
ENSC	Estratégia Nacional de Segurança do Ciberespaço
EUA	Estados Unidos da América

F

FFAA	Forças Armadas
FFSS	Forças de Segurança

G

GCS	Gabinete Coordenador de Segurança
GNR	Guarda Nacional Republicana
GNS	Gabinete Nacional de Segurança
GT-PIC	Grupo de Trabalho para a Proteção de Infraestruturas Críticas

I

IC	Infraestrutura Crítica
ICE	Infraestrutura Crítica Europeia
ICN	Infraestrutura Crítica Nacional
IUM	Instituto Universitário Militar

L

LSC	Lei de Segurança do Ciberespaço
LSI	Lei de Segurança Interna

M

Maj	Major

MDN	Ministério da Defesa Nacional
N	
NATO	Organização do Tratado do Atlântico Norte (OTAN)
O	
OE	Objetivo Específico
OG	Objetivo Geral
P	
PAO	Plano de Articulação Operacional
PAPARIC	Plano de Ação para a Proteção e Aumento da Resiliência das Infraestruturas Críticas
PCCCOFSS	Plano de Coordenação, Controlo e Comando Operacional das Forças e Serviços de Segurança
PCM	Presidência do Conselho de Ministros
PGR	Procuradoria-Geral da República
PIC	Proteção de Infraestruturas Críticas
PMA	Presidência e da Modernização Administrativa
PNPIC	Programa Nacional de Proteção de Infraestruturas Críticas
PSO	Plano(s) de Segurança do Operador
PSPE	Plano(s) de Segurança e Proteção Exterior
Q	
QC	Questão Central
QD	Questão Derivada
R	
RASI	Relatório Anual de Segurança Interna
S	
SG-SSI	Secretário-Geral do Sistema de Segurança Interna
SIS	Serviço de Informações de Segurança
SSI	Sistema de Segurança Interna
T	
TCor	Tenente-coronel
U	
UE	União Europeia
US DHS	*United States Department of Homeland Security*
W	
WEF	*World Economic Forum*

Introdução

A necessidade de proteção de ativos e serviços considerados simultaneamente estratégicos e críticos para a execução de funções vitais, como a atual sociedade assim o espera, tem raízes profundas (Lazari, 2014). Contudo, foi a partir dos ataques de 11 de setembro de 2001 nos Estados Unidos da América (EUA) que a área da Proteção de Infraestruturas Críticas (PIC) passou a ter maior relevo e importância para os diferentes países e organizações. Com efeito, é precisamente nos EUA que esta área tem tido maiores desenvolvimentos. Todavia, a nível europeu, só os ataques terroristas de Madrid e Londres realçaram o risco deste tipo de ataques contra infraestruturas europeias, pelo que em junho de 2004, o Conselho Europeu solicitou à Comissão que elaborasse uma estratégia global de PIC (União Europeia [UE], 2005). A sua materialização ocorreu através da Diretiva 2008/114/CE que estabelece um procedimento de identificação e designação das Infraestruturas Críticas Europeias (ICE) e uma abordagem comum relativa à avaliação da necessidade de melhorar a sua proteção, de modo a contribuir para a proteção das pessoas (UE, 2008). Esta diretiva teve posteriormente a sua transcrição para a legislação nacional através do Decreto-Lei n.º 62/2011 (Ministério da Defesa Nacional [MDN], 2011). Contudo, como consta da literatura (Martinho, 2017; Ferreira H. M., 2016; Pestana, 2016), vários anos volvidos, a implementação efetiva da totalidade das medidas inicialmente previstas parece estar ainda por finalizar, sendo que muitas questões ainda se levantam e estão em discussão.

No entanto, as ameaças contra Infraestruturas Críticas (IC) são bem reais, não só em termos físicos, mas também no ciberespaço. Ou melhor, as ciberameaças às infraestruturas e a outros ativos são uma preocupação crescente dos responsáveis políticos em todo o mundo (Hakim, Clark, & Blackstone, 2017). Em Portugal, essa ameaça vem explanada no último Relatório Anual de Segurança Interna (RASI) onde é referido concretamente que "a exemplo do que se verifica noutros países europeus, os ataques cibernéticos para exfiltração de informação e dados, mantiveram a tendência de crescimento já assinalada no ano anterior, realidade que ameaça a segurança dos dados e informação classificada à guarda de infraestruturas críticas […]" (SSI [Sistema de Segurança Interna], 2019, p. 85). Estará Portugal devidamente organizado, suficientemente empenhado e preparado para fazer face a estas ameaças? Num momento de desafios globais, riscos, ameaças, incertezas múltiplas e inquietantes, assiste-se a uma afirmação da Segurança Interna como pilar fundamental do Sistema de Segurança Nacional (Lourenço, Lopes, Rodrigues, Costa, & Silvério, 2015). Conjugado como o facto de Portugal viver uma época de contenção orçamental e de escassez

de recursos, torna-se cada vez mais necessário combinar esforços e meios, para se garantir uma resposta adequada face aos atuais desafios impostos à segurança e defesa nacional.

Nesse sentido, este trabalho de investigação que tem como tema – «A Intervenção das Forças de Segurança na Proteção de Infraestruturas Críticas e o papel das Forças Armadas», é relevante na medida em que se pretende apresentar contributos para uma melhor compreensão da problemática da PIC em Portugal, e quais os papéis que desempenham ou que poderão desempenhar diferentes entidades, nomeadamente as Forças de Segurança (FFSS) e as Forças Armadas (FFAA). Assim, depois da análise preliminar da literatura, definiu-se como objeto de investigação as IC, que serão abordadas na ótica da proteção das mesmas. Como delimitação ao objeto de estudo foram considerados os domínios temporal, espacial e concetual. A delimitação temporal é feita ao período posterior a 2001 até à atualidade, pois foi a partir dos ataques de 11 de setembro, que se começa a perceber a importância da proteção das IC. Em termos de espaço, o estudo limita-se ao território nacional, ou seja, aplica-se ao caso concreto Português. Por outro lado, visto a PIC ser uma área tão vasta e com a intervenção de diferentes entidades delimita-se esta investigação em termos concetuais à componente *security* (incluindo o *cyber*), deixando de fora a vertente *safety*, como explicitaremos mais adiante. De referir ainda que o presente estudo incide essencialmente na intervenção da Guarda Nacional Republicana (GNR), pois é esta força que tem na sua área de jurisdição cerca de 70% das IC identificadas até ao momento (Delgado, 2017, cit. por Martinho, 2017). Subsidiariamente foi também estudado o papel das FFAA, considerando o "critério da afetividade" que recomenda uma seleção do campo e tema específico ligado a uma forte motivação pessoal do investigador (Santos & Lima, 2016). Também, esta razão advém do próprio objetivo dos trabalhos de investigação do Instituto Universitário Militar (IUM), que visam produção de conhecimento em áreas de especial interesse para as FFAA e/ou GNR (IUM, 2018a).

O problema de investigação é um elemento central numa investigação porque, de alguma forma, dele derivam todos os outros elementos constituintes do processo (Santos & Lima, 2016). Assim, para orientar o estudo definiu-se como Objetivo Geral (OG) da investigação «Analisar a intervenção das forças de segurança na proteção das infraestruturas críticas e identificar situações em que as Forças Armadas possam ser utilizadas nesta área». Pela decomposição do OG em aspetos mais elementares formularam-se três Objetivos Específicos (OE). Também, visto que segundo Quivy e Campenhoudt (2008), a formulação do problema reveste geralmente a forma de uma pergunta, e no sentido de orientar e

sistematizar o processo de investigação, procedeu-se à identificação de uma Questão Central (QC) e formularam-se três Questões Derivadas (QD). Portanto, no Quadro 1, apresentam-se esquematicamente os objetivos e as questões de investigação.

Quadro 1 – Objetivos e questões de investigação

OG: «Analisar a intervenção das forças de segurança na proteção das infraestruturas críticas e identificar situações em que as Forças Armadas possam ser utilizadas nesta área»	
QC: «Como é que as forças de segurança conduzem a sua intervenção na proteção das infraestruturas críticas e em que situações as Forças Armadas podem ser utilizadas nesta área?»	
OE1: «Analisar o atual quadro legal Português relativo à proteção de infraestruturas críticas, verificando se este é inteligível, adequado e bem articulado»	**QD1**: «O atual quadro legal Português relativo à proteção de infraestruturas críticas é inteligível, adequado e bem articulado?»
OE2: «Caracterizar a intervenção da GNR na proteção das infraestruturas críticas»	**QD2:** «Como é que a GNR conduz a sua intervenção na proteção das infraestruturas críticas, se tem as capacidades adequadas e quais são as principais dificuldades e necessidades?»
OE3: «Identificar situações em que as Forças Armadas possam vir a ser utilizadas na proteção de infraestruturas críticas»	**QD3:** «Em que situações as Forças Armadas poderão ser utilizadas na proteção das infraestruturas críticas?»

A metodologia seguida, sustentada num raciocínio dedutivo e com uma estratégia de investigação essencialmente qualitativa, utiliza o estudo de caso da GNR para compreender a intervenção das FFSS na proteção das Infraestruturas Críticas Nacionais (ICN). Ou seja, o estudo desenvolve-se centrado na GNR, mas enquadrado pelas diversas entidades intervenientes na PIC, nas componentes *security* e *cyber*.

Este documento encontra-se estruturado em quatro capítulos e respetivas conclusões. Inicialmente começa-se por identificar o contexto em que a investigação se insere e apresenta-se o estado da arte nesta matéria, passando-se depois ao enquadramento concetual e explanação da metodologia seguida. No segundo capítulo caracterizam-se as IC no contexto nacional, refletindo-se sobre as ameaças e vulnerabilidades, bem como expondo o quadro legal em vigor. No capítulo seguinte apresentam-se as diferentes entidades analisadas neste estudo com intervenção na PIC, efetuando a análise documental, mas também utilizando dados recolhidos em entrevistas. Posteriormente, no quarto capítulo, são apresentados os resultados do estudo de caso da GNR, discutindo-se os principais resultados obtidos. Finaliza-se o trabalho com as conclusões, onde se recapitula as grandes linhas da investigação, apresentando também, outras possíveis opções a seguir em investigações futuras.

1. Enquadramento conceptual e metodologia

"No research without action, no action without research."

(Kurt Levin)

1.1. Identificação do contexto

Em Portugal, embora se tenha iniciado antes o desenvolvimento do projeto de PIC[1] com o objetivo de uma definição estratégica das infraestruturas nacionais a proteger, só em 2011 ganha suporte legal, através do Decreto-Lei n.º 62/2011 (DL 62) de 9 de maio (MDN, 2011) que, transpondo a Diretiva n.º 2008/114/CE do Conselho da União Europeia (UE, 2008), estabelece os procedimentos de identificação e de proteção das infraestruturas essenciais para a saúde, a segurança e o bem-estar económico e social da sociedade nos sectores da energia e transportes. É, pois, neste diploma que se estabelece a obrigatoriedade de elaboração de planos de segurança por parte dos operadores de IC e determina a existência de planos de segurança externos, da responsabilidade das FFSS e da proteção civil. Concretamente, em Portugal não existe uma entidade que exerça uma liderança formal nas matérias de PIC, sendo as competências repartidas entre a Autoridade Nacional de Proteção Civil (ANPC)[2] na área do *safety* e o Secretário-Geral do Sistema de Segurança Interna (SG-SSI) na área do *security* (Pais, 2016, cit. por Ferreira, 2016). Contudo, cabe ao SG-SSI a validação e homologação dos Planos de Segurança do Operador (PSO). Há ainda que acrescentar a estas duas dimensões a vertente *cyber*, uma área com legislação recentemente aprovada, nomeadamente a Lei 46/2018 de 13 de agosto (Assembleia da Républica [AR], 2018), designada de Lei de Segurança do Ciberespaço (LSC), que não vem prejudicar o cumprimento DL 62, mas antes acrescentar um conjunto de obrigações aos operadores de infraestruturas neste âmbito. Neste caso, a entidade com autoridade neste domínio é o Centro Nacional de Cibersegurança (CNCS). Portanto, em Portugal os principais intervenientes envolvidos na PIC, além dos respetivos operadores, são o SG-SSI com as FFSS

[1] Note-se que em Portugal, o projeto de PIC foi elaborado pelo então Conselho Nacional de Planeamento Civil de Emergência (CNPCE) que veio a ser extinto em 2012, passando as suas atribuições para a ANPC (Decreto-Lei n.º 73/2012, de 26 de março).

[2] A nova designação da ANPC é Autoridade Nacional de Emergência e Proteção Civil (ANEPC) conforme Decreto-Lei n.º 45/2019 (Presidência do Conselho de Ministros [PCM], 2019). Contudo, por esta designação ser bastante recente, optou-se por manter aqui a designação ANPC sendo fiel à diversa documentação e entrevistas analisadas.

territorialmente competentes, a ANPC e o CNCS, cada um com responsabilidade nas respetivas dimensões: *security*, *safety* e *cyber*.

Por outro lado, recentemente, alguns países, como por exemplo a França, têm recorrido às FFAA para missões de reforço da segurança pública (Mirones, 2017), pelo que importa analisar a possibilidade de intervenção das FFAA Portuguesas na PIC. Com efeito, no Conceito Estratégico de Defesa Nacional (CEDN) estão identificadas um conjunto de ameaças e riscos emergentes que devem ser tidos em consideração para a PIC, dos quais se destacam o terrorismo transnacional, o ciberterrorismo, a cibercriminalidade, os desastres naturais e as alterações climáticas (PCM, 2013).

Igualmente, a Estratégia Nacional de Combate ao Terrorismo (ENCT) prevê que "a cooperação entre as FFAA e as forças e serviços de segurança é aprofundada, no quadro constitucional e legal: […] Em situações de intervenção perante agressões terroristas […]. De acordo com o PNPIC [Programa Nacional de Proteção de Infraestruturas Críticas], atribuindo ainda especial atenção à vigilância e ao controlo das acessibilidades marítima, aérea e terrestre ao território nacional" (PCM, 2015a, p. 1022-(4)).

1.2. Estado da arte

Num processo de investigação deve ter-se em conta, na sua fase inicial, os contributos dados pelos autores de trabalhos sobre o mesmo tema, ou com ele relacionado (Santos & Lima, 2016). Assim, apesar de existirem já alguns autores (Natário & Nunes, 2014; Oliveira, 2015; Ferreira H. M., 2016; Pestana, 2016; Martinho, 2017; Ferreira A. , 2017) que recentemente se debruçaram sobre a temática, o tema em si é tão vasto que muito ainda há que investigar, particularmente no caso Português. Por exemplo, o estudo de Ferreira H. (2016) investigou sobre as metodologias de identificação e caraterização de IC, verificando que a metodologia da ANPC é baseada naquela usada em organizações e países de referência. Por outro lado, Ferreira A. (2017) considera que a análise das vulnerabilidades é um dos passos iniciais no processo de PIC, pelo que apresenta uma metodologia de análise de vulnerabilidades de IC, a qual foi testada e validada num aquartelamento militar, já desativado, mas sugerindo validar a aplicação do modelo proposto a uma IC nacional concreta. Já Martinho (2017) utilizando como objeto de estudo os procedimentos de identificação e de PIC, avalia o papel e o peso que o atual modelo de abordagem atribuiu às FFAA e forças e serviços de segurança no esforço interoperável para garantir a PIC, e propõe um modelo de procedimento de PIC, sustentado através de quatro fases estruturantes – (1) análise do risco do operador da IC, (2) elaboração do PSO, (3) planeamento de exercícios e

(4) elaboração do PNPIC. Contudo, desconhece-se a validação prática deste modelo, não tendo sido particularizado o que faz cada uma das entidades intervenientes. Deste modo, o presente estudo pretende continuar a desenvolver este tema da PIC, tão importante para a sociedade atual.

Já no que diz respeito a possíveis áreas de intervenção e cooperação das FFAA em matéria da segurança interna veja-se as situações que Borges (2013, cit. por Rebisco, 2016) identifica como possíveis para a colaboração em regime de complemento com as FFSS no combate a ameaças de cariz transnacional, das quais se destaca a defesa antiaérea, a defesa biológica e química, a inativação de engenhos explosivos, a ciberdefesa, a vigilância e fiscalização e operações especiais. O mesmo autor refere também que poderia haver o empenhamento de pequenos escalões das FFAA em apoio/reforço às FFSS no caso da PIC, de modo a que estas fiquem libertas para atuarem na ordem pública e mais genericamente em funções de natureza policial, sem ser necessário declarar um estado de exceção (Rebisco, 2016). Assim, importa perceber de um modo mais abrangente, mas detalhado, quais as capacidades e meios das FFAA, que podem eventualmente estar disponíveis para serem usados no âmbito da PIC. Veja-se o exemplo da Bélgica, em que as FFAA, sob controlo operacional da polícia, contribuem para a PIC e de pontos sensíveis e executam patrulhas conjuntas com a polícia e reforçando o dispositivo de segurança (Dubois, 2017, cit. por Mirones, 2017). Todavia, existem muitas barreiras, eventualmente legais, mas também concetuais, diferenças doutrinais, de formação, a génese operacional, etc., que vêm dificultar a possibilidade de articulação operacional das FFAA na segurança interna. Por exemplo, Lourenço (2015, p. 34) refere que "a utilização de forças militares em ações de intervenção junto da população civil tem merecido sérias dúvidas dos mais variados quadrantes académicos, políticos e de oficiais das FFAA e das forças policiais e de instituições internacionais", sendo que esta perceção parece permanecer ainda bastante atual.

1.3. Base concetual

Uma questão importante para prosseguir com a investigação, é a identificação dos conceitos nucleares a utilizar. A base concetual assenta essencialmente no normativo existente no edifício legal nacional, por esta matéria se encontrar legislada. Assim, um dos conceitos principais que importa perceber é o de «infraestrutura crítica», que é o objeto de estudo da presente investigação.

Ora, em Portugal a definição constante na legislação em vigor, e que é uma transcrição da legislação da UE entende uma IC como:

> a componente, sistema ou parte deste situado em território nacional que é essencial para a manutenção de funções vitais para a sociedade, a saúde, a segurança e o bem-estar económico ou social, e cuja perturbação ou destruição teria um impacto significativo, dada a impossibilidade de continuar a assegurar essas funções. (MDN, 2011; AR, 2018a)

Define-se também Infraestrutura Crítica Europeia (ICE) como a aquela IC:

> situada em território nacional cuja perturbação ou destruição teria um impacto significativo em, pelo menos, mais um Estado membro da União Europeia, sendo o impacto avaliado em função de critérios transversais, incluindo os efeitos resultantes de dependências intersectoriais em relação a outros tipos de infraestruturas. (MDN, 2011)

Contudo, importa aqui aludir ao facto de que a legislação hoje em dia tem um conjunto de conceitos que têm como elemento comum a criticidade, isto é, de regulação de algumas atividades que são consideradas críticas (L. Santos, entrevista presencial, 18 de março de 2019). Nesse sentido, além do conceito de IC, surge mais recentemente, o conceito de «serviço essencial» definido na LSC como "um serviço essencial para a manutenção de atividades societais ou económicas cruciais, que dependa de redes e sistemas de informação e em relação ao qual a ocorrência de um incidente possa ter efeitos perturbadores relevantes na prestação desse serviço" (AR, 2018a), sendo o «operador de serviços essenciais», "uma entidade pública ou privada que presta um serviço essencial" (AR, 2018a). Portanto, somos a abreviar que uma IC, conforme referido por J. Pestana (entrevista presencial, 22 de março de 2019), é crítica porque a interrupção desse serviço provoca um efeito cascata que impede outras IC de funcionar, sendo que esse conjunto de supressões de serviço tem um impacto muito forte na sociedade e num nível geograficamente alargado.

Vejamos agora o conceito de «proteção» que, por não ter sido transcrito para a norma Portuguesa, socorremo-nos da diretiva Europeia que a define como "todas as atividades destinadas a assegurar a funcionalidade, continuidade e integridade de uma infraestrutura crítica tendo em vista coarctar, atenuar e neutralizar uma ameaça, risco ou vulnerabilidade" (UE, 2008). Conjugando agora estas definições percebe-se o conceito de «proteção de infraestrutura crítica», que se resume como sendo as atividades destinadas a assegurar a funcionalidade, continuidade e integridade de uma infraestrutura que é essencial para manutenção de funções vitais para a sociedade.

1.4. Metodologia e método

O percurso metodológico da presente investigação seguiu de acordo como preconizado nas Orientações Metodológicas para a Elaboração de Trabalhos de Investigação (Santos & Lima, 2016) e conforme as normas de investigação em vigor no IUM[3], compreendendo as fases exploratória, analítica e conclusiva. Assim, na fase exploratória, foram pesquisadas fontes que permitiram uma compreensão do tema nas suas diferentes dimensões, bem como, a construção do problema de investigação e a definição dos objetivos. Depois de identificado e delimitado o objeto de estudo, definiu-se um modelo de análise com base na revisão da literatura (Apêndice A), que permitiu a construção dos instrumentos de recolha de dados. Na fase analítica, efetuou-se a análise documental, de entrevistas e de um questionário. Por fim, na fase conclusiva procurou-se responder às questões inicialmente levantadas, refletindo sobre a avaliação e discussão dos resultados.

