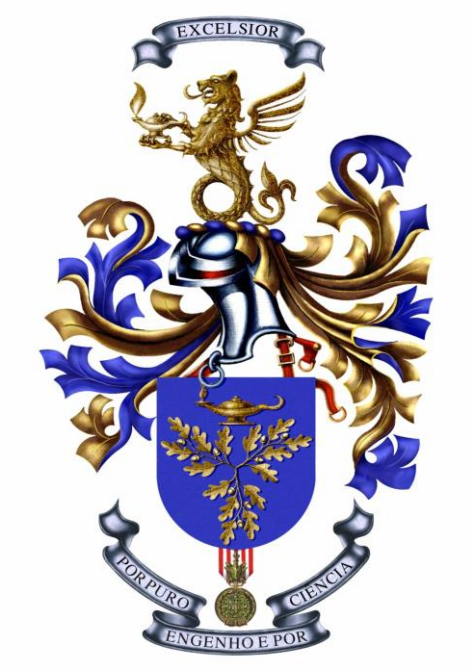
INSTITUTO UNIVERSITÁRIO MILITAR
DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS
CURSO DE PROMOÇÃO A OFICIAL GENERAL
2017/2018



TRABALHO DE INVESTIGAÇÃO INDIVIDUAL

O CIBERESPAÇO NA DEFESA COLETIVA E NA GESTÃO DE CRISES: ARTICULAÇÃO ENTRE A CIBERSEGURANÇA E A CIBERDEFESA

José Manuel dos Santos Coelho
Capitão-de-mar-e-guerra, Engenheiro Maquinista Naval

INSTITUTO UNIVERSITÁRIO MILITAR

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

O CIBERESPAÇO NA DEFESA COLETIVA E NA GESTÃO DE CRISES: ARTICULAÇÃO ENTRE A CIBERSEGURANÇA E A CIBERDEFESA

CMG EMQ José Manuel dos Santos Coelho

Trabalho de Investigação Individual do CPOG

Pedrouços 2018

INSTITUTO UNIVERSITÁRIO MILITAR
DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

O CIBERESPAÇO NA DEFESA COLETIVA E NA GESTÃO DE CRISES: ARTICULAÇÃO ENTRE A CIBERSEGURANÇA E A CIBERDEFESA

CMG EMQ José Manuel dos Santos Coelho

Trabalho de Investigação Individual do CPOG

Orientador: COR TIR TM Luís Filipe Camelo Duarte Santos

Pedrouços 2018

Declaração de compromisso antiplágio

Eu, **José Manuel dos Santos Coelho**, declaro por minha honra que o documento intitulado **"O ciberespaço na defesa coletiva e na gestão de crises: articulação entre a cibersegurança e a ciberdefesa"** corresponde ao resultado da investigação por mim desenvolvida enquanto auditor do **Curso de Promoção a Oficial General 2017/2018** 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**, 27** de **julho** de **2018**

CMG EMQ José Manuel dos Santos Coelho

Agradecimentos

Ao Coronel Tirocinado Luís Camelo, meu orientdor, pelo apoio ao longo da execução desta investigação.

Aos Coronel Amaral Lopes e ao Capitão-tenente Câmara de Assunção, pelo auxílio prestado nos contactos com os participantes, respetivamente, nos exercícios *Crisis Management Exercise* 2017 e *Cyber Coalition* 2017.

Aos Contra-Almirante Gameiro Marques, Comodoro Jorge Pires, Coronel João Barbas, Capitão-de-mar-e-guerra Correia Policarpo, Capitão-de-mar-e-guerra Fialho de Jesus e Major Rogério Raposo, pela disponibilidade, conhecimento transmitido e reflexões desafiadoras, que muito orientaram e auxiliaram nesta investigação.

Aos camaradas auditores do Curso de Promoção a Oficial General, pela motivação proporcionada e amizade manifestada, em especial ao Capitão-de-mar-e-guerra Sobral Domingues e Coronel Lemos Pires que, com os seus contributos e incentivos, viabilizaram a chegada desta barca a bom porto.

Índice

Índice de Apêndices

Índice de Figuras

Índice de Quadros

Resumo

A relação civil/militar no ciberespaço, entendida como o papel a desempenhar pelas Forças Armadas ao longo do espetro do conflito naquele ambiente, requer um elevado nível de articulação entre a ciberdefesa e a cibersegurança, desafiando a forma tradicional como os Estados se organizam para providenciar o estado de segurança desejado.

Recorrendo a uma estratégia de investigação essencialmente qualitativa, assente num método de raciocínio dedutivo e seguindo um desenho de pesquisa de estudo de caso, estabeleceu-se a segurança nacional no ciberespaço como objeto da investigação. Pretendeu-se identificar contributos que habilitem o Estado Português a empregar, sempre que necessário, incluindo em situação de crise, a ação unificada dos instrumentos, civis e militares, na resposta a incidentes de segurança no ciberespaço, considerando a organização nacional para a segurança no ciberespaço em países de referência e a situação atual em Portugal.

Como resultado da investigação propõe-se o conceito de Centro Nacional de Operações de Segurança no Ciberespaço, que considera a partilha, entre as entidades da organização nacional para a segurança no ciberespaço, quer de recursos humanos tecnicamente especializados em operações ofensivas, quer de um conhecimento situacional acionável sobre o ciberespaço.

Palavras-chave

Ciberespaço, relação civil/militar, segurança nacional, cibersegurança e ciberdefesa.

Abstract

Cyberspace poses challenges to how states organize themselves to ensure the appropriate level of security in this environment. The civil/military relationship in cyberspace, as the role to be performed by the Armed Forces throughout the spectrum of the conflict, including in situations other than war, forces the articulation between cyber-defence and cybersecurity.

Using an essentially qualitative research strategy, with a deductive reasoning method and a case study research design, the investigations' object was national security in cyberspace. The purpose was to identify contributes for the improvement of civil/military relationship in cyberspace within the Portuguese State's organizational context, considering the organization for security in cyberspace in reference countries and the current situation in Portugal. Those contributes were made in order to facilitate, when necessary, including in crisis, the unified action of relevant entities, civil and military, in response to incidents in cyberspace.

As a result of the research, the concept of a National Center for Security Operations in Cyberspace is proposed, which comprehends the sharing, among the entities of the national organization for security in cyberspace, of human resources technically specialized in offensive operations and an actionable cyberspace situational awareness.

Keywords

Cyberspace, civil/military relationship, national security, cybersecurity and cyber defence.

Lista de abreviaturas, siglas e acrónimos

ACT	*Allied Command for Transformation*
ANPC	Autoridade Nacional de Proteção Civil
AR	Assembleia da República
C2	Comando e Controlo
C2CoE	NATO *Command and Control Centre of Excellence*
CC2017	*Cyber Coalition* 2017
CCD	Centro de Ciberdefesa
CCDCoE	*Cooperative Cyber Defence Centre of Excellence*
CEDN	Conceito Estratégico de Defesa Nacional
CERT	*Computer Emergency Response Team*
CERT.PT	*Computer Emergency Response Team*, Portugal
CISMIL	Centro de Informações e Segurança Militares
CMDRCoE	*Crisis Management and Disaster Response Centre of Excellence*
CMX2017	*Crisis Management eXercise* 2017
CNCS	Centro Nacional de Cibersegurança
CNOSC	Centro Nacional de Operações de Segurança no Ciberespaço
CNOSC-CGes	Comité de Gestão do Centro e dos RHETO (CNOSC)
CNOSC-CGov	Comité de Governação do Centro e dos RHETO (CNOSC)
CNOSC-eCCC	Estrutura no CNOSC-Setor_CC responsável pelas ações de combate ao crime no ciberespaço
CNOSC-eCNCS	Estrutura no CNOSC-Setor_CNCS responsável pela coordenação operacional da cibersegurança nacional
CNOSC-eI/CI(C)	Estrutura no CNOSC-Setor_I/CI(C) responsável pelas ações de informações e contrainformações no ciberespaço
CNOSC-eI/CI(M)	Estrutura no CNOSC-Setor_OM responsável por conduzir operações de informações e de contrainformações militares no ciberespaço
CNOSC-eOMC	Estrutura no CNOSC-Setor_OM responsável pelas operações militares no ciberespaço
CNOSC-ETP	Equipa Técnica Própria
CNOSC-IAO	Informação de Ações/Operações (CNOSC)

CNOSC-IAOp	Informação de Ações/Operações partilhada (CNOSC)
CNOSC-IGC	Informação para a Gestão do Conhecimento (CNOSC)
CNOSC-IRP	Informação sobre Regras de Partilha (CNOSC)
CNOSC-RHETO	Recursos Humanos com Especialização Técnica Ofensiva (CNOSC)
CNOSC-Setor_CC	Estrutura do Estado responsável pelas ações de combate ao crime (CNOSC)
CNOSC-Setor_CNCS	Estrutura do Estado responsável pela coordenação estratégica da cibersegurança nacional (CNOSC)
CNOSC-Setor_I/CI(C)	Estrutura do Estado responsável pelas ações de informações e de contrainformações civis (CNOSC)
CNOSC-Setor_OM	Estrutura do Estado responsável pelas operações militares (CNOSC)
CPOG	Curso de Promoção a Oficial General
CRN	Célula de Resposta Nacional
CSC	Conhecimento Situacional do Ciberespaço
CSIRT	*Computer Security Incident Response Team*
CSSC	Conselho Superior de Segurança do Ciberespaço
CUE	Conselho da União Europeia
DEF	Setor da Defesa no governo de um Estado
DIOPC	Diretiva Iniciadora com a Orientação Política para a Ciberdefesa
DIRCSI	Direção de Comunicações e Sistemas de Informação
DoDAF	*Department of Defense Architectural Framework*
EMGFA	Estado-Maior General das Forças Armadas
ENSC	Estratégia Nacional de Segurança no Ciberespaço
EP	Estado Português
EUA	Estados Unidos da América
FFAA	Forças Armadas
GOV-PT	Governo de Portugal
IC	Infraestruturas Críticas
ICSE	Infraestruturas Críticas e Serviços Essenciais
IDN	Instituto da Defesa Nacional

IESM	Instituto de Estudos Superiores Militares
IUM	Instituto Universitário Militar
JP	*Joint Publication*
LSI	Lei de Segurança Interna
M2C2IO	Modelo de Maturidade C2 para a Interoperabilidade Organizacional
M2C2IO-A	Variável propósito e **A**spirações da dimensão Etos do M2C2IO
M2C2IO-C	Variável **C**omunicação da dimensão Compreensão do M2C2IO
M2C2IO-D	Variável **D**outrina da dimensão Preparação do M2C2IO
M2C2IO-E	Variável **E**xperiência da dimensão Preparação do M2C2IO
M2C2IO-F	Variável con**F**iança da dimensão Etos do M2C2IO
M2C2IO-N	Variável co**N**hecimento da dimensão Compreensão do M2C2IO
M2C2IO-P	Variável **P**apéis e responsabilidades da dimensão Governação do M2C2IO
M2C2IO-S	Variável distribuição de direitos de deci**S**ão da dimensão Governação do M2C2IO
M2C2IO-T	Variável **T**reino da dimensão Preparação do M2C2IO
M2C2IO-U	Variável c**U**ltura e sistema de valores da dimensão Etos do M2C2IO
MDN	Ministério da Defesa Nacional
NAC	*North Atlantic Council*
NATO	*North Atlantic Treaty Organization*
NE	Setor dos Negócios Estrangeiros no governo de um Estado
NEP/ACA	Norma Académica de Execução Permanente
NICCS	*National Initiative for Cybersecurity Careers and Studies*
OE	Objetivo Específico
OG	Objetivo Geral
ONSC	Organização Nacional para a Segurança no Ciberespaço
ONSC-CCC	Combate ao Crime no Ciberespaço (mandato da ONSC)
ONSC-Coord.Est.	Coordenação ao nível estratégico (mandato na ONSC)
ONSC-Coord.Oper.	Coordenação ao nível operacional (mandato na ONSC)
ONSC-GCC	Gestão de Crises no Ciberespaço (mandato na ONSC)

ONSC-IeCI	Informações e Contrainformações (mandato da ONSC)
ONSC-OMC	Operações Militares no Ciberespaço (mandato da ONSC)
ONSC-Part.Info.	Partilha de Informação (mandato na ONSC)
ONSC-PIC	Proteção de Infraestruturas Críticas (mandato da ONSC)
ONSC-PT	Organização Nacional para a Segurança no Ciberespaço em Portugal
PB	Países Baixos
PB-DCC	*Defence Cyber Command* dos Países Baixos
PB-DCS	*Defence Cyber Strategy* dos Países Baixos
PB-DefCERT	*Defence Computer Emergency Response Team* dos Países Baixos
PB-DISS	*Defence Intelligence and Security Service* dos Países Baixos
PB-GISS	*General Intelligence and Security Service* dos Países Baixos
PB-GOV	Governo dos Países Baixos
PB-JSCU	*Joint Sigint Cyber Unit* dos Países Baixos
PB-NCSC	*National Cyber Security Center* dos Países Baixos
PB-NCSCt	*National Coordinator for Security and Counterterrorism* dos Países Baixos
PB-NCSS2	*National Cyber Security Strategy 2* dos Países Baixos
PCE	Planeamento Civil de Emergência
PE	Parlamento Europeu
PL119/XIII	Proposta de Lei n.º 119/XIII
PM	Nível de governo do Primeiro-Ministro ou de gabinete que o apoia diretamente no governo de um Estado
PSD	Prestadores de Serviços Digitais
PT	Portugal
QC	Questão Central
QD	Questão Derivada
RCM	Resolução do Concelho de Ministros
Rede CSIRT	Rede *Computer Security Incident Response Team*
RU	Reino Unido
RU-CGSD	*Cyber and Government Security Directorate* do Reino Unido
RU-CSOC	*Cyber Security Operations Centre* do Reino Unido

RU-GCHQ	*Government Communications Headquarters* do Reino Unido
RU-GOV	Governo do Reino Unido
RU-NCA	*National Crime Agency* do Reino Unido
RU-NCCU	*National Cyber Crime Unit* do Reino Unido
RU-NCSC	*National Cyber Security Center* do Reino Unido
RU-NSC	*National Security Council* do Reino Unido
SGSSI	Secretário-Geral do Sistema de Segurança Interna
SI/J	Setor da Segurança Interna ou da Justiça no governo de um Estado
SIS	Serviço de Informações de Segurança
SNGC	Sistema Nacional de Gestão de Crises
SOC	*Security Operations Center*
UE	União Europeia
UNC3T	Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica
USDoD	*United States Department of Defense*
USJCS	*United States Joint Chiefs of Staff*

Introdução

Enquadramento e justificação do tema

Esta investigação enquadra-se na materialização da vontade, soberania e salvaguarda da liberdade da ação na persecução do interesse nacional no ciberespaço e que inclui a necessidade de providenciar um estado de segurança que proteja os bens jurídicos, quer dos cidadãos, quer dos agentes sociais e económicos em geral, bem como o cumprimento dos compromissos internacionais assumidos por Portugal (PT)[1].

O Conceito Estratégico da Defesa Nacional (CEDN) estabelece, como elemento essencial da estratégia nacional, o estatuto de Portugal como coprodutor de segurança internacional, sublinhando, neste particular, as Forças Armadas (FFAA), mas também outros setores do Estado Português (EP), relevando a necessidade de se definir uma estratégia integrada, civil e militar, para fazer face às ameaças e riscos. Neste documento o Governo de Portugal (GOV-PT) salienta ainda o potencial disruptivo de ataques efetuados no e através do ciberespaço, perpetrados por Estados, terroristas, criminalidade organizada e indivíduos isolados, podendo afetar Infraestruturas Críticas (IC), bem como o normal funcionamento da economia e da sociedade de informação global (GOV-PT, 2013a).

A publicação da Estratégia Nacional de Segurança no Ciberespaço (ENSC) formalizou o reconhecimento de que o ciberespaço se constitui como uma oportunidade para "(…) disponibilizar benefícios económicos e sociais, estimular a criação de emprego, a sustentabilidade e a inclusão social (…)", mas que, como contraponto à transposição da "(…) vida real para um mundo virtual (…)" são reproduzidos para este ambiente todos os riscos associados às interações políticas, económicas e sociais, colocando em risco as pessoas, as empresas e a própria soberania do Estado (GOV-PT, 2015).

É com a constatação da necessidade de uma abordagem multissetorial e integrada para providenciar o adequado nível de segurança nacional no ciberespaço, conforme preconizado no CEDN, que se levanta a interrogação central deste trabalho relativamente à articulação entre a cibersegurança e a ciberdefesa, entendidas como atividades da responsabilidade, respetivamente, das estruturas civil e militar do Estado, apresentando-se três evidências que justificam este estudo:

- Constata-se a dificuldade de identificação do papel da FFAA, no caso de necessidade de emprego em situações de não-guerra, não existindo um modelo

[1] Sigla e designação abreviada do país conforme norma 3166-1 alpha-2 da *International Organization for Standardization* em utilização na União Europeia (UE), adaptado de UE (2015).

consensual de implementação da relação civil/militar no ciberespaço (Boeke, Heinl e Veenendaal, 2015);

- A ENSC, no seu parágrafo 4.3)b), refere que as atribuições de planeamento e resposta imediata e efetiva a uma crise no ciberespaço são do Centro de Ciberdefesa[2] (CCD). No entanto, no seu parágrafo 4.5), a ENSC refere a necessidade de se estabelecer um gabinete para gestão de crises no ciberespaço; contudo, não providencia qualquer tipo de orientação relativamente ao papel anteriormente referido para o CCD (GOV-PT, 2015);
- No último exercício de nível político-estratégico da *North Atlantic Treaty Organization* (NATO), designado por *Crisis Management Exercise 2017* (CMX2017) e realizado em outubro de 2017, com a finalidade de praticar, testar e validar a gestão, as medidas e os mecanismos relacionados com o processo de consulta e de tomada de decisão coletiva na resposta a crises, apesar dos respetivos objetivos incluírem a exercitação ao nível da ciberdefesa, das comunicações estratégicas em ambiente híbrido e da interação civil/militar em crise (GOV-PT, 2017b; d), Policarpo (2017) referiu que, nem o CCD, nem a assessoria jurídica, foram mobilizados para a Célula de Resposta Nacional (CRN), tendo ainda sublinhado os constrangimentos de coordenação resultantes da inexistência de um Sistema Nacional de Gestão de Crises (SNGC).

Objeto de estudo e a sua delimitação

Da análise da formulação do tema proposto emerge a focalização na relação civil/militar decorrente da ênfase na articulação entre a cibersegurança e a ciberdefesa, emergindo o interesse de um posicionamento estratégico coerente das entidades envolvidas, de forma a que, em caso de necessidade, o EP possa mobilizar todos os seus instrumentos, incluindo o militar e a assistência internacional, num emprego articulado, tempestivo e eficaz. Assim, o objeto de estudo é a segurança nacional no ciberespaço.

O estudo é delimitado nos seguintes termos:

- Conteúdo: relação civil/militar nacional no ciberespaço, entendida como o papel a ser desempenhado pelas FFAA no contexto da segurança nacional, incluindo a respetiva estratégia, em situações de não-guerra, desde a situação de normalidade até à de crise;

[2] O CCD é um órgão na estrutura da Direção de Comunicações e Sistemas de Informação (DIRCSI) do Estado-Maior General das Forças Armadas (EMGFA) (GOV-PT, 2014a).

- Espaço: Organização Nacional para a Segurança no Ciberespaço (ONSC) em Portugal (ONSC-PT);
- Tempo: na atualidade.

Complementarmente o percurso da investigação foi moldado nos seguintes termos:

- A análise concetual teve como referência principal a doutrina do *United States Department of Defense* (USDoD), a doutrina da NATO e a teoria de Comando de Controlo (C2), sem prejuízo de outras fontes pontualmente consideradas;
- Explora-se ainda o corpo concetual e doutrinário de organizações de referência, designadamente os NATO *Command and Control Centre of Excellence* (C2CoE), NATO *Cooperative Cyber Defence Centre of Excellence* (CCDCoE) e NATO *Crisis Management and Disaster Response Centre of Excellence* (CMDRCoE) (CCDCoE, 2017; C2CoE, 2017; CMDRCoE, 2017);
- O estudo compreende ainda a análise de legislação nacional relativa a situações de crise, especialmente no ciberespaço;
- Como instrumento, foi estudada a ONSC de Estados de referência, designadamente Reino Unido (RU)[3] e Países Baixos (PB)[3];
- Para efeitos deste estudo a ONSC-PT é encarada como uma componente da defesa coletiva e da gestão de crises no contexto da NATO. Assim, a relação nacional/internacional da ONSC-PT com a NATO, quer no contexto da defesa coletiva, quer no da gestão de crises, será marginalmente abordada nesta investigação;
- Não serão abordados neste estudo: a relação público/privado, requisitos técnicos, ferramentas operativas e os aspetos táticos/técnicos de ações/operações de cibersegurança/ciberdefesa, independentemente de estarem ou não restringidas à relação civil/militar no ciberespaço.

[3] De acordo com UE (2015, 2018), a designação abreviada em português destes dois países está conforme a tradução oficial em vigor naquela instituição. Por questões de legibilidade, as siglas adotadas correspondem às iniciais da designação em português.

Graficamente a delimitação do tema está ilustrada na figura 1:

Figura 1 - Ilustração gráfica da delimitação do objeto de estudo

Objetivos da investigação

Tendo em consideração o objeto de estudo e a sua delimitação, os objetivos da investigação visam orientar o respetivo percurso e permitir aferir o sucesso da investigação. Assim, através da análise das estratégias e estruturas de países de referência, assim como as do EP, considerando o estado normal até à situação de crise, especialmente a gestão de crises no ciberespaço, pretende-se caracterizar a relação civil/militar da ONSC, para depois habilitar a identificação de contributos para melhorar a capacidade do EP no emprego, de forma coerente e articulada, de todos os instrumentos disponíveis, civis e militares, para, caso necessário, responder a uma situação de crise no ciberespaço. Desta forma, podemos assim estabelecer os Objetivos Geral (OG) e Específicos (OE) da investigação:

Quadro 1 - Objetivos Geral e Específicos

OG	**Identificar contributos para melhorar a coerência e articulação da resposta do Estado Português a situações de crise no ciberespaço, designadamente nos momentos em que seja necessário mobilizar todos os instrumentos nacionais relevantes, civis e militares, considerando o enquadramento normativo, organizações de referência e instrumentos de interoperabilidade organizacional.**
OE1	Caracterizar a relação civil/militar em organizações nacionais de segurança no ciberespaço, considerando a estratégia, estrutura e instrumentos de articulação operacional estabelecidos.
OE2	Analisar a coerência estratégica e articulação operacional no emprego dos instrumentos, civis e militares, do Estado Português, na resposta a uma crise no ciberespaço.
OE3	Formular linhas de ação para melhorar a eficácia da resposta do Estado Português a situações de crise no ciberespaço, considerando as diferentes entidades nacionais com responsabilidades na segurança deste ambiente.

Questões da investigação

Considerando o objeto do estudo, a delimitação do tema e após terem sido definidos os objetivos de investigação, importa agora formular a Questão Central (QC) e as respetivas Questões Derivadas (QD), a fim de estruturar o processo de investigação:

Quadro 2 - Questões Central e Derivadas

QC	**Considerando o enquadramento normativo, organizações de referência, assim como instrumentos de interoperabilidade organizacional, que contributos é que podem ser identificados para melhorar a resposta do Estado Português a situações de crise no ciberespaço, considerando a ação das diferentes entidades, civis e militares, com responsabilidade na segurança deste ambiente?**
QD1	Quais os padrões que emergem da estratégia, estrutura e instrumentos de articulação operacional de países de referência, com relevância para caracterizar a relação civil/militar em organizações nacionais de segurança no ciberespaço?
QD2	Considerando o emprego de todos os instrumentos, civis e militares, disponíveis, quais as características, ao nível da coerência estratégica e da articulação operacional, da organização de resposta do Estado Português a uma crise no ciberespaço?
QD3	Quais as linhas de ação para melhorar a eficácia da resposta do Estado Português a situações de crise no ciberespaço, considerando as entidades nacionais, civis e militares, com responsabilidades na segurança deste ambiente?

Breve síntese da metodologia da investigação

Este estudo enquadra-se no âmbito das Ciências Militares na área nuclear do Estudo das Crises e dos Conflitos Armados e, complementarmente, na área nuclear de Comando, Controlo, Comunicações, Computadores e Informação.

Recorrendo a um modelo de referência organizacional para os Estados providenciarem segurança no ciberespaço e a um modelo de maturidade de interoperabilidade

organizacional, o presente estudo explora o raciocínio dedutivo, na medida em que se parte "(…) de uma teoria em busca de uma verdade particular" (Santos et al., 2016, p.21), e adota uma estratégia de investigação qualitativa, com a análise de doutrina da NATO e dos Estados Unidos da América (EUA), assim como da ONSC de países de referência, complementada, no caso português, com uma análise quantificada da interoperabilidade organizacional, a fim de posteriormente retirar contributos para a melhorar a resposta da ONSC-PT a uma crise no ciberespaço.

O desenho de pesquisa foi de estudo de caso, considerando a análise da documentação e bibliografia relevante, os padrões encontrados em organizações de países de referência e, ainda, a interoperabilidade organizacional de entidades que, no contexto do EP, efetuaram recentemente exercícios relevantes.

Organização do estudo

A organização do estudo seguiu as recomendações metodológicas para a organização de trabalhos académicos no Instituto Universitário Militar (IUM[4]) (IESM, 2015b; Santos et al., 2016), sendo composto por uma introdução, quatro capítulos e a conclusão.

No primeiro capítulo efetua-se a revisão da literatura, incluindo uma análise crítica sobre a relevância dos conceitos apresentados para o presente trabalho, terminando com a descrição da metodologia adotada. No segundo capítulo efetua-se a descrição e análise crítica da forma como outros países se organizam para providenciar segurança no ciberespaço, com especial relevância para a relação civil/militar à luz do modelo de referência adotado e onde se procuram deduzir os padrões que possam ser relevantes para o caso português. No terceiro capítulo descreve-se e analisa-se criticamente a organização do EP para providenciar segurança no ciberespaço, incluindo a apresentação dos resultados de um questionário de interoperabilidade organizacional respondido pelos participantes nacionais nos exercícios CMX2017 e *Cyber Coalition* 2017 (CC2017). Tendo em vista melhorar a coordenação estratégica e a articulação operacional da relação civil/militar na ONSC-PT, no quarto capítulo apresentam-se as linhas de ação que foram identificadas. A encerrar, na conclusão, descreve-se o trajeto efetuado, os resultados obtidos, incluindo os contributos para melhorar a coerência e articulação da resposta do EP a uma crise no ciberespaço, identificando-se ainda contributos para o conhecimento, limitações desta investigação e eventuais linhas de desenvolvimento a considerar.

[4] Anterior Instituto de Estudos Superiores Militares (IESM).

1. Revisão de literatura e metodologia

1.1. Revisão da literatura

Os conceitos mais relevantes para este estudo são apresentados e discutidos nesta secção. O restante corpo de conceitos está descrito no apêndice A.

1.1.1. Segurança nacional no ciberespaço

A teleologia oferece a conceptualização de que as finalidades das unidades políticas são a Segurança e o Bem-Estar (Dias e Sequeira, 2017, p.13). Este é um entendimento consolidado já exposto por Couto (1987, p.307), quando refere que "(…) toda a unidade política visa duas finalidades fundamentais: a sua segurança ou sobrevivência e o seu progresso e bem-estar". A definição para segurança[5] proposta pelo Instituto da Defesa Nacional (IDN), para além das vertentes tradicionalmente consideradas na conceção vestefaliana, preconiza a adoção de soluções regionais e internacionais, não dividindo conceptualmente a segurança nacional em interna e externa, uma vez que os riscos e ameaças (p.e.: crime organizado, terrorismo, ou exploração abusiva de recursos comuns), são "(…) estruturalmente complexos, dispõem de grande mobilidade e possuem um caráter transnacional e difuso (…)", não respeitando os limites políticos e jurisdicionais das fronteiras geográficas (Ribeiro, 2017, p.50).

