INSTITUTO UNIVERSITÁRIO MILITAR

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

CURSO DE ESTADO-MAIOR CONJUNTO

2020/2021

TII

A PREVENÇÃO E O COMBATE DE AMEAÇAS HÍBRIDAS: IDENTIFICAR INSTRUMENTOS DE MEDIDA: VARIÁVEIS E INDICADORES DE RESILIÊNCIA NACIONAIS FACE ÀS AMEAÇAS HÍBRIDAS (INFORMACIONAL)

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

Luís Filipe Xavier C. de Mendonça Dias

MAJOR, TRANSMISSÕES

INSTITUTO UNIVERSITÁRIO MILITAR
DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

A PREVENÇÃO E O COMBATE DE AMEAÇAS HÍBRIDAS: IDENTIFICAR INSTRUMENTOS DE MEDIDA: VARIÁVEIS E INDICADORES DE RESILIÊNCIA NACIONAIS FACE ÀS AMEAÇAS HÍBRIDAS (INFORMACIONAL)

MAJOR, TRANSMISSÕES Luís Filipe Xavier C. de Mendonça Dias

Trabalho de Investigação Individual do CEMC 2020/2021

Pedrouços 2021

INSTITUTO UNIVERSITÁRIO MILITAR
DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

A PREVENÇÃO E O COMBATE DE AMEAÇAS HÍBRIDAS: IDENTIFICAR INSTRUMENTOS DE MEDIDA: VARIÁVEIS E INDICADORES DE RESILIÊNCIA NACIONAIS FACE ÀS AMEAÇAS HÍBRIDAS (INFORMACIONAL)

MAJOR, TRANSMISSÕES Luís Filipe Xavier C. de Mendonça Dias

Trabalho de Investigação Individual do CEMC 2020/2021

Orientador: MAJOR, TRANSMISSÕES
Tiago Filipe Abreu Moura Guedes

Pedrouços 2021

Declaração de compromisso Antiplágio

Eu, **Luís Filipe Xavier Cavaco de Mendonça Dias,** declaro por minha honra que o documento intitulado **"A PREVENÇÃO E O COMBATE DE AMEAÇAS HÍBRIDAS: IDENTIFICAR INSTRUMENTOS DE MEDIDA: VARIÁVEIS E INDICADORES DE RESILIÊNCIA NACIONAIS FACE ÀS AMEAÇAS HÍBRIDAS (INFORMACIONAL)"** corresponde ao resultado da investigação por mim desenvolvida enquanto auditor do **Curso de Estado-Maior Conjunto 2020/2021** 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, **12** de **maio** de **2021**

Luís Filipe Xavier Cavaco de Mendonça Dias

Assinado por : **Luís Filipe Xavier Cavaco de Mendonça Dias**
Num. de Identificação: BI12395475
Data: 2021.06.20 22:33:59+01'00'

CHAVE MÓVEL

Agradecimentos

Em primeiro lugar, um agradecimento ao Major Tiago Guedes, o meu orientador, pela amizade e apoio incondicional. A forma profissional, rigorosa e a permanente disponibilidade com que encarou a orientação deste trabalho, começando no projeto de investigação, permitiram a condução do trabalho num caminho constante e sem desvios.

Ao Major Diogo Serrão, pela camaradagem e amizade, bem como o incentivo que me deu e conduziu à escolha deste tema. A partilha de conhecimento e de contactos da rede interministerial de resposta a ameaças híbridas, a promoção de reuniões com o Dr. Jorge Aranda, a quem também agradeço pela disponibilidade e partilha de informação, a promoção e divulgação de seminários no âmbito do tema em estudo, foram algumas ações que particularmente agradeço e que em muito contribuíram para o sucesso deste trabalho.

Um agradecimento especial ao Coronel Tirocinado Paulo Viegas Nunes, pela camaradagem, disponibilidade e prestimosos contributos no desenvolvimento do modelo de análise e do guião de entrevistas.