Detalhando agora os métodos, procedimentos, técnicas e instrumentos de recolha e tratamento de dados e de interpretação de resultados (IUM, 2018a) utilizados, importa, em primeiro lugar, mencionar de forma clara o posicionamento filosófico do autor, adotado perante a presente investigação. Assim, em termos ontológicos, o autor posiciona-se no campo do construtivismo, por considerar que "os fenómenos sociais e os seus significados estão a ser executados pelos atores sociais" (Bryman, 2012, cit. por Santos & Lima, 2016, p. 18). Quanto ao posicionamento epistemológico, a posição é o interpretativíssimo, pelo que o estudo teve o foco nas organizações e as suas interações, sendo que as organizações são feitas por pessoas, competindo ao investigador não só verificar os fenómenos, mas também compreender os significados subjetivos desses mesmos fenómenos sociais (Bryman, 2012, cit. por Santos & Lima, 2016). A metodologia de investigação adotada foi baseada no raciocínio dedutivo, com uma estratégia de investigação essencialmente qualitativa, de natureza descritiva, tendo como objetivo alcançar um entendimento mais profundo e subjetivo do objeto de estudo, sem preocupações com medições e análises estatísticas (Vilelas, 2009 cit. por Santos & Lima, 2016). Quanto ao desenho de pesquisa, foi adotado o estudo de caso, onde se procurou recolher informação sobre um fenómeno particular inserido no seu contexto (Saunders, Lewis, & Thornhill, 2009). Ou seja, procurou-se recolher informação sobre a intervenção da GNR na PIC inserido no seu contexto. As técnicas de recolha de dados utilizadas foram principalmente a análise

[3] Nomeadamente, a NEP/INV-001 – Trabalhos de Investigação (IUM, 2018a) e a NEP/INV-001 – Estrutura e regras de citação e referenciação de trabalhos escritos (IUM, 2018b).

documental e a entrevista. Contudo, numa fase mais avançada da investigação recorreu-se também à elaboração de um inquérito por questionário, construído depois de realizadas as entrevistas, que apresenta basicamente as mesmas questões destas, mas num formato que mais facilmente permitiu recolher a opinião dos inquiridos. Ademais, e por o universo de aplicação dos questionários ser perfeitamente definido, este foi efetuado em formato anónimo, o que de alguma maneira assegura maior autenticidade nas respostas. Quanto à análise documental, esta assentou essencialmente na legislação Portuguesa, abordando também a da UE. Relativamente às entrevistas, estas foram focadas para a vertente operacional de intervenção na PIC, de carácter semiestruturado, e foram aplicadas a um conjunto de cinco especialistas das instituições que tratam do objeto de estudo (considerando a limitação deste), conforme se pode observar no Quadro 2, e que pela sua posição e responsabilidades têm um bom conhecimento do problema.

Quadro 2 – Informação relativa aos entrevistados

	Nome	Entidade	Função	Local e Data
E1	Subintendente João Pestana	SSI	Representante do gabinete da Secretária-geral do SSI no âmbito da Proteção de Infraestruturas Críticas	SSI, Rua Defensores de Chaves, Lisboa. Em 22 de março de 2019
E2	Maj Pedro Ares	SSI	Oficial de ligação da GNR no secretariado permanente do Gabinete Coordenador de Segurança do SSI	SSI, Rua Defensores de Chaves, Lisboa. Em 20 de março de 2019
E3	TCor Pedro Graça	GNR	Chefe da Divisão de Contrainformação e Segurança da Direção de Informações do Comando Operacional da GNR	Comando Geral da GNR, Lisboa. Em 06 de março de 2019
E4	Lino Santos	CNCS	Coordenador do CNCS	CNCS, Rua da Junqueira, Lisboa. Em 18 de março de 2019
E5	CMG Vizinha Mirones	EMGFA	Assessor militar do CEMGFA	EMGFA, Avenida ilha da Madeira, Lisboa. Em 26 de março de 2019
	Anónimo	GNR	Comandantes dos Comandos Territoriais (15 respostas de 20 possíveis)	Entrevista convertida para o formato de inquérito por questionário. Realizado em linha, de 2 a 10 de abril de 2019

A transcrição das entrevistas encontra-se no Apêndice B. Relativamente ao questionário (Apêndice C), que trata fundamentalmente as mesmas questões das entrevistas, mas convertidas para o formato de inquérito, este foi direcionado a todos os comandantes territoriais da GNR tentando-se, desta forma, aprofundar mais a problemática a um nível mais tático.

2. Caracterização das infraestruturas críticas

"Todos têm direito à liberdade e à segurança."

(Constituição da República Portuguesa)

Neste capítulo apresenta-se uma caracterização geral das IC, essencialmente a nível teórico, onde se reflete sobre as ameaças e vulnerabilidades e se percorre o quadro legal. Além da análise documental recorre-se já ao conteúdo das entrevistas recolhidas ao painel de especialistas selecionado. Deste modo, pretende-se aqui responder parcialmente à QD1.

2.1. Enquadramento

A rede elétrica, a rede de transportes e os sistemas de informação e comunicações são comumente reconhecidos como IC, e que são essenciais para manter as funções vitais da sociedade. Contudo, muitos mais setores são referidos na literatura como contendo IC, abrangendo também a componente cibernética (ver Figura 1).

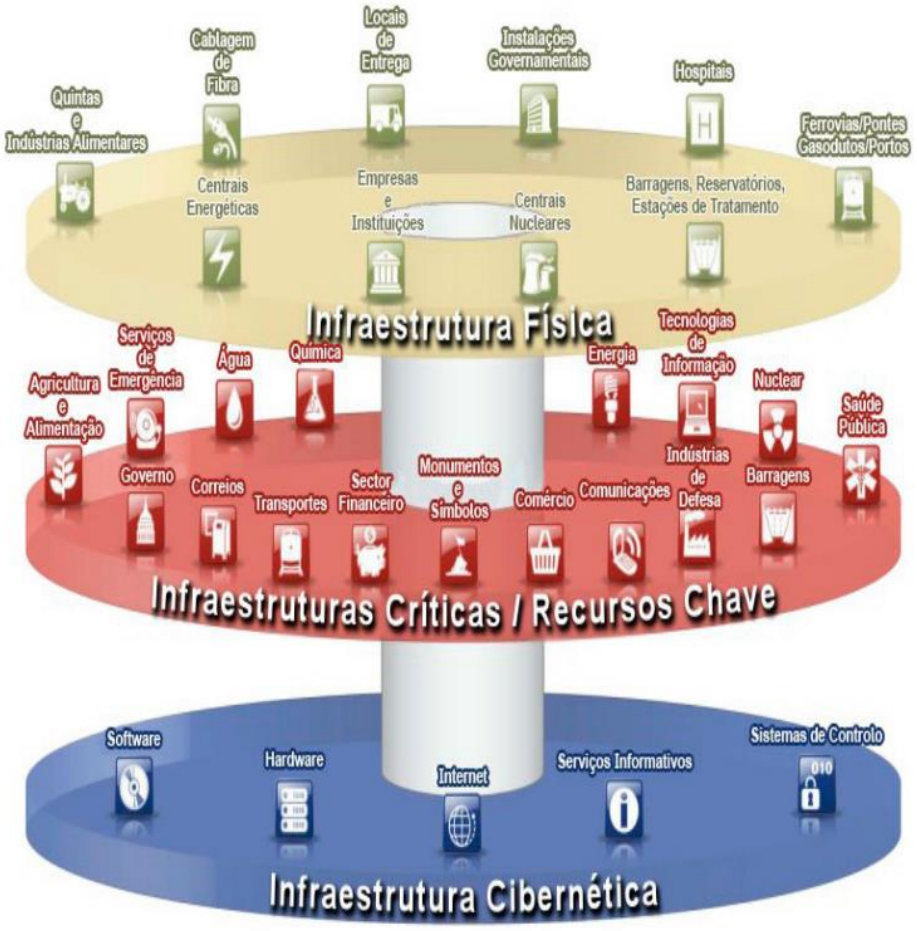


Figura 1 – IC nas suas componentes física e cibernética

Fonte: Natário & Nunes (2014).

Os EUA, por exemplo, identificam 16 sectores de IC, cujos os ativos, sistemas e redes, sejam eles físicos ou virtuais, são considerados vitais para o país (US DHS, 2019). Apesar disso, como veremos adiante, nem tudo o que se possa pensar *a priori* ser uma IC, pode efetivamente não sê-lo em termos formais/legais.

Concretamente, em Portugal, e de acordo com legislação em vigor, atualmente são considerados como IC apenas aquelas dos setores da energia e dos transportes. Mas se olharmos ao conceito de "serviços essenciais" apresentado no capítulo anterior, novos setores estão englobados, conforme se apresenta no Quadro 3.

Quadro 3 – Setores e subsetores das IC

Setor	**Subsetor**	**Decreto-Lei n.º 62/2011** "operadores de infraestruturas críticas"	**Lei n.º 46/2018** "operadores de serviços essenciais"
Energia	Eletricidade	X	X
	Petróleo	X	X
	Gás	X	X
Transportes	Transporte aéreo	X	X
	Transporte ferroviário	X	X
	Transporte marítimo e por vias navegáveis interiores (1)	X	X
	Transporte rodoviário	X	X
Bancário	-		X
Infraestruturas do mercado financeiro	-		X
Saúde	Instalações de prestação de cuidados de saúde		X
Fornecimento e distribuição de água potável	-		X
Infraestruturas digitais	-		X

(1) Neste diploma este subsetor é dividido em dois: a) Transportes por vias navegáveis interiores; b) Transportes marítimos, incluindo de curta distância e portos.

Contudo, J. Pestana (*op. cit.*) afirma que em Portugal considera-se que existem 12 sectores (Energia, Transportes, Comunicações/TIC, Indústria, Comércio, Serviços Financeiros, Órgãos de Soberania, Governação, Segurança e Defesa, Água, Alimentação e Saúde), o que leva a crer ser essa a tendência em futura revisão do DL 62.

2.2. Ameaças e vulnerabilidades

São imensas as definições encontradas na literatura para definir «ameaça» e «vulnerabilidade», por vezes díspares, e que podem levar a mal-entendidos. Por isso, em concordância com a delimitação do nosso objeto de estudo, adota-se nesta investigação o preceituado pelo SSI. Comecemos por apresentar o conceito de «ameaça» definido como:

> Qualquer acontecimento ou ação, ainda não concretizados mas passíveis de o serem, protagonizados por um agente com intenção e capacidade para os executar, que contrarie a consecução de um ou mais objetivos de uma qualquer entidade (desde um Estado ou uma organização pública internacional até comunidades ou indivíduos) através de danos materiais ou morais. (GCS-SSI, 2014)

Esta definição não considera vetores de outra natureza que não os derivados da ação intencional e da capacidade de um agente, o que leva à perspetiva da tradicional divisão entre *safety* e *security*, materializadas na metodologia em vigor, como veremos mais adiante.

Seguidamente importa perceber o conceito de «vulnerabilidade»:

> Qualquer fraqueza ou fragilidade, intrínseca ou provocada num determinado bem (infraestrutura, em sentido amplo, e tudo o que contenha) ou em quem tem a responsabilidade pela sua proteção, que possa ser explorada pela Ameaça para nele produzir um dano. Ou seja, se uma determinada fraqueza não for suscetível de ser explorada pela ameaça, ela não chega a ser uma vulnerabilidade. Desta forma, a identificação de vulnerabilidades implica não só o conhecimento da ameaça, mas também da forma como ela se poderá materializar junto do seu alvo. (GCS-SSI, 2014)

Olhando agora à probabilidade de uma dada fonte de ameaça explorar um determinado potencial de vulnerabilidade, levando a consequências danosas para a IC, chega-se ao conceito de «risco»:

> Resultado da avaliação da probabilidade de materialização da(s) ameaça(s) sobre uma infraestrutura e das respetivas consequências – que pode apresentar variações em função da sazonalidade. (GCS-SSI, 2014)

Isto é, risco = (ameaça x vulnerabilidade) x consequências. Este conceito é importante, na medida em que a gestão do risco deve ser o foco da atuação na PIC, devendo ser desencadeadas ações pró-ativas de gestão do risco destinadas a evitar que uma ameaça tente ou consiga destruir ou desativar uma IC (Lazari, 2014). No cálculo do risco, a probabilidade

é estimada em função da ameaça e da vulnerabilidade, pelo que importa perceber então quais as ameaças e vulnerabilidades com que nos deparamos nos dias de hoje e como o sistema nacional se encontra organizado.

Assim, em Portugal, existe um sistema de alerta no âmbito das medidas de segurança interna, que compreende, entre outros, os graus de ameaça em território nacional, sendo que estes se destinam a definir as diversas ameaças que impendem sobre instalações, sendo tidas em consideração, nomeadamente, para proteção e segurança de IC (GCS-SSI, 2014). Portanto, de acordo com os últimos RASI, a ameaça terrorista é classificada como moderada (SSI, 2018; SSI, 2019), ou seja, a segunda posição mais baixa numa escala de cinco níveis (5 - Reduzido, 4 - Moderado, 3 - Significativo, 2 – Elevado e 1 - Imediato), o que significa que não deve ser menorizada mas também não representa um nível que permita alocar mais recursos para lhe fazer face. Porquanto não há indícios que culminam na execução de atentados (SSI, 2018).

Não obstante, perante o atual quadro de ameaças e riscos associados à espionagem, Portugal tem um acervo considerável de interesses a proteger, quer nos domínios geoestratégico, político e militar quer nos setores vitais da sua economia, pelo que cabe aos Serviço de Informações de Segurança (SIS) produzir avaliações de ameaça que concorram para reduzir as vulnerabilidades e consequente diminuição dos riscos em caso de atentado terrorista, em particular contra IC ou outros alvos relevantes no quadro da segurança interna (SIS, 2019). Neste âmbito salienta-se o programa do SIS, apelidado de “Programa Krítica”, que tem em vista a melhoria da PIC, pontos sensíveis e outras infraestruturas relevantes de sectores económicos estratégicos portugueses, face a eventuais ameaças terroristas (SIS, 2019) sobre o qual, desde 2012, se têm desenvolvido uma série de atividades no âmbito da produção de avaliações de ameaça terrorista e de sensibilização dos operadores de IC. De facto, é reconhecido o contributo deste programa para o desenvolvimento de uma cultura de segurança integrada (SIS, 2019), mas será que o país está suficientemente empenhado na proteção das suas IC? Iremos tentar responder a esta questão ao longo do trabalho.

Paralelamente, o relatório mais recente sobre riscos globais do *World Economic Forum* (WEF) aborda alguns dos desafios mais prementes que hoje enfrentamos, onde inclui ameaças à segurança do ciberespaço, devido à tendência crescente do aumento da dependência deste domínio (WEF, 2019). Por isso, é cada vez mais importante ter em conta as ciberameaças, sendo estas provavelmente a maior vulnerabilidade da PIC, e não tanto o campo da ameaça física (P. Ares, entrevista presencial, 20 de março de 2019). Na verdade,

se olharmos ao CEDN de 2013 verifica-se que, entre os principais riscos e ameaças à segurança nacional que aí constam explanados e que interessam para o presente estudo, destaca-se a "cibercriminalidade, porquanto os ciberataques são uma ameaça crescente a IC, em que potenciais agressores (terroristas, criminalidade organizada, Estados ou indivíduos isolados) podem fazer colapsar a estrutura tecnológica de uma organização social moderna" (PCM, 2013). Um exemplo muito concreto, tendo inclusivamente já acontecido noutros países, seria um ciberataque à rede elétrica, que poderia colocar o país numa situação grave ou mesmo caótica.

Abordando agora, não a infraestrutura em si, mas todo o processo de PIC, foi questionado a todos os intervenientes selecionados para o corrente estudo, qual a sua perceção relativa à importância e às vulnerabilidades das IC. Foi referido que, de uma forma geral, existe a preocupação e o cuidado dos operadores em proteger as suas infraestruturas (J. Pestana, *op. cit.*)[4], até porque são eles próprios os principais interessados. Contudo, é também apontado como grande vulnerabilidade o modelo de *governance* da PIC, que deveria ter uma visão mais funcional e integrada, ou seja, que tivesse apenas uma "cabeça" (L. Santos, *op. cit.*). Também, como vulnerabilidades podem apontar-se outras questões organizacionais, e/ou legais que têm impacto na resposta concreta que é possível colocar na PIC. Do lado das FFAA, por exemplo, V. Mirones (entrevista presencial, 26 de março de 2019) aponta como vulnerabilidade nesta área a inexistência de um Plano de Articulação Operacional (PAO) entre as forças e serviços de segurança e as FFAA, conforme previsto na ENCT.

Em suma, dir-se-ia que muito há a evoluir em termos de coordenação de todas as áreas de proteção das IC, parecendo existir a falta de uma liderança formal nesta matéria que congregue todos os esforços da Nação, por forma a melhor estar preparada para enfrentar as possíveis ameaças.

[4] Os resultados mais concretos obtidos do estudo de caso da GNR são apresentados no capítulo 4.

2.3. Quadro legal

Vejamos agora o quadro legal vigente, apresentando-se para tal no Quadro 4 a legislação mais relevante no âmbito das IC, onde se pode constatar da multiplicidade de diplomas que aludem a esta temática.

Quadro 4 – Legislação relevante no âmbito das IC

Legislação nacional	
DL 62 Decreto-Lei n.º 62/2011 de 9 de maio (MDN, 2011)	Esta é a principal lei relativa às IC em Portugal. Nos termos do seu art.º 1.º tem por objeto estabelecer "os procedimentos de identificação e de proteção das infraestruturas essenciais para a saúde, a segurança e o bem-estar económico e social da sociedade nos setores da energia e transportes".
LSI Lei de Segurança Interna - Lei n.º 53/2008 de 29 de agosto, alterada pela Lei 59/2015 (AR, 2008)	De particular importância para a articulação das FFSS, necessários à gestão de incidentes tático-policiais graves, competência esta atribuída ao SG-SSI. Classifica como incidentes tático-policiais graves os que ocorram em IC. Por outro lado, refere também que as FFAA colaboram em matéria de segurança interna nos termos da Constituição e da lei, competindo ao SG-SSI e ao CEMGFA assegurarem entre si a articulação operacional.
ENCT Estratégia Nacional de Combate ao Terrorismo - RCM 7-A/2015 de 20 de fevereiro (PCM, 2015a)	Entre outros, vem elencar a necessidade de se desenvolver o Plano de Ação para a Proteção de Aumento da Resiliência das IC nacionais e europeias, com os respetivos PSO e planos de segurança externos da responsabilidade das FFSS e da ANPC. Refere também que a cooperação entre as FFAA e as FFSS é aprofundada em situações de intervenção perante agressões terroristas de acordo com o Plano de Articulação Operacional.
ENSC Estratégia Nacional de Segurança no Ciberespaço - RCM 36/2015 de 12 de junho (PCM, 2015b)	Tem como objetivo fortalecer e garantir a segurança do ciberespaço, das IC e dos serviços vitais nacionais.
LSC Lei de Segurança do Ciberespaço - Lei 46/2018 de 13 de agosto (AR, 2018)	Estabelece a estrutura de segurança do ciberespaço, e vem exigir o cumprimento de requisitos de segurança e obrigações de notificação de incidentes nomeadamente aos operadores de IC, bem como aos "operadores de serviços essenciais", que passam a ser definidos neste diploma.
CEDN Conceito Estratégico de Defesa Nacional RCM 19/2013 de 5 de abril (PCM, 2013)	Faz referência à implementação de um Programa Nacional de Proteção das Infraestruturas Críticas. Definem-se como linhas de ação prioritárias: garantir a proteção das infraestruturas de informação críticas, através da criação de um Sistema de Proteção da Infraestrutura de Informação Nacional.
Legislação Europeia	
Comunicação da Comissão relativa a um Programa Europeu de PIC - COM(2006) 786 final	
Diretiva n.º 2008/114/CE do Conselho da União Europeia (Concelho da UE, 2008).	

Tomando por base as entrevistas realizadas, praticamente todos os entrevistados reconhecem a necessidade de rever a legislação nacional existente no que diz respeito às IC, e à luz das novas ameaças, nomeadamente no domínio *cyber*. A prova disso é que já foi trabalho pelo SSI a atualização do DL 62, em coordenação com a ANPC, aguardando-se oportunidade legislativa para prosseguir com o diploma (J. Pestana, *op. cit*.). Mas este só deverá avançar depois da legislação Europeia nesta matéria ser atualizada (P. Ares, *op. cit*.). De facto, há aspetos sobre a segurança que não se justificam atualmente e que podem ser melhorados, nomeadamente o foco em questões mais operativas (J. Pestana, *op. cit*.). Ou seja, parece não haver dúvida relativa à necessidade de rever o DL 62 em vigor (que foi na altura a transposição da diretiva Europeia), sendo que um dos pontos essenciais a alterar passa por abranger outros sectores das IC.

No que concerne às infraestruturas de informação críticas, designadamente aos "operadores de serviços essenciais", conforme estipulado na LSC (AR, 2018a) recentemente aprovada, o caminho já começou a ser trilhado. Na identificação desses operadores não se teve em conta somente a questão da disrupção da infraestrutura, mas também o impacto do ponto de vista de funcionamento do mercado e não numa lógica de impacto direto societal, não estando ainda definido se vai ser exigido um plano de segurança semelhante ao PSO, pois pretende-se seguir uma lógica diferente (L. Santos, *op. cit.).* Isto é, o CNCS vai definir os requisitos que o operador tem de cumprir, nomeadamente exigir a análise de risco e a implementação de um conjunto de medidas a partir de um quadro de referência, posteriormente existirão mecanismos de auditoria para verificar se as medidas implementadas são ou não suficientes (L. Santos, *op. cit.).*

2.4. Planos

Indubitavelmente que a legislação é essencial, mas, para operacionalizar o que nela consta é por vezes necessário recorrer à construção de diversos planos. É o que acontece na área da PIC. Assim, pela análise da legislação enquadrante referida na secção anterior, chega-se a uma listagem de vários planos aí referidos, apresentando-se essa informação no Quadro 5, juntamente com um ponto de situação relativo à operacionalização de cada um desses planos.