A conceptualização de um sistema de segurança que vise a utilização de todos os instrumentos à disposição do Estado, onde se deverá ainda incluir outros instrumentos da Nação, designadamente organizações e agentes não-estatais, numa perspetiva abrangente e holística, para além da componente polemológica da segurança fundada nas relações de poder, visa considerar, adicionalmente, os aspetos sociais, económicos, culturais e ambientais (Ribeiro, 2017, p.61). O CEDN sublinha este entendimento quando enuncia a necessidade de implementação de estratégias multissetoriais e integradas, desde logo na esfera do Estado (informações, segurança pública, proteção civil, investigação criminal, defesa), mas também que incluam o setor privado e, verticalmente, os níveis internacional, nacional e local (GOV-PT, 2013a).

A ENSC postula que a segurança do ciberespaço faz parte da segurança nacional e, enquanto estratégia multissetorial, entre outras medidas elencadas, refere a edificação da capacidade de ciberdefesa como um pilar da segurança nacional no ciberespaço (GOV-PT, 2015). Assim, a ENSC constitui-se como um instrumento para alcançar um estado desejado de segurança no ciberespaço de interesse nacional.

[5] Conceito exposto no apêndice A.

1.1.2. Caracterização do ciberespaço

O ciberespaço é um ambiente onde indivíduos, comunidades, organizações e Estados interagem para, por exemplo, socializar, estabelecer relações comerciais, efetuar transações financeiras, controlar a cadeia logística, gerir infraestruturas, incluindo as críticas, ou conduzir operações militares. Mas este "espaço" é passível de se tornar um ambiente de competição e mesmo de confronto, com níveis conflituais variáveis, desde crimes comuns, passando por crime organizado, espionagem, sabotagem ou terrorismo, incluindo ações que se podem configurar como ameaças à segurança nacional (USDoD, 2015).

A definição de ciberespaço tem vindo a desenvolver-se de forma a melhor capturar a evolução de que tem sido objeto, conduzida pela transformação tecnológica e pelos seus efeitos em praticamente toda a atividade humana[6]. Inicialmente considerando apenas o hardware, software, redes e sistemas de informação, constata-se a tendência para incluir aspetos de interação, socialização e os próprios humanos (Klimburg, 2012, p.8). Parecendo um exagero, esta evolução reflete a dificuldade de estabelecer uma definição concetualmente coerente e operacionalmente útil. Para este estudo consideram-se três definições propostas por Ottis e Lorents (2010), Schmitt (2013)[7] e NATO (2014), que se apresentam no apêndice A, e de onde se salientam as características de globalidade, interligação e a existência de componentes físicos e não físicos (virtuais). Adicionalmente, a definição apresentada por Ottis (2010) salienta distintivamente a dimensão de dependência do tempo, no sentido em que o ciberespaço se transforma (altera) ao longo desta dimensão, a um ritmo muito elevado, criando desafios de segurança, desde logo de conhecimento/compreensão situacional.

Complementarmente, o *United States Joint Chiefs of Staff* (USJCS) publicou a *Joint Publication* (JP) *3-12(R) Cyberspace Operations* (USJCS, 2013) que descreve o ciberespaço através de uma conceptualização em três camadas, conforme ilustrado na figura 2:

[6] O CCDCoE (2018) mantém uma lista com 29 definições diferentes.
[7] *Tallinn Manual on the International Law Applicable to Cyber Warfare*

Figura 2 - Descrição do ciberespaço
Fonte: adaptado de USJCS (2013)

Com exceção do espetro eletromagnético, o ciberespaço é um ambiente artificial construído pela humanidade, manifestando propriedades disruptivas e desafiantes (Tikk, 2011; IDN, 2013, p.10; Nunes, 2016): dinâmico (ambiente artificial em permanente mutação), assimétrico (baixo custo de entrada / elevado impacto), inimputabilidade (enorme potencial de anonimato), *continnuns* disruptivos (sem fronteiras físicas) e transversalidade (interação com ambiente físico)[8].

1.1.3. O espetro do conflito no ciberespaço

As características do ciberespaço apresentadas em 1.1.2., designadamente os *continuuns* disruptivos civil/militar, público/privado e nacional/internacional, colocam desafios organizacionais e de conhecimento/compreensão situacional aos Estados, conforme resulta do sublinhado de Tikk (2011, pp.70–71) "*The analyses of recent international cyber incidents show that a cyber-incident may range anywhere between a simple breach of internal regulations to ideologically motivated or organized cybercrime to national security relevant cyber attacks*". Considerando o propósito de analisar a forma como o Estado se

[8] No apêndice B descreve-se com mais detalhe as propriedades do ciberespaço aqui elencadas.

organiza para providenciar um nível de segurança aceitável neste ambiente, o espetro do conflito no ciberespaço deverá ser colocado a um nível político-estratégico, considerando um grau conflitual crescente, conforme apresentado na figura 3:

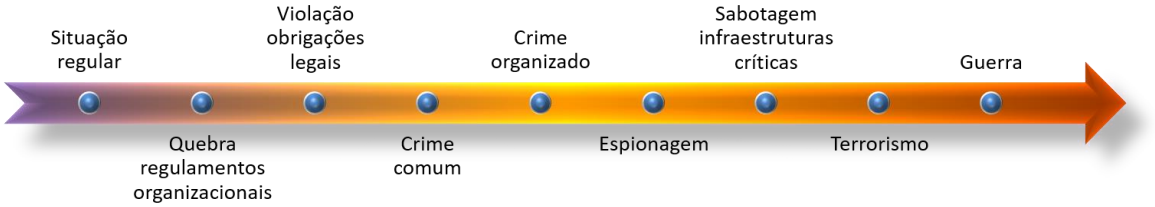


Figura 3 - Espetro do conflito no ciberespaço
Fonte: adaptado de Tikk (2011, p.69)

Ao longo do espetro do conflito o Estado mandata diferentes entidades para desenvolver diversas atividades no ciberespaço, desde a coordenação da resposta nacional a incidentes, o combate ao cibercrime, até à exploração ativa para a identificação de ameaças e mesmo à execução de operações militares, sublinhando-se a necessidade de coordenação e de partilha de informação que habilite um Conhecimento Situacional do Ciberespaço (CSC) partilhado e acionável.

1.1.4. Defesa coletiva e gestão de crises

A natureza do ciberespaço sugere que o Estado deverá preparar-se para mobilizar instrumentos de diversa natureza para a proteção dos interesses de Portugal, podendo incluir o recurso ao apoio de organizações internacionais. Este aspeto é evidenciado no atual CEDN (não apenas para o ciberespaço), quando atribui uma importância vital e decisiva à integração numa rede de alianças estáveis e coerente, designadamente a UE e a NATO (GOV-PT, 2013a, p.1982).

No caso da NATO, o atual conceito estratégico (NATO, 2010) estabelece a defesa coletiva[9] e a gestão de crises como duas[10] das missões centrais da Aliança. Para a NATO, numa situação de crise, que pode ou não incluir a componente militar, os Estados-Membro não têm a obrigação formal de responder a um pedido de apoio que seja solicitado por um dos membros. Este aspeto é relevante porque a situação de crise compreende um conjunto de tipologias que podem ir desde o simples apoio na sequência de um desastre natural, até situações que podem envolver força armada, estando previsto poder fazê-lo, em formatos que terão que ser ser decididos caso-a-caso pelo *North Atlantic Council* (NAC) (Marinov, 2014). Releva-se a circunstância de se reconhecer a impossibilidade de, à partida, se

[9] Ver definição no apêndice A.
[10] Sendo que a terceira é a segurança cooperativa.

conhecer todos os contornos relevantes de uma situação de crise, estando o empenhamento da NATO sempre dependente de decisão da mais alta instância política (NAC).

Uma crise no ciberespaço num Estado-Membro é tratada no enquadramento geral de gestão de crises da NATO. É oportuno sublinhar a possibilidade de modalidades de ação híbridas perpetradas por adversários que, mantendo o efeito das ações abaixo do nível suscetível de se considerar um ataque armado, o que faria despoletar uma resposta ao nível do artigo 5.º, criam a ambiguidade suficiente para suscitar dúvida e incerteza, afetando o processo de decisão do Estado-Membro em causa, e da própria Aliança (NATO, 2017b, pp.4–2). Adicionalmente, ainda que a NATO (2016) tenha considerado o ciberespaço como o quinto domínio operacional, as características descritas na secção 1.1.2. fazem dele um ambiente de eleição para este tipo de ações, criando ambiguidade e incerteza sobre a natureza e autoria da ação e, portanto, dificultando, a resposta adequada a providenciar, incluindo o respetivo processo de decisão.

É este aspeto de ambiguidade, num contexto de dúvida e incerteza sobre a autoria e natureza do que esteja a ocorrer, e que pode colocar em causa interesses vitais, que configura uma situação de crise[11] e que desafia os Estados a manterem estruturas nacionais de coordenação efetivas e um CSC credível e acionável, de forma a assegurar uma resposta coerente de todas as entidades que possam estar envolvidas, desde logo ao nível nacional e, caso necessário, em articulação com as entidades internacionais relevantes. Neste contexto, como referido anteriormente, designadamente na respetiva delimitação, esta investigação debruça-se sobre as capacidades, organização e estrutura do EP, especificamente na relação civil/militar, em termos que possibilitem e considerem a operacionalização de instrumentos associados à defesa coletiva e à gestão de crises no ciberespaço, no quadro das alianças internacionais do país, no papel, quer de fornecedor, quer de recetor desses instrumentos de segurança, refletindo, desta forma, a demarcação que sobressai do título desta investigação.

1.1.5. Relação civil/militar no ciberespaço

Caracterizando a relação civil/militar no ciberespaço como o papel a ser desempenhado pelas FFAA na ONSC, Boeke, Heinl e Veenendaal (2015) referem que esta não é uma matéria consensual, uma vez que, nos casos analisados de países da Europa e da Ásia, são reportadas diferentes soluções, revelando assim abordagens ainda experimentais.

[11] No apêndice A apresentam-se duas definições de crise, uma da NATO, e outra nacional. Para este estudo, focado na ONSC-PT e nos respetivos mecanismos de resposta a incidentes de segurança no ciberespaço, aplica-se a definição nacional, que deve ainda ser conjugada com a definição de Crises (Sistema de Gestão de), também em apêndice A.

Uns países colocam o organismo responsável pela segurança no ciberespaço na área da Justiça e outros na Segurança Interna. Há ainda países que atribuem a proteção das infraestruturas críticas à área da Defesa. Adicionalmente, da análise de Boeke, Heinl e Veenendaal (2015) emergem ainda três aspetos com relevância:

- Estrutura: existe um reconhecimento geral para a necessidade de uma abordagem holística à segurança no ciberespaço, que inclua vertentes políticas, económicas, jurídicas e de segurança, e de cooperação entre todas as entidades relevantes, públicas, incluindo militares, e privadas; a esta dimensão transversal adiciona-se o reconhecimento da possibilidade de conflitos de interesse de uma determinada entidade relativamente ao interesse geral, pelo que a entidade cimeira da estrutura deverá estar colocada ao mais alto nível dirimindo interesses, incluindo a definição sobre que informação deverá ser partilhada;
- Partilha de informação: devem ser estabelecidas as regras para partilha de informação, de forma a alcançar um CSC partilhado e acionável, que inclua informação sobre ameaças;
- Treino e procedimentos: face à miríade de entidades e de níveis organizacionais envolvidos, a execução de exercícios com uma frequência adequada é vital para testar operacionalmente a estrutura e promover a aprendizagem organizacional.

1.1.6. Modelo de maturidade de interoperabilidade organizacional

O JP 3-08 *Interorganizational Cooperation* (USJCS, 2016) apresenta o conceito de cooperação interorganizacional como um processo que visa encontrar propósitos, objetivos ou princípios comuns entre diferentes organizações, visando estabelecer as condições para se materializar uma atuação unificada e alavancar as capacidades interorganizacionais que assegurem a unidade de esforço durante a execução. Refere ainda que, para se atingir uma atuação unificada, não é necessário que as organizações em causa tenham a mesma estrutura de comando, mas sim que os esforços de cada uma estejam em harmonia com os objetivos acordados, conforme ilustrado na figura 4, onde se apresentam os elementos habilitantes preconizados, que o investigador relaciona com os conceitos de coerência estratégica e de articulação operacional, para produzir a ação unificada pretendida. A interoperabilidade organizacional é utilizada neste estudo como um instrumento de análise materializado num modelo de maturidade que se apresenta nesta secção.

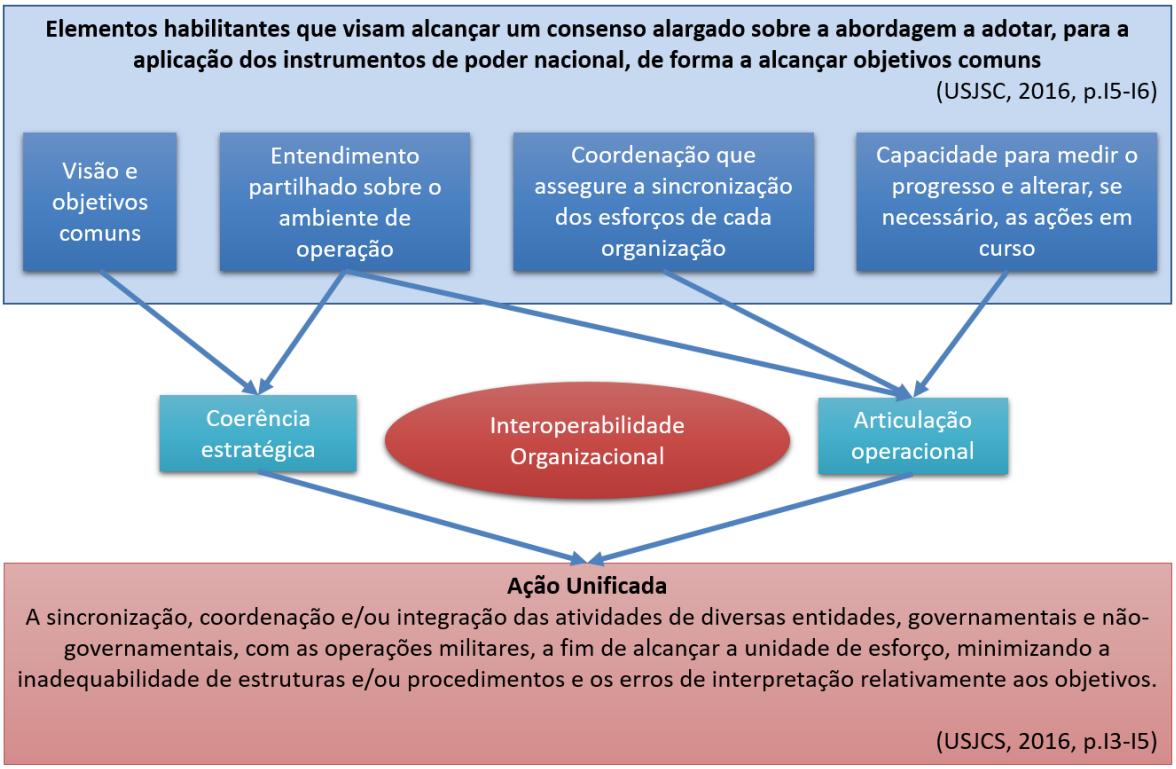


Figura 4 - Ação Unificada
Fonte: adaptado de USJCS (2016)

Por outro lado, a teoria de C2, que enfatiza a criticidade do fator tempo e o alto custo do erro (Alberts e Hayes, 2005, p.13), procura providenciar respostas para a gestão de missões mais complexas e dinâmicas, num enquadramento em que é requerida a conjugação das capacidades de diversas organizações para providenciar o sucesso em janelas de oportunidade cada vez mais curtas (Alberts e Hayes, 2006, pp.1–2). Esta descrição, sobre os problemas que o C2 visa resolver, ajusta-se às dificuldades de gestão de conflitos no ciberespaço, desafios exacerbados pelas características deste ambiente virtual descritas em 1.1.2, designadamente a enorme dificuldade em adquirir um conhecimento/compreensão situacional, incluindo a atribuição de eventuais ações maliciosas, com impacto direto na efetividade do processo de decisão.

Adicionalmente, numa linha de desenvolvimento que visa materializar o conceito de C2 em torno da *Department of Defense Architectural Framework* (DoDAF)[12], Clark e Jones (1999) propõem um Modelo de Maturidade[13] de C2 para a Interoperabilidade Organizacional[14] (M2C2IO). Para efeitos desta investigação, este modelo foi enriquecido

[12] Evolução da anterior linha de desenvolvimento designada por *Command, Control, Communications, Computers, and Intelligence Surveillance Reconnaissance Architecture Framework* (USDoD, 2018).
[13] Conceito exposto no apêndice A.
[14] Entendida como a capacidade para duas ou mais organizações se articularem com sucesso, o modelo de maturidade estabelece níveis de avaliação dessa capacidade. Em trabalhos posteriores que desenvolveram

com os contributos resultantes da abordagem proposta por Williams (2010). O modelo decompõe-se em cinco níveis de maturidade que são descritos de acordo com a efetividade e sofisticação com que são materializadas as dimensões caracterizadoras (quadro 3) que, por sua vez, são decompostas em variáveis (quadro 4):

Quadro 3 - M2C2IO - Descrição e dimensões

Nível	Maturidade da Interação	Dimensões
5	Unificada	Nível de preparação Compreensão partilhada Governação Etos
4	Combinada	
3	Colaborativa	
2	Ad hoc	
1	Independente	

Fonte: modelo adaptado de Clark e Jones (1999) e enriquecido a partir de Williams (2010)

Quadro 4 - M2C2IO - Dimensões e variáveis

Dimensões	Variáveis	Abreviatura[15]
Preparação	**D**outrina	M2C2IO-D
	Experiência	M2C2IO-E
	Treino	M2C2IO-T
Compreensão	**C**omunicação	M2C2IO-C
	partilha de **I**nformação	M2C2IO-I
	partilha de co**N**hecimento	M2C2IO-N
Governação	Distribuição direitos deci**S**ão	M2C2IO-S
	Papéis e responsabilidades	M2C2IO-P
Etos	c**U**ltura e sistema de valores	M2C2IO-U
	Propósito e **A**spirações	M2C2IO-A
	con**F**iança	M2C2IO-F

Fonte: modelo adaptado de Clark e Jones (1999) e enriquecido a partir de Williams (2010)

O modelo apresentado foi instrumentado e apresentado no formato de questionário[16] aos elementos que participaram no CMX2017 e no CC2017, permitindo, desta forma, analisar a interoperabilidade organizacional das entidades da ONSC-PT envolvidas nos exercícios.

1.2. Metodologia

Procedeu-se à revisão da literatura, de documentação NATO, da doutrina do USDoD e da legislação nacional relevantes, o que permitiu efetuar o enquadramento do estudo. Ao longo

modelos de medição de natureza mais tecnológica, designadamente em Guédria, Naudet e Chen (2011) e Russel et al. (2016), este constructo foi identificado como um modelo de maturidade para a interoperabilidade organizacional. No apêndice D efetua-se a descrição detalhada da caracterização dos níveis do M2C2IO.

[15] As abreviaturas das variáveis do modelo serão utilizadas ao longo deste documento quando tal for apropriado, por questões de apresentação e legibilidade, tipicamente em tabelas. Quando tal não for necessário, será utilizada a respetiva designação.

[16] O questionário foi elaborado com base na descrição detalhada do M2C2IO, inicialmente a partir Clark e Jones (1999) e, posteriormente, enriquecido a partir do modelo de maturidade para a intensidade da interação apresentado por Williams (2010).

do processo emergiram duas referências de análise: o modelo de referência para a ONSC (Klimburg, 2012) e o M2C2IO já apresentado na secção 1.1.6. Relativamente ao primeiro, é uma estrutura analítica que cruza os mandatos ao nível do Estado, transversais e setoriais, com o ciclo de vida de um incidente de segurança no ciberespaço, e é utilizado nesta investigação para analisar as funções e responsabilidades da estrutura da ONSC, permitindo desta forma identificar sobreposições, lacunas, necessidades de coordenação estratégica e/ou articulação operacional. Tendo em conta a delimitação do estudo, quer na relação civil/militar, quer na resposta do Estado a um incidente no ciberespaço que pode escalar até à situação de crise, para efeitos da operacionalização da análise considerou-se um subconjunto, quer dos mandatos, quer dos elementos do ciclo de vida dos incidentes de segurança, conforme descrito no apêndice C e ilustrado na figura 5:

Notas: (1) Elemento não considerado na análise sinalizado com ✖
(2) Para efeitos de análise, o mandato de Coordenação foi separado para o nível estratégico e para o nível operacional.
(3) Para efeitos de análise, os mandatos de GCC e PIC foram separados.
(4) Relativamente ao ciclo de vida de incidentes de segurança no ciberespaço, estão considerados para a análise os elementos com relevância para a resposta a uma crise no ciberespaço
(5) As siglas dos mandatos, conforme estabelecidas na figura, aparecem na lista de abreviaturas com o prefixo ONSC.

Figura 5 - Referência de análise da ONSC
Fonte: adaptado de Klimburg (2012)

Com estes dois instrumentos de análise a investigação foi desenvolvida conforme ilustrado na figura 6:

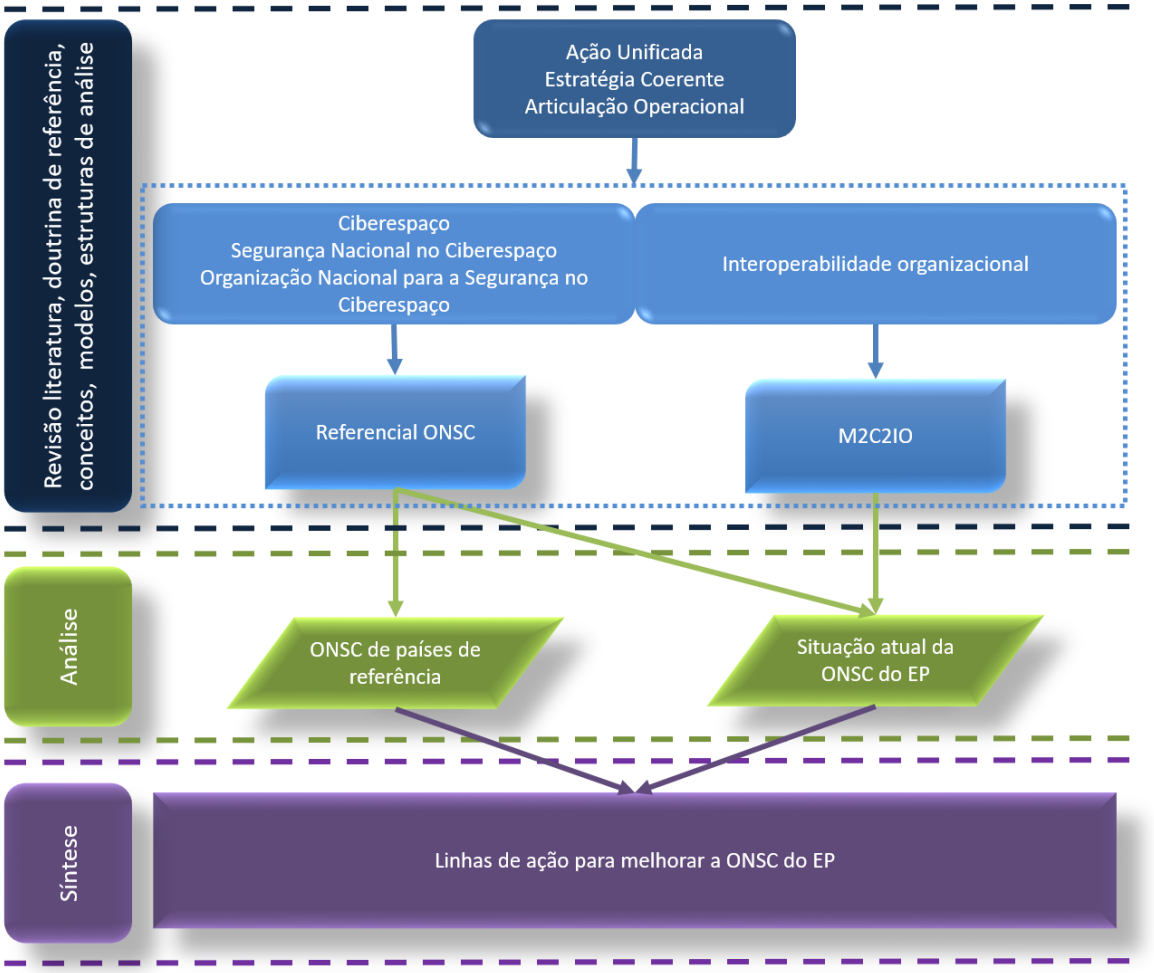


Figura 6 - Percurso da investigação

2. Caracterização da Organização Nacional para a Segurança no Ciberespaço em países de referência

Com base no referencial de análise apresentado na figura 5 foram identificados e caracterizados os organismos mais relevantes para a segurança no ciberespaço do RU e dos PB, providenciando-se uma visão estrutural das respetivas ONSC. Descreve-se, em termos gerais, a visão e objetivos da respetiva estratégia, para posteriormente se apresentar a análise efetuada por mandatos, terminando com um quadro onde se consolida a estrutura de acordo com o referencial de análise utilizado. A terminar, apresentam-se ainda alguns aspetos comuns às duas estratégias analisadas.

2.1. Reino Unido

2.1.1. Visão e objetivos

A promulgação da *National Cyber Security Strategy 2016-2021* pelo Governo do Reino Unido (RU-GOV[17]) no final de 2016, representou uma alteração estrutural profunda da ONSC no RU, e estabeleceu três objetivos: (i) defender de ameaças no ciberespaço através de uma postura que assegure a resiliência do ambiente e que capacite o RU aos diversos níveis (Estado, Organizações e População); (ii) dissuadir através da investigação e disrupção de ações hostis, perseguindo e acusando os agentes perpetradores, incluindo a possibilidade de executar ações ofensivas; e (iii) desenvolvimento sustentado através de uma forte ligação à academia e indústria, assegurando que o ecossistema providencia os incentivos corretos para alavancar a investigação, desenvolvimento e inovação.

2.1.2. Coordenação estratégica

A *Cyber and Government Security Directorate* (RU-CGSD) é a entidade responsável por apoiar o governo na elaboração de políticas de segurança para o ciberespaço, incluindo a respetiva estratégia, e faz parte do *Cabinet Office*[18] (RU-GOV, 2018b).

2.1.3. Coordenação operacional

O *National Cyber Security Centre* (RU-NCSC), inserido no *Government Communications Headquarters* (RU-GCHQ)[19], é a autoridade nacional de cibersegurança, e tem a função de partilhar conhecimento, compreender as ameaças, promover parcerias e

[17] As siglas das organizações de cada um dos países, RU e PB, são compostas com a sigla do respetivo país como prefixo.

[18] Departamento ministerial que apoia o Primeiro-Ministro. Adicionalmente, apoia o *National Security Council* (RU-NSC) e a *Joint Intelligence Organisation* a coordenar a resposta do governo em situação de crise e a governar a segurança do RU no ciberespaço (RU-GOV, 2018a).

[19] Entidade da estrutura dos serviços de informações, com foco na área de *Signal Intelligence*, fazendo parte da estrutura do *Foreign & Commonwealth Secretary* (RU-GOV, 2010).

responder a incidentes de grande dimensão no ciberespaço. A sua criação consolidou e substituiu diversas entidades (RU-GOV, 2016).

2.1.4. Partilha de informação

A partilha de informação sobre ciberameaças é uma das tarefas mais sublinhadas para o RU-NCSC, potenciada pela inserção do centro na estrutura dos serviços de informações. Esta partilha de informação deve ocorrer também a partir das forças policiais, empresas privadas e outros agentes, fazendo do RU-NCSC um centro de fusão de informação sobre ameaças no ciberespaço, com o propósito de a partilhar com diversas entidades, incluindo com o sector privado (p.e.: IC) e a população em geral. Manifestada a intenção de desenvolver mecanismos que habilitem a recolha e partilha automática de informação sobre ameaças, diretamente entre sistemas, e que inclua o setor privado (RU-GOV, 2016).

2.1.5. Gestão de crises no ciberespaço

O RU-NCSC deverá gerir operacionalmente a resposta a um grande incidente no ciberespaço. A coordenação ao nível político-estratégico de situações de crise nacionais é efetuada pelo RU-NSC (RU-GOV, 2018a).

2.1.6. Proteção de infraestruturas críticas

O RU-NCSC é responsável, em articulação com operadores de IC públicos e privados, pela postura geral de segurança no ciberespaço das IC e pela coordenação da resposta, neste ambiente, a incidentes de segurança que as afetem (RU-GOV, 2016).