O meu especial agradecimento, pela disponibilidade, experiência e conhecimentos que partilharam, a todos os entrevistados, militares e civis: Contra-Almirante Gameiro Marques, Major-General Nuno Lemos Pires, Coronel Óscar Rocha, Coronel Tirocinado Paulo Viegas Nunes, Professor Doutor Miguel Pupo Correia, e Engenheiro Rafael Aranha. As respostas às entrevistas permitiram diferentes perspetivas e assumiram um papel academicamente relevante, para a credibilidade dos argumentos que sustentam este trabalho.

Gostaria de manifestar os meus agradecimentos ao Diretor de Curso, o Capitão-de-Mar-e-Guerra Luís Daniel Carona Jimenez, pela constante preocupação e disponibilidade, orientando-nos no decorrer do curso.

Um agradecimento muito especial ao Tenente-Coronel José Carlos Lourenço Martins, pela amizade e disponibilidade para a análise crítica e profunda que fez na revisão do trabalho, permitindo em muito melhorar o produto final.

Aos auditores do Curso de Estado-Maior Conjunto 2020/2021, pela amizade e ambiente de saudável convívio. O debate de ideias, a partilha de experiências, de perspetivas diversas e de conhecimento, em muito facilitaram a conclusão do presente trabalho de investigação.

À minha família, pela compreensão, paciência e apoio incondicional, como sempre!

Índice

Índice de Apêndices

Índice de Figuras

Índice de Quadros

Índice de Tabelas

Resumo

As ameaças híbridas, impulsionadas no ciberespaço, visam deliberadamente as vulnerabilidades dos Estados democráticos e das instituições, mantendo-se abaixo do limiar de deteção e imputação. Por um lado, temos o problema da dependência tecnológica que aumenta o risco dos ciberataques, por outro, a internet alavancou a comunicação em massa e permite a qualquer indivíduo ser uma fonte de notícias, potenciando a propaganda e a desinformação fácil.

O presente trabalho, estuda a resiliência nacional face a ameaças híbridas no ambiente informacional, propondo critérios e indicadores de ciber-resiliência e de resiliência face à desinformação.

Seguindo um raciocínio dedutivo e uma estratégia qualitativa baseada no estudo de casos, através da revisão da literatura e análise documental, focando ações e recomendações das organizações internacionais a que Portugal pertence, deduziram-se os indicadores de resiliência. Esses indicadores foram adequados ao contexto nacional através de entrevistas realizadas a especialistas desta temática.

Conclui-se que a resiliência não é responsabilidade única de nenhuma entidade, e só pode ser garantida com uma abordagem holística, reunindo a sociedade, setor privado, militares e políticos num novo ecossistema de segurança. Nesta linha de pensamento, são propostos 54 indicadores para a ciber-resiliência e 23 indicadores para resiliência nacional face à desinformação, englobando todas as funções críticas do Estado.

Palavras-chave: Ameaças Híbridas, Ciber-resiliência, Desinformação, Cibersegurança, Ciberdefesa, Indicadores de Resiliência Nacional

Abstract

Hybrid threats, driven in cyberspace, deliberately target the vulnerabilities of democratic states and institutions, keeping below the threshold of detection and attribution. On the one hand, we have the problem of technological dependence that increases the risk of cyber-attacks, on the other, the internet has leveraged mass communication and allows any individual to be a source of information, leveraging propaganda and disinformation.

This paper studies the national resilience against hybrid threats in the information environment, proposing criteria and indicators of cyber resilience and resilience against disinformation.

Following a deductive reasoning and a qualitative strategy based on case study, through literature review and document analysis, focusing on actions and recommendations of international organizations to which Portugal belongs, the resilience indicators were deduced. These indicators were validated through interviews with experts in this subject.