Quadro 5 – Principais planos referidos na legislação com relevância para a PIC

PLANOS	Referido em					
	DL 62	**LSI**	**ENCT**	**ENSC**	**LSC**	**CEDN**
Programa Nacional de Proteção de Infraestruturas Críticas (PNPIC) Não existe efetivamente, pode dizer-se que o plano nacional é o conjunto de instrumentos que existem relacionados com esta matéria, tais como os PSO, os PSPE, a doutrina que se produz, etc. (J. Pestana, *op. cit.*). Um exemplo deste tipo de plano é o dos EUA, designado por *National Infrastructure Protection Plan* (US DHS, 2013).	-	-	X	-	-	X
Plano de Ação para a Proteção e Aumento da Resiliência das Infraestruturas Críticas (PAPARIC) Esse plano faz parte da estratégia, não é público, e visa operacionalizar o Decreto-Lei n.º 62/2011, estabelecendo uma lógica de tempo para que sejam realizadas determinadas ações, como por exemplo a conclusão dos PSO (J. Pestana, *op. cit.*).	-	-	X	-	-	-
Plano de Ação Nacional para a Proteção contra as Ciberameaças O CNCS desconhece a existência deste plano que está na alçada do SSI (L. Santos, *op. cit.*).	-	-	X	-	-	-
Plano de Segurança do Operador (PSO) Para estes planos existe uma matriz que é idêntica para todos, pelo que neste momento estão elaborados e todos aprovados para as IC identificadas (P. Graça, entrevista presencial, 6 de março de 2019).	X	-	X	X	-	-
Plano de Segurança e Proteção Exterior (PSPE) Estes planos são competência das FFSS sendo que, neste momento, está-se a estabelecer uma matriz comum e criar um plano tipo para as FFSS adaptarem depois à realidade local de cada IC (P. Graça, *op. cit.*).	X	-	X	-	-	-
Plano de Articulação Operacional (PAO) Este plano ainda não existe. Sendo que, nesta fase, está a ser discutido entre a SG-SSI e o CEMGFA os mecanismos e protocolos de atuação das FFAA na Segurança Interna (J. Pestana, *op. cit.*).	-	-	X	-	-	X
Plano de Coordenação, Controlo e Comando Operacional das Forças e Serviços de Segurança (PCCCOFSS) Este plano é classificado e regula o modo como se integra a intervenção das FFSS em caso de existir um incidente tático-policial, sendo que se for considerado um incidente tático-policial grave [como é o caso das IC], este é assumido pelo SG-SSI (P. Ares, *op. cit.*).	-	X	X	-	-	-

Note-se, porém, que sendo estes planos de natureza sensível, sujeitos a classificação de segurança, não foi possível a sua consulta, o que permitiria uma melhor perceção do que trata efetivamente cada plano. Mesmo assim, pela análise da legislação existente e pelos dados recolhidos nas entrevistas, consegue-se aqui retirar algumas ilações. Desde logo, que alguns deles, embora apareçam referidos na legislação, acabaram por não ser concretizados ou, mesmo passado alguns anos, estão ainda em fase de elaboração. Depois, verifica-se que o documento que mais planos elenca é a ENCT, e que atribui à Unidade de Coordenação Antiterrorismo a coordenação desses planos e das ações previstas nessa Estratégia (PCM, 2015a), o que nos permite inferir da associação que o legislador fez entre o terrorismo e a necessidade de aumentar a resiliência da IC. Também, de salientar que a referência ao PAO aparece inicialmente no CEDN e depois na ENCT.

Relativamente aos Planos de Segurança propriamente ditos são referidos dois: o PSO, da responsabilidade do operador da IC e o PSPE da responsabilidade da FFSS territorialmente competente. O PSO é elaborado e revisto anualmente pelos operadores e submetido a parecer prévio das FFSS e da ANPC, com vista à sua validação pelo SG-SSI (MDN, 2011). Este plano deve ser articulado com o PSPE, que deverá ser elaborado pela respetiva FFSS. Depois de um longo processo de identificação das ICN, neste momento não há PSO pendentes de aprovação (P. Graça, entrevista presencial, 6 de março de 2019) mas, o mesmo não se verifica relativamente aos PSPE que, não obstante oito anos volvidos desde a publicação da legislação que os refere, ainda se encontram por elaborar.

Por último, alude-se à resolução da Assembleia da República n.º 119/2018 que "recomenda ao Governo a conclusão urgente dos processos de classificação de ICN e de validação dos planos de segurança do operador das mesmas" (AR, 2018b), para concluir que muito ainda há por fazer relativamente aos planos de segurança para PIC.

3. A intervenção na proteção das infraestruturas críticas

"A coisa mais incompreensível sobre o mundo é que ele é compreensível."

(Albert Einstein)

Neste capítulo pretende-se, através de análise documental e análise das entrevistas, apresentar a forma como as diferentes entidades conduzem a sua intervenção na proteção das ICN, nomeadamente perceber qual o papel do SSI, das FFSS, do CNCS e das FFAA nesta matéria. Deste modo, pretende-se aqui responder parcialmente à QD2 e QD3.

3.1. Enquadramento

Analisando a organização, as atribuições e as competências que constam da legislação referida anteriormente são vários os intervenientes na PIC, conforme se pode observar na Figura 2.

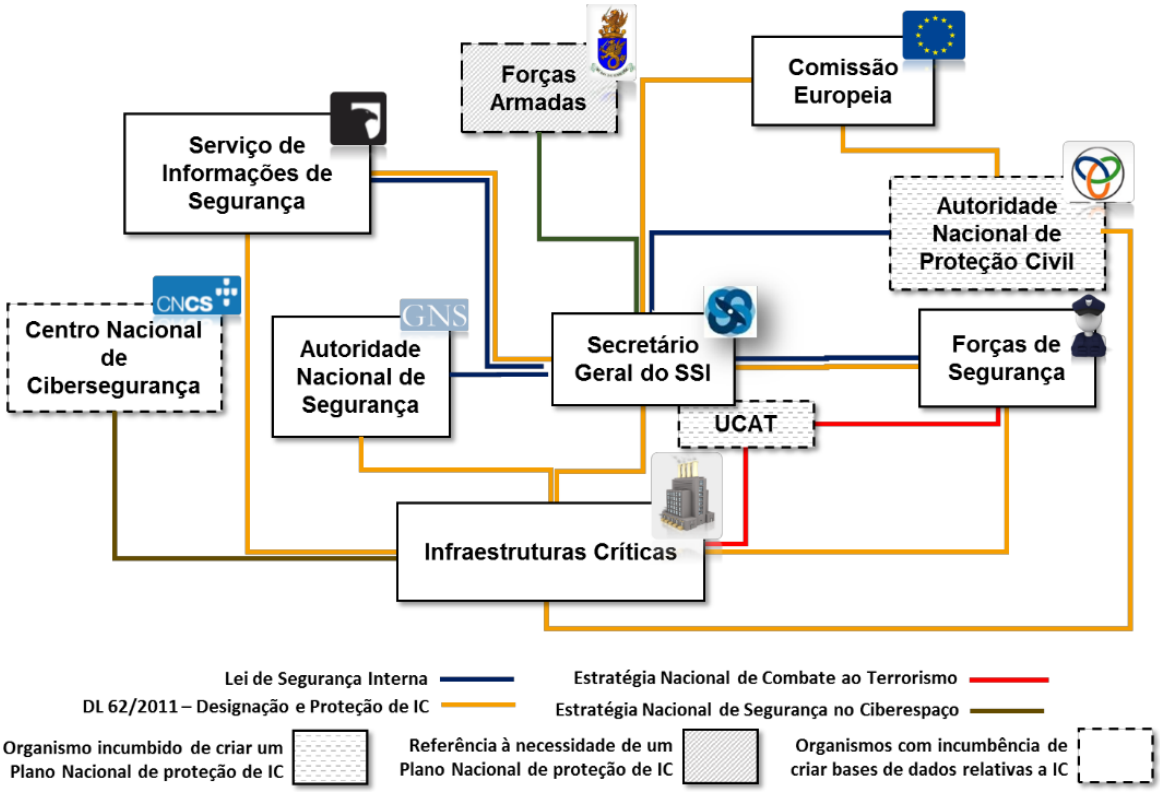


Figura 2 – Relações entre os diferentes atores intervenientes na PIC

Fonte: Pestana (2016).

Assim, constata-se que em Portugal, além da multiplicidade de intervenientes na PIC, as competências estão essencialmente repartidas entre o SSI, na vertente da segurança (*security*) e a ANPC, para o socorro (*safety*). Surge ainda na literatura a vertente *cyber*, mas

esta não está atualmente operacionalizada neste âmbito. Na Figura 3 pode-se observar o processo de elaboração e aprovação do PSO, onde se retratam estas três dimensões.

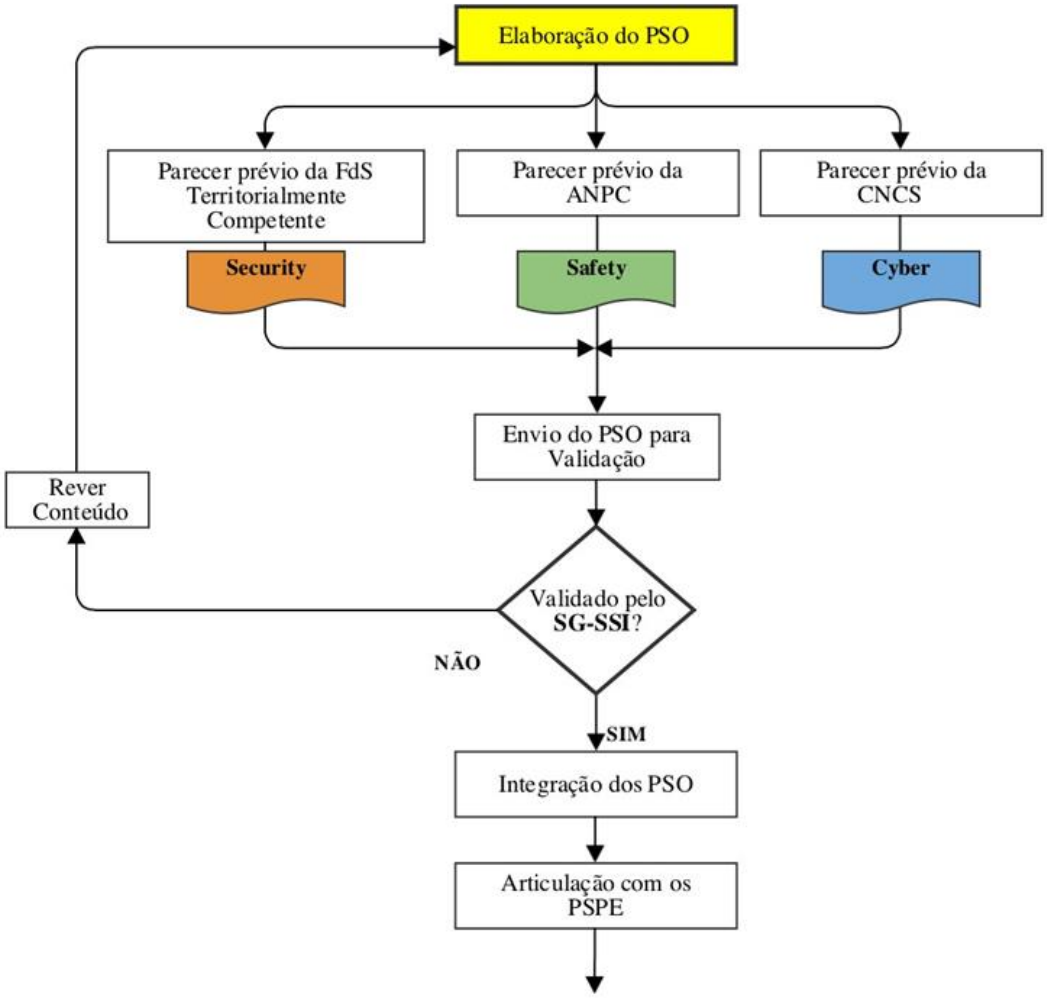


Figura 3 – Processo e entidades intervenientes no PSO

Fonte: Adaptado de Martinho (2017).

Vejamos de seguida mais pormenorizadamente as competências e atribuições de algumas dessas entidades.

3.2. O Sistema de Segurança Interna

O SSI assenta num modelo integrado de organização, que envolve as forças e serviços de segurança, a cooperação internacional e outros sistemas e serviços do Estado (SSI, 2018). Os órgãos do SSI são o Conselho Superior de Segurança Interna (CSSI), o SG-SSI e o Gabinete Coordenador de Segurança (GCS-SSI) (AR, 2008). Para o presente estudo importa manifestar a particular relevância do GCS-SSI, que é o órgão especializado de assessoria e consulta para a coordenação técnica e operacional da atividade das forças e dos serviços de segurança, funcionando na direta dependência do Primeiro-Ministro ou, por sua delegação,

do Ministro da Administração Interna (AR, 2008). Este é presidido pelo SG-SSI que coordena o secretariado permanente deste Gabinete que é constituído por oficiais de ligação provenientes de diversas entidades, nomeadamente da GNR e da PSP, mas efetivamente não integra elementos do CNCS nem das FFAA. Outrossim, na alteração da Lei de Segurança interna (LSI) de 2015 (AR, 2015) onde é, entre outros, acrescentado o coordenador do CNCS ao CSSI, deixa de fora o elemento do CNCS para o GCS-SSI, o que poderia aproximar mais a área *cyber* do *security*, colmatando a atual lacuna identificada. Isto é, a componente de cibersegurança dos PSO não é (ainda) trabalhada no CNCS, mas sim pela FFSS territorialmente competente.

Um importante plano no âmbito do SSI, e já mencionado no capítulo anterior, é o PCCCOFSS, que estabelece o conceito de Incidente Táctico-Policial como tratando-se da "ocorrência inopinada e de carácter reactivo, configurando uma situação de flagrante delito ou que exija a imediata intervenção policial, cuja natureza, características e resolução envolvam, por motivos diversos, o emprego de recursos que ultrapassem os, normal e quotidianamente, utilizados" (Rodrigues, 2014, p. 46). Neste âmbito, releva-se que, de acordo com as disposições da LSI, os ataques a infraestruturas classificadas como ICN são considerados incidentes tático-policiais graves, competindo ao SG-SSI, no âmbito das suas competências de controlo e através dos respetivos dirigentes máximos, a articulação das forças e dos serviços de segurança necessários (AR, 2008) para resolver o incidente.

Ainda relativamente ao SSI, de referir que cabe ao SG-SSI a aprovação dos PSO e PSPE, e que atualmente decorre sob a sua alçada o Grupo Trabalho para a Proteção das IC (GT-PIC) na componente *security*, e que conta com elementos das FFSS[5].

3.3. As Forças de Segurança

Como Forças de Segurança (FFSS) existentes em Portugal, e por a LSI (AR, 2008), não distinguir exatamente quais são as FFSS e quais são os Serviços de Segurança, considera-se neste trabalho aquelas normalmente referidas em sentido estrito, sendo elas: a GNR, a Polícia de Segurança Pública (PSP) e a Polícia Marítima (PM), como se pode verificar na Figura 4.

[5] Nesta investigação foram entrevistados três elementos desse GT: o chefe, o oficial de ligação da GNR no GCS-SSI e o oficial indicado pela GNR para integrar esse grupo.

Figura 4 – Forças Armadas e Forças e Serviços de Segurança

Fonte: GNR (2014).

Julgamos pertinente salientar a particular natureza da GNR que encontra o seu posicionamento institucional no conjunto das Forças Militares e das Forças de Segurança, para referir que esta força pode eventualmente assumir um papel mais preponderante na PIC. E é precisamente isso que a GNR identifica nas suas potencialidades, ou seja, a capacidade especialmente vocacionada para a segurança de IC (GNR, 2014).

Em termos genéricos, as FFSS têm o país dividido em razão do território, quanto à respetiva responsabilidade policial (Lourenço, Lopes, Rodrigues, Costa, & Silvério, 2015), pelo que a responsabilidade sobre a intervenção na PIC cabe à força competente na zona onde se localiza tal infraestrutura. Daí a relevância do papel do SSI em coordenar e uniformizar procedimentos relativos à atuação nas IC, como é o caso dos planos de segurança. Nesse sentido, cabe às FFSS a emissão dos pareceres para a componente *security* dos PSO, e a consequente elaboração do respetivo PSPE que se articule com o PSO e que traduz a resposta a dar caso haja um incidente numa IC. Neste particular, impõe-se acrescentar que "os procedimentos e a doutrina geral de empenhamento policial não se pode aplicar, sem a necessária adaptação, aos ambientes próprios (e geralmente perigosos) que caraterizam as IC" (Pestana, 2016), daí a relevância em se estruturar um plano de atuação. Ou seja, as forças têm que ter um padrão de conhecimento mínimo sobre as IC que estão na sua área, pelo que deverão treinar o respetivo plano.

3.4. O Centro Nacional de Cibersegurança

Cabe ao CNCS exercer os poderes de autoridade nacional competente em matéria de cibersegurança, relativamente ao Estado e aos operadores de IC nacionais (Presidência e da Modernização Administrativa [PMA], 2017). Como já foi anteriormente mencionado, o CNCS ainda não tem intervenção direta na elaboração dos PSO. Contudo, o atual coordenador do CNCS reconhece que ainda não existiu oportunidade para o fazer, mas, isso deveria ser feito pelo CNCS (L. Santos, *op. cit.*). E acrescenta: – "espero que o capítulo de cibersegurança do PSO passe a ser avaliado pelo CNCS. Em todo o caso, deveremos lá chegar pelo regime jurídico de segurança do ciberespaço, até porque o Estado daria uma péssima imagem se o mesmo operador recebesse instruções relativas ao mesmo tema de duas autoridades diferentes" (L. Santos, *op. cit.*). Também do lado das FFSS é reconhecido que o CNCS terá que ter um papel mais ativo e ser mais integrado na matéria da PIC, devendo caber-lhe a elaboração do parecer da componente *cyber* dos PSO (J. Pestana, *op. cit.*; P. Ares, *op. cit.*; P. Graça, *op. cit.*). Perante isto, impõe-se questionar: porque é que isso ainda não é assim? É certo que o CNCS ainda é um organismo relativamente recente, mas parece-nos que existe a necessidade de uma liderança que chame a si todas estas matérias por forma a incrementar o nível de operacionalização.

Abordando agora os "serviços essenciais", que não estão enquadrados nas IC ditas "clássicas" (J. Pestana, *op. cit.*) mas que tem a mesma essência de assegurar a continuidade de funções vitais para a sociedade, verifica-se que, se está a percorrer um caminho paralelo ao que tem vindo a ser feito para as IC. Esta abordagem resulta também da transposição de uma diretiva Europeia[6], sendo que, de acordo com o coordenador do CNCS, o que falta fazer é finalizar o procedimento de notificação de incidentes relevantes e estabelecer um critério que identifique o que é um incidente relevante num determinado sector (L. Santos, *op. cit.*).

Ou seja, não estão a ser exploradas sinergias entre o CNCS e os restantes intervenientes nas IC, podendo acontecer que uma dada infraestrutura possa ser classificada como IC pelo SSI/ANPC e simultaneamente como serviço essencial pelo CNCS. Não obstante, relativamente a matérias de cibersegurança, a lei prevê apenas uma Autoridade Nacional de Cibersegurança, que é o CNCS (L. Santos, *op. cit.*), pelo que este organismo deverá ser cada vez mais chamado a intervir.

[6] Diretiva (UE) n.º 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União.

3.5. As Forças Armadas

De acordo com Constituição da República Portuguesa (CRP), na sua atual redação, às FFAA incumbe a defesa militar da República e podem ser incumbidas, nos termos da lei, de colaborar em missões de proteção civil, em tarefas relacionadas com a satisfação de necessidades básicas e a melhoria da qualidade de vida das populações, e em ações de cooperação técnico-militar no âmbito da política nacional de cooperação (n.ºs 1 e 6 do artigo 275.º da CRP) (AR, 2019). Portanto, a atuação das FFAA em território nacional fora dos estados de exceção (AR, 2012), e em matéria de Segurança Interna tem levantado sérias dúvidas constitucionais. Os referidos estados, de sítio ou emergência, só podem ser declarados nos casos de agressão efetiva ou iminente por forças estrangeiras, de grave ameaça ou perturbação da ordem constitucional democrática ou de calamidade pública (AR, 2012). Assim, durante o estado de sítio as FFSS ficarão colocadas, para efeitos operacionais, sob o comando do Chefe do Estado-Maior-General das Forças Armadas (CEMGFA), por intermédio dos respetivos comandantes-gerais. Já no estado de emergência é previsto o apoio das FFAA às autoridades administrativas civis, nomeadamente às FFSS. Fora dos estados de exceção as relações de comando entre as FFAA e as FFSS não estão reguladas (Mirones, 2017) impondo-se ainda as dúvidas constitucionais à intervenção das FFAA na Segurança Interna. Neste contexto de dúvida, o Ministro da Defesa solicitou um parecer em outubro de 2001 à Procuradoria-Geral da República (PGR) questionando se as FFAA "podem ser incumbidas de colaborar em missões de prevenção de riscos colectivos e de apoio ou reforço de medidas de segurança a locais onde se situam instalações relevantes de sectores essenciais da vida nacional […] em casos de agressão ou de ameaças externas" (PGR, 2002). Este parecer enuncia a possibilidade do emprego das FFAA perante agressões ou ameaças externas, referindo, contudo, os diversos limites legais da atuação das FFAA em território nacional. Mas, este parecer retira qualquer vazio legal à argumentação da possível ilegalidade de atuação das FFAA em território nacional (Costa, 2017). Porém, não é objetivo desta investigação elaborar acerca dos aspetos legais relativos à intervenção das FFAA no âmbito da Segurança Interna, assunto já largamente estudado, embora com conclusões díspares, mas antes assumir essa possibilidade como pressuposto e, a partir daí, identificar situações em que as FFAA possam vir a ser utilizadas na PIC.

Assim, de acordo com o art.º 35.º da LSI, as FFAA colaboram em matéria de segurança interna nos termos da Constituição e da lei, competindo ao SG-SSI e ao CEMGFA assegurarem entre si a articulação operacional (AR, 2008). No entanto, essa colaboração ainda não se encontra operacionalizada, estando entretanto comtemplada na Diretiva Estratégica do CEMGFA para 2018-2021, que define exatamente uma linha de ação para desenvolver a articulação operacional para a proteção de ICN, em conjunto com o SG-SSI, e realizar exercícios interagências que permitam validar o plano (Estado-Maior-General das Forças Armadas [EMGFA], 2018). Neste sentido, estão a ser discutidos os mecanismos e protocolos de atuação das FFAA na Segurança Interna (J. Pestana, *op. cit.*). Assim, dependendo do que decorra do documento em discussão, podem ser elencadas algumas medidas no âmbito da PIC (J. Pestana, *op. cit.*).

Todos os entrevistados[7] são unânimes em considerar útil o emprego das FFAA na proteção das ICN, mas sempre de uma forma supletiva às FFSS. Como exemplo de situações concretas de empenhamento das FFAA, é referido a questão da vigilância e presença humana nas IC, a questão do controlo do espaço aéreo ou marítimo, entre outros apoios de ordem logística, comunicações, etc. É ainda mencionado que, e no âmbito da estratégia nacional do ciberespaço, as FFAA poderiam ter um papel mais ativo nesta área. Ou seja, as FFAA têm um papel também para a PIC, tem é que ser definido (P. Ares, *op. cit.*). Do lado das FFAA, e segundo V. Mirones (*op. cit*.) "as FFAA têm capacidade, mantendo a sua estrutura de comando, para apoiar as FFSS na segurança de IC e de pontos sensíveis [...] numa situação de necessidade justificante, em reforço e complemento, podendo a intervenção ocorrer, durante os estados de exceção, quando se verifiquem as condições previstas na Constituição da República ou, fora deles, quando a avaliação do SG-SSI indicar e suscitar tal necessidade".