2.1.7. Operações militares no ciberespaço

O *Cyber Security Operations Centre* (RU-CSOC) visa garantir a resiliência e segurança das redes e plataformas das FFAA, assegurar a continuidade das operações e a liberdade de ação global das FFAA do RU no ciberespaço. O CSOC partilha informação com o RU-NCSC e providencia apoio no caso de um ataque no ciberespaço com impacto nacional significativo. No que diz respeito à capacidade ofensiva no ciberespaço, é referenciado o *National Offensive Cyber Programme*, uma parceria entre o *Ministry of Defence* e o RU-GCHQ, para melhorar as capacidades ofensivas das duas organizações e incorporar a capacidade nas operações militares (RU-GOV, 2016).

2.1.8. Informações e contrainformações

A RU-GCHQ desempenha um papel fundamental ao ser a entidade que, em parceria com as FFAA e com a *National Crime Agency*[20] (RU-NCA), desenvolve atividade de

[20] Agência não ministerial com autonomia administrativa e operacional e que é supervisionada pelo *Home Office* (RU-GOV, 2018c).

intelligence com o propósito de identificar ameaças no ciberespaço, principalmente as patrocinadas por Estados e por cibercriminalidade organizada (RU-GOV, 2016). Salienta-se, na fase de prevenção do ciclo de vida dos incidentes de segurança, as ações de exploração ativa (*intelligence*) para recolha de informação sobre ameaças no ciberespaço.

2.1.9. Combate ao crime no ciberespaço

A *National Cyber Crime Unit* (RU-NCCU), que faz parte da RU-NCA, foi criada para coordenar a resposta nacional ao crime no ciberespaço e atua em articulação com o RU-NCSC. Adicionalmente, para situações mais exigentes de cibercriminalidade organizada, é referida a parceria com o RU-GCHQ e com as FFAA para defender de e contrariar (dissuadir) estas ameaças mais sofisticadas (RU-GOV, 2016, 2018c).

2.1.10. Consolidação da organização nacional para a segurança no ciberespaço do Reino Unido

No quadro 5 apresenta-se a consolidação estrutural da ONSC no RU:

Quadro 5 - ONSC no RU - Mandatos, ciclo de vida incidentes e setores governamentais

MANDATOS DA ONSC[21]	**Ciclo de vida incidentes**			**Setores Governamentais**[22]				**Referência**
	Prevenção	**Preparação**	**Resposta**	**PM**	**SI/J**	**DEF**	**NE**	
Coord.Est.	CGSD[23]			X				2.1.2
Coord.Oper.	NCSC						X	2.1.3
Part.Info.	NCSC						X	2.1.4
GCC		NSC (Nível estratégico)		X				2.1.5
	NCSC (Nível Operacional)						X	
PIC	NCSC						X	2.1.6
OMC	CSOC e GCHQ					X	X	2.1.7
IeIC	GCHQ						X	2.1.8
CCC	NCCU				X			2.1.9

Fonte: construído a partir de análise de documentos do RU-GOV (2010, 2016, 2018a; b; c)

2.2. Países Baixos

2.2.1. Visão e objetivos

O Governo dos Países Baixos (PB-GOV) publicou, em fevereiro de 2017, a *International Cyber Policy* (PB-GOV, 2017) como complemento à *National Cyber Security Strategy 2* (PB-NCSS2) (PB-GOV, 2013a), que se constitui como o documento enquadrador

[21] A sigla dos mandatos é composta com o prefixo ONSC; no quadro 5 este prefixo está suprimido; Coordenação Estratégica (Coord.Est.), Coordenação Operacional (Coord.Oper.), Partilha de Informação (Part.Info.), Gestão de Crises no Ciberespaço (GCC), Proteção de Infraestruturas Críticas (PIC), Operações Militares no Ciberespaço (OMC), Informações e Contrainformações (IeCI), Combate ao Crime no Ciberespaço (CCC).

[22] PM - Nível de governo do Primeiro-Ministro ou de gabinete que o apoia diretamente no governo de um Estado; SI/J - Setor da Segurança Interna ou da Justiça no governo de um Estado; DEF - Setor da Defesa no governo de um Estado; NE - Setor dos Negócios Estrangeiros no governo de um Estado.

[23] No quadro 5, o prefixo RU da sigla das organizações está suprimido.

da respetiva estratégia de segurança nacional no ciberespaço. Adicionalmente, o corpo legislativo é ainda ampliado com a *Defence Cyber Strategy* (PB-DCS) (PB-GOV, 2015a). Para além dos objetivos comuns às estratégias nacionais analisadas, sintetizados em 2.3., a PB-NCSS2 estabelece os objetivos de aumentar a resiliência aos ataques no ciberespaço e proteger os interesses vitais nacionais através da integração da ação dos privados e do setor público, incluindo a componente civil e militar do Estado.

2.2.2. Coordenação estratégica

O *Cyber Security Council* (PB-CSC) é um organismo de conselho do Governo para definir, supervisionar e dar coerência estratégica a todas as iniciativas da PB-NCSS2. O PB-CSC é um organismo com uma constituição mista, com sete elementos de organismos públicos e sete de organizações privadas, sendo que destes, quatro são da academia (PB-CSC, 2018). Este arranjo reflete o entendimento de que as questões relativas ao ciberespaço devem ter uma abordagem transversal a toda a sociedade, logo ao nível estratégico.

2.2.3. Coordenação operacional

O *National Cyber Security Center* (PB-NCSC) tem como missão compreender as ameaças no ciberespaço, providenciar a coordenação da resposta a incidentes, incluindo a coordenação da gestão de crises no ciberespaço, constituindo-se ainda como um *Security Operations Center* (SOC)[24] com ações de consciencialização, deteção e alerta. Adicionalmente, está investido de autoridade especializada para aconselhar entidades, quer públicas, quer privadas, incluindo IC, a pedido ou por iniciativa própria. O PB-NCSC está subordinado ao *National Coordinator for Security and Counterterrorism* (PB-NCSCt) do *Ministry of Security and Justice* (PB-GOV, 2013a).

2.2.4. Partilha de informação

O PB-NCSC tem ainda a função de recolha, partilha de informação e conhecimento sobre ameaças no ciberespaço, providenciando consciencialização e aconselhamento, quer ao nível da prevenção, quer das respostas técnicas a incidentes de segurança, desde logo às entidades governamentais, mas também aos operadores de IC e à população em geral (Kaska, 2015). Recebe informação de *intelligence* (ver 2.2.7), sendo esta uma área em que é salientada a necessidade de melhorar a forma como é partilhada informação classificada entre os diferentes atores.

[24] Definição exposta no apêndice A.

2.2.5. Gestão de crises no ciberespaço e proteção de infraestruturas críticas

No âmbito das suas funções de ONSC-GCC e de ONSC-PIC, o PB-NCSC enquadra o *ICT*[25] *Response Board* que é uma organização permanente de aconselhamento, no formato de parceria público-privada, que envolve as companhias de telecomunicações, bancos e entidades governamentais, e que aconselha os órgãos nacionais de gestão de crise relativamente a ações de mitigação e/ou de recuperação, principalmente no caso de grandes incidentes no ciberespaço. As entidades governamentais participantes neste conselho são os ministérios de *Security and Justice*, *Economic Affairs* e *Defense* e, também, os *Public Prosecution Service*, *General Intelligence and Security Service* e *National Police Services Agency*. Providencia ainda treino e exercícios nacionais de gestão de crises no ciberespaço (Kaska, 2015). Em caso de crise efetiva no ciberespaço, o NCSC-PB insere-se na estrutura de gestão de crises[26] e efetua a coordenação operacional da resposta nacional no ciberespaço (PB-NCSC, 2018).

2.2.6. Operações militares no ciberespaço

A PB-DCS estabelece como objetivos: assegurar a resiliência digital das redes da defesa; melhorar a capacidade de adquirir *intelligence* no ciberespaço e desenvolver capacidades para serem empenhadas no ciberespaço como parte integrante das operações militares (defensiva, ofensiva e *intelligence*). O *Joint Information Management Command* é responsável por assegurar a resiliência dos sistemas e redes da defesa, através do *Defence Computer Emergency Response Team* (PB-DefCERT) que funciona num regime H24, e de apoiar as autoridades civis, a pedido, no caso de um incidente com impacto nacional no ciberespaço. Esta cooperação estende-se à partilha de informação e conhecimento, e apoio mútuo. Adicionalmente, para estruturar capacidades de proteção dos sistemas de armas no ciberespaço, foi anunciada a edificação de um SOC que funcionará em estreita cooperação com o PB-DefCERT. O *Defence Cyber Command* (PB-DCC), organismo conjunto sob a gestão do Exército dos PB, tem o foco em operações defensivas, de *intelligence* e ofensivas (PB-GOV, 2015b). As capacidades militares no ciberespaço podem ser empregues nacionalmente a pedido das autoridades civis (PB-GOV, 2013a).

[25] *Information and Communications Technology*

[26] Coordenada pelo PB-NCSCt; adicionalmente, o manual de gestão de crises dos PB estabelece a política, organização, estrutura e modelo do processo de decisão relativos à gestão de uma crise nacional, que poderá ter que ser gerida ao nível do PM (PB-GOV, 2013b).

2.2.7. Informações e contrainformações

Os PB manifestam uma grande preocupação com a espionagem no ciberespaço e com o papel que as suas agências de *intelligence* desempenham para habilitar conhecimento sobre essas ameaças. Os organismos mais relevantes são os *Defence Intelligence and Security Service* (PB-DISS) na Defesa e *General Intelligence Security Service* (PB-GISS) no SI/J. Reconhecendo a enorme dificuldade no recrutamento e retenção de talentos altamente especializados para esta área, foi criada a *Joint Sigint Cyber Unit*[27] (PB-JSCU), cuja gestão é partilhada pelos dois serviços mencionados. A PB-JSCU é supervisionada por um conselho composto pelos Secretários-Gerais dos *Ministry of General Affairs* (que preside), *Interior and Kingdom Relations* e *Defence*. As agências mantêm os seus mandatos, providenciam pessoal e financiamento, e asseguram a partilha de informação sobre ameaças com as respetivas comunidades de interesse, o PB-GISS com o PB-NCSC, e o PB-DISS articula com a Defesa a utilização desta informação nas operações militares (Kaska, 2015; PB-GOV, 2015b).

2.2.8. Combate ao crime no ciberespaço

O PB-NCSC articula com as autoridades policiais o combate ao crime no ciberespaço, com ênfase muito acentuado na cooperação internacional designadamente com o *Europol´s European Cyber Crime Centre* e outros fóruns (Hathaway e Spidalieri, 2017).

[27] Esta unidade foi recentemente notícia ao infiltrar-se na rede dos atores que, alegadamente, foram responsáveis pela intrusão no Partido Democrático americano durante as eleições presidenciais de 2016 nos EUA (Smeets, 2018).

2.2.9. Consolidação da organização nacional para a segurança no ciberespaço dos Países Baixos

No quadro 6 apresenta-se a consolidação estrutural da ONSC dos PB:

Quadro 6 - ONSC dos PB - Mandatos, ciclo de vida incidentes e setores governamentais

MANDATOS DA ONSC[28]	Ciclo de vida incidentes			Setores Governamentais			Referência
	Prevenção	Preparação	Resposta	PM	SI/J	DEF	
Coord.Est.	CSC[29]				X		2.2.2
Coord.Oper.	NCSC				X		2.2.3
Part.Info.	NCSC				X		2.2.4
GCC		NCSCt (Nível Estratégico)		X	X		2.2.5
	NCSC (Nível Operacional)				X		
PIC	NCSC				X		2.2.5
OMC	DCC, DefCERT					X	2.2.6
IeCI	GISS e DISS				X	X	2.2.7
CCC	NCSC				X		2.2.8

Fonte: construído a partir de análise documental (PB-GOV, 2013a; b, 2015a; b; Kaska, 2015; Hathaway e Spidalieri, 2017; PB-GOV, 2017; PB-CSC, 2018; PB-NCSC, 2018)

2.3. Aspetos comuns às estratégias do Reino Unido e dos Países Baixos

Para além da aplicação do referencial de análise da ONSC, importa ainda salientar alguns aspetos comuns às duas estratégias (RU-GOV, 2016; PB-GOV, 2013a):

- Reconhecimento de uma enorme dependência do meio digital, em todas as dimensões da sociedade;
- Constatação de que o ciberespaço é um meio intrinsecamente inseguro e que necessita de uma abordagem estratégica abrangente e integrada que exige a mobilização de todos os instrumentos do Estado;
- Segurança no ciberespaço é uma questão de soberania e de proteção da população, considerando três públicos alvo: os indivíduos, as organizações e o Estado propriamente dito;
- Os interesses nacionais vitais só poderão ser protegidos pela ação unificada dos setores privado e público, civil e militar, designadamente quanto à proteção das IC operadas maioritariamente por privados;
- Reconhecimento da incapacidade para providenciar a segurança pretendida sem a dimensão internacional, quer bilateral, quer multilateral, ao nível da UE, NATO e Organização das Nações Unidas;

[28] No quadro 6, o prefixo ONSC da sigla dos mandatos está suprimido.
[29] No quadro 6, o prefixo PB da sigla das organizações está suprimido.

- As estratégias dão ainda uma grande relevância à investigação, desenvolvimento e inovação para alavancar a segurança no ciberespaço e viabilizar a respetiva exploração segura por parte da sociedade;
- Finalmente, as duas estratégias dão um grande relevo à exiguidade de recursos humanos nesta área, designadamente os mais qualificados, pretendidos para funções relacionadas com a segurança nacional, incluindo para o setor da Defesa.

2.4. Síntese conclusiva

Neste capítulo analisaram-se as ONSC no RU e nos PB. A consolidação da informação mais relevante para a relação civil/militar no ciberespaço é efetuada nos quadros 7 e 8:

Quadro 7 - ONSC no RU - Aspetos relevantes para a relação civil/militar no ciberespaço

Síntese da análise à ONSC no RU[30]	
Mandatos da ONSC	**Aspetos relevantes para a relação civil/militar no ciberespaço**
Coord.Est.	Coordenação estratégica efetuada ao mais alto nível.
Coord.Oper. GCC PIC	NCSC coordena ações de resposta nacionais, incluindo a resposta a ataques às IC e, em situação de crise, insere-se na estrutura nacional de gestão de crises. O NCSC está inserido na estrutura do GCHQ que é um serviço de informações civil. A coordenação estratégica das operações em crise é efetuada ao mais alto nível pelo NSC.
Part.Info	NCSC consolida informação proveniente de diversas fontes, incluindo policiais, defesa, empresas privadas e outros agentes. Responsável por partilhar informação, nalguns casos de forma automática entre sistemas, com todos os públicos-alvo, ainda que em formatos e termos diferenciados.
OMC	CSOC partilha informação com NCSC e apoia, se necessário e a pedido, a resposta a um incidente com impacto nacional; Capacidade ofensiva das FFAA a ser edificada em parceria com o GCHQ.
IeCI CCC	O GCHQ é a entidade com a incumbência de identificar ameaças no ciberespaço, designadamente quanto à cibercriminalidade organizada e à patrocinada por Estados. Parcerias com as FFAA e com a NCA para contrariar de forma ativa as ameaças mais sofisticadas e que podem afetar a segurança nacional.
Outros aspetos	Preocupação manifestada relativamente à disponibilidade de recursos humanos qualificados. Enunciadas diversas iniciativas de longo prazo, mas também de curto prazo para resolver deficiências existentes.

[30] No quadro 7, os prefixos, ONSC da sigla dos mandatos e RU da sigla das organizações, estão suprimidos.

Quadro 8 - ONSC dos PB - Aspetos relevantes para a relação civil/militar no ciberespaço

Síntese da análise à ONSC dos PB[31]	
Mandatos da ONSC	**Aspetos relevantes para a relação civil/militar no ciberespaço**
Coord.Est.	A coerência estratégica é providenciada por um conselho muito plural, constituído por organismos governamentais e entidades privadas, incluindo da academia.
Coord.Oper. GCC PIC CCC	O órgão com funções de coordenação operacional é o NCSC, estruturalmente colocado na área da SI/J, com funções de consciencialização, deteção, resposta e recuperação de incidentes no ciberespaço, incluindo a coordenação de situações de crise, momento em que passa a responder no contexto da organização nacional para a gestão de crises. Para a GCC, o NCSC enquadra um comité que é um órgão de aconselhamento e atuação no caso de um grande incidente com impacto nacional e do qual fazem parte diversos operadores de IC. O NCSC articula com as autoridades policiais o combate ao crime no ciberespaço.
Part.Info	O NCSC tem a responsabilidade de recolha e de partilha de informações sobre ameaças no ciberespaço. Recebe informação de *intelligence* e, neste particular, foi manifestada a necessidade de melhorar a capacidade de partilhar informação classificada e de assegurar que está acessível aos atores relevantes com funções de contrariar as ameaças mais sofisticadas.
OMC	O DefCERT é a entidade responsável pela segurança dos sistemas e redes da defesa, apoia o NCSC, se necessário e a seu pedido, e partilha informação e conhecimento. O DCC tem como missão executar operações defensivas, ofensivas e de *intelligence*, no ciberespaço. As capacidades militares podem ser empregues nacionalmente a pedido das autoridades civis.
IeCI	Grande ênfase na exploração ativa do ciberespaço para identificação de ameaças, salientando-se a solução inovadora de concentrar numa unidade as capacidades que requerem competências mais exigentes, com um modelo de gestão em que as duas agências de *intelligence*, civil e militar, partilham esses recursos e asseguram o cumprimento dos respetivos mandatos, com o foco na capacidade de reconhecimento e identificação das ameaças no ciberespaço, para partilha entre diversas entidades, incluindo no contexto de execução de operações militares.
Outros aspetos	Os PB manifestam uma grande preocupação com a capacidade de reconhecimento de ameaças no ciberespaço e a partilha de informação com as diversas entidades constituintes, designadamente as entidades governamentais, as organizações privadas, incluindo as operadoras de IC, e a população em geral.

[31] No quadro 8, os prefixos, ONSC da sigla dos mandatos e PB da sigla das organizações, estão suprimidos.

Com a caracterização das ONSC no RU e nos PB identificaram-se os seguintes padrões:

- Ao nível da estratégia, ênfase na capacidade para identificar e contrariar ameaças mais sofisticadas (cibercriminalidade organizada e patrocinada por Estados), logo na fase de prevenção do ciclo de vida dos incidentes de segurança no ciberespaço;
- Ao nível da estrutura, verifica-se a edificação de capacidades partilhadas, quer de *intelligence*, quer ofensivas, entre organismos civis e militares, para a execução de ações/operações no ciberespaço;
- Ao nível da articulação operacional, enfoque na partilha de informação, principalmente na fase de prevenção, em formatos e termos diferenciados entre todos os atores da ONSC, incluindo a partilha de informação classificada.

Em suma, com esta análise das ONSC do RU e dos PB, identificaram-se os padrões que emergem da estratégia, estrutura e instrumentos de articulação operacional em países de referência, com relevância para a caracterização da relação civil/militar no ciberespaço, em situações de não-guerra, permitindo assim responder à QD1 da presente investigação.

3. A Organização Nacional para a Segurança no Ciberespaço em Portugal

Neste capítulo analisa-se a ONSC-PT em duas fases: num primeiro momento caracteriza-se a ONSC-PT à luz do referencial de análise apresentado na figura 5, para posteriormente se apresentar a análise/avaliação da maturidade de alguns dos organismos participantes nos exercícios CMX2017 e CC2017, de acordo com o referencial de interoperabilidade organizacional apresentado em 1.1.6, através de um questionário aplicado aos respetivos representantes na CRN de cada um dos exercícios.

3.1. Caracterização da organização nacional para a segurança no ciberespaço

3.1.1. Visão e objetivos

A ENSC, publicada em 2015, salienta a natureza insegura do ambiente digital e a necessidade do Estado, as organizações e as pessoas, se capacitarem para operar em segurança no ciberespaço (GOV-PT, 2015). Em termos gerais a ENSC enuncia preocupações com temas também abordados nas estratégias do RU e dos PB[32], algumas numa fase de desenvolvimento mais modesta em que é referenciada a respetiva necessidade de edificação[33], como a capacidade de ciberdefesa e de gestão de crises mas, contrariamente ao enunciado naquelas estratégias, não é mencionado qualquer papel para os serviços de informações na avaliação preventiva e proactiva das ameaças no ciberespaço, bem como a necessidade de partilha dessa informação com a comunidade de interesse.

Atualmente está em curso a transposição da Diretiva da UE n.º 1148/2016 do Parlamento Europeu (PE) e do Conselho da União Europeia (CUE), que estabelece as medidas que visam garantir um elevado nível comum de segurança das redes e da informação na UE e que deverá ser transposta para o direito interno até 09 de maio de 2018 (PE e CUE, 2016). Esta transposição, corporizada na Proposta de Lei n.º 119/XIII[34] (PL119/XIII), foi já aprovada em Conselho de Ministros e está em processo legislativo na Assembleia da República (AR), pelo que, face à sua relevância para este estudo, considera-se oportuna a respetiva incorporação na análise da ONSC-PT.

[32] Como o combate ao cibercrime, a proteção de IC, a educação e consciencialização, a investigação e desenvolvimento e a cooperação nacional e internacional, em diversos fóruns, designadamente NATO e UE.

[33] As estratégias do RU e dos PB focam-se em melhorar estruturas já existentes nestas áreas e a explicar o contributo da Defesa e das FFAA, não só para cada uma delas, mas também, em termos gerais, para a segurança nacional dos respetivos países no ciberespaço.

[34] A PL119/XIII exclui do âmbito de aplicação as "(…) redes e sistemas de informação diretamente relacionados com o comando e controlo do Estado-Maior-General das Forças Armadas e dos ramos das Forças Armadas" e as "(…) redes e sistemas de informação que processem informação classificada" (GOV-PT, 2018, p.5).

Adicionalmente, a Diretiva Iniciadora com a Orientação Política para a Ciberdefesa (DIOPC) estabelece como objetivos a proteção das redes e sistemas da Defesa, a exploração proactiva do ciberespaço, quando necessário e determinado, e a cooperação com a cibersegurança nacional (GOV-PT, 2013b).

3.1.2. Coordenação estratégica

O estabelecimento da coordenação político-estratégica para a segurança nacional no ciberespaço é a primeira medida do "eixo um" da ENSC (GOV-PT, 2015). Esta intenção veio a concretizar-se com a criação do Conselho Superior de Segurança do Ciberespaço (CSSC), em 2017 como um grupo de projeto com mandato até 31 de maio de 2018 (GOV-PT, 2017a) e, com a publicação em curso do regime jurídico da segurança do ciberespaço, a respetiva institucionalização definitiva (GOV-PT, 2018, p.2). O CSSC é um órgão de consulta do Primeiro-Ministro para as questões relativas à segurança do ciberespaço e é constituído, para além do membro do governo responsável pela área da cibersegurança, que preside, por dezasseis entidades da Administração Central do Estado, entre as quais o Diretor da DIRCSI do EMGFA, sete organismos públicos (Institutos / Agências / Empresas) e uma entidade privada (Rede Nacional de Equipas de Resposta a Incidentes de Segurança Informática[35]), totalizando 25 entidades. Tem como propósito principal assegurar a coordenação político-estratégica para a segurança no ciberespaço, incluindo a proposta de revisão e acompanhamento da implementação da ENSC (GOV-PT, 2018).

3.1.3. Coordenação operacional

Ao Centro Nacional de Cibersegurança (CNCS) está atribuído o papel de Autoridade Nacional de Cibersegurança, com funções de prevenção para lidar com incidentes no ciberespaço, através de medidas e instrumentos que melhorem a postura de segurança das entidades do Estado, dos operadores de Infraestruturas Críticas e Serviços Essenciais (ICSE) e, ainda, dos Prestadores de Serviços Digitais (PSD), estando inserido na estrutura do Gabinete Nacional de Segurança (GOV-PT, 2017c). Pode emitir instruções de cibersegurança, tem competências de regulação, supervisão, fiscalização e de sancionamento, e define o nível nacional de alerta de cibersegurança. Deve articular e cooperar com "(…) as estruturas nacionais responsáveis pela ciberespionagem, ciberdefesa, cibercrime e ciberterrorismo" (GOV-PT, 2018, p.12) e com as contrapartes internacionais. O CERT.PT[36] é a equipa de resposta a incidentes de segurança no ciberespaço, funciona no

[35] Conhecida por Rede *Computer Security Incident Response Team* (Rede CSIRT)
[36] Esta é a designação do órgão e significa *Computer Emergency Response Team*, Portugal

CNCS e está-lhe atribuída a coordenação operacional da resposta a incidentes de segurança no ciberespaço (GOV-PT, 2018).

3.1.4. Partilha de informação

Infere-se da ENSC que a responsabilidade relativa à partilha de informação está principalmente atribuída ao CNCS, através da participação em fóruns, partilha de boas práticas e na resposta a incidentes, incluindo a coordenação da ação da Rede CSIRT (GOV-PT, 2015). Por outro lado, os organismos do Estado, operadores de ICSE e PSD, são obrigados a comunicar incidentes no ciberespaço que os afetem (GOV-PT, 2018). Adicionalmente, numa rede de partilha mais restrita, que envolve o Serviço de Informações de Segurança (SIS) e a Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica (UNC3T) da Polícia Judiciária, o SIS partilha informação sobre ameaças no ciberespaço (Raposo, 2018). Além disso, esta informação é também partilhada com o CCD, através do Centro de Informações e Segurança Militares[37] (CISMIL) (Jesus, 2018). No entanto, salienta-se que, quer Jesus (2018), quer Raposo (2018), referiram que, tendo em consideração a necessidade do respetivo processamento tempestivo, aquela informação é disponibilizada num suporte inadequado.

3.1.5. Gestão de crises no ciberespaço

A PL119/XIII não faz qualquer referência a incidentes de grande magnitude no ciberespaço, nomeadamente a situações de crise. A ENSC faz referência à necessidade de constituição de um gabinete de gestão de crises no ciberespaço inserido num SNGC, e atribui ao CCD a competência para efetuar o "(…) planeamento e resposta imediata e efetiva a uma crise no ciberespaço" (GOV-PT, 2015, p.3740). O diploma que regulava o SNGC (GOV-PT, 2004) foi revogado em 2008 pela Lei de Segurança Interna (LSI), que por sua vez estabelece uma competência de coordenação, em situação de crise, do Secretário-Geral do Sistema de Segurança Interna (SGSSI), entre os serviços e forças de segurança e entidades com responsabilidades em segurança ambiental, rodoviária, de transporte e de emergência médica, em articulação com o Planeamento Civil de Emergência (PCE) (AR, 2017, p.5). Por outro lado, o PCE é uma atribuição atual da Autoridade Nacional de Proteção Civil (ANPC) e enquadra as atividades de "(…) planeamento e coordenação das necessidades nacionais (…) com vista a fazer face a situações de crise ou de guerra", no âmbito das quais está definido um conjunto de organismos que suportam este propósito (GOV-PT, 2014b, pp.5617–5618). Neste contexto, está atribuído ao CNCS "(…) o planeamento da utilização

[37] Órgão na estrutura do EMGFA (GOV-PT, 2014a)

não militar do ciberespaço em situação de crise ou de conflito armado, no âmbito do planeamento civil de emergência" (GOV-PT, 2017c, p.5882).

3.1.6. Proteção de infraestruturas críticas

A coordenação operacional para a proteção das IC está atribuída ao CNCS, quer na ENSC, quer na PL119/XIII, salientando-se que abrange os operadores de ICSE e os PSD (GOV-PT, 2015, 2018).

3.1.7. Operações militares no ciberespaço

A DIOPC estabelece o CCD como o órgão que executa operações no ciberespaço (defensivas, de exploração e ofensivas), operações de informações e contrainformações, e enuncia a necessidade de partilha de informação com a Rede CSIRT, instituições privadas e organizações internacionais (NATO e UE) (GOV-PT, 2013b).

O CCD atingiu a sua capacidade inicial em junho de 2016, compreendendo a monitorização e proteção das redes das FFAA e da Defesa contra ciberataques, numa "(…) filosofia de operação tipo CERT (…)" (Santos, 2017, p.60) e efetua, neste âmbito de CERT, a troca de informação e de experiências com o CNCS (Jesus, 2018), depreendendo-se não estarem ainda edificadas capacidades de natureza ofensiva.