It is concluded that resilience is not solely responsibility of one entity, and can only be guaranteed with a holistic approach, bringing together society, private sector, military, and politicians in a new security ecosystem. In this line of thought, this work proposes 54 indicators for cyber resilience and 23 indicators for national resilience in the face of disinformation, encompassing all the critical functions of the state.

Keywords: *Hybrid Threats, Cyber resilience, Disinformation, Cyber security, Cyber defence, National Resilience Indicators*

Lista de abreviaturas, siglas e acrónimos

A

AMWG	*Active Measures Working Group*
AH	Ameaças Híbridas
ANACOM	Autoridade Nacional de Comunicações
AP	Administração Pública

C

CAIH	*Cyber Academia and Innovation Hub*
CCD	Centro de Ciberdefesa
CCDCOE	*Cooperative Cyber Defence Centre of Excellence* ou Centro de Excelência em
CD	Ciberdefesa
CE	Comissão Europeia
CEGER	Centro de Gestão da Rede Informática do Governo
CERT	Equipa de Resposta a Incidentes de Segurança Informática
CERT.PT	Equipa de Resposta a Incidentes de Segurança Informática Nacional
CNCS	Centro Nacional de Cibersegurança
CNE	Comissão Nacional de Eleições
CNPD	Comissão Nacional de Proteção de Dados
CS	Cibersegurança
CSIRT	*Computer Security Incident Response Team*
CyOC	*Cyberspace Operations Centre*

D

DDoS	Ataque de Negação de Serviço Distribuído
DEEMGFA	Diretiva Estratégica do Estado-Maior-General das Forças Armadas
DSA	*Digital Services Act*

E

EC3	*European Cybercrime Centre*
EDA	*European Defence Agency*
EMGFA	Estado-Maior-General das Forças Armadas
ENISA	*European Union Agency for Cybersecurity*
ENSC	Estratégia Nacional de Segurança no Ciberespaço
EUA	Estados Unidos da América
ERC	Entidade Reguladora para a Comunicação Social

F

FED	Fundo Europeu de Defesa
FFAA	Forças Armadas
G	
G4	Grupo dos Quatro (Centro Nacional de Cibersegurança, Centro de
GH	Guerra Híbrida
H	
Hybrid CoE	Centro Europeu de Excelência para o Combate às Ameaças Híbridas
I	
InfoOps	Operações de Informação
IoT	*Internet of Things*
I&D&I	Investigação, Desenvolvimento e Inovação
J	
JP	*Joint Publication*
K	
KGB	Serviços Secretos da União Soviética
M	
MAI	Ministério da Administração Interna
MCDC	*Multinational Capability Development Campaign*
MDN	Ministro da Defesa Nacional
MPECI	Militar, Político, Económico Civil e Informacional
N	
NATO	Organização do Tratado do Atlântico Norte, ou *North Atlantic Treaty*
NCIRC	NATO *Computer Incident Response Capability*
NIST	*National Institute of Standards and Technology*
NSA	*National Security Agency*
O	
OCS	Órgãos de Comunicação Social
OE	Objetivo Específico
OG	Objetivo Geral
OpCiber	Operações no Ciberespaço
OTAN	Organização do Tratado do Atlântico Norte
P	
PACE	Exercícios Coordenados e Paralelos
PADE	Plano de Ação para a Democracia Europeia

PADUE	Plano de Ação contra a Desinformação (da União Europeia)
PESCO	*Permanent Structured Cooperation*
PMESII	Político, Militar, Económico, Social, Infraestruturas e Informacional
PsyOps	Operações Psicológicas
Q	
QC	Questão Central
QD	Questão Derivada
QNRCS	Quadro Nacional de Referência para a Cibersegurança
R	
RASI	Relatório Anual de Segurança Interna
RCM	Resolução do Conselho de Ministros
RGPD	Regulamento Geral sobre a Proteção de Dados
S	
SAR	Sistema de Alerta Rápido
SCEPVA	*Sovereign Cyber Effects Provided Voluntarily by Allies*
SEAE	Serviço Europeu para a Ação Externa
SIS	Serviços de Informações de Segurança
SNPCE	Sistema Nacional de Planeamento Civil de Emergência
SSI	Sistema de Segurança Interna
SRI	Diretiva de Segurança das Redes e Sistemas de Informação
T	
TCE	Tribunal de Contas Europeu
TII	Trabalho de Investigação Individual
U	
UE	União Europeia
UNC3T	Unidade Nacional de Combate ao Cibercrime e Criminalidade Tecnológica
URSS	União das Repúblicas Socialistas Soviéticas ou simplesmente União Soviética
W	
WEF	*World Economic Forum*