Denota-se que o CEDN de 2013 tinha uma intenção de cada vez mais conjugar esforços e meios, na prossecução de uma resposta conjunta aos novos desafios securitários, intenção essa reforçada na ENCT, mas continua-se ainda sem definir o modo de articulação das FFAA na Segurança Interna, pelo que o papel das FFAA na PIC é atualmente praticamente inexistente.

Impõe-se ainda acrescentar que nas missões das FFAA, no âmbito da missão M1.6 - Ciberdefesa, menciona explicitamente o "apoio na proteção e defesa das ICN e do governo eletrónico do Estado" (MDN, 2014, p. 3), missão esta que deverá ser

[7] Para mais detalhe vide no Apêndice B as respostas à questão 5.2.

operacionalizada em coordenação com o CNCS. Há ainda a referência à "defesa de infraestruturas críticas" (MDN, 2014, p. 3), na missão M1.7 - Cooperação com as forças e serviços de segurança.

Por fim, não podemos escamotear o facto de a atuação das FFAA no âmbito da Segurança Interna ser um assunto sempre muito sensível, conforme foi notado no decorrer da presente investigação aquando das entrevistas efetuadas, o que pode colocar interesses corporativos à frente dos interesses da Nação, e que em nada contribui para a PIC. Não obstante, a opinião generalizada dos entrevistados é que as FFAA devem ser sempre usadas em último recurso e não como primeira linha de intervenção.

4. O caso da Guarda Nacional Republicana

"O que prevemos raramente ocorre; o que menos esperamos geralmente acontece."

(Benjamin Disraeli)

Neste capítulo apresentam-se os resultados do estudo de caso da GNR, permitindo refinar / complementar as respostas às três QD já parcialmente respondidas nos capítulos anteriores. Efetua-se aqui também a discussão dos resultados obtidos com vista a apresentar um conjunto de propostas que contribuam para melhorar a intervenção na PIC.

4.1. Enquadramento

A estrutura orgânica da GNR, conforme se pode observar na Figura 5, compreende a Estrutura de Comando, as Unidades e o Estabelecimento de Ensino. Assim, dentro Estrutura de Comando e fazendo parte dos órgãos superiores de comando e direção existe o Comando Operacional onde se encontra a Divisão de Contrainformação e Segurança, da Direção de Informações que é atualmente a estrutura responsável pelas IC ao nível operacional, sendo que o seu chefe integra o GT-PIC que decorre no SSI.

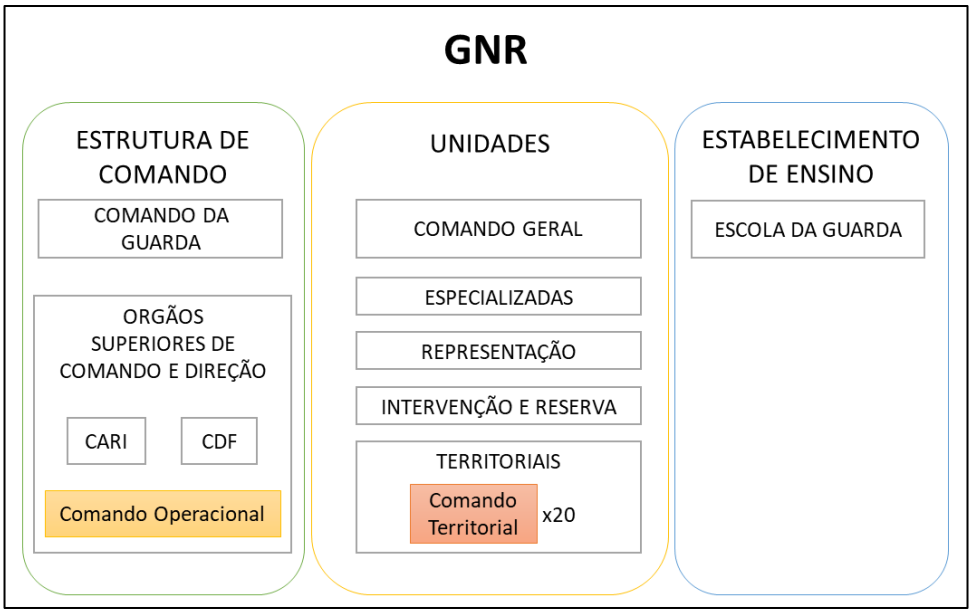


Figura 5 – Estrutura orgânica da GNR

Fonte: Adaptado a partir de GNR (2014).

Por outro lado, e descendo ao nível tático, verifica-se que GNR tem uma implantação em todo o Território Nacional, contando para tal com 20 Comandos Territoriais, incluindo o Comando Territorial da Madeira e o dos Açores. Deste modo, sendo as atribuições da

Guarda prosseguidas numa base territorial, cabe aos respetivos comandos a operacionalização da intervenção na PIC na sua área de responsabilidade. Note-se que, a GNR tem na sua área de jurisdição cerca de 70% das IC identificadas (Delgado, 2017, cit. por Martinho, 2017) daí a relevância desta força de segurança para o nosso objeto de estudo.

Olhando ao último Relatório de Atividades publicado pela GNR (GNR, 2017), esta força identifica nas suas potencialidades a "capacidade especialmente vocacionada para a segurança dos Órgãos de Soberania, e IC […]" (GNR, 2017, p. 45), pelo que revela do seu empenho na área das IC. Deste modo, visando concretizar as orientações plasmadas na Estratégia da Guarda (GNR, 2014), esta define como uma prioridade a edificação e melhoria das capacidades operacionais em várias áreas, onde se inclui a PIC. Concretamente, nesse documento, é referido que "atendendo à pertinência e atualidade da PIC, é urgente promover a organização, os processos, os procedimentos e os sistemas necessários à oportuna tomada de decisão que permitam a GNR adquirir uma maior capacidade de intervenção ao nível da segurança e resiliência das IC" (GNR, 2017, p. 62). Ainda nesse relatório, é elencada uma medida de "Consolidação da capacidade de Cibersegurança da GNR", em que, é reconhecida e necessidade de "[…] prevenir, prever e reprimir, de forma cada vez mais eficaz, as atividades criminais que decorrentes de atos preparatórios com origem no ciberespaço ou aquelas que põem em risco a segurança de Informação das ICN […]" (GNR, 2017, p. 63).

Portanto, é oficialmente reconhecida a importância que a GNR atribui à proteção das ICN e a respetiva necessidade de incrementar a sua capacidade de intervenção. Contudo, pretendeu-se perceber mais detalhadamente qual o nível de operacionalização atual que a GNR apresenta, apresentando-se na secção seguinte os resultados obtidos no inquérito efetuado aos Comandantes Territoriais.

4.2. Apresentação e discussão dos resultados

O questionário foi enviado aos 20 Comandantes Territoriais tendo sido obtidas 15 respostas. Do conjunto das questões, quatro destas são de resposta fechada sendo aqui apresentados os resultados em formato de gráfico. As restantes são de resposta aberta, pelo que a análise do respetivo conteúdo é apresentada em formato de tabela com indicação da percentagem de inquiridos que respondeu com determinada ideia-chave, aqui designada por segmento de resposta, o que corresponde a "uma análise tipológica por semelhança" (Santos & Lima, 2016, p. 122), ordenada por ordem decrescente de relevância.

4.2.1. Questões relativas à importância das infraestruturas críticas

Conforme destacado no segundo capítulo, em que foram elencadas algumas vulnerabilidades do sistema de PIC, pretendeu-se aqui obter a perceção junto dos inquiridos sobre a importância dada a esta temática pela GNR em particular, e pelo país em geral. Assim, efetuaram-se as questões A, B e C que a seguir se apresentam.

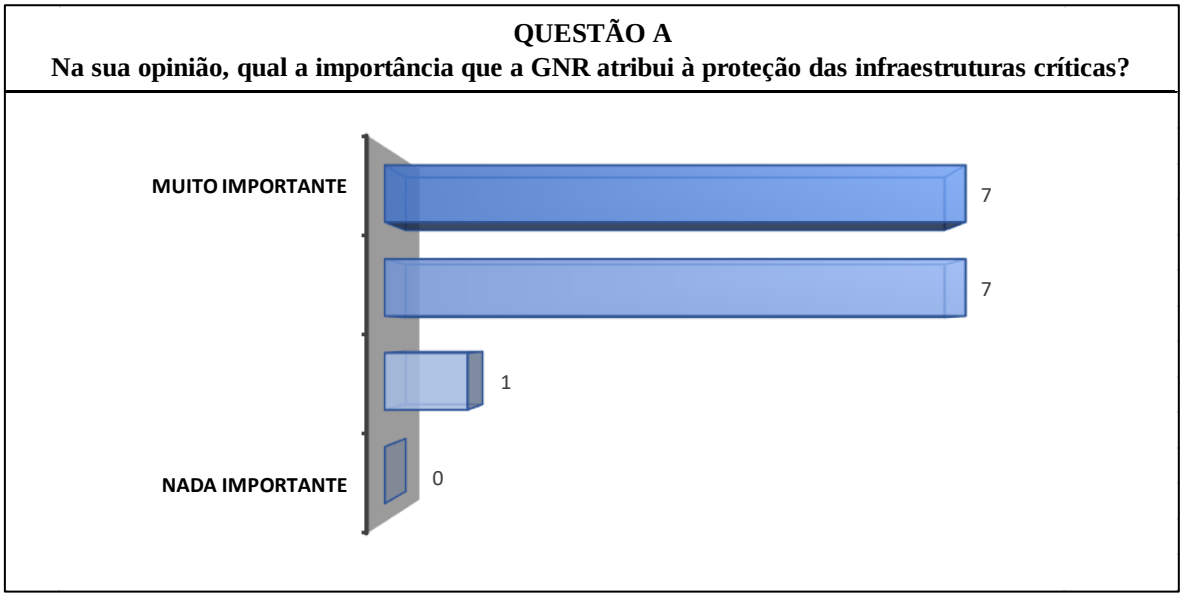


Figura 6 – Questão A

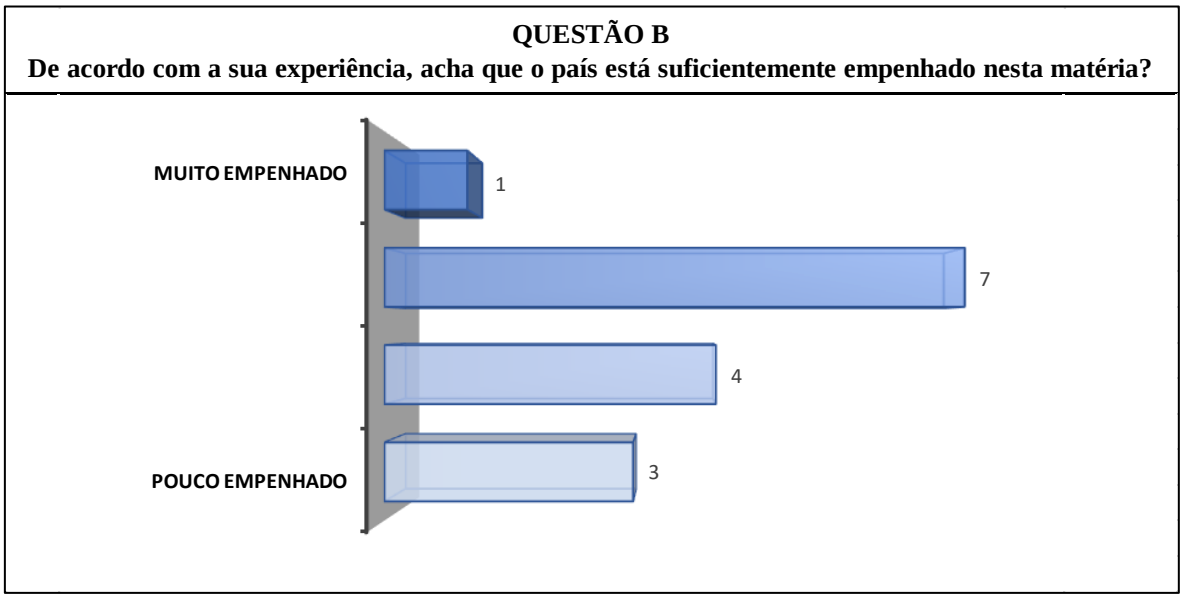


Figura 7 – Questão B

Portanto, podemos extrair como resultado que, praticamente todos os inquiridos consideram que a instituição a que pertencem, a GNR, atribui bastante ou muita importância à PIC, mas, já o país como um todo, não parece estar assim tão empenhado nesta matéria.

Inclusive três dos inquiridos atribui a classificação mais baixa em termos de empenhamento do país, o que revela que muito ainda há a fazer para atingir um nível adequado de proteção.

Vejamos agora quais as principais vulnerabilidades elencadas (Figura 8).

QUESTÃO C **Quais considera serem as principais vulnerabilidades nesta área, e que implicações isso acarreta?**		
Segmento resposta		**% Inquiridos**
C1	Falta de cultura de segurança e sensibilidade para a matéria / Falta de consciência das vulnerabilidades	27%
C2	Necessidade de sensibilização, formação e doutrina	20%
C3	A falta de segurança permanente / Falta de vigilância / Incumprimento das medidas de segurança adequadas	20%
C4	Escassez de recursos	13%
C5	Planos excessivamente burocráticos ou desadequados	13%
C7	Falta de planeamento	7%
C9	Falta da realização periódica de exercícios	7%
C10	Infraestruturas antigas, com sistemas de segurança baseados em mão de obra humana	7%
C11	Problemas de partilha de informação	7%
C12	Multiplicidade crescente de diferentes tipos de ameaça	7%
C13	O recrudescimento de atividades terroristas e de índole subversiva	7%
C14	Necessidade de maior coordenação entre as diferentes entidades responsáveis	7%
C15	As Forças de Segurança não disporem de meios aéreos próprios	7%
C16	Falta de investimento a vários níveis no processo	7%
C17	Os sectores básicos do Estado estarem a ser geridos por Empresas de capital estrangeiro	7%
C18	Redes viária e ferroviária; rede de captação, tratamento e distribuição de água; locais de armazenamento e processamento de explosivos e de armas	7%

Figura 8 – Questão C

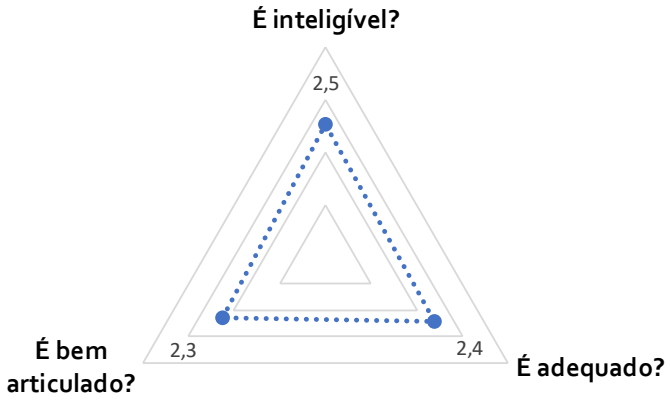
Verifica-se que as vulnerabilidades mais referidas são falta de cultura de segurança e sensibilidade para a matéria, a necessidade de sensibilização, formação e doutrina, como também a falta da vigilância permanente nas IC com o incumprimento das medidas de segurança adequadas. Com alguma relevância é referida a escassez de recursos e os planos serem excessivamente burocráticos ou desadequados. Outra questão apontada, refere-se à própria falta de consciência das vulnerabilidades, isto é, à falta de sensação da necessidade de proteção das IC.

Em termos de implicações, de salientar que "o incumprimento das medidas de segurança adequadas, pode colocar as IC numa situação risco. Pois considerar que nada acontece e que não existe insegurança no país pode levar a que não sejam atualizadas as medidas de segurança em função das circunstâncias atuais" – refere um dos inquiridos. Foi aludido também que a segurança das IC implica um enorme empenhamento de militares que atualmente não existem na GNR.

4.2.2. Questões relativas ao quadro legal

Passemos agora às questões relativas ao quadro legal, que se encontram sumarizadas na Figura 9.

QUESTÃO D
Como classifica o quadro legal existente relativo às infraestruturas críticas (proteção e intervenção)?



	Inquiridos															MÉDIA
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
É inteligível?	2	3	3	3	3	2	2	3	2	2	2	3	3	2	3	2,5
É adequado?	2	2	3	3	2	2	2	2	2	2	2	3	3	3	3	2,4
É bem articulado?	1	3	2	3	3	2	2	1	2	2	2	3	3	2	3	2,3

ESCALA: 1 - Nada / Mal | 4 - Completamente / Bem

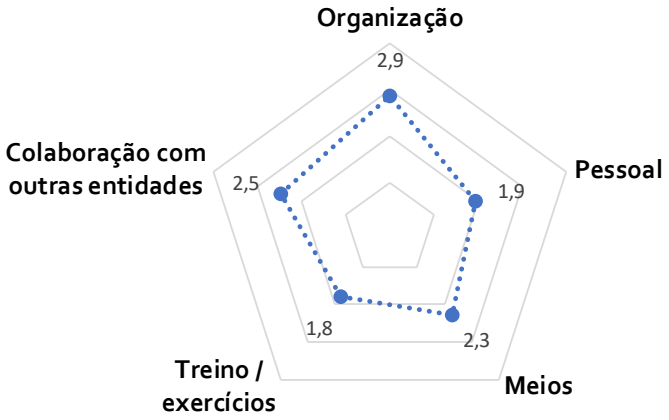
Figura 9 – Questão D

Aqui, destaca-se que em termos de adequabilidade, inteligibilidade e articulação, o valor é ligeiramente inferior para a articulação, tendo dois dos inquiridos respondido que o quadro legal é mal articulado. No geral, percebe-se por esta questão, que o quadro legal atualmente em vigor satisfaz pouco os inquiridos, devendo por isso ser melhorado.

4.2.3. Questões relativas às capacidades

Seguidamente apresentam-se os resultados das três questões (E, F e J) que pretendem percecionar se a GNR tem as capacidades adequadas para intervir na proteção das IC e quais são as principais dificuldades e necessidades. Estes resultados contribuem diretamente para dar resposta à QD2.

QUESTÃO E
As capacidades atualmente existentes na GNR são adequadas e suficientes para intervir na PIC?



	Inquiridos															MÉDIA
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
Organização	2	3	2	3	3	3	3	2	3	3	4	3	3	3	3	2,9
Colaboração com outras entidades	2	2	2	2	3	2	2	2	1	3	4	3	3	3	3	2,5
Meios	2	2	1	2	2	2	2	2	3	2	3	3	3	3	3	2,3
Pessoal	2	2	1	2	2	2	2	2	3	1	2	2	2	2	2	1,9
Treino / exercícios	2	1	1	1	2	2	2	1	1	2	3	3	2	2	2	1,8
															MÉDIA GLOBAL	2,3

ESCALA: 1 - Nada adequados / Insuficientes | 4 - Completamente adequados / Suficientes

Figura 10 – Questão E

Verifica-se que a média global obtida nesta questão é ligeiramente positiva, o que significa que as capacidades atualmente existentes na GNR são consideradas satisfatoriamente adequadas e suficientes para intervir na PIC. Mas registaram-se variáveis com pontuação negativa como é o caso do Pessoal e do Treino / exercícios, que demonstra a insatisfação relativamente a estes vetores de capacidade.

QUESTÃO F Na sua opinião, quais são as principais dificuldades e necessidades?		
Segmento resposta		**% Inquiridos**
F1	Treino / exercícios	33%
F2	Reforço de Pessoal	33%
F3	Formação específica	27%
F4	Reforço de meios Materiais	20%
F5	Coordenação e articulação da proteção das IC	20%
F6	Ausência de cultura relacionada com a importância das IC	7%
F7	Desinvestimento do Estado nas FFSS com vista à manutenção dessa capacidade	7%
F8	Imensidão de missões atribuídas	7%
F9	Prioridades no cumprimento da missão	7%
F10	Desenvolver e aprofundar o quadro legal, e modelos de intervenção segundo o grau de ameaça	7%
F11	Identificação das vulnerabilidades de cada tipo de infraestrutura e a conceptualização das medidas adequadas	7%

Figura 11 – Questão F

Nesta questão, os resultados confirmam o obtido na questão anterior, aparecendo a necessidade de realização de treino / exercícios e o reforço de pessoal como as principais necessidades a desenvolver na GNR para incrementar a PIC. Realçar ainda as necessidades identificadas da formação específica, além da necessidade de um reforço de meios materiais e uma melhor coordenação e articulação.

De destacar que, além do treino, surgiu a variável da formação que não foi previamente identificada na questão anterior, mas que aparece como relevante em termos de necessidades nesta área. Por outro lado, a variável mais pontuada da questão anterior, a Organização, não aparece agora aqui referida, permitindo concluir que, em termos de organização não se considera existir dificuldades e necessidades.

QUESTÃO G Quais deveriam ser as capacidades a edificar na GNR para incrementar a PIC?		
Segmento resposta		**% Inquiridos**
G1	Formação	33%
G2	Reforço de Pessoal	33%
G3	Reforço de meios Materiais	33%
G4	Treino	13%
G5	Doutrina	13%
G6	Criação de um plano de intervenção	7%
G7	A instituição deveria estar dotada de helicópteros e mais UAV	7%
G8	A GNR já possui capacidade e estruturas próprias vocacionadas para este tipo de missão específica	7%
G9	Especializar forças para a missão, entre a USHE e os DI dos CT	7%
G10	Efetuar levantamento exaustivo de todas as infraestruturas e voltar a classificar atribuindo níveis de risco atualizados	7%
G11	Um melhor acompanhamento por parte dos diversos órgãos da Guarda	7%
G12	Participar na conceptualização das IC e seguidamente estabelecer planos de segurança	7%
G13	A implementação de sistemas de videovigilância em complementaridade da segurança física	7%
G14	A missão da proteção de IC esta deveria ser atribuída à Unidade de Segurança e Honras de Estado, que deveria criar uma Subunidade para este fim	7%
G15	Um núcleo especializado para estudar a intervenção nas IC	7%
G16	Não sei	7%

Figura 12 – Questão G

Quanto às capacidades a edificar na GNR para incrementar a PIC, de realçar as necessidades de formação e a necessidade de um reforço de pessoal e de meios materiais. Com menor relevância é mencionado o treino e aparece também aqui a variável doutrina. Nesta questão pode também observar-se na Figura 12, algumas medidas concretas a implementar na GNR neste âmbito, como é o caso de atribuir a missão de PIC a uma subunidade criada especificamente para esse fim.