3.1.8. Informações e contrainformações

O papel dos serviços de informações na ONSC-PT não é explicitado, nem na ENSC, nem na PL119/XIII. Ainda assim, para além do anteriormente referido em 3.1.4, o SIS faz parte da Rede CSIRT como observador (Raposo, 2018). Adicionalmente, a DIOPC, ainda que refira a importância da identificação ativa de ameaças no ciberespaço, salienta esta ação no contexto das operações militares, depreendendo-se que será também uma atividade atribuída ao CCD, não efetuando qualquer referência aos serviços de informações militares. Ainda assim, como referido em 3.1.4, o SIS partilha informação sobre ameaças no ciberespaço através do CISMIL.

3.1.9. Combate ao crime no ciberespaço

O combate ao cibercrime é efetuado a nível nacional pela UNC3T (GOV-PT, 2015) que participa na rede restrita referida em 3.1.4.

3.1.10. Consolidação da organização nacional para a segurança no ciberespaço em Portugal

No quadro 9 apresenta-se a consolidação estrutural da ONSC-PT:

Quadro 9 - ONSC-PT - Mandatos, ciclo de vida incidentes e setores governamentais

MANDATOS DA ONSC[38]	Ciclo de vida incidentes			Setores Governamentais			Referência
	Prevenção	Preparação	Resposta	PM	SI/J	DEF	
Coord.Est.	CSSC			X			3.1.2
Coord.Oper.	CNCS-CERT.PT			X			3.1.3
Part.Info.	CNCS			X			3.1.4
GCC	SGSSI, ANPC-PCE				X		3.1.5
	CNCS, CCD (Oper)			X		X	
PIC	CNCS			X			3.1.6
OMC	CCD					X	3.1.7
IeCI	SIS, CISMIL			X		X	3.1.8
CCC	UNC3T				X		3.1.9

Fonte: construído a partir de análise documental e entrevistas (GOV-PT, 2013b, 2014b, 2015, 2017c, 2018; Raposo, 2018; Jesus, 2018)

3.2. Casos práticos - Exercícios CMX2017 e CC2017

Como referido em 1.1.6, o M2C2IO foi instrumentado com um questionário que se apresenta no apêndice F, sendo posteriormente submetido a parte dos representantes dos organismos nacionais participantes nos exercícios CMX2017 e CC2017.

3.2.1. Caracterização do processo de recolha e tratamento dos dados

Relativamente ao CMX2017, dos dezoito participantes foram contactados catorze para responder (dos quais treze representantes de organismos não-militares), tendo respondido nove ao questionário. Relativamente ao CC2017, dos vinte-e-sete participantes foram contactados doze (dos quais um participante de organismo não-militar), tendo respondido onze. O questionário era anónimo, não recolhia qualquer informação de contexto e continha vinte perguntas/afirmações, dezassete das quais com resposta numa escala de concordância com seis níveis e três perguntas com opções objetivas de resposta para selecionar uma. A descrição detalhada da parametrização do questionário consta do apêndice E.

[38] No quadro 9, o prefixo ONSC da sigla dos mandatos está suprimido.

3.2.2. Respostas ao questionário dos participantes nacionais nos exercícios *Crisis Management Exercise* 2017 e *Cyber Coalition* 2017

O resultado global da aplicação do questionário foi de 3,24 para o CMX2017 e de 3,83 para o CC2017, conforme ilustrado na figura 7:

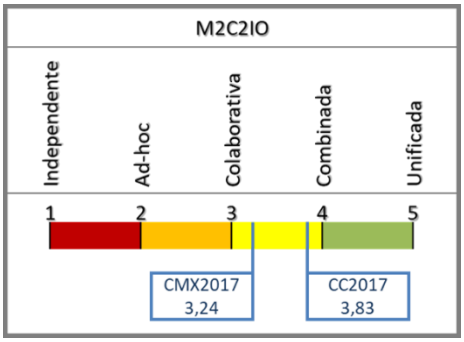


Figura 7 - M2C2IO - Resultado global da aplicação do questionário aos participantes nacionais nos exercícios CMX2017 e CC2017

Após um tratamento das respostas aos questionários, na figura 8 apresenta-se, por dimensão, a média obtida em cada uma das variáveis[39] e, na figura 9, o resultado da média para cada uma das dimensões:

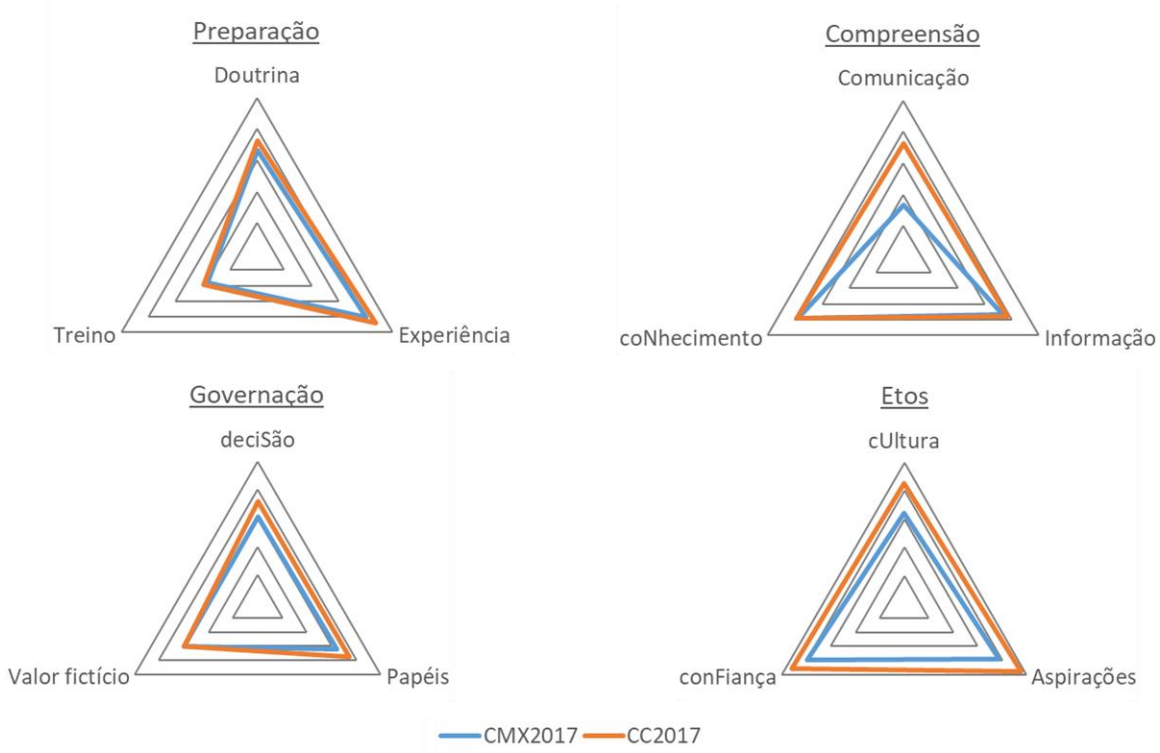


Figura 8 - M2C2IO - Resultados de cada variável (média), no contexto da respetiva dimensão, para os CMX2017 e CC2017

[39] O formato de apresentação selecionado foi o gráfico radar que apresenta a escala de 1 a 5 do M2C2IO do centro para a periferia. No caso da dimensão governação, como só tem duas variáveis, foi incluído um valor fictício para que os dados pudessem ser adequadamente apresentados neste tipo de gráfico.

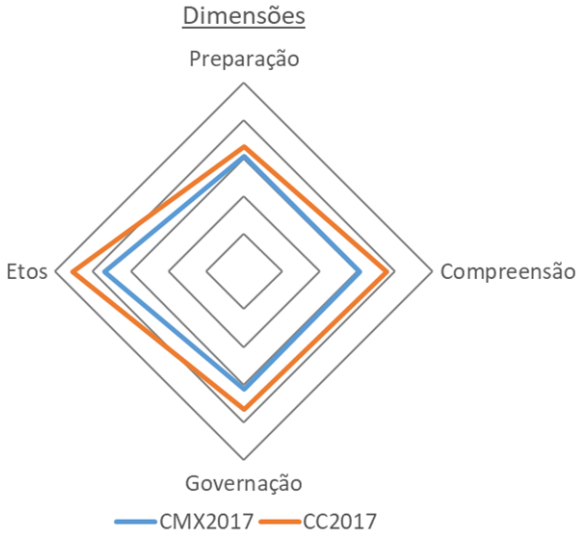


Figura 9 - M2C2IO - Resultado global por dimensão (média), para os CMX2017 e CC2017

De forma a proporcionar uma melhor noção da distribuição das respostas na escala de níveis do M2C2IO, efetuou-se uma contagem de ocorrências (frequência) em cada um deles e normalizou-se ao número de perguntas e variáveis, conforme descrição detalhada no apêndice E. Assim, das figuras 10 à 13 apresentam-se, para cada variável no contexto da respetiva dimensão, a frequência de respostas em cada nível do modelo. Finalmente, na figura 14 é apresentado, para cada dimensão, o resultado global de frequência de respostas em cada nível do modelo. O valor de 100% corresponde a, no caso do CMX2017, nove respostas e, no caso do CC2017, onze respostas.

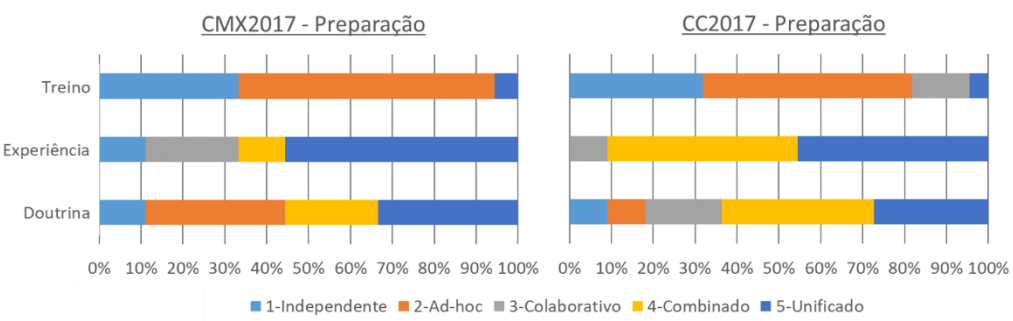


Figura 10 - M2C2IO - Frequência normalizada das respostas ao questionário, por níveis do modelo e variáveis da dimensão Preparação, para os CMX2017 e CC2017

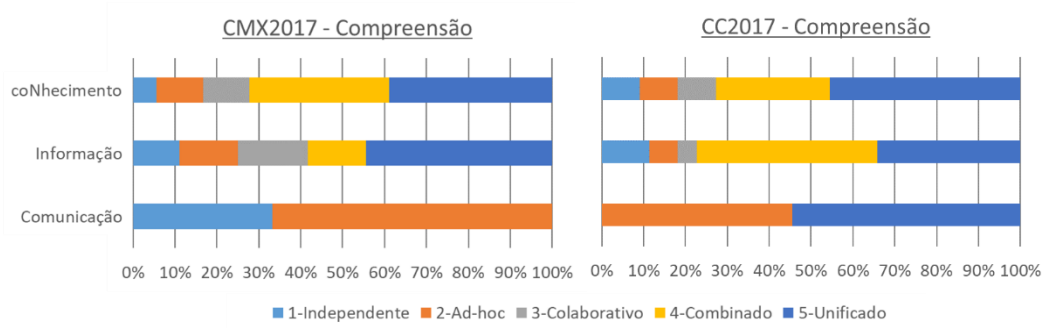


Figura 11 - M2C2IO - Frequência normalizada das respostas ao questionário, por níveis do modelo e variáveis da dimensão Compreensão, para os CMX2017 e CC2017

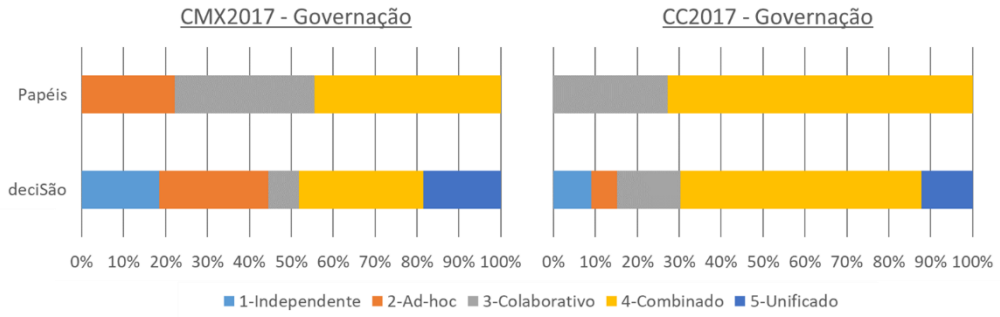


Figura 12 - M2C2IO - Frequência normalizada das respostas ao questionário, por níveis do modelo e variáveis da dimensão Governação, para os CMX2017 e CC2017

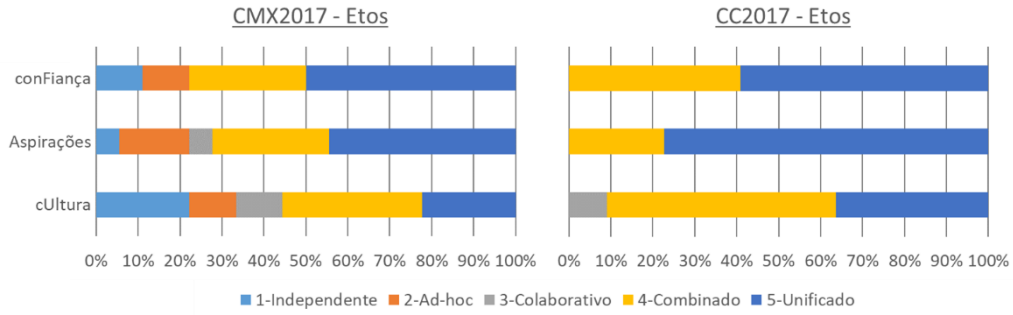


Figura 13 - M2C2IO - Frequência normalizada das respostas ao questionário, por níveis do modelo e variáveis da dimensão Etos, para os CMX2017 e CC2017

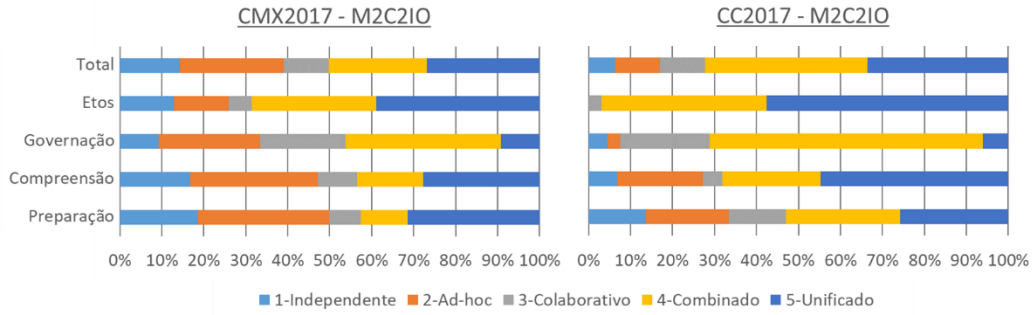


Figura 14 - M2C2IO - Frequência normalizada das respostas ao questionário, por níveis e dimensões do modelo, para os CMX2017 e CC2017

3.2.3. Discussão dos resultados dos questionários

O melhor resultado do CC2017 (3,83 que compara com 3,24 do CMX2017) era já esperado, tendo em consideração que os respetivos participantes têm uma proveniência

cultural mais uniforme. Nos dois casos o resultado fica aquém do desejável, uma vez que, da análise da descrição detalhada da caracterização dos níveis do M2C2IO (ver apêndice D), para este tipo de interação é desejável que seja atingido um nível igual ou superior a quatro.

Efetuou-se uma análise de tendência da frequência de ocorrências de resposta em cada variável, que é apresentada no quadro 10:

Quadro 10 - Grupos de tendência nas respostas aos questionários do CMX2017 e CC2017

Linhas de tendência	**CMX2017**	**CC2017**
Nível igual ou superior a 4 e com ocorrências > 90%		Experiência > 90% conFiança 100% Aspirações 100% cUltura > 90%
Nível igual ou superior a 4 e com ocorrências entre 60% e 90%	Experiência > 60% coNhecimento > 70% conFiança > 70% Aspirações >60%	Doutrina > 60% Informação > 70% coNhecimento > 70% deciSão > 60%
Nível igual ou inferior a 2	Treino > 90% Comunicação = 100%	Treino > 80%
Sem tendência; distribuído ao longo da escala	Doutrina Informação deciSão cUltura	Comunicação
Sem ocorrências nos extremos	Papéis	Papéis

Esta análise de frequências confirma a natureza mais uniforme dos participantes do CC2017, com apenas uma variável sem tendência, enquanto que, no CMX2017, sobressaíram quatro, denotando uma menor perceção comum relativamente ao objeto de medição dos atributos em causa. Em qualquer dos exercícios os respondentes valorizaram a conFiança e Aspirações, que mediu a forma como os participantes percecionaram os outros organismos e o valor do exercício para a respetiva organização, o que sugere a existência de uma base de entendimento propício a que se sistematize e consolide a execução de um programa que inclua exercícios, mas também atividades de outra natureza, visando, precisamente, melhorar as variáveis com menor desempenho, designadamente a Comunicação e o Treino, mas também, no contexto do CMX2017, as variáveis Doutrina, Informação, deciSão e cUltura.

Durante a análise foi suscitada a dúvida sobre se existiriam diferenças nas respostas às perguntas com escala de concordância e as que tinham opções de resposta objetivas. Estendeu-se um pouco a análise e considerou-se a categorização das perguntas em 3 tipos: perguntas sobre a própria entidade/pessoa, perguntas sobre o grupo e perguntas com opções objetivas. O resultado é apresentado na figura 15:

Figura 15 - M2C2IO - Análise por tipo de pergunta

Efetuou-se posteriormente a comparação dos resultados de cada tipo de pergunta com o resultado final obtido em cada exercício, apresentando-se na figura 16 essa diferença em percentagem:

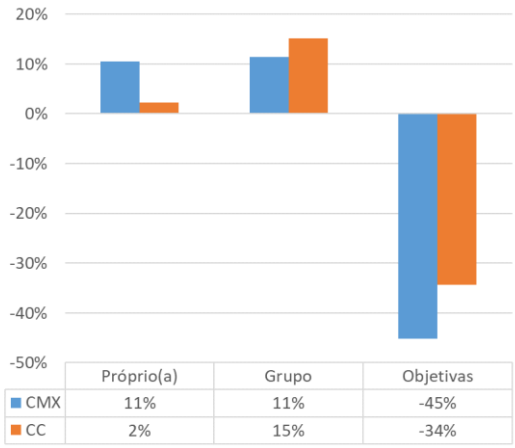


Figura 16 - M2C2IO - Variação entre a resposta a cada tipo de pergunta e o resultado global de cada exercício

Nas respostas às perguntas sobre a própria entidade/pessoa e sobre o grupo, em qualquer dos conjuntos de respondentes verifica-se uma ligeira valorização relativamente ao resultado global obtido em cada um (3,24 para o CMX2017 e 3,83 para o CC2017), variando entre os 2% e os 15%. Por outro lado, relativamente às perguntas com opções de resposta objetivas verifica-se uma grande diferença, com menos 45% no caso do CMX2017 e menos 34% no caso do CC2017. As perguntas com opções de resposta objetivas estão associadas às variáveis Treino e Comunicação e essa diferença transparece nos gráficos apresentados na figura 8. Significa que foram as respostas a estas perguntas que fizeram baixar o resultado

final de cada um dos exercícios, o que sugere que as perguntas com resposta em escala de concordância terão uma latitude de interpretação demasiado elevada para o propósito do questionário, o que é um aspeto que deverá ser corrigido em investigações futuras nesta área.

3.3. Síntese conclusiva

Neste capítulo efetuou-se a análise da ONSC-PT, inicialmente utilizando o referencial de análise apresentado na figura 5, o que permitiu analisar as funções e responsabilidades das entidades na ONSC-PT e, posteriormente, complementou-se com um caso prático de análise da maturidade organizacional dos organismos participantes nas células nacionais de dois exercícios internacionais recentes, o CMX2017 e o CC2017, de acordo com a estrutura de análise apresentada em 1.1.6.

Com a criação do CSSC em 2017, inicialmente como grupo de projeto e, num processo legislativo ainda em curso, como estrutura permanente colocada ao mais alto nível, está em vias de concretização o desiderato enunciado na ENSC de estabelecer a coordenação politico-estratégica da ONSC-PT. A constituição é quase totalmente pública, ou para-pública (24 em 25 entidades), e inclui o Diretor da DIRCSI do EMGFA. Um dos principais objetivos do CSSC é o de rever a ENSC.

O CNCS tem estatuto de Autoridade Nacional de Cibersegurança com poderes de regulação, supervisão, fiscalização e de sancionamento, relativamente às entidades do Estado, ICSE e PSD. O CERT.PT, que funciona no CNCS, coordena operacionalmente a resposta a incidentes de segurança no ciberespaço, incluindo os que afetem as ICSE e PSD.

Apesar de existir troca de informação (Rede CSIRT) e procedimentos acordados numa rede mais restrita que envolve algumas entidades do EP, entre as quais o CNCS, SIS e UNC3T, existem oportunidades para melhorar a partilha de informação de forma mais tempestiva numa infraestrutura que permita também a comunicação de informação classificada. Existe alguma partilha de informação e conhecimento com o CCD.

Ao nível do mandato ONSC-GCC, o que resulta da análise é que existe alguma incoerência, quer na ONSC-PT, quer na estrutura nacional de coordenação estratégica em situação de crise: a ENSC atribui ao CCD a resposta imediata a uma crise no ciberespaço mas, por outro lado, no contexto do PCE, que está atualmente inserido na estrutura da ANPC, está atribuído ao CNCS o planeamento da utilização não-militar do ciberespaço em situação de crise e, adicionalmente, ao SGSSI, também em situação de crise, são atribuídas funções de coordenação. Finalmente, a coordenação do CMX2017, um exercício de gestão de crises, foi atribuída ao Ministério da Defesa Nacional (MDN). A esta situação não será alheia a

inexistência de um SNGC, tal como preconizado no Decreto-Lei n.º 173/2004 que foi revogado em 2008 pela LSI, sem que tenha ocorrido a institucionalização de um sistema alternativo.

A DIOPC atribui as operações militares no ciberespaço ao CCD que atingiu uma capacidade inicial de monitorização e resposta a incidentes das redes militares em 2016, articulando ainda alguma informação e troca de conhecimento com o CNCS. Não estão edificadas capacidades ofensivas.

Nos documentos analisados não é mencionado qualquer papel para os serviços de informações, civis ou militares, na execução de ações de exploração ativa do ciberespaço para eventual identificação de ameaças. Apesar de desempenharem um papel na partilha de informação sobre ameaças no ciberespaço, isso é efetuado de forma pouco prática e efetiva.

Da análise da interoperabilidade organizacional, decorrente da aplicação de um questionário aos participantes nos exercícios CMX2017 e CC2017, resultou um nível de maturidade, no caso do CC2017, de 3,83 e, no caso do CC2017, de 3,24, o que é explicado pela maior uniformidade cultural dos representantes dos organismos participantes no CC2017, que se refletiu nas respostas ao questionário, principalmente ao nível das dimensões Compreensão e Etos. Ainda assim, para que se efetive uma ação unificada das diferentes entidades, será desejável que se atinja um nível de maturidade de interoperabilidade organizacional igual ou superior a quatro. As variáveis com maior margem de progressão são o Treino e a Comunicação, mas também, no caso do CMX2017, as variáveis Doutrina, Informação, deciSão e cUltura.

Desta análise identificam-se os seguintes aspetos da relação civil/militar no ciberespaço:

- Ao nível estratégico verifica-se a necessidade de clarificar o papel atribuído aos serviços de informações civis e militares, bem como a coordenação estratégica e operacional em situação de crise no ciberespaço, incluindo a criação de um SNGC;
- Ao nível da articulação operacional, com o enfoque na partilha de informação, ainda que existam práticas que a consubstanciam, constatam-se oportunidades de melhoria, principalmente na fase de prevenção do ciclo de vida dos incidentes de segurança no ciberespaço, incluindo a partilha de informação classificada entre todos os atores da ONSC-PT; adicionalmente, os resultados do questionário aplicado aos participantes nos exercícios CMX2017 e CC2017 indicam oportunidades de melhoria em diversos atributos da interoperabilidade

organizacional, designadamente ao nível das variáveis Treino, Comunicação, Doutrina, Informação, deciSão e cUltura.

Em suma, com esta análise da ONSC-PT caracterizou-se a relação civil/militar nacional no ciberespaço, em situações de não-guerra, nomeadamente em situação de crise, ao nível da coerência estratégica e da articulação operacional das entidades, civis e militares, com responsabilidades na segurança do ciberespaço de interesse nacional, permitindo assim responder à QD2 da presente investigação.

4. Contributos para a melhoria da Organização Nacional para a Segurança no Ciberespaço em Portugal

Do resultado da análise efetuada nos capítulos 2 e 3 salientam-se, pela sua relevância e impacto para a relação civil/militar no ciberespaço, os quatro aspetos seguintes:

- Postura estratégica da ONSC-PT;
- Exiguidade de recursos humanos altamente qualificados para as funções tecnicamente mais exigentes, designadamente as ações/operações de exploração (*intelligence*) e ofensivas;
- Partilha de informação entre um conjunto de entidades relevantes com responsabilidades na segurança do ciberespaço e que atuam nas fases de prevenção, preparação e de resposta a crises;
- A importância da existência de um SNGC onde as estruturas da ONSC-PT se insiram de modo a que seja possível viabilizar a coordenação necessária, incluindo a de natureza político-estratégica.

4.1. Postura estratégica da Organização Nacional para a Segurança do Ciberespaço em Portugal

Para efetuar a caraterização e posterior comparação da postura estratégica da ONSC-PT, recorreu-se à matriz proposta por Klimburg (2012, p.78) que categoriza, por mandatos da ONSC[40], o cruzamento da tipologia da atividade maliciosa no ciberespaço com a severidade do respetivo impacto nacional, e da qual se apresenta uma adaptação na figura 17:

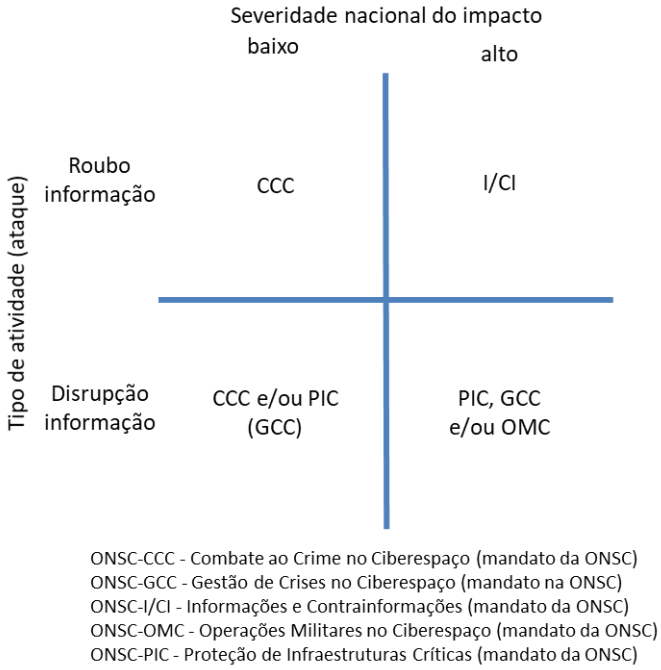


Figura 17 - Categorização por mandatos da severidade do impacto nacional de atividade maliciosa no ciberespaço
Fonte: adaptado de Klimburg (2012, p.78)

Uma estratégia que revele preocupação com as ameaças mais disruptivas à segurança nacional desenvolve-se de forma a incluir os quadrantes de impacto alto na figura 17. Por outro lado, se a preocupação for mais a segurança dos cidadãos e das organizações em geral, então desenvolve-se numa vertente mais de combate ao cibercrime e de proteção das IC, correspondente aos quadrantes de impacto baixo na figura 17 (Klimburg, 2012, p.79).

Da análise efetuada, embora todas as estratégias analisadas procurem endereçar as preocupações emergentes dos quadrantes esquerdos da figura 17, a ONSC, quer no RU, quer nos PB, manifestam objetivos, linhas de ação e orientações para responder a todo espetro de ameaças à segurança nacional: a estratégia do RU manifesta intenções claras para que os seus serviços de informações efetuem ações ofensivas de exploração com o propósito de identificar proactivamente ameaças no ciberespaço e de partilhar essas informações, quer

[40] Conforme referência descrita na figura 5.

com a entidade de combate ao crime no ciberespaço, para perseguir judicialmente esses atores, quer com as FFAA para, eventualmente, encetar ações de disrupção dessas atividades; adicionalmente, a estratégia dos PB explicita também esta preocupação com este tipo de ameaças à segurança nacional no ciberespaço, patente na atividade dos seus serviços de informações, civis e militares, bem como para a partilha de informação confidencial com diversos atores da ONSC dos PB, designadamente a entidade de combate ao crime no ciberespaço, as FFAA e o PB-NCSC. Estes países consideram que estas atividades, que visam prevenir e combater as ameaças com maior severidade de impacto, reforçam também a segurança dos cidadãos e das organizações em geral, caracterizando-se assim como uma abordagem que visa dar resposta às ameaças à segurança nacional no ciberespaço, ao longo de todo espetro do conflito (ver 1.1.3).

No caso da ONSC-PT, considerando a estratégia em vigor[41], existem oportunidades de melhoria, mesmo no caso de atividades maliciosas com baixo impacto, designadamente quanto à clarificação da estrutura nacional de Gestão de Crises (ver 4.3.). No caso da resposta a atividades com impacto alto, não é explicitado qualquer papel para os serviços de informações, quer civis, quer militares, apesar de existirem práticas operacionais, ainda que com eficácia limitada, de partilha de alguma informação sobre ameaças no ciberespaço. Relativamente a operações ofensivas no ciberespaço, a DIOPC faz essa referência, mas num enquadramento de edificação da capacidade militar, e não numa perspetiva abrangente de operacionalização de um instrumento passível de ser articulado e explorado com as restantes entidades da ONSC-PT, designadamente com os serviços de informações ou com a entidade de combate ao crime no ciberespaço.

4.2. Exiguidade de recursos humanos altamente qualificados

4.2.1. Aspetos relevantes da análise efetuada

Relativamente à edificação da capacidade para executar operações no ciberespaço, principalmente as de exploração (*intelligence*) e ofensivas, constata-se uma grande preocupação relativamente à capacidade de arregimentar os recursos humanos altamente qualificados que são necessários. A tendência que emergiu da análise das ONSC no RU e nos PB é a de partilha de capacidades e recursos humanos entre entidades, precisamente no âmago da delimitação deste estudo, a relação civil/militar no ciberespaço: no RU a capacidade ofensiva das FFAA está a ser edificada numa parceria com o GCHQ-RU

[41] De acordo com Marques (2018) a revisão da ENSC está em curso, tendo já sido submetida ao CSSC pelo grupo de trabalho constituído para o efeito.

(entidade civil) e, nos PB, foi criada uma unidade que executa ações/operações de exploração ativa do ciberespaço (*intelligence*) e que é governada pelos serviços de informações civis e militares.

No caso da ONSC-PT não existem iniciativas para a partilha de recursos humanos entre as diversas entidades constituintes. No entanto, este problema da exiguidade de recursos humanos altamente qualificados foi salientado por Marques (2018) e por Pires (2018), representando, neste particular, um dos maiores desafios a enfrentar para a edificação de capacidades nesta área (Jesus, 2018).

4.2.2. Centro Nacional de Operações de Segurança no Ciberespaço

O Centro Nacional de Operações de Segurança no Ciberespaço (CNOSC) é um conceito que se apresenta como proposta para, não só dar resposta à exiguidade de recursos humanos altamente qualificados nesta área, mas também por se constituir como uma concetualização que visa lidar melhor com a natureza dinâmica, de enorme potencial de anonimato e sem fronteiras (*continuuns* disruptivos) do ciberespaço.

O objetivo é o de habilitar, sempre que necessário e sob decisão legítima, incluindo conformidade legal, um CSC partilhado e acionável entre diversas entidades da ONSC-PT, em função do estado de alerta/ameaça e ao longo do ciclo de vida do incidente (prevenção, preparação e resposta), incluindo situação de crise, a fim de operacionalizar, quando determinado e de forma tempestiva, a ação unificada de todos os instrumentos do EP, incluindo o militar, ao longo de todo o espetro do conflito.

O conceito suporta-se em dois elementos essenciais: por um lado a partilha de recursos humanos qualificados entre entidades da ONSC-PT e, por outro, a consubstanciação do CSC partilhado e acionável, entre aqueles organismos, suportado no estabelecimento de regras para a partilha de informação.

Inicia-se esta exposição com a definição de entidades genéricas (quadro 11), utilizando os mandatos do referencial de análise apresentado na figura 5, e que irão ser utilizadas para apresentação do conceito ao longo desta secção:

Quadro 11 - CNOSC - Definição de entidades genéricas

Sigla[42]	**Descrição**
Setor_OM	Estrutura do Estado responsável pelas operações militares.
Setor_I/CI(C)	Estrutura do Estado responsável pelas ações de informações e de contrainformações civis.
Setor_CC	Estrutura do Estado responsável pelas ações de combate ao crime.
Setor_CNCS	Estrutura do Estado responsável pela coordenação estratégica da cibersegurança nacional.
eOMC	Estrutura no Setor_OM responsável pelas operações militares no ciberespaço.
eI/CI(M)	Estrutura no Setor_OM responsável por conduzir operações de informações e de contrainformações militares no ciberespaço.
eI/CI(C)	Estrutura no Setor_I/CI(C) responsável pelas ações de informações e contrainformações no ciberespaço.
eCCC	Estrutura no Setor_CC responsável pelas ações de combate ao crime no ciberespaço.
eCNCS	Estrutura no Setor_CNCS responsável pela coordenação operacional da cibersegurança nacional.
CGov	Comité de Governação do Centro e dos RHETO (CNOSC).
CGes	Comité de Gestão do Centro e dos RHETO (CNOSC).
RHETO	Recursos Humanos com Especialização Técnica Ofensiva. Representam a força de trabalho com qualificações para executar tecnicamente ações/operações de exploração (*intelligence*) e ofensivas no ciberespaço.

Para efeitos de apresentação do conceito enuncia-se a tipologia da informação que se preconiza existir na esfera do CNOSC e cuja descrição se complementa com o diagrama (figura 18) de relacionamento com as entidades identificadas no quadro 11:

– Informação de Ações/Operações[43] (IAO): respeitante à condução de ações/operações, designadamente a informação tática relevante (objetivos, alvos, meios próprios utilizados, identificação de ameaças concretas, etc.), pelo que, inicialmente, ela está apenas disponível para a entidade que primariamente a controla. É a partir desta informação que será criada a área de Informação de Ações/Operações partilhada[43] (IAOp), entre duas ou mais entidades, de forma

[42] Estas siglas são compostas com o prefixo CNOSC, aparecendo completas na lista de abreviaturas. No quadro 11 e, ao longo do restante capítulo, por razões de legibilidade, as siglas são apresentadas sem o referido prefixo.

[43] A sigla completa, tal como aparece na lista de abreviaturas, é composta com o prefixo CNOSC. Ao longo do restante capítulo, por razões de legibilidade, a sigla é apresentada sem prefixo.

automática ou sujeita a processo de decisão. Viabiliza, quando necessário e decidido, o CSC partilhado;

– Informação sobre Regras de Partilha[43] (IRP): representa o conjunto de regras ao abrigo das quais a informação é partilhada entre as diferentes entidades, numa modalidade que poderá ser diferenciada entre elas, constituindo-se como o outro grande elemento do conceito (para além dos RHETO);
– Informação para a Gestão do Conhecimento[43] (IGC): respeitante ao conjunto de técnicas e procedimentos para executar ações/operações no ciberespaço, tendo sido previamente higienizada de modo a não conter qualquer informação tática (no aplicável). Fomenta a partilha de conhecimento e a utilização de técnicas e procedimentos em diferentes contextos táticos, sem revelar as ações/operações concretas em que elas já tenham sido empregues.

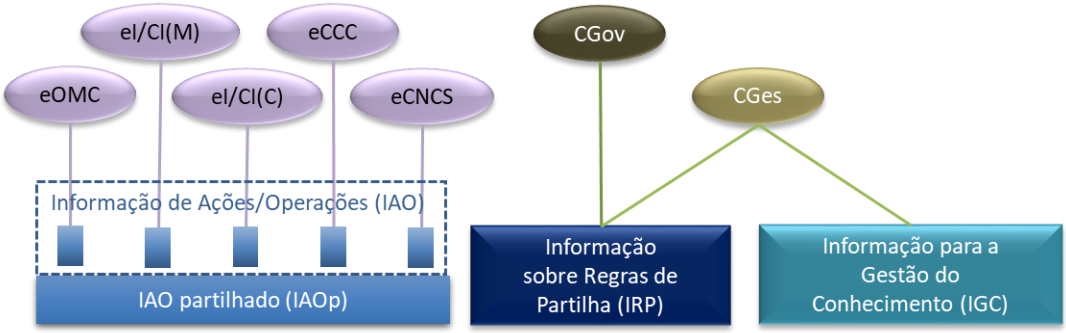


Figura 18 - Diagrama com a relação de controlo / autoridade em função da tipologia da informação

Na análise efetuada ao longo desta investigação emergem alguns princípios que devem enformar o conceito do centro, desde logo sobre a partilha de informação, mas também sobre a governação, designadamente o aspeto muito sensível dos processos de decisão, bem como os aspetos de segurança física e da informação. De forma a clarificar melhor o conceito é relevante afirmar que, por um lado, é completamente agnóstico relativamente a localizações físicas e, por outro, que não tem qualquer pressuposto de centralização ou de integração dos mandatos em causa, sendo este um aspeto extraordinariamente relevante que deverá ser objeto de particular atenção como explanado seguidamente.

Relativamente à governação:

– O conceito pressupõe que as entidades envolvidas mantêm totalmente os respetivos mandatos. É aliás imprescindível que assim seja. De acordo com Klimburg (2012) existem tensões que, entre outros aspetos, resultam da natureza democrática das sociedades ocidentais como, por exemplo, as preocupações com a privacidade, que recomendam que, ao mesmo tempo que se promove a partilha de informação e uma

ação unificada de diferentes entidades no ciberespaço, se devem instituir os mecanismos de governação que assegurem a conformidade legal das práticas seguidas e que, eventuais ações que possam comprometer o Estado, ou colocar em causa valores fundamentais da sociedade, tenham o adequado respaldo de uma tomada de decisão legítima. Concretizando, tal como explicitado por Boeke, Heinl e Veenendaal (2015) existem tensões, por exemplo, entre a eI/CI e as restantes entidades, todas legitimamente a defender a respetiva perspetiva: a eI/CI poderá entender que a vulnerabilidade num sistema não deve ser divulgada para ganhar vantagem sobre um adversário, enquanto a eCNCS considera que essa informação deverá ser divulgada à sua comunidade de interesse (IC e população em geral); a eI/CI poderá ainda entender que um determinado evento, que pode representar a materialização de um crime, não deverá ser divulgado, na mesma lógica de ter uma vantagem que pretende explorar mais tarde, enquanto que a eCCC entenderá a situação de outra maneira, podendo ser mesmo obrigada a agir criminalmente; e, finalmente, com a eOMC poderão ocorrer também situações de tensão relacionados, por exemplo, com as diferentes perspetivas sobre a oportunidade de revelar determinada informação, a propósito de uma operação que a eOMC pretenda efetuar, podendo a situação envolver a segurança de pessoas ou colocar mesmo em risco a respetiva vida. Adicionalmente, o envolvimento explícito e declarado da eOMC deverá ser sempre ponderado porque, na dialética do conflito, ainda que não-intencionalmente, poderá ser percecionado como um escalamento do nível de conflitualidade, devendo existir mecanismos explícitos para evitar que isso ocorra (Heinl, 2016). Algumas destas tensões/dilemas não poderão ser resolvidos previamente porque a decisão final dependerá do respetivo contexto tático, operacional e, por vezes, estratégico.

– Alguma da informação a partilhar poderá estar sujeita a regras acordadas e previamente definidas pelo que, neste particular, passíveis de implementação automática. No entanto, como referido, antecipam-se situações em que a decisão terá que ser tomada em contexto concreto. Assim, é imprescindível que estejam instituídos órgãos que deverão dirimir estas situações e, caso não o consigam, deverão estar previstos mecanismos para fazer escalar a questão. Esta decisão pode fazer parte de uma operação em curso, pelo que estes órgãos devem ser entendidos como operacionais (independentemente do nível de decisão, estratégico,

operacional ou tático em que se encontrem). No conceito do CNOSC este papel é desempenhado pelo CGes e pelo CGov e, caso não seja possível consensualizar e chegar a uma decisão, deverá estar previsto escalar para uma entidade supra setorial (figura 19).

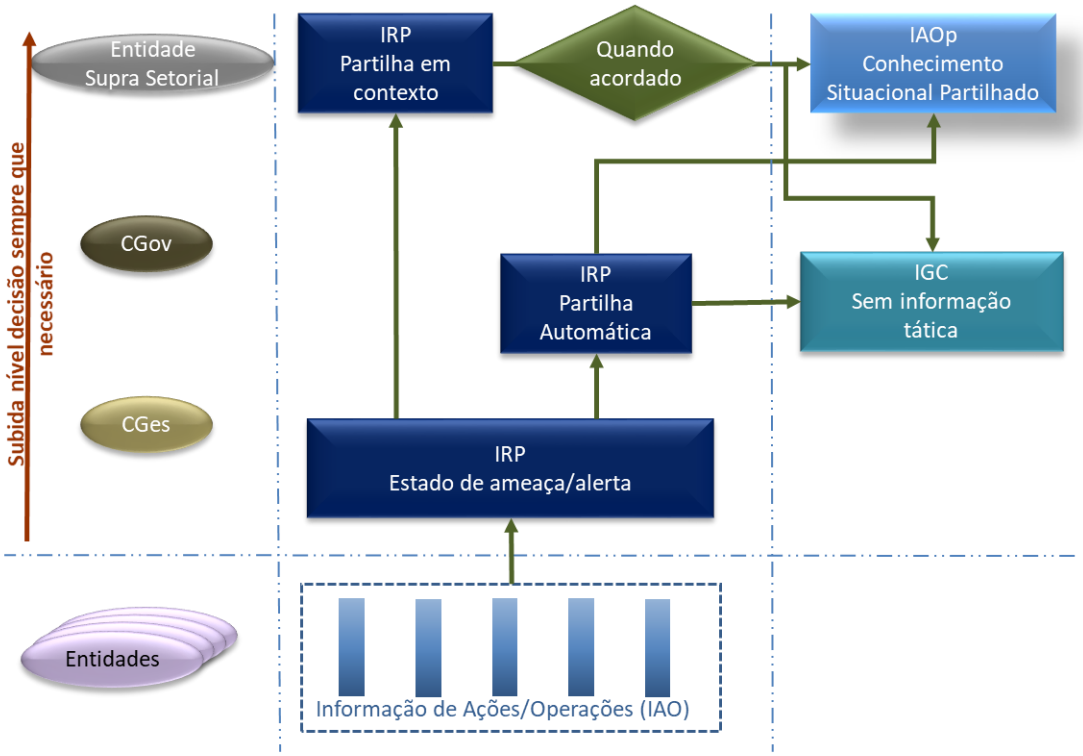


Figura 19 - CNOSC - Transformação de informação setorial em partilhada

Relativamente à partilha de informação, releva-se o seguinte:

- Como já referido, parte da informação poderá ser automaticamente partilhada e outra dependerá de processo de decisão no contexto da situação em concreto;
- O processo mental para a partilha de informação deverá ter o ponto de partida de que toda a informação é, por princípio, partilhável. A partir deste ponto é que se deverá identificar a informação que, por razões funcionais/operacionais e/ou legais, não possa/deva ser partilhada;
- As regras de segregação que limitam a informação disponibilizada às diferentes entidades devem prever a alteração do conjunto de informação partilhada em função do grau de alerta/ameaça. A alteração do estado de alerta/ameaça, sob decisão legítima, deverá ter implicação tempestiva nas regras de partilha. Por exemplo, em situação normal, pode não ser aceitável, por questões legais de privacidade, que uma determinada informação seja partilhada, mas, em situação de crise, o bem maior poderá determinar a respetiva partilha, quer automaticamente, quer sob

decisão no momento. Pode existir mesmo informação que, em situação normal, necessita de uma decisão tomada em contexto para ser partilhada e, em situação de crise, essa mesma informação ser automaticamente partilhada;

- Adicionalmente, caso a situação escale para uma situação de crise em que seja recomendável/decidido a ativação do apoio de entidades internacionais (ver 4.3.), deverão existir mecanismos para que a partilha de informação suporte essa interação.

Relativamente à segurança do centro e da informação, releva-se o seguinte:

- O ambiente informacional do centro deve estar preparado para processar, armazenar e transmitir informação classificada, não classificada, mas restrita ao centro, e informação pública, todas devidamente segregadas. Todas as entidades necessitam de se relacionar com entidades externas, pelo que o ambiente deverá acomodar e incorporar esses requisitos;
- Para além dos processos informais para estabelecimento de relações de confiança, todas as entidades e elementos envolvidos devem estar sujeitos a processos formais de credenciação e, de uma forma geral, devem ser assegurados todos os requisitos de segurança físicos, lógicos e de pessoal, de acordo com a classificação de segurança da informação manipulada no centro.

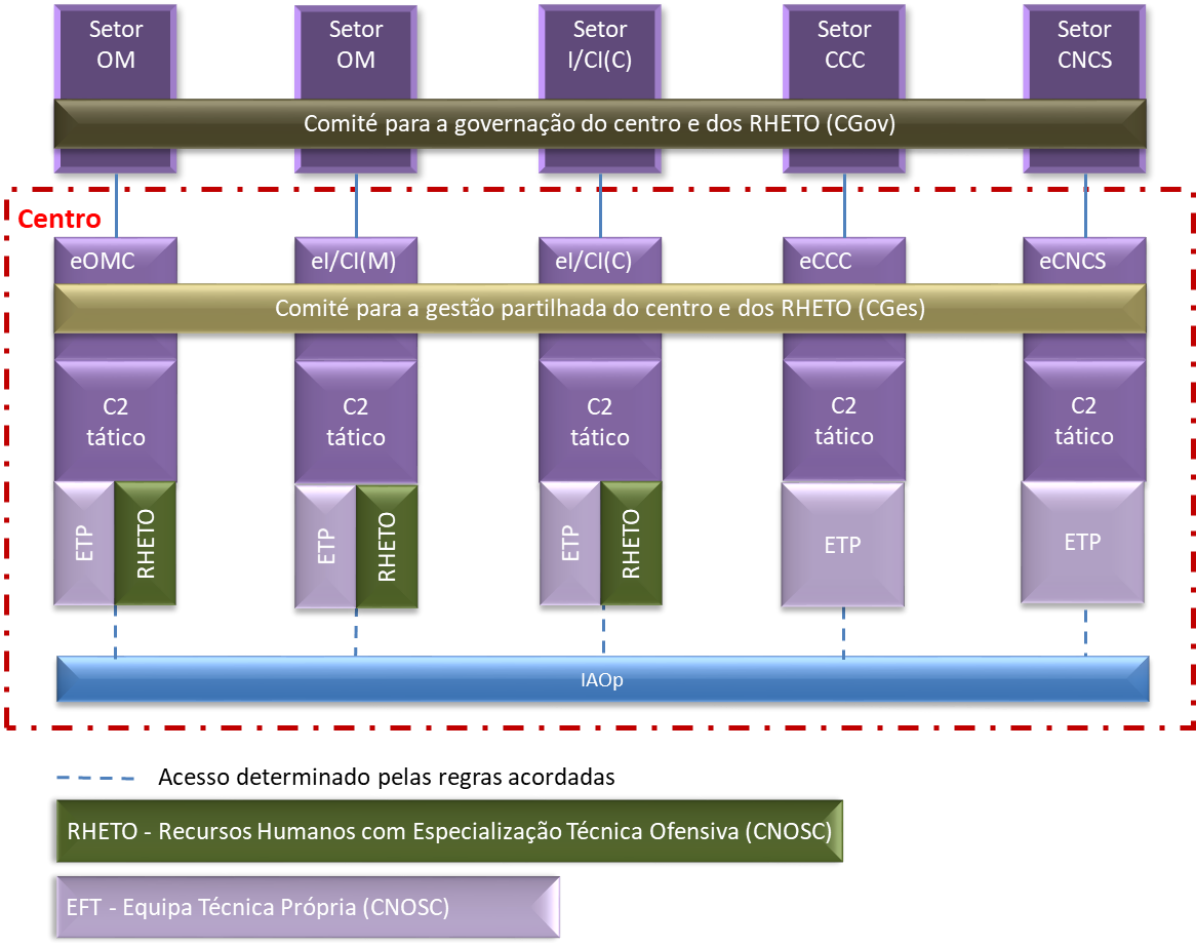


Figura 20 - CNOSC - Conceito do centro para a partilha de RHETO e de informação entre as entidades da ONSC

As eOMC, eI/CI(M) e eI/CI(C), nas ações/operações que executam, controlam taticamente e exploram, de forma partilhada, os RHETO. Para além do acesso a informação não partilhada de cada entidade (não representada na figura 20), acedem, quando necessário e decidido, à IAOp que foi estabelecida de acordo com os princípios gerais já descritos e ilustrados na figura 19. É mantido o vínculo de governação e controlo estratégico aos respetivos setores, sendo este o nível do CGov. O arranjo relativamente a ações/operações conjuntas, entre duas ou mais entidades, é também sujeito aos mesmos princípios de poder ser determinado de forma permanente, no caso de ações/operações contínuas ou, caso-a-caso, em função do contexto concreto da situação.

4.3. Sistema Nacional de Gestão de Crises

A existência de legislação incoerente ou, no mínimo, que suscita dúvidas sobre as estruturas, organização e processo de decisão em situação de crise, é uma enorme vulnerabilidade da ONSC-PT. Ainda que a articulação interna entre as entidades da ONSC-PT seja perfeita, isso não dispensa a existência de um SNGC. A emergência de ações híbridas, em que atores estatais e não-estatais exploram a ambiguidade e incerteza dos efeitos

das suas ações, mantendo-os abaixo do limiar que levaria a uma reação mais firme (no caso da NATO é conhecido como o limiar do artigo 5.º), recomenda vivamente a existência de um CSC acionável e de processos de decisão claros e tempestivos, tendo em conta a incerteza, quer quanto ao que esteja a acontecer, quer quanto à respetiva autoria. Acresce a circunstância de que este tipo de ações, embora explorem profusamente o ciberespaço, não se circunscrevem nele, pelo que o conhecimento/compreensão da situação poderá passar por outros elementos de informação que não estarão disponíveis quando consideramos apenas as entidades da ONSC-PT.

Ainda relacionado com a coerência do SNGC a instituir, deverão ser considerados os estados de não-guerra, designadamente as situações de incidente grave e de catástrofe (AR, 2015), bem como os regimes de estado de emergência e de sítio (AR, 1986), e a adequação dos procedimentos para a respetiva declaração aos riscos e ameaças associadas a um ambiente com as caraterísticas do ciberespaço. Adicionalmente, caso seja necessário formalizar o pedido de apoio a organizações internacionais, sendo uma decisão que ocorre a um nível político-estratégico, será desejável a disponibilidade de toda a informação relevante para apoiar essa decisão, independentemente dos efeitos ocorrerem dentro ou fora do ciberespaço. Assim, será imprescindível que o SNGC esteja edificado e clarificada a forma como as entidades que constituem a ONSC-PT se articulam com esse sistema, devendo mesmo fazer parte dele.

Por outro lado, a análise da interoperabilidade organizacional das entidades participantes nos exercícios CMX2017 e CC2017, poderá/deverá ser utilizada como instrumento de avaliação para determinar áreas de melhoria, como as identificadas em 3.2.3. para os casos analisados, uma vez que, para além dos exercícios que possam ser realizados, é imprescindível que exista um alinhamento em todas as dimensões do modelo, de forma a que se materialize uma efetiva ação unificada quando necessário e determinado.

4.4. Síntese conclusiva

Neste capítulo procedeu-se a síntese da análise efetuada nos capítulos 2 e 3, estruturada em torno dos aspetos mais relevantes para a relação civil/militar no ciberespaço, designadamente a postura estratégica da ONSC-PT, as soluções adotadas pelos países analisados para lidar com a exiguidade de RHETO, a partilha de informação entre as entidades com responsabilidade direta na ONSC-PT e que atuam nas fases de prevenção, preparação e de resposta do ciclo de vida dos incidentes de segurança no ciberespaço, incluindo em situação de crise e, finalmente, as implicações da inexistência de um SNGC.

Neste enquadramento, formulam-se as seguintes linhas de ação para melhorar a eficácia da resposta em todo o ciclo dos incidentes de segurança no ciberespaço, incluindo em situação de crise, envolvendo todas as entidades da ONSC-PT:

- Postura estratégica da ONSC-PT: deverá ser dado um maior enfoque à identificação proactiva de ameaças no ciberespaço, logo na fase de prevenção, através de ações de exploração (*intelligence*) promovidas pelos serviços de informações, civis e militares, e na partilha dessa informação, no aplicável, com CCD, UNC3T e CNCS, para que essa informação, em diferentes formatos e termos, possa chegar aos operadores de ICSE, PSD e população; clarificação sobre a entidade que assume a coordenação operacional nacional da resposta a crises no ciberespaço;
- Edificação de capacidades ofensivas no ciberespaço: no contexto do conceito CNOSC apresentado, com a partilha de RHETO entre os serviços de informações, civis e militares, e o CCD;
- Partilha de informação: edificar o CSC partilhado e acionável entre as entidades da ONSC-PT, que deverá ainda contemplar entidades privadas, designadamente os operadores de ICSE e PSD, e organizações internacionais, de forma a promover uma ação unificada, em todas as fases do ciclo de vida dos incidentes de segurança no ciberespaço, incluindo em situação de crise, assegurando sempre os termos em que a informação é partilhada conforme enunciado no conceito CNOSC;
- SNGC: instituir um sistema que acomode coerentemente os regimes de exceção, num processo de escalada que seja adequado às propriedades do ciberespaço e que permita integrar a ONSC-PT para responder a situações com manifestações dentro e fora do ciberespaço, de forma coerente e unificada.

Em suma, de forma a que seja promovida e facilitada a ação unificada das entidades, civis e militares, com responsabilidades de segurança ao longo de todo o espetro do conflito, as linhas de ação formuladas representam um contributo para melhorar a eficácia da resposta do EP a uma situação de crise no ciberespaço, permitindo assim responder à QD3 da presente investigação.

Conclusões

Sumário com as grandes linhas de procedimento metodológico

A presente investigação teve como objeto de estudo a segurança nacional no ciberespaço e desenvolveu-se com base nos princípios da investigação científica. O raciocínio de base privilegiado foi o dedutivo, materializado na aplicação de duas referências: a primeira, que permite analisar a forma como os Estados se organizam para providenciarem segurança no ciberespaço, foi utilizada para analisar a ONSC do RU e dos PB, bem como a ONSC-PT e, a segunda, corporizada num modelo de maturidade para a interoperabilidade organizacional, que foi instrumentado num questionário aplicado aos representantes dos organismos participantes nas células nacionais dos exercícios CMX2017 e CC2017.

Em termos metodológicos, adotou-se uma estratégia predominantemente qualitativa, com a análise de documentação NATO, da doutrina dos EUA, legislação nacional e da ONSC de países de referência, complementada, através da aplicação do M2C2IO a entidades da ONSC-PT, com uma análise quantificada de interoperabilidade organizacional. A metodologia adotada permitiu enquadrar a segurança no ciberespaço no ecossistema da segurança nacional, englobando as ações da componente civil do Estado, designada por cibersegurança, e as operações da componente militar do Estado, designada por ciberdefesa, como atividades que contribuem para a segurança nacional no ciberespaço. Caracterizou-se o ciberespaço, identificando-se as suas propriedades desafiantes: dinamismo, assimetria, inimputabilidade, *continnuns* disruptivos e transversalidade. O espetro do conflito no ciberespaço salienta a necessidade do Estado se organizar para providenciar segurança neste ambiente, desde a situação de normalidade até à situação de crise, incluindo os estados de exceção.