4.2.5. Questões relativas aos planos de segurança

Embora pelas entrevistas efetuadas antes da realização do inquérito, e como foi referido nos capítulos anteriores, se tenha percebido que os planos de segurança (PSO e PSPE) ainda não estão oficialmente nas mãos dos Comandantes Territoriais, fomos mesmo assim a questioná-los, por forma a perceber o nível de envolvimento destes comandos nos respetivos planos. Vejamos então as próximas duas questões.

QUESTÃO H **No seu entender, os Planos de Segurança da responsabilidade dos Operadores (PSO) estão a ser bem executados, são adequados e suficientes?**		
	Segmento resposta	**% Inquiridos**
H1	Falta coordenação e execução de simulacros / exercícios	40%
H2	Não sei / Desconheço / Sem opinião	33%
H3	Genericamente são suficientes / Cumprem o que a legislação determina / Podem ser melhorados	20%
H4	Insuficientes e pouco adequados	13%
H5	Planos de segurança nem sempre estão devidamente atualizados e concebidos em coordenação com todos os intervenientes na proteção das IC	7%
H6	As solicitações hoje são tantas que não há tempo para os testar e treinar a um nível desejável e quiçá prudente	7%
H7	Falta de comunicação entre as entidades responsáveis	7%
H8	Aqueles que conheço sim	7%

Figura 13 – Questão H

Relativamente aos PSO, apenas um terço dos inquiridos não respondeu a esta questão alegando desconhecimento ou falta de opinião no assunto, o que demonstra que a maior parte dos Comandos Territoriais tem, de alguma forma, um conhecimento de alguns dos PSO, o que é natural pois estes planos já têm vindo a ser desenvolvidos há algum tempo. Portanto, estes planos são considerados genericamente suficientes por 20% dos inquiridos, mas, o aspeto mais apontado sobre estes planos é a falta coordenação e execução de simulacros / exercícios (40% dos inquiridos). Contudo, há 13% dos inquiridos que consideram os PSO insuficientes e mesmo desadequados, sendo referido que, "na maioria dos casos não passam de meras intenções redigidas a escrito, uma vez que nunca foram realizados simulacros para aquilatar da sua adequabilidade e exequibilidade" – refere um dos inquiridos.

QUESTÃO I **Relativamente aos Planos de Segurança e Proteção Exterior (PSPE), que estão em elaboração, quais são as principais dificuldades da sua implementação?**		
	Segmento resposta	**% Inquiridos**
I1	Não sei / Desconheço / Sem opinião	47%
I2	Necessidade de testar os Planos de Segurança e posteriormente corrigir o que se mostrar necessário	7%
I3	Falta de meios, dificuldade nas acessibilidades às IC	7%
I4	Planos demasiado exaustivos e complexos que dificultam em muito a sua implementação	7%
I5	Pecam por falta de exercícios, por forma a os consolidar	7%
I6	As principais dificuldades residem na ineficaz integração de todas as entidades que têm participação nos PSPE, e a inexistente troca de informações relativas aos riscos e ameaças identificados nas IC	7%
I7	Falta de cultura de segurança	7%
I8	Adequação às reais necessidades, tendo por base uma completa identificação das ameaças	7%
I9	Adequação dos meios face à capacidade de resposta necessária	7%

Figura 14 – Questão I

Relativamente aos PSPE, e como era espectável, quase metade dos inquiridos alegou desconhecimento destes planos (relembra-se que ainda se está na fase de elaboração de um modelo de plano). Contudo, pelas respostas obtidas denota-se que algum trabalho tem vindo a ser feito ao nível dos Comandos Territoriais relativamente aos PSPE, elencando-se aqui aspetos como a falta de meios, a dificuldade nas acessibilidades às IC, a necessidade de testar os planos e posteriormente corrigir o que se mostrar necessário, as dificuldades de integração de todas as entidades que têm participação nos PSPE, entre outros.

4.2.7. Outras questões

No último bloco de questões pretendeu-se obter a sensibilidade dos inquiridos relativamente à participação das FFAA na PIC, entre outros comentários relativos à intervenção da GNR na PIC.

QUESTÃO J **Assumindo que as Forças Armadas pudessem colaborar na PIC (ultrapassados os aspetos legais e normativos), pode dar exemplos de situações em que estas pudessem ser utilizadas?**		
	Segmento resposta	**% Inquiridos**
J1	Não / Não vejo como / Não concordo / Não me pronunciarei	27%
J2	Segurança de perímetro exterior / Vigilância exterior e controlo de acessos / Segurança física	20%
J3	Garantir a proteção em situações de crise	7%
J4	Tendo em consideração a importância das IC e a capacidade da Guarda, poderiam apoiar, mas sempre sobe a coordenação da Guarda	7%
J5	Poderiam colaborar em ações de patrulhamento sob a coordenação das FFSS	7%
J6	Em reforço e estreita coordenação com a força de segurança territorialmente competente	7%
J7	As Forças Armadas só devem ser empenhadas de modo supletivo	7%
J8	Para libertar recursos humanos da GNR a empregar na multiplicidade das suas crescentes funções e responsabilidades	7%
J9	Só em casos limites	7%
J10	O emprego das FFAA em missões de segurança interna descaracterizá-las-á para o cumprimento das missões militares que estão na génese da sua existência	7%

Figura 15 – Questão J

De notar que embora alguns dos inquiridos não concordarem ou não se pronunciem sobre esta questão, os restantes entendem que as FFAA poderiam intervir na PIC, sendo, contudo, frisada que só em casos limites e, empenhadas de modo supletivo. Em termos de tarefas elencadas menciona-se a segurança de perímetro exterior, a vigilância exterior e controlo de acessos, mas também é referido a colaboração em ações de patrulhamento sob a coordenação das FFSS. Pertinente também é a referência à utilização das FFAA para libertar recursos humanos da GNR a empregar na multiplicidade das suas crescentes funções e responsabilidades.

Tendo sido deixado espaço em aberto para outros comentários relativos à intervenção da GNR na PIC considera-se preminente apresentar na Figura 16 as ideias recolhidas.

QUESTÃO K **Outros comentários relativos à intervenção da GNR na proteção das infraestruturas críticas:**	
	Resposta
F1	Assumir esta responsabilidade como força com caraterísticas e implementação territorial única.
F2	Importa, com a maior brevidade possível, que a GNR assuma as suas competências nestas matérias, designadamente com forças especializadas e promovendo a formação necessária para o efeito.
F3	O conhecimento é recurso essencial para contribuir para a prevenção.
F4	A GNR necessita ter um comportamento ainda mais proactivo nesta matéria, devendo reforçar as medidas de segurança, os meios humanos e materiais para minimizar os riscos das infraestruturas críticas.
F5	Natural necessidade de atribuir meios humanos e materiais às FFSS para as missões que lhe são naturalmente atribuídas.
F6	Face à importância da matéria a Guarda deveria ser mais interventiva (organizar/coordenar exercícios) e ter em consideração aquando da atribuição de meios (materiais e humanos).
F7	A GNR mantém atualizados os planos de segurança das infraestruturas que tem identificadas por iniciativa própria.
F8	A posição única da GNR, no Sistema de Forças Nacional, pela sua natureza e missões, evidencia a instituição por ser interoperável, quer com as Forças Armadas, quer com as restantes Forças e Serviços de Segurança. A GNR tem à sua responsabilidade policial mais de 95% do Território Nacional, sendo crucial para a proteção das IC.
F9	A limitação de recursos, sobretudo humanos.
F10	Não coloco em causa esse empenhamento e responsabilidade, antes pelo contrário, no entanto penso que importaria ter uma ideia mais consentânea com a real valia e capacidade de intervenção em caso de necessidade. Para tanto importava, a meu ver, fazer mais exercícios e simulacros que permitissem aferir e treinar o efetivo.
F11	A GNR, pela sua natureza militar, dispositivo territorial, conhecimento do TO e nível de qualificação técnico-profissional, ao nível da condução e execução de missões no âmbito da Segurança Interna, deverá assumir-se como EPR na segurança de áreas e pontos críticos, independentemente do grau de ameaça.

Figura 16 – Questão K

Deste conjunto de notas destaca-se o facto de que, importa com a maior brevidade possível, que a GNR assuma as suas competências na matéria da PIC, designadamente com forças especializadas e promovendo a formação necessária para o efeito, e depois fazer exercícios e simulacros que permitam aferir e treinar o efetivo, o que sintetiza a ideia geral sugerida na globalidade do inquérito.

4.3. Avaliação das descobertas e contributos para o conhecimento

O estudo de campo levado a cabo e a revisão da literatura efetuada, permite-nos elaborar sobre o estado atual da intervenção na PIC e propor algumas medidas com vista a melhorar essa atuação. Em primeiro lugar, verifica-se da necessidade de proceder à revisão do DL 62/2011, no sentido de o tornar mais inteligível e melhor articulado. A articulação e a cooperação são um aspeto de elevada importância, dada a diversidade das entidades intervenientes, pelo que deverá ser garantida uma liderança única sobre a matéria das IC.

Não se propõe a criação de mais um órgão para superintender a PIC, mas antes clarificar e reforçar as competências de determinadas entidades, nomeadamente do SSI. No caso específico da GNR, a criação de uma subunidade para intervir na PIC foi também uma hipótese evidenciada, sendo que, a existência de forças especializadas para atuar em IC seria, sem dúvida, uma mais-valia no sistema. Contudo, e face à dispersão territorial, parece óbvio que devem ser os Comandos Territoriais a desempenhar um papel fundamental, articulando-se com os respetivos operadores das IC na sua área de jurisdição.

De um modo geral, constatou-se que as capacidades atualmente existentes na GNR são consideradas satisfatoriamente adequadas e suficientes para intervir na PIC, mas existem muitos aspetos a melhorar, nomeadamente no reforço de pessoal atribuído aos Comandos Territoriais e na efetivação de treinos e exercícios que ponham à prova os respetivos planos. Algumas infraestruturas são antigas, com sistemas de segurança baseados em mão de obra humana, que implica enorme empenhamento de militares que atualmente não existem. Por isso, devem ser equacionados meios complementares como por exemplo a videovigilância para fazer face a eventuais ameaças a essas infraestruturas. De notar que a maioria das IC pertencem ao sector privado, pelo que, ao contrário do passado, o Estado passa a ter um papel mais regulador e menos interventivo, pelo que deve ser privilegiada a relação entre o setor público e o privado. Todos os diferentes *stakeholders* devem trabalhar em conjunto, criando oportunidades de cooperação, de forma a reduzir o risco de degradação ou destruição da operacionalidade das IC.

Um dos principais obstáculos identificado prende-se com o incumprimento das medidas de segurança adequadas, o que pode colocar as IC numa situação risco. Considerar que nada acontece e que não existe insegurança no país pode levar a que não sejam atualizadas as medidas de segurança em função das circunstâncias atuais. Isto deve-se aos diminutos, ou quase inexistentes, ataques dirigidos a estas infraestruturas, o que não possibilita uma cultura de segurança adequada nesta matéria em Portugal.

Assim, os planos existentes, apesar de cumprirem de uma forma geral com a legislação, revelam-se inadequados para diversas infraestruturas, apresentam-se por vezes excessivamente burocráticos e não são treinados de forma periódica, o que implica que em casos de acidentes certamente existirá confusão na execução dos mesmos.

Considerando o explanado até este momento, muito há a melhorar no sistema de PIC, sendo que outros atores poderão ser envolvidos como é o caso das FFAA. Veja-se a Figura 17 que resume de forma esquemática a intervenção das FFSS na PIC e o enquadramento que

as FFAA poderão ter nesta matéria. De notar que, quando a intervenção seja considerada no âmbito de um incidente tático-policial, o controlo é assumido pelo SSI, e será esta a situação que se vislumbra possível de atuação das FFAA, mas sempre numa lógica de supletividade e não numa primeira linha de intervenção.

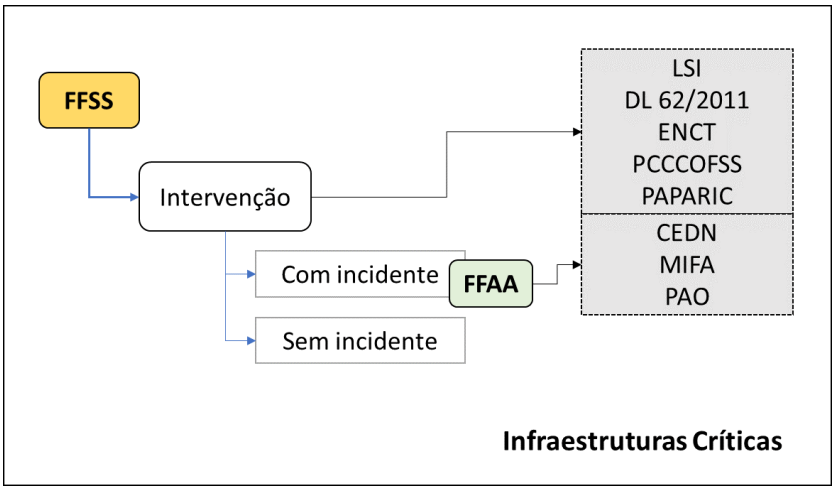


Figura 17 – Intervenção nas IC

Um exemplo concreto será a intervenção das FFAA na vigilância / segurança exterior de uma IC, numa situação extrema em que a GNR não dispusesse de recursos suficientes, que desta forma os libertaria para outras atividades. Contudo, isso tem implicações legais, nomeadamente quanto à legitimidade de uma ordem dada por esses militares a qualquer cidadão, bem como à utilização de armamento, por isso será necessário definir exatamente quais a regras de empenhamento a aplicar nessas situações. Por outro lado, o envolvimento das FFAA na PIC permitiria também adquirir o conhecimento necessário para incrementar a segurança das instalações militares e de pontos sensíveis contra a ameaça terrorista, pois estariam mais integradas em todo o sistema nacional, sendo que numa situação de exceção (estado de sítio e o estado de emergência) estariam muito melhor preparadas para desempenhar a sua missão.

Conclusões

Sendo de relevante importância, o debate sobre a identificação das infraestruturas que devem ser consideradas como críticas, não foi intenção deste trabalho abordar essa questão já largamente desenvolvida em contexto de investigação, mas antes partir da base de que as IC estão perfeitamente identificadas e focar o nosso estudo na proteção dessas infraestruturas, nomeadamente na forma como as FFSS conduzem a sua intervenção. Assim, em termos de trabalho de campo, foram realizadas entrevistas a diversos especialistas acerca do objeto de estudo – as IC –, pessoas que conhecem o tema, e que pela sua posição e responsabilidades, têm um bom conhecimento do problema. Deste modo, fizeram parte deste estudo elementos do nível operacional e tático, não se pretendendo obter contributos de questões mais de âmbito estratégico.

Tendo sido tomado como estudo de caso a GNR, por ser a força com a maior quantidade de IC na sua área de jurisdição, a primeira entrevista foi conduzida ao responsável pela área das IC nesta força de segurança. Seguidamente foram conduzidas entrevistas a outros elementos do grupo de trabalho criado no SSI para esta temática. Fruto da área *cyber* identificada na revisão da literatura como integrante da PIC, e confirmada nas entrevistas, foi também entrevistado o coordenador do CNCS, a fim de melhor se entender como esta área se integra na PIC. Posteriormente, e sendo também objetivo do trabalho perceber qual o papel das FFAA nesta matéria, foi também entrevistado o assessor militar do CEMGFA que está envolvido na operacionalização dos mecanismos de cooperação entre as FFAA e as FFSS. Por fim, foi aplicado um inquérito por questionário dirigido a todos os Comandantes Territoriais da GNR, tendo sido obtidas 15 respostas das 20 possíveis. Deste modo, o método dedutivo utilizado, em que, partindo da base concetual se fez o caminho do geral para o particular, associado à abordagem qualitativa que foi utilizada nesta investigação com o objetivo de descrever e interpretar, mais do que avaliar, permitiu chegar a algumas conclusões e atingir os objetivos inicialmente definidos. Assim, estamos em condições de responder à QC – «Como é que as forças de segurança conduzem a sua intervenção na PIC e em que situações as FFAA podem ser utilizadas nesta área?».

Em primeiro lugar, de referir que além da diversa legislação enquadrante, nomeadamente a LSI e as diferentes leis orgânicas, o diploma central para a PIC é o DL 62/2011 que, pelo exposto ao longo do trabalho, necessita de uma revisão para responder a uma melhor adequação à realidade atual. Entre outras alterações, a inclusão de outros sectores para integrarem a classificação de IC, para além dos atuais sectores da energia e dos

transportes, parece bastante relevante e necessária. Ainda neste especto, uma melhor articulação entre o conceito de IC com o de "serviço essencial" (no âmbito da lei do ciberespaço), sendo que este último que já se aplica a mais setores, permitiria uma melhor integração e resposta face aos atuais desafios securitários. Portanto, a necessidade de revisão do DL 62/2011 ficou bem evidenciada ao longo da investigação, parecendo, no entanto, não existir neste momento opção política para o concretizar, apesar da revisão técnica do diploma já ter sido levada a cabo. Deste modo, julga-se respondida a QD1 – «O atual quadro legal Português relativo à PIC é inteligível, adequado e bem articulado?», ou seja, o quadro legal é satisfatório, mas necessita de melhorias.

Em segundo lugar, importa relembrar que a intervenção na PIC envolve diversas entidades, sendo que o SSI desempenha um papel fundamental, como a entidade que aprova os principais planos nesta matéria, isto é, os PSO e os PSPE. Contudo, se por um lado todos os PSO das IC identificadas até ao momento se encontram aprovados, por outro lado, ainda se está em fase de definição de um modelo de PSPE. Portanto, pode dizer-se que a efetiva intervenção das FFSS na PIC ainda está numa fase inicial, existindo ainda um reduzido número de exercícios ou simulacros, face ao treino que seria desejável, conforme demonstram os dados de campo obtidos nesta investigação. Nesse sentido, deve ser evitado que os planos sejam excessivamente burocráticos e que prevejam a realização periódica de exercícios, pois em caso de incidentes nas IC certamente existirá confusão na execução dos planos se estes não tiverem sido previamente treinados.

Em terceiro lugar, e tomando o caso de estudo da GNR, constata-se que genericamente esta força detém as capacidades adequadas para intervir na PIC, mas sobressaíram do estudo algumas áreas onde será necessária alguma ação ou melhoria. Desde logo, a falta de pessoal ao nível de alguns Comandos Territoriais para a imensidão de missões que lhes estão atribuídas, pelo que existe a necessidade de um reforço de meios humanos que se possam dedicar a estas tarefas da PIC. Depois, é também elencada a necessidade de reforço de meios materiais. E é também apontado a necessidade de uma melhor coordenação e articulação dos diferentes intervenientes na PIC. Ademais, para incrementar a efetiva intervenção na PIC, e como referido por alguns dos inquiridos, uma subunidade vocacionada para intervir em IC seria uma mais-valia, pelo que se propõe que seja equacionado no seio da GNR esse desiderato. Por fim, de referir que entre as principais vulnerabilidades enunciadas destaca-se a falta de uma cultura de segurança e sensibilidade para a matéria, pelo que a necessidade de sensibilização e formação revelam-se de particular importância para PIC. Portanto, assim se

responde à QD2 – «Como é que a GNR conduz a sua intervenção na PIC, se tem as capacidades adequadas e quais são as principais dificuldades e necessidades?», sendo que a GNR poderá assumir um papel central na PIC, caso assim o pretenda.

Relativamente à intervenção das FFAA na PIC, conclui-se que esta ainda não se encontra estruturada, muito embora esteja atualmente elencada numa linha de ação estratégica do CEMGFA para operacionalizar esse desiderato. A intervenção das FFAA nesta área deverá estar incluída no quadro global de emprego das FFAA na Segurança Interna que venha a ser definida, em que sejam estabelecidos os mecanismos de articulação operacional, com as respetivas relações de comando e regras de empenhamento. Nesse sentido, e como contributos desta investigação para o possível PAO sugere-se equacionar as seguintes tarefas/ações às FFAA, num papel de supletividade relativamente às FFSS:

– Colaborar na elaboração dos PSO e PSPE e nos respetivos treinos desses planos, nomeadamente na cenarização de ameaças e na organização dos exercícios;

– Apoio de forças para proteger determinadas IC, nomeadamente através da vigilância e controlo de acessos;

– Disponibilização de meios específicos às FFSS, tais como meios aéreos;

– Controlo do espaço aéreo ou marítimo;

– Outros apoios de ordem logística, comunicações, etc.

Julga-se ainda pertinente a colocação de um elemento de ligação do EMGFA no SSI, e que passe a integrar o GT-PIC. Deste modo, quando solicitadas a tal, as FFAA poderão colaborar com as FFSS, em reforço e complemento, podendo a intervenção ocorrer, durante os estados de exceção, quando se verifiquem as condições previstas na Constituição ou, fora deles, quando a avaliação do SG-SSI o julgue adequado. Desta forma considera-se respondida a QD3 – «Em que situações as FFAA poderão ser utilizadas na PIC?».

Não obstante o atingir das respostas a todas as questões inicialmente formuladas, os resultados obtidos permitem-mos ainda extrair mais algumas conclusões. Uma delas é relativa ao quadro conceptual, que em Portugal, divide a PIC nas áreas de *safety*, do *security* e do *cyber*. Quer dizer, embora este pareça adequado, permitindo a divisão das responsabilidades pelas diversas entidades, conclui-se existir necessidade de uma melhor coordenação entre as diferentes áreas. Assim, uma visão holística à segurança das IC, que congregue e harmonize todos os esforços será mais adequada, pelo que parece evidente a necessidade da existência de "uma cabeça" que superintenda e coordene todas as atividades de PIC. E, em nosso entender, o SSI poderá ser a entidade a assumir essa função,

essencialmente pelo seu papel interdisciplinar, sendo para tal reconhecida a necessidade de legislação clara que coloque essa missão na sua dependência. Ou seja, dada a necessidade identificada da existência de uma estrutura para lidar com as IC, e dada a dimensão do país, não se justifica a criação de uma nova estrutura, mas sim reforçar o papel que o SSI possa desempenhar nesta matéria, alterando o seu quadro orgânico para o efeito. É ao estado que cabe a liderança do processo de PIC, por isso, julga-se que este deve ser mais intervencionista, pelo que, deve ter profissionais que se dediquem em exclusivo a esta temática, o que não acontece atualmente. Deste modo, conseguir-se-ia implementar um modelo de *governance* da PIC com uma visão mais funcional e integrada.