A relação civil/militar no ciberespaço refere-se ao papel das FFAA neste ambiente, ao longo do espetro do conflito e até à situação de crise, no enquadramento da respetiva articulação com os instrumentos civis do Estado, na designada ONSC, de forma a que seja alcançado um nível de segurança compatível com os interesses nacionais estabelecidos. Apesar da dimensão internacional se constituir como um aspeto incontornável da segurança nacional no ciberespaço, de que é exemplo o relacionamento com a NATO, esta vertente foi esporadicamente explorada ao longo da investigação que se focou, essencialmente, na relação civil/militar dentro da ONSC-PT.

Avaliação dos resultados obtidos

O objetivo desta investigação visou identificar contributos para melhorar a coerência e articulação da resposta do EP a situações de crise no ciberespaço, designadamente nos momentos em que seja necessário mobilizar todos os instrumentos nacionais, civis e militares, disponíveis e necessários, enformando, desta forma, os termos da relação civil/militar na ONSC-PT.

A investigação foi estruturada em três fases:

- Utilizando o referencial de análise das ONSC foi caracterizada a relação civil/militar nas ONSC de países de referência (RU e PB), a fim de identificar padrões relevantes para a caracterização da relação civil/militar em organizações nacionais;
- Empregando inicialmente o referencial de análise das ONSC e, posteriormente, o M2C2IO aplicado aos participantes nos exercícios CMX2017 e CC2017, foi analisada a coerência estratégica e articulação operacional do EP no emprego de todos os instrumentos nacionais, civis e militares, na resposta a uma crise no ciberespaço, a fim de identificar oportunidades de melhoria desse emprego, especialmente ao nível da relação civil/militar;
- Com base nas análises efetuadas nas fases anteriores foram formuladas linhas de ação para melhorar a eficácia da resposta do EP a situações de crise no ciberespaço, especialmente no emprego coerente e unificado dos instrumentos civis e militares.

Com a caracterização das ONSC no RU e nos PB identificaram-se os seguintes padrões com potencial de aplicação na ONSC-PT:

- Ao nível da definição estratégica é fortemente relevada a intenção de identificar e contrariar ameaças mais sofisticadas (cibercriminalidade organizada e patrocinada por Estados), logo na fase de prevenção do ciclo de vida dos incidentes;
- Ao nível da estrutura releva-se a adoção de soluções dirigidas à reconhecida exiguidade de recursos humanos altamente qualificados nesta área, designadamente com especialização técnica ofensiva, de que são exemplo, no caso do RU, a edificação de forma conjunta, pelos serviços de informações civis e FFAA, da capacidade para efetuar ações/operações de *intelligence* e ofensivas no ciberespaço e, no caso dos PB, a criação de uma unidade para efetuar ações de identificação proactiva de ameaças no ciberespaço, gerida conjuntamente pelos serviços de informações civis e militares;

- Ao nível da articulação operacional é sublinhada a relevância da partilha de informação, incluindo a classificada, e que compreenda ainda a partilha de conhecimento sobre ameaças no ciberespaço, logo na fase de prevenção do ciclo de vida dos incidentes de segurança, principalmente quanto às que representam maior ameaça à segurança nacional, para depois habilitar a respetiva partilha em formatos e termos diferenciados, entre todos os atores da ONSC, incluindo operadores de IC e população em geral.

Da análise global efetuada à ONSC-PT identificaram-se os seguintes aspetos da relação civil/militar no ciberespaço:

- Ao nível dos objetivos e estrutura estabelecidos na estratégia verifica-se a necessidade de clarificar o papel de coordenação em situação de crise no ciberespaço, quer ao nível estratégico (SGSSI, PCE, MDN), quer ao nível operacional (CCD, CNCS), até que esta situação seja desejavelmente definida com a criação de um SNGC; adicionalmente, verifica-se a necessidade de estabelecer/definir o papel a desempenhar pelos serviços de informações, civis e militares, na ONSC-PT;
- Na articulação operacional, constata-se a existência de oportunidades de melhoria para a partilha de informação, incluindo classificada, entre todos os atores da ONSC-PT, principalmente na fase de prevenção do ciclo de vida dos incidentes de segurança no ciberespaço; adicionalmente, da aplicação do questionário com base no M2C2IO, resultou um nível de maturidade de interoperabilidade organizacional de, no caso do CC2017, 3,83 e, no caso do CMX2017, 3,24. No CC2017 a origem dos participantes é muito mais uniforme o que explica a melhor pontuação nalgumas variáveis. Em qualquer dos casos, para obter uma ação unificada é desejável alcançar um resultado maior ou igual a quatro, pelo que existem oportunidades de melhoria ao nível das variáveis Treino e Comunicação e, no caso do CMX2017, também nas variáveis Doutrina, Informação, deciSão e cUltura.

Para melhorar a eficácia da resposta em todas as fases do ciclo de vida dos incidentes de segurança no ciberespaço, incluindo em situação de crise, envolvendo todas as entidades da ONSC-PT, formularam-se as seguintes linhas de ação:

- Postura estratégica da ONSC-PT: deverá ser dado um maior enfoque à identificação proactiva de ameaças no ciberespaço, logo na fase de prevenção, através de ações de exploração (*intelligence*) promovidas pelos serviços de informações, quer civis,

quer militares, e na partilha dessa informação, no aplicável, com o CCD, UNC3T e CNCS, para que essa informação, em diferentes formatos e termos, possa ainda ser partilhada com os operadores de ICSE, PSD e população; deverá ser clarificado qual a entidade com responsabilidade operacional de coordenação nacional na resposta a crises no ciberespaço;

- Edificação de capacidades ofensivas no ciberespaço: no enquadramento do conceito CNOSC apresentado, propõe-se a partilha de RHETO entre o serviço de informações civil, o serviço de informações militares e o CCD;
- Partilha de informação: edificar o CSC partilhado entre as entidades da ONSC-PT, nos termos dos princípios enunciados no conceito CNOSC, incluindo a partilha de informação com organizações internacionais e entidades privadas, de forma a promover uma ação unificada em todas as fases do ciclo de vida dos incidentes de segurança no ciberespaço, incluindo em situação de crise, assegurando sempre os termos em que a informação é partilhada;
- SNGC: instituir um sistema que acomode coerentemente, quer os regimes de exceção, quer as situações de incidente grave e catástrofe, num processo de escalamento definido, adequado às propriedades do ciberespaço e que considere a articulação harmoniosa com as entidades da ONSC-PT, habilitando uma maior eficácia na resposta a situações com incidências dentro e fora do ciberespaço, de forma coerente e unificada.

Em suma, com os contributos identificados, no formato de propostas de linhas de ação para melhorar a resposta do Estado Português a situações de crise no ciberespaço, atendendo à ação das diferentes entidades, civis e militares, com responsabilidade na segurança deste ambiente e considerando o enquadramento normativo, organizações de referência, assim como instrumentos de interoperabilidade organizacional, conclui-se que os resultados obtidos permitem responder à QC e, desta forma, alcançar os objetivos estabelecidos para esta investigação.

Contributos para o conhecimento

Considera-se que o M2C2IO tem potencial para se constituir como um instrumento de análise mais abrangente. Para além de poder ser utilizado como ferramenta de planeamento para estruturar ações que visem a promoção da interoperabilidade organizacional, que é a sua utilização habitual, a sua instrumentação, no formato de questionário, constituiu uma

abordagem complementar que, introduzido de forma sistemática em exercícios, poderá ser explorado para alimentar um processo de aprendizagem interorganizacional.

O conceito do CNOSC proposto, nas suas duas vertentes, quer de partilha de RHETO, quer da existência crucial de um CSC partilhado, com os princípios enunciados de governação que incluem a adequação dos processos de decisão à natureza do ciberespaço, a partilha de informação e, ainda, aspetos de segurança, quer física, quer da informação, constitui-se como um ponto de partida para a sua densificação posterior, contribuindo para alavancar a edificação consistente e sustentada de capacidades ofensivas no ciberespaço.

Recomendações e outras considerações de ordem prática

A aplicação do M2C2IO revelou algumas deficiências que podem ser corrigidas incrementando a quantidade de perguntas com opções de resposta objetivas. A maior parte das perguntas continha respostas em escala de concordância, que se constatou estarem sujeitas a uma abrangência de interpretação demasiado alargada.

O estabelecimento de um programa consistente de exercícios, incluindo parciais e com grau de dificuldade crescente, acompanhado por ações concretas de melhoria dos protocolos de articulação e pelo estabelecimento de formas mais estruturadas de comunicação e de partilha de informação, permitirá aumentar o nível de conhecimento/compreensão partilhada e elevar o nível de maturidade de interoperabilidade organizacional, com impacto na eficácia da ação conjunta e unificada das entidades envolvidas.

Limitações da investigação e abertura para pesquisas futuras

Os questionários de análise da interoperabilidade organizacional efetuada aos participantes nacionais dos exercícios CMX2017 e CC2017 tinham dezassete perguntas com respostas em escala de concordância, num total de vinte. As outras três perguntas tinham opções de resposta objetiva para selecionar uma. Observou-se uma diferença acentuada nas respostas a cada um dos tipos de perguntas, pelo que se pode considerar que o questionário apresentado fomentou respostas que proporcionaram um resultado final sobrevalorizado. Adicionalmente, deverá ter-se em consideração a exiguidade da população-alvo.

Relacionado com o conceito CNOSC poderão ser abertas várias linhas de investigação para estudar e densificar diversos aspetos, sugerindo-se os seguintes:

- Estruturação dos termos de referência dos órgãos de governação e de gestão, com o envolvimento das entidades da ONSC-PT;

- Modelo de gestão dos RHETO, designadamente a sua obtenção e estruturas referenciais de remuneração, incluindo a viabilidade de enquadramento à luz da legislação portuguesa;
- Modelo de gestão partilhada dos RHETO, designadamente quanto ao respetivo controlo tático por diferentes entidades na execução de ações/operações;
- Modelação da arquitetura de informação para responder aos princípios de partilha enunciados no conceito;
- Estudo/avaliação dos dilemas de partilha de informação, principalmente quando uma das partes é um serviço de informações.

Bibliografia

Abreu, F., 2002. *Fundamentos de Estratégia Militar e Empresarial*. Lisboa: Sílabo Gestão.

Abreu, F., 2003. Estratégia: da Conflitualidade à Competição. *Nação e Defesa*. [Em linha] Nr Extra (A Revolução nos Assuntos Militares-III Conferência dos Colégios de Defesa Ibero-Americanos). Lisboa: Instituto da Defesa Nacional. Disponível em: https://www.idn.gov.pt/publicacoes/nacaodefesa/textointegral/NeD_ExtraAbril03.pdf. [Acedido em 15 de março 2018].

ACT, 2017. *Cyber Coalition 2017 Exercise Specification*. Norfolk: NATO.

Alberts, D.S. e Hayes, R.E., 2005. *Power to the Edge: Command, Control in the Information Age*. 3.ª ed. [Em linha] Washington DC: Department of Defense Command and Control Research Program. Disponível em: www.dodccrp.org/files/Alberts_Power.pdf. [Acedido em 15 de março 2018].

Alberts, D.S. e Hayes, R.E., 2006. *Understanding Command and Control*. [Em linha] Washington DC: Department of Defense Command and Control Research Program. Disponível em: www.dodccrp.org/files/Alberts_UC2.pdf. [Acedido em 15 de março 2018].

AR, 1986. *Regime do estado de sítio e do estado de emergência* (Lei n.º 44/86, de 30 de setembro; versão consolidada até Lei Orgânica n.º 1/2012, de 11 de maio). [Em linha] Lisboa: Diário da República. Disponível em: http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1712&tabela=leis&so_miolo=. [Acedido em 20 de novembro 2017].

AR, 2015. *Lei de bases da protecção civil* (Lei n.º 27/2006, de 03 de julho; versão consolidada até Lei n.º 80/2015, de 03 de agosto). [Em linha] Lisboa: Diário da República. Disponível em: http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1735&tabela=leis&so_miolo=S. [Acedido em 20 de novembro 2017].

AR, 2017. *Lei da Segurança Interna* (Lei n.º 53/2008 de 29 de agosto; versão consolidada até Decreto-Lei n.º 49/2017, de 24 de maio). [Em linha] Lisboa: Diário da República. Disponível em: http://data.dre.pt/eli/lei/53/2008/p/cons/20170524/pt/html. [Acedido em 20 de novembro 2017].

Assembleia Constituinte, 1976. *Constituição da República Portuguesa* (Versão consolidada até Lei Constitucional n.º 1/2005). [Em linha] Lisboa: Diário da República. Disponível em: https://dre.pt/web/guest/legislacao-consolidada/-

/lc/337/201712031035/exportPdf/normal/1/cacheLevelPage?_LegislacaoConsolidada_WAR_drefrontofficeportlet_rp=indice. [Acedido em 20 de novembro 2017].

Boeke, S., Heinl, C.H. e Veenendaal, M.A., 2015. Civil-military relations and international military cooperation in cyber security: Common challenges & state practices across Asia and Europe. Em: M. Maybaum, A.M. Osula e L. Lindström, eds., *2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace*. [Em linha] Tallinn: NATO CCDCoE Publications, pp.69–80. Disponível em: http://www.ccdcoe.org/cycon/2015/proceedings/CyCon_2015_book.pdf. [Acedido em 15 de dezembro 2017].

C2CoE, 2017. *C2CoE*. [Em linha] Disponível em: https://c2coe.org/. [Acedido em 19 de dezembro 2017].

Cardoso, L.A.G., 1979. Editorial. *Nação e Defesa*. [Em linha] Ano IV (N.º 12), pp.7–12. Lisboa: Instituto da Defesa Nacional. Disponível em: https://www.idn.gov.pt/publicacoes/nacaodefesa/textointegral/NeD12.pdf. [Acedido em 15 de fevereiro 2018].

CCDCoE, 2017. *CCDCoE*. [Em linha] Disponível em: https://ccdcoe.org/. [Acedido em 19 de dezembro 2017].

CCDCoE, 2018. *Resources - Cyber Definitions*. [Em linha] Disponível em: https://ccdcoe.org/cyber-definitions.html. [Acedido em 15 de março 2018].

Clark, T. e Jones, R., 1999. Organisational interoperability maturity model for C2. *Proceedings of the 1999 Command and Control Research and Technology Symposium*. [Em linha] pp.1–13. Newport: Command and Control Research Program (U.S.). Disponível em: http://www.dodccrp.org/events/1999_CCRTS/pdf_files/track_5/049clark.pdf. [Acedido em 15 de dezembro 2017].

CMDRCoE, 2014. *Concept of the Crisis Management and Disaster Response Centre of Excellence*. [Em linha] Sofia: CMDRCoE. Disponível em: https://www.cmdrcoe.org/download.php?id=791. [Acedido em 17 de dezembro 2017].

CMDRCoE, 2017. *Crisis Management and Disaster Response Centre of Excellence*. [Em linha] Disponível em: https://www.cmdrcoe.org/index.php. [Acedido em 19 de dezembro 2017].

Conselho de Chefes de Estado-Maior, 2014. *Conceito Estratégico Militar*. Lisboa.

Couto, A.C., 1987. *Elementos de Estratégia - Apontamentos para um curso - Volume I*.

Lisboa: Instituto de Altos Estudos Militares.

Dias, C.M.M. e Sequeira, J.M.D., 2015. *Estratégia - Fundamentos Teóricos - Tomo I*. Loures: Letras Itinerantes, Edição e Distribuição de Livros, Lda.

Dias, C.M.M. e Sequeira, J.M.D., 2017. *Estratégia - Fundamentos Teóricos - Tomo II*. Loures: Letras Itinerantes, Edição e Distribuição de Livros, Lda.

Fernandes, A.H., 2003. Estratégia: Hostilidade ou Competição? *Nação e Defesa*. [Em linha] Nr Extra (A Revolução nos Assuntos Militares-III Conferência dos Colégios de Defesa Ibero-Americanos), pp.145–156. Lisboa: Instituto da Defesa Nacional. Disponível em: https://www.idn.gov.pt/publicacoes/nacaodefesa/textointegral/NeD_ExtraAbril03.pdf. [Acedido em 15 de março 2018].

GOV-PT, 2004. *Criação do Sistema Nacional de Gestão de Crises* (Decreto-Lei n.º 173/2004 de 21 de Julho). [Em linha] Lisboa: Diário da República - I SÉRIE-A - N.o 170 - 21 de Julho de 2004, pp.4507–4508. Disponível em: https://dre.pt/application/conteudo/505639. [Acedido em 15 de março 2018].

GOV-PT, 2013a. *Conceito Estratégico de Defesa Nacional* (RCM n.º 19/2013 de 21 de março). [Em linha] Lisboa: Diário da República, 1.ª série - N.º 67 - 5 de abril de 2013, pp. 1981-1995. Disponível em: https://dre.pt/application/file/a/259983. [Acedido em 20 de novembro 2017].

GOV-PT, 2013b. *Diretiva iniciadora com a Orientação Política para a Ciberdefesa* (Despacho n.º 13692/2013). [Em linha] Lisboa: Diário da República, 2.ª série - N.º 208 - 28 de outubro de 2013, pp.31976–31979. Disponível em: https://dre.pt/application/conteudo/3295679. [Acedido em 15 de fevereiro 2018].

GOV-PT, 2014a. *Lei Orgânica do EMGFA* (Decreto-Lei n.º 184/2014 de 29 de dezembro). [Em linha] Lisboa: Diário da República, 1.ª série - N.º 250 - 29 de dezembro de 2014, pp.6382–6397. Disponível em: https://dre.pt/application/conteudo/65983261. [Acedido em 12 de dezembro 2017].

GOV-PT, 2014b. *Orgânica da Autoridade Nacional de Proteção Civil* (Decreto-Lei n.º 163/2014 de 31 de outubro). [Em linha] Lisboa: Diário da República, 1.ª série - N.º 211 - 31 de outubro de 2014, pp.5615–5624. Disponível em: https://dre.pt/application/conteudo/58683383. [Acedido em 15 de fevereiro 2018].

GOV-PT, 2015. *Estratégia Nacional de Segurança no Ciberespaço* (RCM 36/2015, de 28 de maio). [Em linha] Lisboa: Diário da República, 1.ª série - N.º 113 - 12 de junho de 2015, pp.3738–3742. Disponível em:

http://data.dre.pt/eli/resolconsmin/36/2015/06/12/p/dre/pt/html. [Acedido em 15 de novembro 2017].

GOV-PT, 2017a. *Cria o grupo de projeto denominado Conselho Superior de Segurança do Ciberespaço (CSSC)* (RCM 115/2017, de 13 de julho). [Em linha] Lisboa: Diário da República, 1.ª série - N.º 163 - 24 de agosto de 2017, pp.5035–5037. Disponível em: http://data.dre.pt/eli/resolconsmin/115/2017/08/24/p/dre/pt/html. [Acedido em 15 de novembro 2017].

GOV-PT, 2017b. *Exercício de Gestão de Crises da Organização do Tratado do Atlântico Norte — CMX17* (Despacho n.º 7834-A/2017). Diário da República, 2.ª série, N.º 171 de 5 de setembro de 2017 - Parte C. Lisboa, p.19562–(2).

GOV-PT, 2017c. *Orgânica do Gabinete Nacional de Segurança* (Decreto-Lei n.º 136/2017 de 6 de novembro). [Em linha] Lisboa: Diário da República, 1.ª série - N.º 213 - 6 de novembro de 2017, pp.5879–5886. Disponível em: https://dre.pt/application/conteudo/114152775. [Acedido em 15 de fevereiro 2018].

GOV-PT, 2017d. *Portugal participa em exercício de gestão de crises da NATO*. [Em linha] Disponível em: https://www.portugal.gov.pt/pt/gc21/comunicacao/noticia?i=portugal-participa-em-exercicio-de-gestao-de-crises-da-nato. [Acedido em 19 de dezembro 2017].

GOV-PT, 2018. *Regime jurídico da segurança do ciberespaço* (Proposta de Lei N.º 119/XIII). [Em linha] Lisboa. Disponível em: http://app.parlamento.pt/webutils/docs/doc.pdf?path=6148523063446f764c324679595842774f6a63334e7a637664326c756157357059326c6864476c3259584d7657456c4a535339305a58683062334d76634842734d5445354c56684a53556b755a47396a&fich=ppl119-XIII.doc&Inline=true. [Acedido em 10 de abril 2018].

Guédria, W., Naudet, Y. e Chen, D., 2011. A maturity model assessing interoperability potential. *Lecture Notes in Business Information Processing*. Vol. 81 (Enterprise, Business-Process and Information Systems Modeling. International Conferences on Business Process Modeling, Development and Support, and on Exploring Modeling Methods for Systems Analysis and Design, JUN2011, London), pp.276–283. Berlin, Heidelberg: Springer.

Hathaway, M. e Spidalieri, F., 2017. The Netherlands Cyber Readiness at a Glance. *Cyber Readiness Index 2.0*. [Em linha] Arlington: Potomac Institute for Policy Studies. Disponível em:

http://www.potomacinstitute.org/images/CRI/FinalCRI20NetherlandsWeb.pdf. [Acedido em 31 de março 2018].

Heinl, C., 2016. The Role of the Military in Cyber Space : Civil-Military Relations and International Military Co-operation. *Pointer - Journal of The Singapure Armed Forces*. [Em linha] Vol.42, pp.37–46. Disponível em: https://www.mindef.gov.sg/oms/safti/pointer/documents/pdf/V42N4.pdf. [Acedido em 15 de março 2018].

IDN, 2013. Estratégia da informação e segurança no ciberespaço. *IDN Cadernos*. [Em linha] N.º 12. Lisboa: Instituto da Defesa Nacional. Disponível em: http://comum.rcaap.pt/handle/10400.26/7757. [Acedido em 17 de dezembro 2017].

IESM, 2015a. *NEP/ACA-010 Trabalhos de investigação*. Lisboa: Instituto de Estudos Superiores Militares.

IESM, 2015b. *NEP/ACA-018 Regras de apresentação e referenciação para os trabalhos escritos a realizar no IESM*. Lisboa: Instituto de Estudos Superiores Militares.

Jesus, H.M.F. de, 2018. *A cooperação civil/militar no ciberespaço* [Entrevista]. Lisboa (28 de novembro de 2018).

Kaska, K., 2015. National Cyber Security Organisation: the Netherlands. *National Cyber Security Organisations*. [Em linha] Tallinn: Cooperative Cyber Defence Centre of Excellence. Disponível em: https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_NETHERLANDS_032015_0.pdf. [Acedido em 15 de fevereiro 2018].

Klimburg, A., 2012. *National Cyber Security Framework Manual*. [Em linha] Tallinn: NATO Cooperative Cyber Defence Centre of Excellence Publication. Disponível em: https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf. [Acedido em 20 de novembro 2017].

Leitão, A., 2016. *Cooperação e colaboração interadministrativas*. [Em linha] Disponível em: http://aprenderamadeira.net/cooperacao-e-colaboracao-interadministrativas/.

Marinov, I., 2014. *NATO Crisis Management*. [Em linha] Sofia: NATO Crisis Management and Disaster Response Centre of Excellence. Disponível em: https://www.cmdrcoe.org/download.php. [Acedido em 15 de março 2018].

Marques, A.J.G., 2018. A segurança do espaço cibernético: Que modelo para Portugal. Em: *Seminário de Operações do Curso de Estado-Maior Conjunto 2017/18 - Ciberdefesa e Cooperação Civil-Militar, domínios de interesse Nacional no âmbito das Atividades de*

Informação (09ABR2018) Painel II - Ciberdefesa: Desafios atuais e futuros. Lisboa: Instituto Universitário Militar.

NATO, 1949. *North Atlantic Treaty*. [Em linha] Washington DC: North Atlantic Treaty Organization. Disponível em: https://www.nato.int/cps/en/natohq/official_texts_17120.htm. [Acedido em 15 de março 2018].

NATO, 2010. *Strategic Concept For the Defence and Security of The Members of the North Atlantic Treaty Organisation*. [Em linha] Lisboa: North Atlantic Treaty Organization. Disponível em: http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120203_strategic-concept-2010-eng.pdf. [Acedido em 15 de março 2018].

NATO, 2014. *NATO Cyber Defence Taxonomy and Definitions* (AC/322-N(2014)0072). Brussels: Consultation, Command and Control (C3) Board.

NATO, 2016. *Warsaw Summit Communiqué*. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/official_texts_133169.htm#cyber. [Acedido em 15 de março 2018].

NATO, 2017a. *Collective defence - Article 5*. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/topics_110496.htm. [Acedido em 15 de novembro 2017].

NATO, 2017b. *NATO Crisis Response System Manual (NCRSM) 2017*. Bruxelas: North Atlantic Treaty Organization.

NICCS, 2017. *A Glossary of Common Cybersecurity Terminology*. [Em linha] National Initiative for Cybersecurity Careers and Studies. Disponível em: https://niccs.us-cert.gov/glossary#C. [Acedido em 17 de dezembro 2017].

Nunes, P.F.V., 2016. Ciberameaças e quadro legal dos conflitos no ciberespaço. Em: J.B. Borges e T.F. Rodrigues, eds., *Ameaças e riscos transnacionais no novo mundo global*, 1.ª Ed. Porto: Fronteira do Caos Editores, Lda, pp.199–215.

Ottis, R. e Lorents, P., 2010. Cyberspace: Definition and Implications. *The Proceedings of the 5th International Conference on Information Warfare and Security*. [Em linha] pp.267–270. Disponível em: http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:No+Title#0. [Acedido em 15 de fevereiro 2018].

PB-CSC, 2018. *Cyber Security Raad - Home*. [Em linha] Disponível em:

https://www.cybersecurityraad.nl/index-english.aspx. [Acedido em 31 de março 2018].

PB-GOV, 2013a. *National Cyber Security Strategy 2*. [Em linha] Haia: Governo dos Países Baixos. Disponível em: https://www.ncsc.nl/binaries/content/documents/ncsc-en/current-topics/national-cyber-security-strategy/1/National%2BCyber%2BSecurity%2BStrategy%2B2.pdf. [Acedido em 31 de março 2018].

PB-GOV, 2013b. *National Manual on Decision-making in Crisis Situations – The Netherlands*. Haia: Governo dos Países Baixos.

PB-GOV, 2015a. *Defense Cyber Strategy*. [Em linha] Disponível em: https://english.defensie.nl/topics/cyber-security/defence-cyber-strategy. [Acedido em 31 de março 2018].

PB-GOV, 2015b. *Letter from the Minister of Defence to the President of the House of Representatives of the States General: Defence Cyber Strategy - Update*. [Em linha] Haia: Governo dos Países Baixos. Disponível em: https://www.government.nl/binaries/government/documents/parliamentary-documents/2015/02/23/letter-concerning-defense-cyber-strategy/PD.Defense_Cyber_Strategy_Update.pdf. [Acedido em 31 de março 2018].

PB-GOV, 2017. *Building Digital Bridges - International Cyber Strategy Towards an integrated international cyber policy*. [Em linha] Haia: Governo dos Países Baixos. Disponível em: https://www.government.nl/binaries/government/documents/parliamentary-documents/2017/02/12/international-cyber-strategy/International+Cyber+Strategy.pdf. [Acedido em 31 de março 2018].

PB-NCSC, 2018. *ICT Crisis Management*. [Em linha] Disponível em: https://www.ncsc.nl/english/Incident+Response/ict-crisis-management.html. [Acedido em 31 de março 2018].

PE e CUE, 2016. *Medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União* (Diretiva (UE) 2016/1148). [Em linha] Bruxelas: Jornal Oficial da União Europeia, p.L194/1-L194/30. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L1148&from=PT. [Acedido em 31 de março 2018].

Pires, F.J., 2018. Painel II - Ciberdefesa: Desafios atuais e futuros (Moderador). Em:

Seminário de Operações do Curso de Estado-Maior Conjunto 2017/18 - Ciberdefesa e Cooperação Civil-Militar, domínios de interesse Nacional no âmbito das Atividades de Informação (09ABR2018). Lisboa: Instituto Universitário Militar.

Policarpo, L.C., 2017. *A cooperação civil/militar no ciberespaço* [Entrevista]. Lisboa (10 de novembro de 2017).

Raposo, R., 2018. *A cooperação civil/militar no ciberespaço* [Entrevista]. Lisboa (23 de março de 2018).

Ribeiro, A.S., 2017. *Teoria Geral da Estratégia: o essencial ao processo estratégico*. Coimbra: Edições Almedina, SA.

RU-GOV, 2010. *National Intelligence Machinery*. [Em linha] London: Governo do Reino Unido. Disponível em: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61808/nim-november2010.pdf. [Acedido em 31 de março 2018].

RU-GOV, 2016. *National Cyber Security Strategy 2016-2021*. [Em linha] London: Governo do Reino Unido. Disponível em: https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021. [Acedido em 31 de março 2018].