Uma outra conclusão, e no que concerne às ciberameaças, em que existem cada vez mais evidências de que os ciberataques representam riscos para as IC, torna-se cada vez mais necessário incrementar ou reforçar medidas neste âmbito. Por isso, e como a lei prevê apenas uma Autoridade Nacional de Cibersegurança, que é o CNCS, este organismo deverá ser cada vez mais chamado a intervir e deverá estar perfeitamente integrado com os restantes intervenientes na PIC. Concretamente deverá ser esta entidade a elaborar o parecer da componente *cyber* dos PSO, o que atualmente ainda não se verifica. Para atingir esse desiderato, a colocação no secretariado permanente do GCS de um oficial de ligação do CNCS poderia facilitar a relação deste organismo com o SSI.

Em síntese, pode dizer-se que há necessidade de conferir uma melhor coerência ao atual quadro legal, garantir uma maior coordenação, harmonização de procedimentos, racionalização de meios e de tempo entre os diferentes intervenientes na PIC, por forma a melhor se preparar a intervenção nessas infraestruturas para fazer face às ameaças que possam vir a concretizar-se. Deste modo, considera-se como atingido o objetivo geral inicialmente definido – «Analisar a intervenção das forças de segurança na PIC e identificar situações em que as FFAA possam ser utilizadas nesta área», sendo que, com o resultado desta investigação fica-se com uma ideia mais clarificada sobre a forma como é conduzida a intervenção na PIC, e quais os papéis e responsabilidades das diferentes entidades intervenientes, como sejam o SSI, as FFSS, o CNCS e as FFAA. Esperamos, deste modo ter contribuído para o conhecimento desta temática cada vez mais relevante na sociedade atual. No entanto, como principais limitações do estudo aponta-se o facto do processo de investigação ter sido confrontado com limitações relativa à confidencialidade dos processos e documentos, a qual retirou uma maior profundidade. Contudo, não foi objetivo proceder a um estudo com classificação de segurança, que também seria relevante para a comunidade

que trabalha as IC, mas antes um estudo aberto à comunidade em geral que permitisse trazer algum contributo para discussão desta importante temática.

Para investigações futuras, sugere-se que sejam estudados os casos das outras FFSS, nomeadamente a PSP e a PM, utilizando o mesmo modelo de análise, por forma a comparar com os dados agora obtidos no estudo de caso da GNR. Uma outra linha de investigação possível, e atendendo a que não se pode proteger aquilo que não se conhece, passa pelo estudo aprofundado e alargado na perspetiva das interdependências entre diversas infraestruturas por forma a reduzir potenciais impactos. Ainda, julga-se pertinente perceber a perspetiva dos operadores das IC face ao que esperam da intervenção das FFSS na sua infraestrutura em caso de incidente, pelo que essa investigação seria pertinente e permitira auxiliar o desenho do modelo dos PSPE. Como considerações de ordem prática, recomenda-se que este estudo seja remetido à GNR por se considerar ter dados pertinentes para essa FFSS e também ao EMGFA, acreditando poder de alguma forma contribuir para uma melhor compreensão deste assunto e incrementar a PIC, que são essenciais para o funcionamento da sociedade atual.

Bibliografia

Alexandre, E. (2017). *Gestão Civil de Crises – Da União Europeia a Portugal.* Instituto Superior de Ciências Policiais e Segurança Interna, Lisboa. Obtido de http://hdl.handle.net/10400.26/20020

AR. (2008). Lei n.º 53/2008 - Lei de Segurança Interna. *Diário da República, 1.ª série — N.º 167 — 29 de Agosto de 2008*, 6135-6141.

AR. (2012). Lei Orgânica n.º 1/2012, de 11 de maio - Segunda alteração à Lei n.º 44/86, de 30 de setembro (Regime do estado de sítio e do estado de emergência). *Diário da República, 1.ª série — N.º 92 — 11 de maio de 2012*, 2465-2470.

AR. (2015). Lei n.º 59/2015 de 24 de junho - Primeira alteração à Lei n.º 53/2008, de 29 de agosto. *Diário da República, 1.ª série — N.º 121 — 24 de junho de 2015*, 4411.

AR. (2018a). Lei n.º 46/2018 - Segurança do ciberespaço. *Diário da República, 1.ª série — N.º 155 — 13 de agosto de 2018*, 4031-4037.

AR. (2018b). Resolução da Assembleia da República n.º 119/2018. *Diário da República, 1.ª série — N.º 85 — 3 de maio de 2018*, 1786.

AR. (2019). *Constituição da República Portuguesa - VII revisão constitucional [2005]*. Obtido de Assembleia da República: https://www.parlamento.pt/Legislacao/Documents/constpt2005.pdf

Atlas, R. (2013). *21st century security and CPTED: designing for critical infrastructure protection and crime prevention.* Boca Raton: CRC Press.

Baldoni, R. (2014). *Critical Infrastructure Protection : Threats, Attacks and Countermeasures.* Roma: Center of Cyber Intelligence and Information Security - Università degli Studi di Roma “La Sapienza”.

Costa, A. (2017). *Participação das Forças Armadas em missões no contexto da Segurança Interna.* Instituto Universitário Militar, Lisboa. Obtido de http://hdl.handle.net/10400.26/21298

EMGFA. (2018). *Diretiva estratégica do Estado-Maior-General das Forças Armadas 2018-2021*. Lisboa: Estado-Maior-General das Forças Armadas. Obtido de https://www.emgfa.pt/documents/435jnqg1vmd7.pdf

Felice, F. & Petrillo, A. (2018). *Human factors and reliability engineering for safety and security in critical infrastructures: decision making, theory, and practice.* New Jersey: Springer.

Ferreira, A. (2017). *Análise de Vulnerabilidade em Infraestruturas Críticas.* Instituto Universitário Militar, Lisboa. Obtido de http://hdl.handle.net/10400.26/21382

Ferreira, H. (2014). *Segurança e Proteção de Infraestruturas Críticas do Setor Energético.* Escola Superior de Tecnologia e Gestão do Instituto Politécnico de Leiria, Leiria. Obtido de http://hdl.handle.net/10400.8/2511

Ferreira, H. M. (2016). *Identificação e Caraterização de Infraestruturas Críticas - Uma Metodologia.* Instituto Universitário Militar, Lisboa. Obtido de http://hdl.handle.net/10400.26/14615

Ganguly, A. R., Bhatia, U., & Flynn, S. E. (2018). *Critical Infrastructures Resilience.* Portland: Taylor and Francis.

GCS-SSI. (2014). Conteúdos dos Planos de Segurança do Operador - Componente Security (Alteração 01). Lisboa: Gabinete Coordenador de Segurança do Sistema de Segurança Interna.

GNR. (2014). *Estratégia da Guarda 2020.* Lisboa: Guarda Nacional Republicana.

GNR. (2017). *Relatório de Atividades 2017.* Lisboa: Guarda Nacional Republicana.

Guterres, E. (2016). Regulação de Riscos e Proteção de Infraestruturas Críticas: Os novos ventos do fenômeno regulatório. *Revista de Direito Setorial e Regulatório, 2*(1), 107-160.

Hakim, S., Clark, R., & Blackstone, E. (2017). *Cyber-Physical Security - Protecting Critical Infrastructure at the State and Local Level.* Switzerland: Springer. doi:10.1007/978-3-319-32824-9

Hedel, R., Boustras, G., Gkotsis, I., Vasiliadou, I., & Rathke, P. (2018). Assessment of the European Programme for Critical Infrastructure Protection in the surface transport sector. *Int. J. Critical Infrastructures, 14*(4), 311-335. doi:10.1504/IJCIS.2018.095616

Henriques, A. (2011). *Metodologia Multicritério de Identificação e Priorização de Infra-Estruturas Críticas.* Instituto Superior Técnico, Lisboa. Obtido de https://fenix.tecnico.ulisboa.pt/downloadFile/395142726453/Dissertação.pdf

Hyslop, M. (2007). *Critical information infrastructures: Resilience and protection.* New York: Springer.

IUM. (2018a). NEP INV 001 - Trabalhos De Investigação. Lisboa: Instituto Universitário Militar.

IUM. (2018b). NEP INV 003 - Estrutura e regras de citação e referenciação de trabalhos escritos a realizar no IUM. Lisboa: Instituto Universitário Militar.

Junta Interamericana de Defesa. (2018). Estudo sobre proteção de infraestrutura crítica em caso de desastre natural.
Obtido de http://scm.oas.org/pdfs/2018/CP39205PRELATORIO.pdf

Kyriakides, E. & Polycarpou, M. (2015). *Intelligent monitoring, control, and security of critical infrastructure systems.* Heidelberg: Springer.

Lazari, A. (2014). *European Critical Infrastructure Protection.* Switzerland: Springer. doi:10.1007/978-3-319-07497-9

Lourenço, N. (2015). As novas fronteiras da Segurança - Segurança Nacional, Globalização e Modernidade. *Revista Segurança e Defesa, 31*, pp. 26-37.

Lourenço, N., Lopes, F., Rodrigues, C., Costa, A., & Silvério, P. (2015). *Segurança Horizonte 2025. Um Conceito de Segurança Interna.* Lisboa: Edições Colibri.

Machado, P. (2015). *O papel da GNR no contexto da Cibersegurança Nacional.* Instituto Universitário Militar, Lisboa. Obtido de http://hdl.handle.net/10400.26/10143

Martinho, J. (2017). *As infraestruturas críticas em Portugal: um modelo de abordagem.* Instituto Universitário Militar, Lisboa.
Obtido de https://comum.rcaap.pt/handle/10400.26/21359

MDN. (2011). Decreto-Lei n.º 62/2011 de 9 de Maio - Infraestruturas Críticas. *Diário da República, 1.ª série — N.º 89 — 9 de Maio de 2011*, 2624-2627.

MDN. (2014). *Missões das Forças Armadas MIFA 2014.* Lisboa: Ministério da Defesa Nacional.

Merabti, M., Kennedy, M., & Hurst, W. (2011). Critical infrastructure protection: A 21st century challenge. *2011 International Conference on Communications and Information Technology, ICCIT 2011*(November 2014), 1-6.

Mirones, V. (2017). *A participação das Forças Armadas portuguesas no combate ao terrorismo.* Instituto Universitário Militar, Lisboa. Obtido de http://hdl.handle.net/10400.26/24541

Natário, R. (2014). *O Ciberespaço e a Vulnerabilidade das Infraestruturas Críticas: Contributos para um Modelo Nacional de Análise e Gestão do Risco Social.* Academia Militar, Lisboa. Obtido de http://hdl.handle.net/10400.26/8609

Natário, R., & Nunes, V. (2014). Risco Social no Ciberespaço. A Vulnerabilidade das Infraestruturas Críticas. *Revista Militar, 2547*, 249-286.

Nunes, P. V., Mendes, C., Ralo, J., Santos, L., Santos, L., Moniz, P., & Casimiro, S. (2018). Contributos para uma Estratégia Nacional de Ciberdefesa. *IDN Cadernos*(28).

Oliveira, M. (2015). *A Segurança das Infraestruturas Críticas em Portugal.* Faculdade de Direito da Universidade Nova de Lisboa, Lisboa. Obtido de https://run.unl.pt/handle/10362/15036

PCM. (2013). Resolução do Conselho de Ministros n.º 19/2013 - Conceito estratégico de defesa nacional. *Diário da República, 1.ª série - N.º 67 - 5 de abril de 2013*, 1981-1995.

PCM. (2015a). Resolução do Conselho de Ministros n.º 7-A/2015 - Estratégia Nacional de Combate ao Terrorismo. *Diário da República, 1.ª série - N.º 36 - 20 de fevereiro de 2015*, 1022-(2)-1022-(4).

PCM. (2015b). Resolução do Conselho de Ministros n.º 36/2015 - Estratégia Nacional de Segurança do Ciberespaço. *Diário da República, 1.ª série - N.º 113 - 12 de junho de 2015*, 3738-3742.

PCM. (2019). Decreto-Lei n.º 45/2019 de 1 de abril - Orgânica da Autoridade Nacional de Emergência e Proteção Civil. *Diário da República, 1.ª série — N.º 64 — 1 de abril de 2019*, 1798-1808.

Pestana, J. (2016). *A Proteção de Infraestruturas Críticas – Contributos para o desenvolvimento de um Plano Nacional de Proteção de Infraestruturas Críticas.* Instituto Superior de Ciências Policiais e Segurança Interna, Lisboa.

PGR. (2002). Parecer n.º 147/2001 do Ministério Público. *Diário da República, 2.ª série — N.º 40 — 16 de fevereiro de 2002*, 3101-3108.

Plataforma Nacional para a Redução do Risco de Catástrofes. (2017). *Boas Práticas de Resiliência de Infraestruturas Críticas.* Obtido de http://www.prociv.pt/bk/EDICOES/OUTRASEDICOES/Documents/Boas_Praticas_Resiliencia_Infraestruturas_Criticas-Setor_Privado_e_Empresarial_Estado_2017.pdf

PMA. (2017). Decreto-Lei n.º 136/2017 de 6 de novembro - Orgânica do Gabinete Nacional de Segurança. *Diário da República, 1.ª série — N.º 213 — 6 de novembro de 2017*, 5879-5886.

Quivy, R., & Campenhoudt, L. V. (2008). *Manual de Investigação em Ciências Sociais.* Lisboa: Gradiva.

Rebisco, P. (2016). Forças Armadas - Intervenção no âmbito da Segurança Interna. *CEDIS Working Papers*(Nº 40 setembro 2016).

Rodrigues, M. (2014). A problemática dos eventos críticos (incidentes táctico-policiais). *Investigação Criminal. Nº 8*, 42-51.

Santos, L., & Lima, J. (2016). Orientações metodológicas para a elaboração de Trabalhos de Investigação. *Cadernos do IESM Nº 8*. Instituto de Ensino Superior Militar: Lisboa.

Saunders, M., Lewis, P., & Thornhill, A. (2009). *Research methods for business students.* England: Pearson.

SIS. (2019). *Serviço de Informações de Segurança*. Obtido em 10 de abril de 2019, de https://www.sis.pt

SSI. (2018). *Relatório Anual de Segurança Interna - Ano 2017.* Lisboa: Sistema de Segurança Interna. Obtido de https://www.portugal.gov.pt/download-ficheiros/ficheiro.aspx?v=9f0d7743-7d45-40f3-8cf2-e448600f3af6

SSI. (2019). *Relatório Anual de Segurança Interna - Ano 2018.* Lisboa: Sistema de Segurança Interna. Obtido de https://www.portugal.gov.pt/download-ficheiros/ficheiro.aspx?v=ad5cfe37-0d52-412e-83fb-7f098448dba7

UE. (2005). Livro Verde relativo a um Programa Europeu de Proteção das Infraestruturas Críticas. COM(2005) 576 final. Bruxelas.

UE. (2008). Directiva 2008/114/CE. *Jornal Oficial da União Europeia*, 75-82.

US DHS. (2013). *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience.* EUA: United States Department of Homeland Security. Obtido de https://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience

US DHS. (2019). *Critical Infrastructure Sectors*. Obtido em 7 de março de 2019, de Department of Homeland Security: https://www.dhs.gov/cisa/critical-infrastructure-sectors

WEF. (2019). *World Economic Forum. The Risks-Trends Interconnections Map 2019*. Obtido em 24 de Jan de 2019, de Global Risks Report 2019: http://reports.weforum.org/global-risks-2019/global-risks-landscape-2019/#trends/T_CYBERDEPENDENCY

Apêndice A — Modelo de análise

Neste apêndice apresenta-se o modelo de análise, elaborado a partir a revisão da literatura e que serviu de base para a preparação do guião de entrevista e posterior inquérito por questionário, permitindo, deste modo, estruturar toda a investigação.

Quadro 6 – Modelo de análise

Conceitos	Dimensões	Indicadores	Questões
Infraestruturas Críticas (IC)	Proteção	Importância	Qual é?
		Vulnerabilidades	Quais são? Que implicações?
Quadro legal	Relativo a IC	Inteligibilidade Adequabilidade Articulação	É inteligível? É adequado? É bem articulado?
	Relativo à intervenção das FFSS na PIC		
	Relativo à intervenção das FFAA na PIC		
Intervenção das Forças de Segurança	Capacidades da GNR	Organização	É aquedada? Qual a desejável?
		Pessoal	É suficiente?
		Meios	São adequados? Quais os necessários?
		Treino / exercícios	Existem? São suficientes?
		Colaboração c/ outras entidades	É eficaz?
Planos de Segurança	Dos operadores de IC	Existência Adequabilidade Treino Vulnerabilidades	Existem? São adequados? São treinados? Problemas?
	Das Forças de Segurança		
	Outros Planos		
Papel das FFAA	Situação atual	Meios Pessoal Situações de emprego	Quais? Como?
	Possibilidades		

Apêndice B — Transcrição das Entrevistas efetuadas

As entrevistas aos diversos especialistas selecionados para o estudo ocorreram durante o mês de março de 2019, foram combinadas as datas para a sua realização de acordo com a disponibilidade dos entrevistados, sendo realizadas no local onde prestam serviço. As entrevistas foram gravadas de forma a facilitar a sua análise, tendo sido solicitado previamente aos entrevistados a sua gravação, e obtido o consentimento para a sua transcrição que aqui se reproduz. A exceção à gravação foi o E5 que depois da entrevista preferiu antes responder às questões por *email*.

Quadro 7 – Entrevistas efetuadas

1. Importância das Infraestruturas Críticas (IC)	
1.1	**Qual a importância que atribui à Proteção de Infraestruturas Críticas (PIC)? Acha que o país está suficientemente empenhado nesta matéria? Por onde poderia evoluir?**
E1	R.: Tem espaço para evoluir. Basta dizer que a diretiva considera só dois sectores: a energia e os transportes. Considera-se em Portugal que existem também 12 sectores e são só dois que estão a ser trabalhados! Portanto, existe espaço para evoluirmos. Por outro lado, tem havido uma concentração muito grande do esforço na designação e identificação, e nos critérios que definem o que é ou não uma IC, sendo que há uma assimetria entre esse esforço efetuado, e depois o esforço de operacionalizar segurança nessas infraestruturas, sendo que aqui também há espaço para evoluir. Passamos vários anos a encontrar critérios de identificação muito técnicos, muito científicos, densos (algoritmos de interdependências criados pelo Instituto Superior Técnico), sendo que tudo isto deu muito trabalho a fazer. Foi o caminho que escolhemos, sendo que outros países seguiram caminhos diferentes, mais simples, mas talvez menos rigorosos. A nossa escolha é um caminho muito rigoroso, mas que também consome tempo o que atrasou a operacionalização dos aspetos mais de segurança em que estamos agora mais empenhados.
E2	R.: Acho que o país está empenhado o suficiente tendo em conta a realidade da segurança nacional, a quantidade de IC existentes (que não são assim tantas) e o grau de ameaça terrorista nacional. O país pode sempre estar mais empenhado, mas, neste momento, mobiliza uma série de atores que nos permite dizer que temos um empenhamento satisfatório.
E3	R.: A importância é elevada, com base no quadro Europeu e Nacional […] É importante e relevante. Nos dois setores que decorrem da lei (transportes e energia) sim o país está suficientemente empenhado. Contudo há necessidade de evoluir nos outros dez sectores das IC. […] Neste momento tem sido dado vários impulsos no sentido de revisão da norma, mas ainda não foi concretizada e não há opção política para se avançar.
E4	R.: As IC, por definição, são essenciais à nossa da sociedade. A sua interrupção ou mau funcionamento pode causar transtorno ou mesmo a inexistência de uma função societal importante. A legislação hoje em dia tem um conjunto de conceitos que têm como elemento comum a criticidade, sendo as IC um deles, que decorre do Decreto-Lei 62/2011, e foca-se nos setores da energia e dos transportes. Nessa altura, aproveitou-se a transposição da diretiva Europeia para construir, ou dar um primeiro passo para a construção, do que seria um sistema de proteção IC nacionais. No entanto, acho que isso foi mal conseguido, ou seja, a construção jurídica acabou por não resultar no que se pretendia, nomeadamente porque se criou uma estrutura bicéfala, a ANPC e o SSI, com a lógica de que de um lado ficava o *security* e do outro lado o *safety*. Se olharmos a outros modelos estrangeiros, acho que não encontramos paralelo. Em Espanha, por exemplo, existe o CNPIC (*Centro Nacional de*