RU-GOV, 2018a. *Cabinet Office - About*. [Em linha] Disponível em: https://www.gov.uk/government/organisations/cabinet-office/about. [Acedido em 31 de março 2018].

RU-GOV, 2018b. *Cyber and Government Security Directorate*. [Em linha] Disponível em: https://www.gov.uk/government/groups/office-of-cyber-security-and-information-assurance. [Acedido em 31 de março 2018].

RU-GOV, 2018c. *National Crime Agency - How we are run*. [Em linha] Disponível em: http://www.nationalcrimeagency.gov.uk/about-us/how-we-are-run. [Acedido em 11 de março 2018].

Russell, S.M., Suri, N., Lenzi, R. e Fouad, H., 2016. Measuring and Evaluating Interoperability for Complex C2 Information Management System-of-Systems. *21st International Command and Control Reserch and Technology Symposium*. [Em linha] pp.1–16. Disponível em: https://static1.squarespace.com/static/53bad224e4b013a11d687e40/t/57d6995f893fc0cb7a12e334/1473681759965/paper_64.pdf.

Santos, L.A.B. dos, Garcia, F.M.G.P.P., Monteiro, F.T., Lima, J.M.M. do V., Silva, N.M.P.

da, Silva, J.C. do V.F. da, Peidade, J.C.L. da, Santos, R.J.R.P. dos e Afonso, C.F.N.L.D., 2016. *Orientações metodológicas para a elaboração de trabalhos de investigação*. Lisboa: IUM.

Santos, L.F.C.D., 2017. *Contributos para uma estratégia nacional de ciberdefesa*. Trabalho de Investigação Individual, Curso de Promoção a Oficial General 2016/17. Instituto Universitário Militar.

Schmitt, M.N., 2013. *Tallinn Manual on The International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.

Smeets, M., 2018. *The Netherlands just revealed its cybercapacity. So what does that mean?* [Em linha] Disponível em: https://www.washingtonpost.com/news/monkey-cage/wp/2018/02/08/the-netherlands-just-revealed-its-cyber-capacity-so-what-does-that-mean/?noredirect=on&utm_term=.e51118f3b734. [Acedido em 31 de março 2018].

Tikk, E., 2011. *Comprehensive legal approach to cyber security*. Dissertation for the Degree of Doctor, Faculty of Law [Em linha] University of Tartu. Disponível em: http://www.tandfonline.com/doi/abs/10.1080/00396338.2011.571016%5Cnhttp://dspace.utlib.ee/dspace/handle/10062/17914. [Acedido em 20 de novembro 2017].

UE, 2015. *Countries, languages and currencies: names, codes and listing order*. [Em linha] Disponível em: http://publications.europa.eu/code/pdf/370000en.htm#unilingue. [Acedido em 19 de fevereiro 2018].

UE, 2018. *Breve apresentação dos países da UE*. [Em linha] Disponível em: https://europa.eu/european-union/about-eu/countries/member-countries_pt. [Acedido em 19 de fevereiro 2018].

USDoD, 2015. *The DoD Cyber Strategy*. [Em linha] Washington DC: United States Department of Defense. Disponível em: http://www.defense.gov/Portals/1/features/2015/0415%7B_%7Dcyber-strategy/Final%7B_%7D2015%7B_%7DDoD%7B_%7DCYBER%7B_%7DSTRATEGY%7B_%7Dfor%7B_%7Dweb.pdf. [Acedido em 20 de novembro 2017].

USDoD, 2018. *DoDAF - Background - Introduction*. [Em linha] Disponível em: http://dodcio.defense.gov/Library/DoD-Architecture-Framework/dodaf20_background/. [Acedido em 15 de março 2018].

USJCS, 2013. *Joint Publication 3-12 (R) Cyberspace Operations* (February 2013). [Em linha] Washington DC: United States Joint Chiefs of Staff. Disponível em:

http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12R.pdf. [Acedido em 15 de fevereiro 2018].

USJCS, 2016. *Joint Publication 3-08 Interorganizational Cooperation*. [Em linha] Washington DC: United States Joint Chiefs of Staff. Disponível em: http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_08pa.pdf?ver=2018-02-08-091414-467. [Acedido em 15 de março 2018].

Williams, A., 2010. Implications of Operationalizing a Comprehensive Approach: Defining what Interagency Interoperability Really Means. *The International C2 Journal*. [Em linha] Vol. 4 (Agility and Interoperability for 21st Century Command and Control), pp.1–32. Command and Control Research Program (USDoD). Disponível em: http://www.dodccrp.org/files/IC2J_v4n1_01_Williams.pdf. [Acedido em 15 de março 2018].

Apêndice A — Corpo de conceitos

Catástrofe	É o acidente grave ou a série de acidentes graves suscetíveis de provocarem elevados prejuízos materiais e, eventualmente, vítimas, afetando intensamente as condições de vida e o tecido socioeconómico em áreas ou na totalidade do território nacional. (AR, 2015)
Ciberdefesa	A aplicação das medidas de segurança para proteger oscomponentes da infraestrutura TIC contra ciberataques, sendo estes ciberataques assumidos como uma forma de guerra cibernética, que pode ocorrer em combinação com um ataque físico ou não, que se destina a perturbar os sistemas de informação de um adversário. (IDN, 2013, p.11)
Ciberespaço	*Is a time-dependent set of interconnected information systems and the human users that interact with these systems.* (Ottis e Lorents, 2010) *The environment formed by physical and non-physical components, characterized by the use of computers and electro-magnetic spectrum, to store, modify and exchange data using computer networks.* (Schmitt, 2013) *The global domain created by communication, information and other electronic systems, their interaction and the information that is stored, processed or transmitted in these systems.* (NATO, 2014)
Cibersegurança	*The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation.* (NICCS, 2017)
Crise	Situação nacional ou internacional em que se manifesta uma ameaça a valores, interesses ou objetivos prioritários das partes envolvidas. (CMDRCoE, 2014, p.12) Situação caracterizada por se situar entre a normalidade e a guerra, que exige a urgência de decisões e de acções, bem como a aplicação de meios adequados de resposta, no sentido do restabelecimento da situação anterior, ou da salvaguarda dos interesses postos em causa. (GOV-PT, 2004)
Crises (Gestão de)	Conjunto de ações coordenadas tendentes a diminuir os fatores de tensão de uma crise, prevenir o seu agravamento para o nível de conflito armado e conter ações hostis caso ocorram. (CMDRCoE, 2014, p.12)
Crises (Sistema de Gestão de)	Sistema que permita, com elevada prontidão, fazer face a cenários, mais ou menos imprevisíveis, não raro difusos e de contornos pouco claros, que poderão afectar a comunidade nacional. (GOV-PT, 2004)

Defesa Coletiva	Princípio plasmado no art.5 do Tratado de Washginton (que criou a NATO), segundo o qual um ataque armado a um Estado-Membro é considerado um ataque a todos os aliados, significando que os restantes Estados-Membros se comprometem a tomar todas as ações necessárias, incluíndo a utilização da força armada, para restabelecer e manter a segurança na área do Atlântico Norte. (NATO, 2017a)
Estratégia	É a Ciência/Arte de, à luz dos fins de uma organização, estabelecer e hierarquizar objetivos e gerar, estruturar e utilizar recursos tangíveis e intangíveis, a fim de se atingirem objetivos, num ambiente admitido como conflitual ou competitivo. Gen. Abel Cabral Couto no prefácio do livro de Abreu (2002) "Fundamentos de Estratégia Militar e Empresarial"
Modelo de Maturidade	Enquadramento de referência que descreve, para uma determinada área de interesse, um conjunto de níveis de efetividade e de sofisticação, com que as atividades na área em causa podem ser executadas. (Guédria, Naudet e Chen, 2011, p.276)
Security Operations Center	In addition to response, SOC comprises other aspects from the cyber security chain, such as awareness, resilience, detection, alerting, reporting and crisis management. (GOV-PB, 2013a, p.10)
Segurança	É a condição da Nação que se traduz pela permanente garantia da sua sobrevivência em paz e Liberdade, assegurando a soberania, independência e unidade, a integridade do território, a salvaguarda coletiva de pessoas e bens e dos valores espirituais, o desenvolvimento normal das tarefas do Estado, a liberdade de ação política dos órgãos de soberania e o pleno funcionamento das instituições democráticas. (Cardoso, 1979)
Segurança Interna	Atividade desenvolvida pelo Estado para garantir a ordem, a segurança e a tranquilidade públicas, proteger pessoas e bens, prevenir e reprimir a criminalidade e contribuir para assegurar o normal funcionamento das instituições democráticas, o regular exercício dos direitos, liberdades e garantias fundamentais dos cidadãos e o respeito pela legalidade democrática. (AR, 2017)

Apêndice B — Propriedades do ciberespaço

Quadro 12 - Propriedades do ciberespaço

Dinâmico	Ambiente artificial, com exceção do espetro eletromagnético totalmente construído pela humanidade e em rápida expansão, quer ao nível dos sistemas que o integram, mas também das respetivas interligações, proporcionando-lhe uma natureza plástica em constante mutação.
Assimétrico	Custo irrelevante no acesso ao conjunto global de recursos, com eventual desenvolvimento de ações hostis de grande impacto. A assimetria revela-se tanto ao nível dos recursos como do conhecimento necessário em virtude da automação passível de ser operacionalizada.
Inimputabilidade	As ações no ciberespaço, sejam legítimas, ilícitas ou que constituam ameaças à Segurança Nacional, têm um enorme potencial de anonimato, o que dificulta a capacidade de dissuasão e de resposta, com impacto adicional no processo de decisão político face à incerteza sobre a origem da ação.
***Continnuns* disruptivos**	Considerado como um *global common*, com alcance global, o ciberespaço não tem fronteiras físicas nem espaços de soberania e jurisdição perfeitamente definidos, desafiando os tradicionais pressupostos de territorialidade (apenas a camada física do ciberespaço tem implantação nesta dimensão). Os *continuuns* civil/militar, privado/público e nacional/internacional adicionam níveis de dificuldade à capacidade do Estado para lidar com este ambiente.
Transversalidade	O ciberespaço integra sensores e atuadores que habilitam o acesso ao mundo físico, capitalizando a capacidade intrínseca de processamento e de armazenamento da informação, assim como de comunicação quase instantânea, com alcance global, para provocar efeitos no mundo físico.

Fonte: adaptado de Tikk (2011), IDN (2013, p.10) e Nunes (2016)

Apêndice C — Caracterização do referencial de análise da Organização Nacional para a Segurança no Ciberespaço

Como referido em 1.2, a estrutura de análise da ONSC, apresentada na figura 5, compreende duas dimensões, por um lado os mandatos organizacionais para providenciar o estado adequado de segurança no ciberespaço e, por outro, o ciclo de vida dos incidentes de segurança de informação no ciberespaço. Este referencial foi apresentado por Klimburg (2012) e, para efeitos deste estudo, foi parcialmente considerado. Neste apêndice descrevem-se os mandatos e as fases do ciclo de vida dos incidentes consideradas para este estudo.

1. Mandatos

No contexto geral da segurança nacional no ciberespaço constata-se a existência de cinco perspetivas diferentes, normalmente institucionalizados em diferentes setores governamentais, constituindo-se como os mandatos setoriais (Klimburg, 2012, pp.31–34) e três mandatos transversais adicionais (Klimburg, 2012, pp.119–120) que corporizam a ONSC. Tendo em consideração a delimitação deste estudo e as adaptações efetuadas para uma melhor operacionalização da análise, foram considerados três mandatos transversais e cinco setoriais, que se descrevem de seguida[44]:

- Coordenação Estratégica[45] (Coord.Est.): mandato transversal de coordenação ao nível político-estratégico;
- Coordenação Operacional[45] (Coord.Oper.): mandato transversal de coordenação ao nível operacional;
- Partilha de Informação (Part.Info.): mandato transversal para a partilha de informação com o foco nas fases de prevenção e resposta;
- Gestão de Crises no Ciberespaço[46] (GCC): mandato setorial para a coordenação nacional de crises no ciberespaço, que se deverá inserir, sempre que necessário, na estrutura nacional de gestão de crises;
- Proteção de Infraestruturas Críticas[46] (PIC): mandato setorial para a coordenação da postura de segurança das IC e da resposta a incidentes que as afetem;
- Operações Militares no Ciberespaço (OMC): mandato setorial para a execução de operações militares no ciberespaço;
- Informações e Contrainformações (IeCI): mandato setorial para a condução de ações de informações e contrainformações no ciberespaço;
- Combate ao Crime no Ciberespaço (CCC): mandato setorial para o combate ao cibercrime no ciberespaço.

2. Ciclo de vida dos incidentes de segurança no ciberespaço

O ciclo de vida dos incidentes de segurança no ciberespaço considerado neste estudo é composto pelas seguintes fases:

- Prevenção;
- Preparação;
- Resposta.

A definição sobre cada uma das fases está também adaptada à delimitação deste estudo, isto é, à relação civil/militar ao longo do espetro do conflito no ciberespaço, desde a situação normal até à situação de crise, descrevendo-se, de seguida, o entendimento adotado adaptado de Klimburg (2012, pp.113–114).

[44] Conforme nota (5) da figura 5 as siglas dos mandatos são compostas com o prefixo ONSC; nesta lista, por razões de legibilidade, o prefixo está suprimido.

[45] Originalmente só é considerado um mandato; no entanto, para efeitos dos objetivos da análise, foi separado em dois.

[46] Originalmente só é considerado um mandato; no entanto, para efeitos dos objetivos da análise, foi separado em dois.

A fase de prevenção considera dois níveis, um mais estratégico que endereça as questões relacionadas com a estruturação da ONSC e outro, situado a um nível operacional, relacionado com o desenvolvimento de ações tendentes a evitar que ameaças/perigos se transformem em incidentes ou a reduzir o efeito de possíveis incidentes.

A fase de preparação é definida como um ciclo contínuo de planeamento, treino, exercitação e avaliação, considerando a tomada de ação corretiva, incluindo ao nível organizacional, dos instrumentos e equipamentos utilizados, num esforço contínuo para assegurar a efetiva coordenação durante a resposta a um incidente de segurança no ciberespaço.

A fase de resposta endereça os efeitos imediatos e de curto-prazo, e procura prevenir danos adicionais após a ocorrência de um incidente de segurança no ciberespaço.

Apêndice D — Modelo de maturidade de Comando e Controlo para a interoperabilidade organizacional

O M2C2IO, apresentado em 1.1.6., é descrito em detalhe neste apêndice com a descrição das dimensões em cada nível do modelo de maturidade:

Quadro 13 - M2C2IO - Caracterização do nível 1 do modelo de maturidade (atuação independente)

Nível 1 - Atuação independente	
Preparação	Neste nível não existe doutrina que oriente o emprego unificado das entidades, nem experiência ou treino entre elas.
Compreensão	Neste nível deverá existir alguma forma de comunicação entre as organizações de forma a partilhar informação. Provavelmente acontece na forma de chamadas de voz, fax, ou reuniões presenciais.
Governação	A delegação de direitos de decisão da organização de origem é marginal e os papéis e responsabilidades interorganizacionais têm uma aceitação residual.
Etos	Não existe uma cultura ou sistema de valores partilhados.

Fonte: adaptado de Clark e Jones (1999) e enriquecido a partir de Williams (2010)

Quadro 14 - M2C2IO - Caracterização do nível 2 do modelo de maturidade (atuação ad-hoc)

Nível 2 - Atuação Ad Hoc	
Preparação	Existem orientações gerais para interoperar com outras organizações. Há pouca ou nenhuma experiência ou treino. Não existe doutrina específica.
Compreensão	O nível de compreensão inclui a partilha de alguma informação e conhecimento. Infraestruturas de comunicação estão disponíveis e são utilizadas.
Governação	Existe alguma flexibilidade na abordagem à interoperabilidade com as outras organizações, através da delegação de alguns direitos de decisão da organização de origem e existe uma aceitação limitada dos papéis e responsabilidades interorganizacionais.
Etos	Existem objetivos e propósitos partilhados para a interoperabilidade, bem como a partilha de valores, mas o etos da organização de origem predomina.

Fonte: adaptado de Clark e Jones (1999) e enriquecido a partir de Williams (2010)

Quadro 15 - M2C2IO - Caracterização do nível 3 do modelo de maturidade (atuação colaborativa)

Nível 3 - Atuação colaborativa	
Preparação	Existem orientações gerais e alguma doutrina para interoperar com outras organizações. Existem mecanismos para treino conjunto que são explorados para providenciar experiência e treino na exploração da doutrina existente.
Compreensão	As infraestruturas de comunicações são partilhadas. É partilhado o conhecimento e contexto situacional.
Governação	Existe flexibilidade na abordagem à interoperabilidade com as outras organizações, através da acentuada delegação de direitos de decisão da organização de origem e existe uma aceitação pronunciada dos papéis e responsabilidades interorganizacionais.
Etos	Objetivos e propósitos partilhados e utilizados, mas alguns aspetos do Etos da organização de origem ainda se fazem sentir.

Fonte: adaptado de Clark e Jones (1999) e enriquecido a partir de Williams (2010)

Quadro 16 - M2C2IO - Caracterização do nível 4 do modelo de maturidade (atuação combinada)

Nível 4 - Atuação combinada	
Preparação	Nível de integração organizacional em que o fator distintivo da preparação é na experiência e treino na execução de atividades de acordo com a doutrina detalhada existente.
Compreensão	A organização tem boas comunicações e bases fortes no conhecimento partilhado.
Governação	Os papéis e responsabilidades interorganizacionais são respeitados e estão bem cimentados, sendo ainda conjugados com uma forte delegação de direitos de decisão, incluindo sobre o empenhamento de recursos da organização de origem.
Etos	Objetivos e propósitos partilhados e utilizados.

Fonte: adaptado de Clark e Jones (1999) e enriquecido a partir de Williams (2010)

Quadro 17 - M2C2IO - Caracterização do nível 5 do modelo de maturidade (atuação unificada)

Nível 5 - Atuação unificada	
Preparação	Não há distinção na preparação das atividades intraorganizacionais e interorganizacionais
Compreensão	A comunicação e o conhecimento partilhado verifica-se universalmente de forma transversal em todo o ambiente interorganizacional.
Governação	Os papéis e responsabilidades interorganizacionais são totalmente aceites e a delegação de direitos de decisão é universal.
Etos	Objetivos e propósitos interorganizacionais partilhados e utilizados, existindo ainda um alinhamento completo da cultura e sistema de valores.

Fonte: adaptado de Clark e Jones (1999) e enriquecido a partir de Williams (2010)

Apêndice E — Questionário de interoperabilidade organizacional nos exercícios CMX2017 e CC2017 - Descrição, parametrização e apresentação detalhada de resultados

O CMX2017 é um exercício anual da NATO, de nível político estratégico, com a finalidade "(…) de praticar, testar e validar a gestão, as medidas e os mecanismos relacionados com o processo de consulta e tomada de decisão coletiva na resposta a crises." (GOV-PT, 2017b, p.19562–(2)). A CRN foi constituída especificamente para o exercício por despacho do Primeiro-Ministro, tendo a coordenação sido atribuída ao Ministério da Defesa Nacional (MDN) (GOV-PT, 2017b).

O CC2017 é um exercício anual da NATO planeado e executado pelo *Allied Command Transformation* (ACT), tem como âmbito a ciberdefesa e a finalidade de exercitar os processos de tomada de decisão, os procedimentos ao nível operacional e tático/técnico, assim com a colaboração entre os participantes (ACT, 2017). Portugal participa desde 2011 através de uma célula de resposta organizada em torno do CCD, que coordena a resposta nacional, reforçado com equipas dos Ramos das FFAA, incluindo a vertente legal, e o CNCS (Jesus, 2018).

A população alvo de cada um dos questionários foi constituída pelos elementos que constituíram a CRN de cada um dos exercícios. Os contactos para a participação destes elementos não abrangeram toda a população. Relativamente ao CMX2017, dos dezoito elementos da CRN catorze foram contactados para responder (treze representantes de organismos não-militares) e, destes, nove responderam ao questionário. Relativamente ao CC2017, dos vinte e sete elementos participantes treze[47] foram contactados para responder (doze elementos pertencentes a organismos militares) e, destes, onze responderam ao questionário.

O questionário, que não recolheu qualquer informação de contexto[48], continha vinte perguntas/afirmações, dezassete das quais solicitavam uma resposta numa escala de condordância, com 6 níveis, de discordo totalmente a concordo totalmente, e três perguntas apresentavam opções de resposta para selecionar uma (quadro 18). A correspondência entre os cinco níveis do M2C2IO e as respostas é apresentada no quadro 19. O questionário esteve disponível para resposta na semana de 16 a 20 de abril na plataforma do IUM.

[47] A listagem dos elementos elegíveis para contacto resultou de um entendimento com a entidade que coordenou o exercício em Portugal (CCD), considerando que não seria adequado a submissão deste tipo de questionário a elementos que faziam parte da mesma equipa, procurando-se, por outro lado, garantir a elegibilidade de elementos da parte técnica, legal e de relações públicas

[48] Considerando que a população alvo do CMX2017 abrangia um conjunto elevado de entidades, de forma a aumentar a probabilidade de ocorrência de resposta, foi decidido, em articulação com a entidade que coordenou o exercício em Portugal, a Direção-Geral de Políticas de Defesa Nacional, não recolher qualquer informação que permitisse caracterizar o respondente.

Quadro 18 - M2C2IO - Distribuição das perguntas pelas dimensões e variáveis do modelo

M2C2IO			Questionário	
Dimensões	**Variáveis**	**Abreviatura**	**N.º Perguntas com Escala Concordância**	**N.º Perguntas com Opções**
Preparação	Doutrina	M2C2IO-D	1	0
Preparação	Experiência	M2C2IO-E	1	0
Preparação	Treino	M2C2IO-T	0	2
Compreensão	Comunicação	M2C2IO-C	0	1
Compreensão	partilha de Informação	M2C2IO-I	4	0
Compreensão	partilha de coNhecimento	M2C2IO-N	2	0
Governação	distribuição direitos deciSão	M2C2IO-S	3	0
Governação	Papéis e responsabilidades	M2C2IO-P	1	0
Etos	cUltura e sistema de valores	M2C2IO-U	1	0
Etos	propósito e Aspirações	M2C2IO-A	2	0
Etos	conFiança	M2C2IO-F	2	0
Total por tipo de pergunta			*17*	*3*
Total de perguntas			20	

Quadro 19 - M2C2IO - Correspondência dos níveis do modelo à escala de concordância e opções de resposta

M2C2IO Nível	Resposta Escala Concordância	Resposta 6 opções	Resposta 5 opções
5-Unificado	6	6	5
4-Combinado	5	5	4
3-Colaborativo	4	4	3
2-Ad-hoc	3 e 2	3 e 2	2
1-Independente	1	1	1

Apresentam-se os resultados do questionário após tratamento, inicialmente por médias e, posteriormente, por contagem de ocorrências (frequência) nos níveis do M2C2IO.

Assim, nos quadros 20 (CMX2017) e 21 (CC2017) apresentam-se os resultados do questionário, após tratamento por médias, com os resultados parciais por dimensões e variáveis, e o resultado global do modelo.

Quadro 20 - M2C2IO - CMX2017 - Resultado global do questionário após tratamento por médias

CMX2017 - M2C2IO										
Preparação			Compreensão			Governação		Etos		
D	E	T	C	I	N	S	P	U	A	F
3,24										
3,06			3,07			3,13		3,06		
3,33	4,00	1,83	1,67	3,67	3,89	3,04	3,22	3,07	3,13	3,69

Quadro 21 - M2C2IO - CC2017 - Resultado global do questionário após tratamento por médias

CC2017 - M2C2IO										
Preparação			Compreensão			Governação		Etos		
D	E	T	C	I	N	S	P	U	A	F
3,83										
3,32			3,79			3,65		4,55		
3,64	4,36	1,95	3,64	3,82	3,91	3,58	3,73	4,27	4,77	4,59

Para se ter uma melhor noção da distribuição das respostas na escala de níveis do M2C2IO, foi efetuada uma manipulação dos dados no sentido de contar ocorrências em cada nível e normalizar tendo em conta a circunstância das variáveis terem um número diferente de perguntas e, adicionalmente, as dimensões terem um número diferente de variáveis (ver quadro 18). Os resultados são apresentados nos quadros 22 e 23 para o CMX2017, e nos quadros 24 e 25 para o CC2017:

Quadro 22 - M2C2IO - CMX2017 - Resultado com a contagem normalizada de ocorrências (ao número de perguntas), por dimensões e variáveis, para cada nível do modelo

NÍVEL	Preparação			Compreensão			Governação		Etos		
	D	E	T	C	I	N	S	P	U	A	F
5-Unificado	8,50			7,50			1,67		10,50		
	3,00	5,00	0,50	0,00	4,00	3,50	1,67	0,00	2,00	4,00	4,50
4-Combinado	3,00			4,25			6,67		8,00		
	2,00	1,00	0,00	0,00	1,25	3,00	2,67	4,00	3,00	2,50	2,50
3-Colaborativo	2,00			2,50			3,67		1,50		
	0,00	2,00	0,00	0,00	1,50	1,00	0,67	3,00	1,00	0,50	0,00
2-Ad-hoc	8,50			8,25			4,33		3,50		
	3,00	0,00	5,50	6,00	1,25	1,00	2,33	2,00	1,00	1,50	1,00
1-Independente	5,00			4,50			1,67		3,50		
	1,00	1,00	3,00	3,00	1,00	0,50	1,67	0,00	2,00	0,50	1,00

Quadro 23 - M2C2IO - CMX2017 - Resultado com a contagem normalizada de ocorrências (ao número de variáveis), por dimensões, para cada nível do modelo

NÍVEL	Preparação	Compreensão	Governação	Etos
5-Unificado	2,83	2,50	0,83	3,50
4-Combinado	1,00	1,42	3,33	2,67
3-Colaborativo	0,67	0,83	1,83	0,50
2-Ad-hoc	2,83	2,75	2,17	1,17
1-Independente	1,67	1,50	0,83	1,17

Quadro 24 - M2C2IO - CC2017 - Resultado com a contagem normalizada de ocorrências (ao número de perguntas), por dimensões e variáveis, para cada nível do modelo

NÍVEL	Preparação			Compreensão			Governação		Etos		
	D	E	T	C	I	N	S	P	U	A	F
5-Unificado	8,50			14,75			1,33		19,00		
	3,00	5,00	0,50	6,00	3,75	5,00	1,33	0,00	4,00	8,50	6,50
4-Combinado	9,00			7,75			14,33		13,00		
	4,00	5,00	0,00	0,00	4,75	3,00	6,33	8,00	6,00	2,50	4,50
3-Colaborativo	4,50			1,50			4,67		1,00		
	2,00	1,00	1,50	0,00	0,50	1,00	1,67	3,00	1,00	0,00	0,00
2-Ad-hoc	6,50			6,75			0,67		0,00		
	1,00	0,00	5,50	5,00	0,75	1,00	0,67	0,00	0,00	0,00	0,00
1-Independente	4,50			2,25			1,00		0,00		
	1,00	0,00	3,50	0,00	1,25	1,00	1,00	0,00	0,00	0,00	0,00

Quadro 25 - M2C2IO - CC2017 - Resultado com a contagem normalizada de ocorrências (ao número de variáveis), por dimensões, para cada nível do modelo

NÍVEL	Preparação	Compreensão	Governação	Etos
5-Unificado	2,83	4,92	0,67	6,33
4-Combinado	3,00	2,58	7,17	4,33
3-Colaborativo	1,50	0,50	2,33	0,33
2-Ad-hoc	2,17	2,25	0,33	0,00
1-Independente	1,50	0,75	0,50	0,00

De seguida apresenta-se a tipologia utilizada para detetar enviesamento das respostas com escala de concordância, quando comparadas com as respostas com opções objetivas[49], e cuja parametrização consistiu em classificar as perguntas em relativas à própria pessoa/entidade (Tipo A), relativas ao grupo (Tipo B) e com opções de resposta objetiva (Tipo C), sendo que os dois primeiros se enquadram nas respostas com escala de concordância:

Quadro 26 - M2C2IO - Parametrização das perguntas por tipo de resposta

Tipo pergunta	Referência da pergunta[50]
Tipo A	A1.1, A1.2, A1.3, A1.4, A1.5, A1.7, A1.9, A1.10, A1.11, A1.12, A1.15, A1.16 e A1.17
Tipo B	A1.6, A1.8, A1.13 e A1.14
Tipo C	A2, A3 e A4

[49] Resultados e discussão apresentados em 3.2.3.