	Protección de Infraestructuras y Ciberseguridad) que é um órgão específico e focalizado na proteção de IC, com as duas componentes (*security* e o *safety*). Este conceito de criticidade, ou de regulação de algumas atividades que são consideradas críticas, tem o conceito de PIC e mais recentemente o conceito operador de serviço essencial (conforme Lei 46/2018 que também decorre da transposição de uma diretiva europeia, a diretiva NIS, e que engloba 14 sectores, mas que deixa de fora as telecomunicações). Estes dois diplomas falam do mesmo, mas com dois ângulos diferentes: o primeiro diz respeito a uma componente infraestrutural (componentes físicas e de suporte infraestruturais, físicas ou lógicas, que são essenciais à sociedade); o segundo tem uma visão que considero mais correta. Ou seja, tem uma visão funcional, isto é, a função que é suportada é que é crítica, sendo que essa função tem toda uma cadeia de valor que também ela é crítica para o serviço que é essencial. E estaria à espera que quer a ANPC quer o SSI dessem esse salto e adotassem esta visão, pois permite melhor trabalhar conceitos como a interdependência, etc. O país não está nada empenhado nesta matéria, tem muito espaço para evoluir.
E5	R.: A PIC é estratégica, sendo as IC, por definição, essenciais para a saúde, a segurança e o bem-estar económico e social da sociedade. A sua disrupção ou destruição teriam um impacto significativo no país como resultado da incapacidade do Estado em manter aquelas funções.
1.2	**Quais considera serem as principais vulnerabilidades nesta área, e que implicações isso acarreta?**
E1	R.: Há IC de todo o tipo, sendo que as vulnerabilidades dependem muito do tipo de infraestrutura, do sector e do subsetor de que estamos a falar. Por exemplo, há infraestruturas como um posto de transformação ou uma infraestrutura que está isolada e não tem ninguém a operar, e há infraestruturas como o aeroporto de Lisboa. Portanto, é difícil identificar vulnerabilidades gerais. Contudo, há IC que têm mais proteção que outras, e mesmo os próprios operadores consideram mais críticas umas em detrimento de outras. É diferente estarmos a falar de um operador com uma grande dimensão (com uma grande infraestrutura) e que tem departamentos próprios para tratar da segurança, ou estarmos a falar de operadores que são empresas de pequena dimensão e que não se podem dar ao luxo de ter propriamente estruturas de segurança e investimentos desses. Ou seja, há realidades muito diferentes. De uma forma geral, existe a preocupação e o cuidado dos operadores em proteger as suas infraestruturas (os seus *assets*).
E2	R.: Provavelmente a maior vulnerabilidade seja o campo ciber, e não tanto o campo da ameaça física que está devidamente acautelado, em que os próprios operadores apostam muito na segurança física.
E3	R.: Necessidade de uma melhor coordenação entre o *safety*, o *security* e o ciber, especialmente o ciber.
E4	R.: O modelo de *governance* da PIC, que deveria ter uma visão mais funcional e integrada como no caso da Espanha. Os espanhóis, como tinham o trabalho bem feito relativamente à PIC, e porque muito provavelmente já tinham esta abordagem funcional, quando surgiu a necessidade de transposição da diretiva NIS, o que eles fizeram foi pegar em todo o plano e requisitos de segurança que tinham para as infraestruturas, e mapearam para as restantes entidades que seguiam os critérios da diretiva NIS. Assim, eles têm uma visão integrada, independentemente de se olhar para a infraestrutura ou olhar para a função, pois obviamente as funções dependem de infraestruturas, e dependem também da cadeia de abastecimento. Um exemplo que costumo dar de uma função crítica à sociedade no Ministério da Educação é a prescrição médica, que é um dos serviços mais importantes prestado pelos SPMS (Serviços Partilhados do Ministério da Saúde). Essa função em particular tem componentes infraestruturais que são críticas. Uma delas é um sistema informático chamado autenticação do cartão do cidadão ou a chave móvel digital que é usada para aceder e conseguir fazer a função de prescrição. Esta, por sua vez, é prestada por um outro Serviço, a AMA (Agência para a Modernização Administrativa). Portanto, esta visão funcional com dependência entre sistemas ou mesmo de infraestruturas físicas (uma ligação entre o SMPS e o sistema da AMA que faz a

	autenticação). Duvido que o processo de elaboração e identificação de IC tenha em consideração este tipo de detalhe. Mas, se fizermos uma avaliação funcional, e virmos as dependências para prestar aquela função com boa qualidade, chegamos rapidamente à conclusão que aquela ligação entre aquelas duas entidades é crítica para a prestação daquele serviço essencial. Ou seja, há pontos críticos que não seriam identificados a priori, se não tivermos esta abordagem funcional. Portanto, na minha opinião, temos que crescer nesse sentido. Também temos que ter um regime que tenha apenas uma "cabeça".
E5	R.: A principal vulnerabilidade prende-se com a inexistência de um Plano de Articulação Operacional entre as Forças e Serviços de Segurança e as Forças Armadas (FFAA). De facto, em Portugal, a Estratégia Nacional de Combate ao Terrorismo (ENCT) "representa um compromisso de mobilização, coordenação e cooperação de todas as estruturas nacionais com responsabilidade direta e indireta no domínio da luta contra esta ameaça". A ENCT contempla um Plano de Articulação Operacional (PAO) e um Programa Nacional de Proteção de Infraestruturas Críticas (PNIC) - já referidos no CEDN de 2013. Contudo aqueles documentos ainda não existem, com impacto na articulação das Forças (FFAA e FSS) no terreno.
2. Quadro legal	
1.1 O quadro legal existente relativo às IC (proteção e intervenção) é inteligível e adequado? É bem articulado?	
E1	R.: Passaram 11 anos desde a Diretiva n.º 2008/114/CE do Conselho da União Europeia, que ainda se encontra em vigor, sendo que está a ser avaliada. A maioria dos países transpôs essa diretiva para os seus ordenamentos nacionais, sendo depois necessário avaliar da eficácia que a diretiva teve neste tempo todo. Para aquilo que era a expectativa inicial houve muito poucas IC Europeias designadas e estas estão muito concentradas em dois ou três países. Por isso, é necessário perceber se o problema está na diretiva, na forma como ela foi redigida, ou se o problema está nos Estados membros, na forma como a interpretaram e como fizeram a transposição. Ou seja, houve um grande número de Estados membros, como é o caso de Portugal, que considerou não classificar algumas das suas IC como IC Europeias, talvez porque não achou necessário ou fácil, ou não considerou ser uma mais-valia.
E2	R.: É inteligível, no entanto alguns pormenores que decorrem da diretiva europeia, como aquele relativo a IC Europeias (ICE), pode não fazer muito sentido o modo como aparecem lá referidas. Por exemplo, ninguém diz como estas se classificam, e depois como se desclassificam e como se coordena a segurança dessas mesmas IC com os outros países. Por isso neste aspeto não é muito clara a legislação. Outra eventual lacuna, mas que está a ser trabalhada no âmbito da revisão das normas europeias para a proteção de IC, são os outros sectores em falta como o da água, alimentação, etc.
E3	R.: Relativamente ao inteligível e bem articulado, sim. Relativamente a ser adequado, parece-me que há necessidade de nova legislação.
E4	R.: Não tenho conhecimento para o avaliar. Mas há quem diga que a forma como se estendeu a transposição da diretiva Europeia não é suficiente para criar um regime de PIC nacionais. Portanto, há sectores de atividade que não estão a colaborar por não encontrarem enquadramento legal para esse trabalho.
E5	Não aplicável / Não responde.
2.1 Há necessidade de nova legislação e/ou regulamentação?	
E1	R.: Sim, há necessidade. A prova disso é que já foi trabalho a atualização do Decreto-Lei n.º 62/2011, em coordenação com a ANPC, aguardando-se oportunidade legislativa. Há coisas que não se justificam atualmente, e outras coisas que podem ser melhoradas, nomeadamente coisas simples como

	os tempos em que os operadores têm de apresentar os PSO´s (estes tempos podem ser dilatados pois as IC não se alteram significativamente todos os anos, não fazendo sentido todos os anos estar a remeter novos planos da mesma coisa). Há aspetos sobre a segurança que podem ser melhorados, nomeadamente o foco em questões mais operativas (como por exemplo verificações de segurança a funcionários que tenham que trabalhar nas infraestruturas, etc.). Enfim, há um conjunto de medidas que estão propostas (está feita a revisão técnica da legislação) que terá que seguir agora o processo legislativo. O diploma que temos em vigor, e que foi na altura a transposição da diretiva europeia, ainda não tinha sido mexido e justifica-se a sua melhoria, em que um dos pontos essenciais é abranger os outros sectores das IC. Olhando ao caso espanhol, verifica-se que eles têm um histórico de questões relacionadas com a segurança que não tem nada a haver com o nosso, tiveram vários tipos de terrorismo e a parte *security* deles é sempre uma componente fortíssima, essencialmente as questões do terrorismo (ataques organizados, atores hostis intencionais, etc.) e é para isso que eles trabalham e se protegem. Nós cá, como não temos a ameaça do terrorismo tão evidente como em Espanha, e por outro lado temos ameaças tais como as ameaças sísmicas, que não são negligenciáveis, é por isso que o *safety* e o *security* estão muito mais equilibrados. Até por que há uma ameaça comum. Vejamos: quando há uma ameaça a uma IC, ela é crítica porque a interrupção desse serviço provoca um efeito cascata que impede outras IC de funcionar, sendo que esse conjunto de supressões de serviço tem um impacto muito forte na sociedade e num nível geograficamente alargado. Nesta lógica, é um pouco indiferente se a interrupção do serviço se deveu a um explosivo que foi colocado num servidor de computadores, a um ataque cibernético efetuado, ou a um trabalhador que deixou cair café sem querer. O que importa é que consequência é igual (a central parou de trabalhar). Por isso, nesta questão das IC é preciso perceber estes dois momentos de intervenção: um é o momento de prevenir atentados e prevenir situações de *safety* ou se houver um problema espera-se que haja a maior resiliência possível, e aqui também as forças de segurança tem preocupações; a partir do momento em que há um problema, a forma como a sociedade se organiza para o resolver, já pouco ou nada tem a ver com ser *security* ou *safety*. É preciso trabalhar em separado numa primeira fase (que é importante e útil), e é também importante e útil trabalhar em conjunto numa fase seguinte. A ANPC não foi convidada para fazer parte do GT-PIC, porque é um grupo que trata as questões *security*. A ANPC pode é ser convidada para participar em algumas reuniões caso se entenda que os temas a abordar são do interesse da ANPC.
E2	R.: Acho que não existe necessidade de nova legislação, apenas rever a legislação nacional existente, à luz daquilo que for feito a nível europeu (mas só depois do que for feito a nível europeu) e à luz das novas ameaças, nomeadamente no domínio ciber. Neste momento está em revisão o Decreto-Lei 62/2011, mas só deverá sair depois a legislação europeia.
E3	R.: Há necessidade de nova legislação, tendo em atenção os outros dez sectores que estão fora do DL 62/2011.
E4	R.: Sim, há necessidade de nova legislação. **[Complemento a esta questão]: O Decreto-Lei nº 62/2011 define operadores de infraestruturas críticas e aplica-se somente aos setores da Energia e Transportes. A Lei n.º 46/2018 (Segurança do Ciberespaço) vem acrescentar os conceitos de operadores de serviços essenciais e prestadores de serviços digitais e aplica-se a mais setores. Qual a principal diferença de um operador de serviços essenciais relativamente a um operador de IC? Como correu a identificação dos operadores de serviços essenciais? Na sua opinião há operador de serviços essenciais que deveriam também ser classificados como operadores de infraestruturas críticas e não o são neste momento?** R.: As IC quando foram inicialmente identificadas seguiram uma lógica de «quais são infraestruturas que a sua entidade tem, cuja a disrupção prolongada possa ter um determinado efeito?». A identificação dos serviços essenciais seguiu uma metodologia semelhante, mas com critérios mais

	concretos. Por exemplo, foi identificado como operador de serviço essencial no sector da banca, o sistema de crédito bancário, aquele que tem uma carteira de clientes acima de um determinado valor. Portanto, não se teve em conta somente a questão da disrupção da infraestrutura, mas também o impacto do ponto de vista de funcionamento do mercado e não numa lógica de impacto direto societal. Em princípio vai ser pedido um plano de segurança a esses operadores e antes disso será pedida uma análise de risco. O que falta fazer na transposição da diretiva NIS é finalizar o procedimento de notificação de incidentes relevantes e estabelecer um critério que identifique o que é um incidente relevante num determinado sector. Neste aspeto, a última coisa que vamos fazer é uma regulamentação ao sector. Ou seja, ao contrário do Plano de Segurança do Operador, que é uma espécie de *biding* (você tem, - cumpriu), o CNCS vai definir os requisitos que o operador tem de cumprir, nomeadamente exigir a análise de risco e depois a implementação de um conjunto de medidas a partir de um quadro de referência (desenvolvido no CNCS baseado na NIST *cybersecurity framework*) de acordo com a análise de risco efetuada. Depois existirão mecanismos de auditoria para verificar se as medidas implementadas são ou não suficientes. Relativamente à segurança física, é possível que se arranjem sinergias com o que é feito para as IC, e se passe a fazer também para os operadores dos serviços essenciais.
E5	Não aplicável / Não responde.
	3. Capacidades das Forças de Segurança (FFSS)
3.1	**O As valências atualmente existentes nas FFSS (GNR, PSP e PM), analisando as dimensões de Organização, Pessoal, Meios, Treino / exercícios, Colaboração com outras entidades, são aquedadas e suficientes para intervir na PIC? Na sua opinião quais deveriam ser as valências a edificar pelas FFSS para incrementar a PIC?**
E1	R.: Essencialmente, na componente de prevenção e proteção e não tanto na resposta em situação de crise, em que não estamos a falar dos impactos da interrupção do serviço mas sim na proteção da infraestrutura, acho que estamos numa fase determinante em que mais do que meios (sendo que as forças têm um conjunto de meios espalhados pelo território), as forças têm que ter um padrão de conhecimento mínimo, que tem de ser significativo, sobre as IC que estão na sua área, nomeadamente através dos PSO que estão neste momento a ser distribuídos (sendo que ainda falta validar alguns deles). E, de acordo com a legislação, as forças de segurança têm que fazer um plano de segurança e proteção exterior (PSPE), que deve casar com o PSO e traduz a resposta a dar caso haja um incidente numa IC. Estes planos são importantes porque, por um lado, garantem que há um contacto, isto é, uma atenção especial por parte da força territorial relativamente a essas infraestruturas. Por outro lado, os planos são importantes pela própria segurança das infraestruturas e pela segurança das pessoas que são chamadas para poderem lá intervir. Pois, uma IC é um ambiente diferente da via pública, algumas delas têm alta tensão, têm água e determinadas canalizações que não podem ser furadas, aspetos mecânicos e industriais, pelo que a intervenção numa IC, salvo raras exceções, obedece a regras próprias que o operador tem, e que é diferente da via pública onde as forças de segurança têm conhecimento para trabalhar nesse ambiente. Nas IC nem tanto, aliás, basta olhar para as mortes que têm havido nos últimos anos nas forças de segurança e uma parte significativa num universo que felizmente é pequeno, tem a haver com atropelamento de comboios, electrocuções em linhas de comboio, portanto, situações que são fora do ambiente regular de atuação das forças de segurança. Assim, é importante que os planos de segurança e proteção do exterior estabelecem exatamente quais são as limitações, as condicionantes e os perigos de atuação nessa infraestrutura. Exemplo: podem ser utilizados cães? Pode ser utilizado uma arma elétrica? Por isso, tendo a infraestrutura um responsável local, deve haver uma integração dos planos do operador com os da força de segurança.
E2	R.: Na proteção física são suficientes e adequadas. Talvez se possa colocar a tónica na PM que tem poucos efetivos de pessoal e que não são suficientes pelo que terá de ter o reforço da GNR e da PSP.

E3	R.: De uma forma geral as valências são adequadas e suficientes. Em termos de Organização, Material, Liderança, Pessoal e Infraestruturas temos o necessário. Estamos a desenvolver a Doutrina e o Treino. Também a questão da Interoperabilidade deve ser melhorada. Neste momento o que há necessidade é de consolidar a capacidade.
E4	R.: Aqui há uma grande componente que é da responsabilidade dos privados, dado que a maior parte das IC estão em mãos privadas. O Plano de Segurança do Operador é talvez a peça mais importante, que é avaliada pelo SSI no sentido de aferir se corresponde aos requisitos que esse plano de segurança deva constar. […] As FFSS devem ter valências na área ciber. Por exemplo, a GNR já tem algumas capacidades com contributos bastante importantes para a estratégia nacional de segurança do ciberespaço, nomeadamente nas áreas da sensibilização (com a iniciativa junto das escolas). Eu sempre defendi, que o ciberespaço é uma extensão do nosso mundo real e por isso, todas as entidades que tenham uma determinada função neste mundo real, devem exercer exatamente a mesma no ciberespaço. Temos um problema grave de falta de recursos humanos, falta de matéria-prima, mas não podemos deixar de perseguir esse designo de que as autoridades que já fazem uma determinada função e têm uma determinada autoridade no mundo físico, que façam o mesmo no ciberespaço.
E5	Não aplicável / Não responde.
3.2 Quais são as principais dificuldades e necessidades?	
E1	Não questionado.
E2	R.: Será necessário um maior entrosamento entre as forças e serviços de segurança e os responsáveis locais de segurança das IC, onde poderá ser trabalhada uma melhor articulação, como por exemplo realizando mais exercícios, que permite as pessoas se conhecerem e saber quais são os procedimentos inerentes à operação em ambiente de uma IC.
E3	R.: Dificuldades de uma melhor coordenação. Com as outras entidades e mesmo internamente na GNR. Os planos ainda não estão todos validados, estando na fase final de validação de todos os PSO.
E4	R.: Nada a referir.
E5	Não aplicável / Não responde.
4. Planos de segurança	
4.1 O Qual o ponto de situação do Programa Nacional de Proteção de Infraestruturas Críticas (PNPIC)?	
E1	R.: Esse plano não existe. Mas pode dizer-se que o plano nacional é o conjunto de instrumentos que existem relacionados com esta matéria, tais como os PSO, os PSPE, a doutrina que se produz; mas efetivamente um plano com nome de PNPIC não existe, ao contrário da Espanha onde plano orientador existe. A existir em Portugal, teria que ser elaborado pelo gabinete da Secretária-geral do SSI, juntamente com a ANPC para envolver a parte *safety*, e deveria ter os instrumentos que fazem parte do plano e o operacionalizam, como também datas, prazos, metas e responsabilidades dos intervenientes. Se este tivesse existido talvez tivesse havido uma capacitação diferente da Administração Pública (SSI e ANPC) para lidar com este assunto. De facto, há poucos recursos a nível estratégico, e de planeamento a trabalhar nesta matéria, pelo se vai evoluindo, mas com alguma demora.
E2	R.: Não existe.
E3	Não questionado.
E4	Não questionado.
E5	Não aplicável / Não responde.

4.2	**No seu entender, os Planos de Segurança da responsabilidade dos Operadores (PSO) estão a ser bem executados, são adequados e suficientes?**
E1	R.: O Decreto-Lei n.º 62/2011 é claro no seguinte: destina-se à IC Europeias nos sectores da energia e dos transportes e aplica-se às IC nacionais. A dúvida aqui é se se aplica só às IC nacionais da energia e transportes ou se se aplica a todos os sectores. Independente de que gostássemos que se aplicasse automaticamente a todos os sectores, parece-me que a interpretação mais verosímil (e que requer menos interpretação) é que se aplica às IC nacionais, mas apenas a estes dois sectores. Há outros sectores que, por força de legislação sectorial muito apertada (dos reguladores), já fazem trabalho de proteção há muitos anos. Basta olhar para o sector aeroportuário. Aliás, o próprio gabinete da Secretária-geral reconheceu que a legislação que é exigida no sector aeroportuário, satisfaz de tal forma os requisitos do Decreto-Lei n.º 62/2011, que emitiu certificados de conformidade, não tendo sido necessários a elaboração de novos planos (sendo que muitas das vezes esses planos até são mais restritivos). A matriz dos PSO foi elaborada com base no código ISPS dos portos e navegação marítima (*International Ships and Ports Security*), daí os portos também terem sido isentados de apresentar esses planos. São planos densos, estruturados, sendo que muitos setores já têm essas preocupações, mas outros não. Mas as próprias autoridades e reguladores devem ser muito exigentes no cumprimento desses planos. No caso do sector portuário e aeroportuário as autoridades são extramente exigentes e rigorosas. Noutros casos a aplicação dos PSO foi proveitoso pois sensibilizou mais os operadores para as questões da segurança.
E2	R.: Antes da entrada em funções do Grupo Trabalho para a Proteção das IC (GT-PIC) houve um período em que havia uma série de PSO´s que estavam pendentes de aprovação e isso demorou algum tempo. Houve o problema de que, quando esses planos foram sujeitos a aprovação, os pressupostos que enformavam esses planos já estavam desatualizados (nomeadamente a ameaça terrorista), sendo que alguns careceram de atualização. Em grosso modo, os PSO dão resposta a praticamente todas as questões no âmbito da segurança física. No âmbito da segurança ciber alguns já dão resposta, mas noutros essa parte está omissa, necessitando de ser trabalhada.
E3	R.: Existe uma norma, uma orientação técnica, e de uma forma geral os planos estão bem organizados, existe uma matriz que é idêntica para todos.
E4	**[Alteração à esta questão]: Tendo o PSO uma secção dedicada à Segurança dos sistemas de informação e Comunicações, o CNCS já tem alguma intervenção na elaboração deste plano ou está previsto vir a ter? No seu entender, estes planos estão bem organizados, estão a ser bem executados, são adequados e suficientes?** R.: Ainda não existiu oportunidade para o fazer, mas, isso deveria ser feito pelo CNCS. E em vez de Segurança dos sistemas de informação, chamar-lhe-ia Cibersegurança porque é mais abrangente, dentro daquela lógica de que as pessoas também são um elemento essencial para a segurança da IC, e a forma de como utilizam as tecnologias ou sistemas de informação é essencial ao seu bom funcionamento. Portanto, não é só uma questão tecnológica, mas uma questão também de pessoas. Espero que o capítulo de Cibersegurança do PSO passe a ser avaliado pelo CNCS. Em todo o caso, deveremos lá chegar pelo regime jurídico de segurança do ciberespaço, até porque o Estado daria uma péssima imagem se o mesmo operador recebesse instruções relativas ao mesmo tema de duas autoridades diferentes.
E5	Não aplicável / Não responde.
4.3	**Relativamente aos Planos de Segurança e Proteção Exterior (PSPE), quais são as principais dificuldades da sua implementação? Como se articulam os PSO com o PSPE?**
E1	R.: O próprio modelo do PSPE está feito para ter que se consultar e obter informação especifica do PSO, por forma a se poderem casar os dois planos. No caso de haver a necessidade de uma intervenção de uma força de segurança numa IC, estes planos têm que funcionar os dois em conjunto, um não

	pode ter disposições que contrariem o outro. Ainda não está decidido se o PSO, por ser um plano policial, vai ser do conhecimento do operador da IC, ainda terá de ser analisado com os operadores. Os PSPE estão idealizados para serem planos pequenos, muito operativos, com os aspetos essenciais que um responsável policial de nível local necessite para dar resposta a uma situação (reação imediata). Ou seja, o plano tem de ser suficientemente informativo para permitir dar uma primeira resposta numa IC, que é diferente da via pública, e ao mesmo tempo tem de ser suficientemente flexível para que a segunda parte da resposta possa ser adaptada a qualquer que seja a situação, devendo o plano entroncar na doutrina policial de cada instituição, na forma como resolve cada uma das ameaças. Não me comprometendo com datas, gostávamos que até ao final do ano tivéssemos os PSPE concluídos.
E2	R.: Os PSPE são da competência das forças de segurança e implica a aprovação prévia do PSO. Neste momento não há PSO pendentes de aprovação e relativamente aos PSPE está-se, em sede do GT PIC, a estabelecer uma matriz comum e criar um plano tipo para as forças de segurança adaptarem depois à realidade local de cada IC. Ou seja, a aprovação do PSO depende sempre do parecer da força de segurança territorialmente componente que depois elabora o PSPE.
E3	R.: Neste momento estamos na fase de elaboração da matriz para ser aprovada e depois disponibilizada. Estamos a consolidar os PSPE no âmbito do grupo de trabalho que tem lugar no SSI e depois de termos chegado a um acordo relativamente à matriz vamos fazer um exercício, quer na área da PSP, quer da GNR, e vamos analisar e daí tirar lições e procurar readaptar se houver necessidade.
E4	Não aplicável / Não responde.
E5	Não aplicável / Não responde.
4.4 Há registo de intervenções com ativação dos respetivos planos em IC? Se sim, pode exemplificar.	
E1	R.: Não.
E2	R.: Não. Até hoje não houve uma única ação contra IC.
E3	R.: Não. Neste momento há exercícios.
E4	Não aplicável / Não responde.
E5	Não aplicável / Não responde.
4.5 Os planos são treinados regularmente?	
E1	R.: Quando os planos estiverem todos prontos irá ter que haver exercícios. No entanto, mesmo ainda sem os PSPE, as forças de segurança já estão a fazer exercícios. O ano passado já houve quatro exercícios, e este ano vamos também realizar um grande exercício em Fátima e na EDP. O que se percebe destes exercícios é efetivamente a necessidade desses planos, pois quando uma força de segurança vai desenvolver uma atividade policial dentro de uma IC há aspetos que são úteis que sejam do conhecimento dessa força antes de chegar à infraestrutura, sendo que esses aspetos devem estar perfeitamente claros no plano.
E2	R.: Sim. Alguns exercícios são da iniciativa dos operadores, que estão muito ativos nessa questão de testar os planos, e outros são da iniciativa das forças de segurança. A Secretária-geral tem competência de direção e coordenação, entendendo o exercício das suas funções numa lógica de não retirar a autonomia das forças, pelo que a realização dos exercícios dependerá maioritariamente das forças de segurança.
E3	R.: Depois dos planos serem aprovados deve ser ponderado pela respetiva Força de Segurança.
E4	Não aplicável.