[50] Referência de acordo com a identificação das perguntas utilizada no questionário, tal como foi apresentado aos respondentes e que se encontra exposto no apêndice F. As perguntas cuja resposta é em escala de concordância (tipo A e B) estão seriadas de acordo com a ordem com que aparecem no questionário (ex.: A1.#).

Apresenta-se de seguida, nos quadros 27 (CMX2017) e 28 (CC2017), os dados das respostas sem tratamento:

Quadro 27 - M2C2IO - CMX2017 - Respostas sem tratamento

N.º Pergunta	Nove respostas								
A1.1	5	1	5	4	2	5	4	2	2
A1.2	5	1	5	4	5	5	5	3	3
A2	2	1	2	2	2	2	1	1	2
A3	1	2	2	2	2	5	2	1	1
A4	1	1	2	2	2	2	2	2	1
A1.3	5	2	5	3	4	3	3	4	1
A1.4	5	2	5	4	5	5	5	2	3
A1.5	1	1	4	3	3	5	5	5	2
A1.6	5	2	5	5	1	5	5	5	4
A1.7	5	4	5	4	5	4	3	5	5
A1.8	5	1	2	4	3	4	4	5	2
A1.9	5	1	4	4	2	4	4	2	2
A1.10	5	1	5	5	2	4	4	4	1
A1.11	5	1	4	2	2	3	3	2	1
A1.12	3	2	4	4	2	3	3	4	4
A1.13	1	1	2	4	3	4	4	5	5
A1.14	5	2	3	4	5	4	4	5	2
A1.15	4	1	5	5	5	5	4	5	2
A1.16	5	2	4	4	1	5	2	5	5
A1.17	4	1	5	5	4	5	5	5	4

Quadro 28 - M2C2IO - CC2017 - Respostas sem tratamento

N.º Pergunta	Onze respostas										
A1.1	5	5	3	2	1	4	4	5	4	3	4
A1.2	5	4	5	4	4	5	4	4	5	3	5
A2	1	2	1	2	2	1	2	2	3	3	2
A3	1	2	1	1	2	2	2	2	5	3	1
A4	2	2	5	5	5	5	5	2	5	2	2
A1.3	1	4	4	4	2	1	4	5	4	3	4
A1.4	5	4	5	4	4	1	4	4	5	4	3
A1.5	5	5	5	4	2	1	4	5	4	4	2
A1.6	5	5	4	5	1	4	5	5	5	5	4
A1.7	1	5	3	4	1	5	5	5	5	2	2
A1.8	5	4	5	4	5	5	4	4	5	4	3
A1.9	3	3	4	2	3	4	4	5	4	3	4
A1.10	5	4	4	3	5	4	4	5	4	4	4
A1.11	1	4	4	2	1	1	4	4	4	4	4
A1.12	4	4	4	3	4	3	4	3	4	4	4
A1.13	5	4	4	4	4	5	5	3	4	4	5
A1.14	5	5	5	4	5	5	5	4	5	4	4
A1.15	5	5	5	5	5	5	5	5	5	5	4
A1.16	5	5	4	4	4	4	4	5	4	4	4
A1.17	5	5	5	4	5	5	5	5	5	5	5

Apêndice F — Questionário de análise da interoperabilidade organizacional aplicado aos representantes das entidades participantes nos exercícios CMX2017 e CC2017

Antes de mais, muito obrigado pela disponibilidade e colaboração!

Antes de começar a responder recorde a sua participação no CMX2017 durante 2 ou 3 minutos.

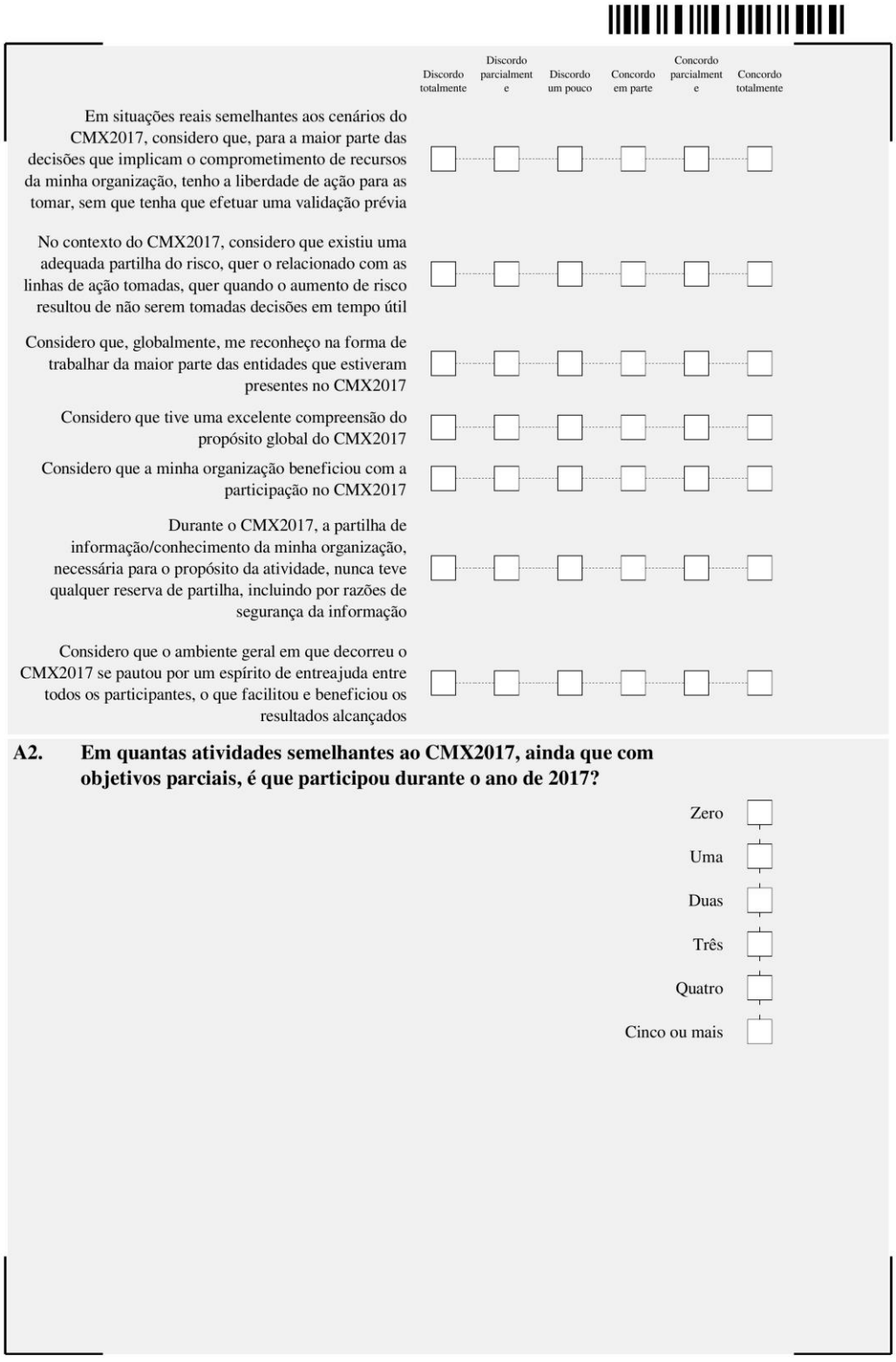
Depois, inicie a resposta ao questionário.

Secção A: Questões CMX2017

A1. Questões com escala de concordância

	Discordo totalmente	Discordo parcialmente	Discordo um pouco	Concordo em parte	Concordo parcialmente	Concordo totalmente
Para situações semelhantes à simulada no CMX2017, a minha organização tem políticas e/ou planos que orientam a articulação operacional de recursos com as outras entidades participantes	☐	☐	☐	☐	☐	☐
No contexto do CMX2017, considero a minha experiência (conhecimento e prática) totalmente adequada para o papel que desempenhei	☐	☐	☐	☐	☐	☐
A minha organização tem uma política para partilha de informação que foi previamente consensualizada com as restantes entidades envolvidas no CMX2017	☐	☐	☐	☐	☐	☐
Considero que estava preparado(a) para providenciar toda a informação que foi necessário partilhar durante o CMX2017	☐	☐	☐	☐	☐	☐
Durante o CMX2017 nunca foi necessário explicar porque é que uma determinada informação necessitava de ser partilhada	☐	☐	☐	☐	☐	☐
Durante o CMX2017 toda a informação que foi requerida à minha organização foi partilhada em tempo útil	☐	☐	☐	☐	☐	☐
Durante o CMX2017 ocorreram situações em que a compreensão sobre a situação foi construída a partir de informação que estava inicialmente na posse de entidades diferentes	☐	☐	☐	☐	☐	☐
Durante o CMX2017 não tive qualquer dificuldade de entendimento relativamente a expressões, siglas, ou outros termos utilizados, até ao nível do respetivo significado	☐	☐	☐	☐	☐	☐
Em situações reais semelhantes aos cenários do CMX2017, considero que existem políticas que enquadram o meu nível de decisão, de forma articulada, com a minha organização	☐	☐	☐	☐	☐	☐
Considero que a minha organização me providenciou os direitos de decisão adequados para situações reais semelhantes aos cenários do CMX2017	☐	☐	☐	☐	☐	☐

Figura 21 - M2C2IO - Questionário CMX2017 - Página 1 de 3

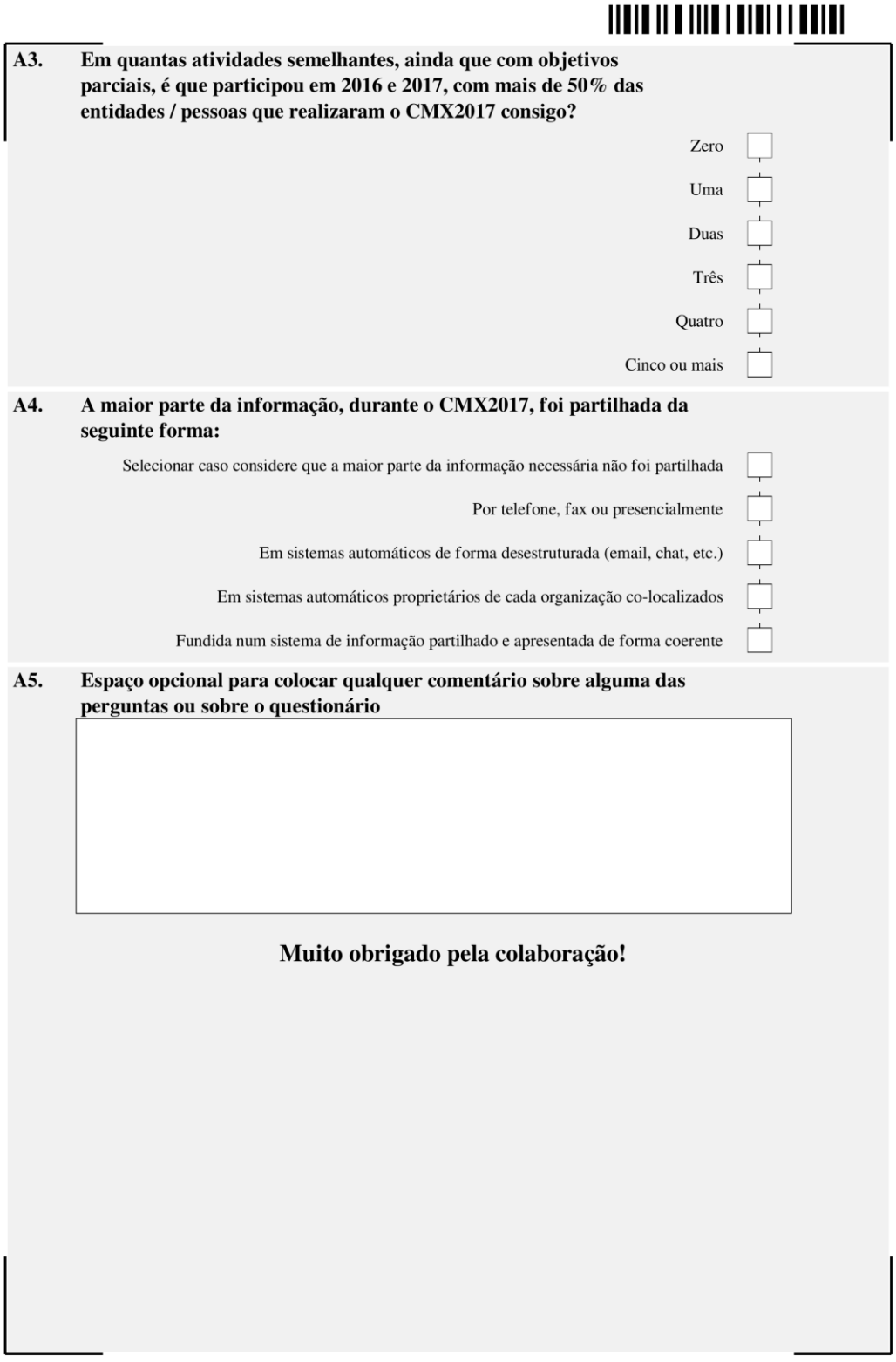


	Discordo totalmente	Discordo parcialmente	Discordo um pouco	Concordo em parte	Concordo parcialmente	Concordo totalmente
Em situações reais semelhantes aos cenários do CMX2017, considero que, para a maior parte das decisões que implicam o comprometimento de recursos da minha organização, tenho a liberdade de ação para as tomar, sem que tenha que efetuar uma validação prévia	☐	☐	☐	☐	☐	☐
No contexto do CMX2017, considero que existiu uma adequada partilha do risco, quer o relacionado com as linhas de ação tomadas, quer quando o aumento de risco resultou de não serem tomadas decisões em tempo útil	☐	☐	☐	☐	☐	☐
Considero que, globalmente, me reconheço na forma de trabalhar da maior parte das entidades que estiveram presentes no CMX2017	☐	☐	☐	☐	☐	☐
Considero que tive uma excelente compreensão do propósito global do CMX2017	☐	☐	☐	☐	☐	☐
Considero que a minha organização beneficiou com a participação no CMX2017	☐	☐	☐	☐	☐	☐
Durante o CMX2017, a partilha de informação/conhecimento da minha organização, necessária para o propósito da atividade, nunca teve qualquer reserva de partilha, incluindo por razões de segurança da informação	☐	☐	☐	☐	☐	☐
Considero que o ambiente geral em que decorreu o CMX2017 se pautou por um espírito de entreajuda entre todos os participantes, o que facilitou e beneficiou os resultados alcançados	☐	☐	☐	☐	☐	☐

A2. Em quantas atividades semelhantes ao CMX2017, ainda que com objetivos parciais, é que participou durante o ano de 2017?

- ☐ Zero
- ☐ Uma
- ☐ Duas
- ☐ Três
- ☐ Quatro
- ☐ Cinco ou mais

Figura 22 - M2C2IO - Questionário CMX2017 - Página 2 de 3



A3. **Em quantas atividades semelhantes, ainda que com objetivos parciais, é que participou em 2016 e 2017, com mais de 50% das entidades / pessoas que realizaram o CMX2017 consigo?**

- ☐ Zero
- ☐ Uma
- ☐ Duas
- ☐ Três
- ☐ Quatro
- ☐ Cinco ou mais

A4. **A maior parte da informação, durante o CMX2017, foi partilhada da seguinte forma:**

- ☐ Selecionar caso considere que a maior parte da informação necessária não foi partilhada
- ☐ Por telefone, fax ou presencialmente
- ☐ Em sistemas automáticos de forma desestruturada (email, chat, etc.)
- ☐ Em sistemas automáticos proprietários de cada organização co-localizados
- ☐ Fundida num sistema de informação partilhado e apresentada de forma coerente

A5. **Espaço opcional para colocar qualquer comentário sobre alguma das perguntas ou sobre o questionário**

Muito obrigado pela colaboração!

Figura 23 - M2C2IO - Questionário CMX2017 - Página 3 de 3

Antes de mais, muito obrigado pela disponibilidade e colaboração!

Antes de começar a responder recorde a sua participação no CC2017 durante 2 ou 3 minutos.

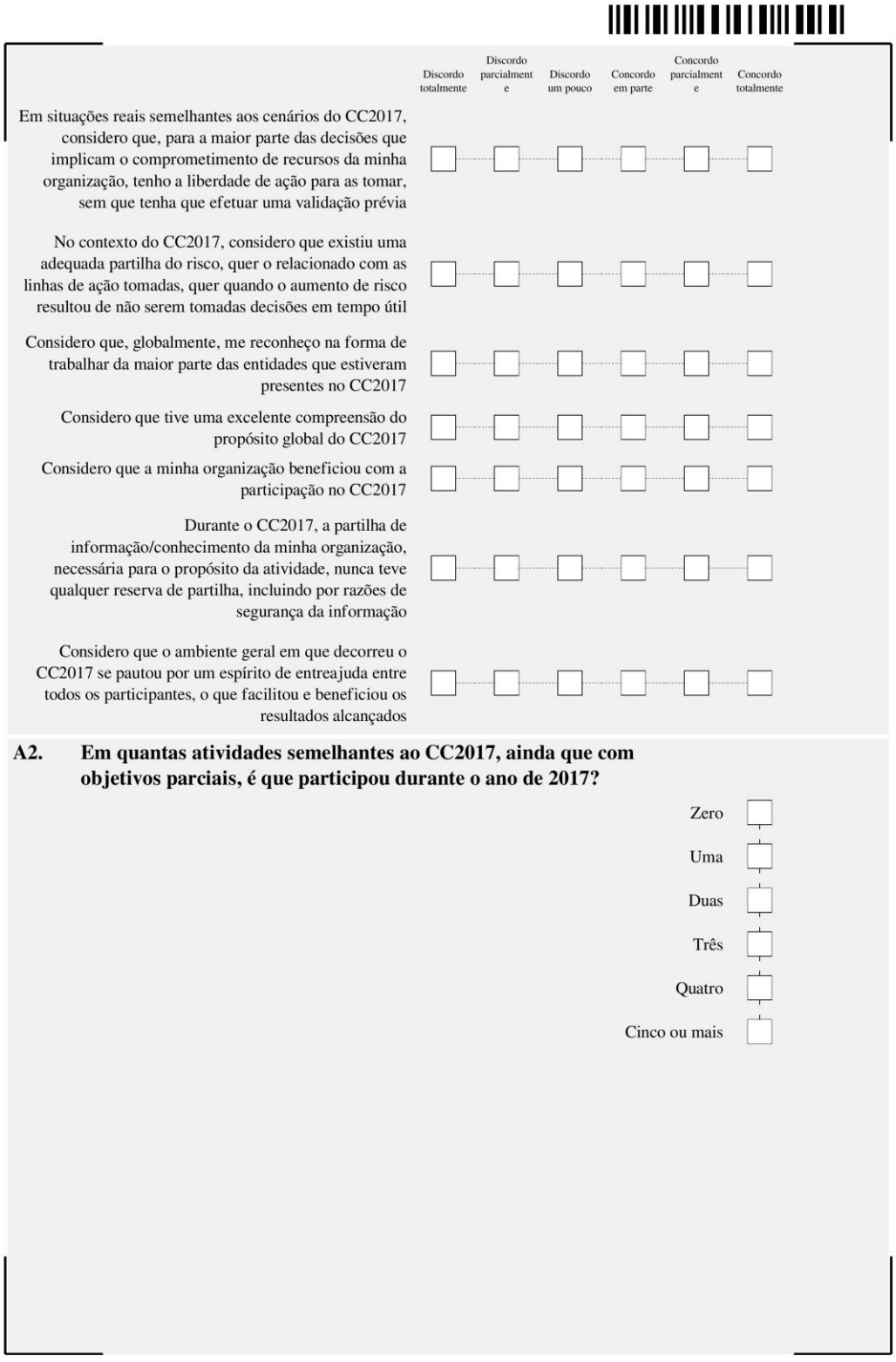
Depois, inicie a resposta ao questionário.

Secção A: Questões CC2017

A1. Questões com escala de concordância

	Discordo totalmente	Discordo parcialmente	Discordo um pouco	Concordo em parte	Concordo parcialmente	Concordo totalmente
Para situações semelhantes à simulada no CC2017, a minha organização tem políticas e/ou planos que orientam a articulação operacional de recursos com as outras entidades participantes	☐	☐	☐	☐	☐	☐
No contexto do CC2017, considero a minha experiência (conhecimento e prática) totalmente adequada para o papel que desempenhei	☐	☐	☐	☐	☐	☐
A minha organização tem uma política para partilha de informação que foi previamente consensualizada com as restantes entidades envolvidas no CC2017	☐	☐	☐	☐	☐	☐
Considero que estava preparado(a) para providenciar toda a informação que foi necessário partilhar durante o CC2017	☐	☐	☐	☐	☐	☐
Durante o CC2017 nunca foi necessário explicar porque é que uma determinada informação necessitava de ser partilhada	☐	☐	☐	☐	☐	☐
Durante o CC2017 toda a informação que foi requerida à minha organização foi partilhada em tempo útil	☐	☐	☐	☐	☐	☐
Durante o CC2017 ocorreram situações em que a compreensão sobre a situação foi construída a partir de informação que estava inicialmente na posse de entidades diferentes	☐	☐	☐	☐	☐	☐
Durante o CC2017 não tive qualquer dificuldade de entendimento relativamente a expressões, siglas, ou outros termos utilizados, até ao nível do respetivo significado	☐	☐	☐	☐	☐	☐
Em situações reais semelhantes aos cenários do CC2017, considero que existem políticas que enquadram o meu nível de decisão, de forma articulada, com a minha organização	☐	☐	☐	☐	☐	☐
Considero que a minha organização me providenciou os direitos de decisão adequados para situações reais semelhantes aos cenários do CC2017	☐	☐	☐	☐	☐	☐

Figura 24 - M2C2IO - Questionário CC2017 - Página 1 de 3

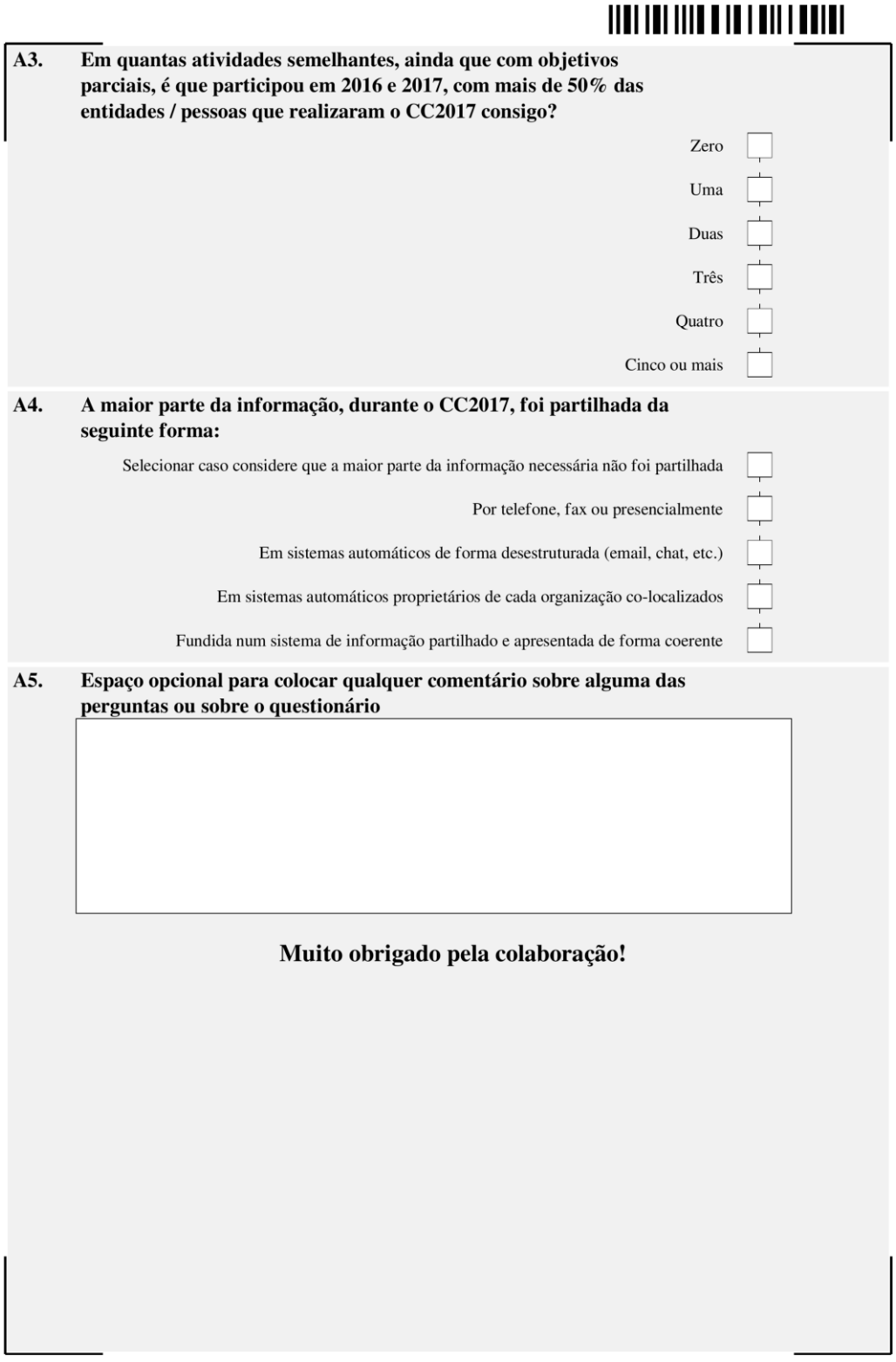


	Discordo totalmente	Discordo parcialmente	Discordo um pouco	Concordo em parte	Concordo parcialmente	Concordo totalmente
Em situações reais semelhantes aos cenários do CC2017, considero que, para a maior parte das decisões que implicam o comprometimento de recursos da minha organização, tenho a liberdade de ação para as tomar, sem que tenha que efetuar uma validação prévia	☐	☐	☐	☐	☐	☐
No contexto do CC2017, considero que existiu uma adequada partilha do risco, quer o relacionado com as linhas de ação tomadas, quer quando o aumento de risco resultou de não serem tomadas decisões em tempo útil	☐	☐	☐	☐	☐	☐
Considero que, globalmente, me reconheço na forma de trabalhar da maior parte das entidades que estiveram presentes no CC2017	☐	☐	☐	☐	☐	☐
Considero que tive uma excelente compreensão do propósito global do CC2017	☐	☐	☐	☐	☐	☐
Considero que a minha organização beneficiou com a participação no CC2017	☐	☐	☐	☐	☐	☐
Durante o CC2017, a partilha de informação/conhecimento da minha organização, necessária para o propósito da atividade, nunca teve qualquer reserva de partilha, incluindo por razões de segurança da informação	☐	☐	☐	☐	☐	☐
Considero que o ambiente geral em que decorreu o CC2017 se pautou por um espírito de entreajuda entre todos os participantes, o que facilitou e beneficiou os resultados alcançados	☐	☐	☐	☐	☐	☐

A2. Em quantas atividades semelhantes ao CC2017, ainda que com objetivos parciais, é que participou durante o ano de 2017?

- ☐ Zero
- ☐ Uma
- ☐ Duas
- ☐ Três
- ☐ Quatro
- ☐ Cinco ou mais

Figura 25 - M2C2IO - Questionário CC2017 - Página 2 de 2



A3. **Em quantas atividades semelhantes, ainda que com objetivos parciais, é que participou em 2016 e 2017, com mais de 50% das entidades / pessoas que realizaram o CC2017 consigo?**

- ☐ Zero
- ☐ Uma
- ☐ Duas
- ☐ Três
- ☐ Quatro
- ☐ Cinco ou mais

A4. **A maior parte da informação, durante o CC2017, foi partilhada da seguinte forma:**

- ☐ Selecionar caso considere que a maior parte da informação necessária não foi partilhada
- ☐ Por telefone, fax ou presencialmente
- ☐ Em sistemas automáticos de forma desestruturada (email, chat, etc.)
- ☐ Em sistemas automáticos proprietários de cada organização co-localizados
- ☐ Fundida num sistema de informação partilhado e apresentada de forma coerente

A5. **Espaço opcional para colocar qualquer comentário sobre alguma das perguntas ou sobre o questionário**

Muito obrigado pela colaboração!

Figura 26 - M2C2IO - Questionário CC2017 - Página 3 de 3