E5	Não aplicável / Não responde.
4.6	**O que é o Plano de Ação para a Proteção e Aumento da Resiliência das Infraestruturas Críticas (PAPARIC)?**
E1	R.: Esse plano faz parte da estratégia, não é público, cola muito com a própria legislação e estabelece uma lógica de tempo para que sejam realizadas determinadas ações, como a conclusão dos PSO. Ou seja, operacionaliza o Decreto-Lei n.º 62/2011 que acaba por ser muito genérico.
E2	R.: Esse plano está no âmbito da Unidade de Coordenação Antiterrorismo (UCAT).
E3	R.: Relativamente a esse plano saliento como medidas relevantes a organização de exercícios e reforçar a partilha de informação entre os diferentes intervenientes.
E4	R.: Desconheço.
E5	Não aplicável / Não responde.
4.7	**Existem outros planos de contingência no âmbito das PIC?**
E1	R.: Não, os referidos são planos suficientes.
E2	R.: Não.
E3	R.: Existe o plano de coordenação, controlo e comando operacional das FSS (PCCCOFSS) que vai integrar a intervenção em caso de existir um incidente tático policial. Caso seja considerado um incidente tático policial grave é assumido pelo secretário-geral do SSI.
E4	**[Alteração a esta questão]: Existem outros planos de contingência no âmbito ciber para a PIC? Se sim, há registo de intervenções com ativação dos respetivos planos e/ou estes são treinados regularmente?** R.: O que o CNCS prende é produzir é norma, que os operadores tenham que respeitar. Ou seja, uma regulamentação que estabeleça um conjunto de requisitos, com revisão anual ou bianual, tendo em conta o quadro de ameaças que também é flutuante e variável. A lei prevê apenas uma Autoridade Nacional de Cibersegurança, que é o CNCS. Nós entendemos que não devemos fazer uma regulamentação de um sector da economia, nas costas de um regulador, tendo sido desenvolvido em colaboração muito estreita com os diversos reguladores. Contudo, a consciência dos diversos sectores é muito diferente. Por exemplo, o sector da banca tem uma consciência muito forte destas áreas e é muito fácil falar como este regulador. Por outro lado, se virmos por exemplo o sector das águas, há ainda um trabalho a fazer por forma a que o diálogo com eles lhe dê capacidades para lidarem com este tema dentro do seu negócio.
E5	Não aplicável / Não responde.
	5. Outros
5.1	**Como se articulam os planos das FFSS relativamente ao ciberespaço? As FFSS têm alguma intervenção nesta área, ou deveriam ter? Qual o papel do CNCS?**
E1	R.: Doutrinariamente o ciber faz parte do *security*, é uma ameaça hostil, intencional, por isso é, ou deveria ser uma parte da segurança por todas as razões. Por um lado, embora os vetores da ameaça sejam uns vetores específicos, que levam a que o tratamento desse vetor seja um bocado diferente (mas também não é assim tão diferente). Veja-se por exemplo a questão das ameaças híbridas (que tem tudo a haver com cibersegurança, segurança de IC, com propaganda, etc.), pelo que hoje em dia não se deve segmentar demasiado estas questões. Claro que há aspetos próprios da cibersegurança tal com há aspetos próprios de outros vetores de ameaça de criminalidade. Portanto, estas questão devem estar sobre um mesmo chapéu. O que acontece é que na Europa foi feito uma diretiva própria de proteção de IC de informação. E quando isto foi feito, acabou por, de alguma forma, por se dar um sinal de que os Estados membros deveriam seguir dois caminhos. Ou seja, esta diretiva nova tem

	também as suas próprias IC, que podem coincidir ou não com estas. No fundo, é como se estivéssemos a falar duas línguas parecidas, mas que não são iguais. Do meu ponto de vista, e não representando aqui a Secretária-geral para este efeito, penso que isto veio baralhar um bocado (e já foi discutido em algumas reuniões), e isto aconteceu também em outros estados membros. Portanto, estes diferentes atores têm que se articular. Nas IC clássicas, isto é, aquelas que estão ao abrigo o Decreto-Lei n.º 62/2011, existe a preocupação com as questões ciber, sendo que cada vez mais o CNCS terá que ser mais integrado em tudo isto. Como consequência disso, até do ponto de vista dos operadores, sente-se uma certa divisão nos departamentos que deveriam ser integrados. Pois se houver uma ciberameça que se concretize num operador de uma IC, existe o combate à ameaça propriamente dita, mas depois existe também a gestão dos danos que estão a ser causados e que envolve comunicação, articulação com outras entidades, ativação de planos de emergência e continuidade de negócio, pelo que tudo isto deva estar devidamente articulado. O CNCS faz parte do concelho superior de segurança interna, não havendo qualquer dificuldade de contacto ou problema com isso. Em termos de dificuldades, julgo que talvez seja uma questão de cultura e de reconhecimento do que já existe. É importante quando se legisla, ter em consideração o contexto de que já há coisas existentes sobre as matérias, e é útil, do meu ponto de vista, que haja pontes, independentemente de existir braços que façam face a situações específicas que vão aparecendo (como a cibersegurança), mas creio que, o que vá ser feito de novo deva ser bem articulado com o que já existe, fazendo referências uns aos outros, o que facilita e obriga os vários intervenientes a conversar uns com os outros. Por exemplo, na revisão do Decreto-Lei n.º 62/2011, é feita a referência à Lei de Segurança do Ciberespaço e à Estratégia Nacional de Segurança do Ciberespaço. Há um domínio estratégico, relacionado com as informações, que é maior que o SSI e garantidamente muito maior que o CNCS. Portanto, há que ter em conta esta sensibilidade, que há infraestruturas dentro das críticas que são muito críticas. Se houver um problema numa IC, por exemplo em uma de informação crítica, se for um problema que se prolongue no tempo, a resposta não vai ser dada exclusivamente pelo CNCS, mas antes por um conjunto muito mais alargado de entidades que envolverá a saúde, governança, soberania, defesa e segurança, e que têm de estar muito articuladas e para as quais tem de haver uma coordenação. Se houver um ataque terrorista a uma infraestrutura num sítio específico, a importância de a força de segurança lá chegar e tentar resolver a situação é um primeiro momento, mas depois há um momento que é se de facto o ataque se concretizar e houver mais dois ou três em infraestruturas combinadas é preciso perceber o impacto que isto tem e como enquanto sociedade nos organizamos para ligar com isto. Podemos olhar para o ciberespaço como ferramenta instrumental (de um crime) ou como um mecanismo essencial de perpetuação de um ciberataque (tal como um *ransomware*) em que o próprio ciberespaço é o canal para o ataque. No caso de ciberataques, o CNCS tem um papel determinante, pois tem mecanismos de deteção, recebe notificações e tem contacto com outros centros semelhantes noutros países. Depois há o domínio da utilização do ciberespaço como todos nós utilizamos, onde colocamos informação, onde se pode tentar fazer burlas, extorsão, engenharia social, etc., sendo que aí as forças de segurança podem ter um papel importante. Veja-se este exemplo simples: se calhar o CNCS consegue detetar um ataque de *ransomware* a um operador de IC, mas não deve ser a instituição/entidade indicada para detetar se um funcionário de uma subestação está a consultar sites de cariz radical. Por isso, deste ponto de vista, as forças de segurança têm um papel a desempenhar, até pela proximidade que tem com os operadores, em que visitam os locais e conhecem a sua dinâmica, sendo por isso o ciberespaço uma extensão do mundo físico onde as forças de segurança também devem atuar.
E2	R.: Uma das questões a rever na legislação futura é o papel do CNCS, que deve passar a ter um papel na componente ciber dos PSO. Ou seja, neste momento o CNCS não tem um envolvimento direto na proteção de IC (no que decorre da Decreto-Lei 62/2011). Na minha opinião, deveriam ser envolvidos

	na aprovação do PSO, isso pode passar por uma articulação informal e serem convidados para integrar o GT PIC (o que nunca foi feito), mas acho que há necessidade de existir uma revisão legislativa.
E3	R.: Neste momento é a parte do *security* que dá o parecer, mas deveria ser o CNCS […] O ciber é transversal ao *safety* e ao *security*. Mas neste momento não está coordenado como deveria ser. […] Acho que deveria haver apoio por parte do CNCS […] todos tínhamos mais a ganhar se o CNCS estivesse mais empenhado nesta circunstância.
E4	**[Alteração a esta questão]: Em síntese, qual o atual papel do CNCS na PIC, e qual deveria ser**? R.: O CNCS tem responsabilidades que decorrem da lei orgânica do GNS [Gabinete Nacional de Segurança] onde o CNCS está inserido. Temos como uma das nossas comunidades de interesse as IC. O que estamos a trabalhar em IC é essencialmente a reação a ciberincidentes (exemplo: serviço de suporte *onsite* a operadores de IC) e a capacitação em cibersegurança.
E5	Não aplicável / Não responde.
5.2	**Em que medida as Forças Armadas (FFAA) colaboram na PIC (pode dar exemplos)? Acha que estas poderiam desempenhar um papel mais preponderante na PIC?**
E1	R.: Acho que sim poderiam desempenhar um papel na proteção das IC. Nesta fase, está a ser discutido os mecanismos e protocolos de atuação das FFAA. Dependendo do que decorra desse plano, podem ser elencadas algumas medidas no âmbito da proteção das IC. As FFAA já desenvolvem missões, como por exemplo a vigilância de florestas para prevenir a ocorrência dos fogos florestais. Num determinado momento em que o empenhamento das forças de segurança não fosse suficiente, e se houvesse um grau de ameaça especificamente dirigido às IC, em que fosse necessário, por exemplo, assegurar a presença física de pessoas em várias IC (que são muitas e serão muitas mais se se avançar para os 12 sectores), naturalmente as FFAA poderiam ser empenhadas na questão da vigilância e presença humana nessas infraestruturas, para dissuadir uma prática ilícita, apoiando assim, suplementarmente, as forças de segurança e desta forma aumentar a proteção e a vigilância destas infraestruturas que estão espalhadas pelo território nacional. Mas aspetos mais concretos, de armamento, de capacidade de reação, terá que ser o plano a definir. Num cenário de normalidade, as forças de segurança têm meios suficientes, *know how* e capacidade para lhe fazer face. Mas, num cenário de ameaça difusa, isto é, no sentido de não se perceber exatamente qual é o alvo, mas ser uma ameaça real com alta probabilidade de ocorrência de ataques contra IC, e dado o número de infraestruturas existentes, não era sustentável dizer-se que as forças de segurança conseguiriam ter total cobertura das IC, pelo que nessa circunstância, havendo um mecanismo que permitisse a intervenção FFAA naturalmente aumentava-se a proteção das IC.
E2	R.: Neste momento não colaboram, sendo que está a ser ultimado um acordo no âmbito do art.º 35.º da Lei de Segurança Interna (colaboração das Forças Armadas com as Forças e Serviços de Segurança) e no âmbito da Estratégia Nacional de Combate ao Terrorismo, entre a Secretária-geral do SSI e o CEMGFA. No entanto, o apoio poderá passar por um papel de supletividade relativamente às forças de segurança, como por exemplo apoio logístico. No campo ciber, poderá haver um papel mais ativo do Centro de Ciberdefesa, mas será sempre um papel supletivo.
E3	R.: As FFAA têm um papel também para a proteção das IC, tem é que ser definido. Neste momento não existe essa definição, se bem que tem lugar legal e em termos das suas capacidades. Exemplos de atuação das FFAA: sempre que há necessidade de intervenção num incidente tático policial, existe sempre várias abordagens e várias necessidades, desde a questão do controlo do espaço aéreo […] ou marítimo, a questão do apoio às comunicações caso seja necessário, o apoio logístico, há sempre um conjunto de ações que podem ser asseguradas pelas FFAA […] tem é de ser definido como é o seu emprego.
E4	R.: As Forças Armadas fazem parte da estratégia nacional do ciberespaço. O designo que as FFAA têm no mundo real (no mundo físico), devem também exercê-la no mundo virtual. Compete às FFAA

	a atuação no âmbito da ciberguerra e também defesa das suas instalações físicas e lógicas, dos seus sistemas de informação.
E5	R.: As FFAA têm capacidade, mantendo a sua estrutura de comando, para apoiar as FFSS na segurança de IC e de pontos sensíveis. Assim quando solicitadas a tal, as FFAA poderão colaborar com as FFSS, numa situação de necessidade justificante, em reforço e complemento, podendo a intervenção ocorrer, durante os estados de exceção, quando se verifiquem as condições previstas na Constituição da República ou, fora deles, quando a avaliação do SGSSI indicar e suscitar tal necessidade.
	Outra informação referida pelo entrevistado
E1	A lei atribui uma série de atribuições à Secretária-Geral do SSI em termos de coordenação da proteção a IC, sendo o seu gabinete que se ocupa de dirigir esse processo e tentar chegar a bom porto com as várias competências que estão distribuídas de acordo com o Decreto-Lei n.º 62/2011. O Subintendente João Pestana desempenha funções na área das IC há cerca de cinco anos. Lidera o Grupo de Trabalho com as forças de segurança para a proteção de IC (designado GT PIC) e é também o ponto de contacto para a área do *security* junto da União Europeia.
E2	-
E3	O grupo de trabalho das IC, constituído em 2016, é liderado pelo SSI e integra elementos da GNR, PSP, PM e SIS. […] Aquilo que carece de uma maior intervenção, porque é transversal, é parte ciber. Não é porque não tenham a capacidade, é porque ainda não estão integrados no sistema como deveriam estar. […] Relativamente à GNR os planos já formam todos entregues ao SSI. Por agora estamos na fase final de validação dos planos. […] Depois de todos os planos aprovados, a fase seguinte é disponibilizá-los aos Comandos Territoriais.
E4	O CNCS não tem assento no grupo de trabalho sobre IC que tem lugar no Sistema de Segurança Interna, mas, deram-nos conta da revisão da Lei 62/2011 no ano passado. **Qual o ponto de situação relativamente ao Plano de Ação Nacional para a Proteção contra as Ciberameaças?** R.: Isso está na tutela do SSI. Deveria ser dada atenção à estratégia de segurança do ciberespaço, cuja a versão 2.0 foi elaborada pelo concelho de segurança no ciberespaço, no qual o SSI tem assento, e está neste momento na tutela para ser aprovada.
E5	**Como é que as FFAA entendem as IC?** R.: AS FFAA cumprem a Lei e podem, no tempo e modo adequado, contribuir para a revisão dos conceitos se tal se afigurar adequado. **Acha que estas poderiam desempenhar um papel mais preponderante na PIC? Têm atualmente meios e pessoal que possam ser empenhados na proteção de IC?** As FFAA têm capacidades que podem empenhar na proteção de IC, se tal for superiormente decidido.

Apêndice C — Questionário aplicado aos Comandantes Territoriais da GNR

*Obrigatório

INSTITUTO UNIVERSITÁRIO MILITAR

CURSO DE ESTADO-MAIOR CONJUNTO 2018/19

A intervenção das Forças de Segurança na proteção de infraestruturas críticas e o papel das Forças Armadas

A presente investigação insere-se no âmbito de um Trabalho de Investigação Individual do Curso de Estado-Maior Conjunto do Instituto Universitário Militar, visando, em contexto académico, perceber como é que a GNR conduz a sua intervenção na proteção das infraestruturas críticas, se tem as capacidades adequadas e quais são as principias necessidades e dificuldades nesta área.

Este questionário é dirigido a todos os Comandantes Territoriais da GNR mas é totalmente anónimo. É composto por 10 questões (de escolha múltipla ou de resposta aberta) agrupadas em 5 secções.

Uma vez que a informação sobre quais as infraestruturas críticas identificadas até ao momento é matéria classificada, independentemente do Sr. Comandante ter infraestruturas críticas (oficialmente designadas) na sua área de jurisdição, para responder às seguintes questões imagine uma infraestrutura que considere crítica e como a poderia proteger.

Muito obrigado pela sua colaboração.

Monteiro Fernandes
Major

1. Importância das infraestruturas críticas

1. **1.1 Na sua opinião, qual a importância que a GNR atribui à proteção das infraestruturas críticas?** *
   Marcar apenas uma oval.

	1	2	3	4	
Pouco importante	◯	◯	◯	◯	Muito importante

*Obrigatório

INSTITUTO UNIVERSITÁRIO MILITAR

CURSO DE ESTADO-MAIOR CONJUNTO 2018/19

A intervenção das Forças de Segurança na proteção de infraestruturas críticas e o papel das Forças Armadas

A presente investigação insere-se no âmbito de um Trabalho de Investigação Individual do Curso de Estado-Maior Conjunto do Instituto Universitário Militar, visando, em contexto académico, perceber como é que a GNR conduz a sua intervenção na proteção das infraestruturas críticas, se tem as capacidades adequadas e quais são as principias necessidades e dificuldades nesta área.

Este questionário é dirigido a todos os Comandantes Territoriais da GNR mas é totalmente anónimo. É composto por 10 questões (de escolha múltipla ou de resposta aberta) agrupadas em 5 secções.

Uma vez que a informação sobre quais as infraestruturas críticas identificadas até ao momento é matéria classificada, independentemente do Sr. Comandante ter infraestruturas críticas (oficialmente designadas) na sua área de jurisdição, para responder às seguintes questões imagine uma infraestrutura que considere crítica e como a poderia proteger.

Muito obrigado pela sua colaboração.

Monteiro Fernandes
Major

1. Importância das infraestruturas críticas

1. **1.1 Na sua opinião, qual a importância que a GNR atribui à proteção das infraestruturas críticas?** *
   Marcar apenas uma oval.

	1	2	3	4	
Pouco importante	◯	◯	◯	◯	Muito importante

2. **1.2 De acordo com a sua experiência, acha que o país está suficientemente empenhado nesta matéria?** *
Marcar apenas uma oval.

	1	2	3	4	
Pouco empenhado	◯	◯	◯	◯	Muito empenhado

3. **1.3 Quais considera serem as principais vulnerabilidades nesta área, e que implicações isso acarreta?** *

2. Como classifica o quadro legal existente relativo às infraestruturas críticas (proteção e intervenção)?

4. **É inteligível?**
Marcar apenas uma oval.

	1	2	3	4	
Nada inteligível	◯	◯	◯	◯	Completamente inteligível

5. **É adequado?** *
Marcar apenas uma oval.

	1	2	3	4	
Nada adequado	◯	◯	◯	◯	Completamente adequado

6. **É bem articulado?** *
Marcar apenas uma oval.

	1	2	3	4	
Mal articulado	◯	◯	◯	◯	Bem articulado

3. As capacidades atualmente existentes na GNR são adequadas e suficientes para intervir na proteção das infraestruturas críticas?

7. **Organização** *
Marcar apenas uma oval.

	1	2	3	4	
Nada adequada	◯	◯	◯	◯	Completamente adequada

8. **Pessoal** *
Marcar apenas uma oval.

	1	2	3	4	
Insuficiente	◯	◯	◯	◯	Completamente adequado

9. **Meios** *
Marcar apenas uma oval.

	1	2	3	4	
Nada adequados e insuficientes	◯	◯	◯	◯	Completamente adequados e suficientes

10. **Treino / exercícios** *
Marcar apenas uma oval.

	1	2	3	4	
Inexistentes ou desadequados	◯	◯	◯	◯	Suficientes e adequados

11. **Colaboração com outras entidades** *
Marcar apenas uma oval.

	1	2	3	4	
Pouca ou má colaboração	◯	◯	◯	◯	Excelente colaboração

12. **3.1 Na sua opinião, quais são as principais dificuldades e necessidades?** *

13. **3.2 Quais deveriam ser as capacidades a edificar na GNR para incrementar a Proteção das Infraestruturas Críticas?** *

4. Planos de segurança

14. **4.1 No seu entender, os Planos de Segurança da responsabilidade dos Operadores (PSO) estão a ser bem executados, são adequados e suficientes?** *

15. **4.2 Relativamente aos Planos de Segurança e Proteção Exterior (PSPE), que estão em elaboração, quais são as principais dificuldades da sua implementação?** *

5. Outras questões

16. **5.1 Assumindo que as Forças Armadas pudessem colaborar na proteção das infraestruturas críticas (ultrapassados os aspetos legais e normativos), pode dar exemplos de situações em que estas pudessem ser utilizadas?** *

17. **Outros comentários relativos à intervenção da GNR na proteção das infraestruturas críticas:**