1. Introdução

Na crise da Crimeia de 2014, as Ameaças Híbridas (AH) manifestaram-se com campanhas de desinformação no ciberespaço que visaram o descrédito das Forças Armadas (FFAA) e a desconfiança da sociedade (fracionada cultural e socialmente) em relação às autoridades do Estado, dando à Rússia o pretexto para a invasão militar (Danyk et al., 2017; Gunneriusson, 2019). Fazem também parte do ambiente das AH, os ciberataques a infraestruturas críticas ou serviços essenciais, a ciberespionagem, a influência em eleições, a instrumentalização política e desinformação em torno do vírus Covid-19 (Giannopoulos et al., 2020; Jakovljevic et al., 2020; Patel et al., 2020).

Após a anexação da Crimeia, a União Europeia (UE) e a Organização do Tratado do Atlântico Norte (OTAN), ficaram alerta para o problema que claramente não é estritamente militar, tendo incrementado a cooperação entre ambas desde então. Na sequência da Cimeira de Varsóvia de 2016, essa cooperação manifestou-se com uma declaração conjunta, da UE e OTAN, visando a cooperação no planeamento civil-militar, ciberdefesa, partilha de informação e comunicação estratégica coordenada (Shea, 2016).

O Centro Europeu de Excelência para o Combate às AH (Hybrid CoE), criado em 2017, foi um primeiro projeto conjunto da UE e da OTAN neste âmbito. Portugal, reconhecendo a dimensão do problema, que é transversal às sociedades democráticas, aderiu ao Hybrid CoE em dezembro de 2019. Conforme referiu Ana Zacarias à data da adesão, estas ameaças "[...] muitas vezes, são dirigidas ao Estado, aos órgãos políticos, a interferências em processos eleitorais, mas também afetam empresas, serviços financeiros [...]" (LUSA, 2019).

O Hybrid CoE, define AH como uma ação coordenada e sincronizada, conduzida por atores estatais ou não estatais, cujo objetivo é minar ou prejudicar um alvo, influenciando a sua tomada de decisões a nível local, regional, estatal ou institucional (Hybrid CoE, s.d.). Estas ameaças visam deliberadamente as vulnerabilidades dos estados democráticos e das instituições, utilizando uma vasta gama de meios e concebidas para se manterem abaixo do limiar de deteção e imputação, entre o aceitável e inaceitável, o legal e ilegal, na designada "*gray zone"* (Giannopoulos et al., 2020, p. 4). Contudo, nem todas as combinações de meios, nem o seu uso isolado, constituem uma AH (Giannopoulos et al., 2020, p. 26).

A cooperação no seio da UE e da OTAN é fundamental, mas "[…] a principal responsabilidade na luta contra as AH cabe aos Estados-Membros […] sendo necessária uma abordagem global da segurança que abranja […] toda a sociedade […]" (Conselho da UE,

2019). O combate às AH não são responsabilidade única de uma entidade especifica e é necessário adotar abordagens holísticas, *whole-of-government* e *whole-of-society,* promovendo a aproximação, confiança e partilha de informação regular entre organismos do estado (civis e militares), extensível à sociedade e setor privado, num novo ecossistema de segurança preparado para responder a crises de forma mais eficiente (MCDC, 2019). Quanto ao papel da defesa, o secretário-geral da OTAN referiu que: "[…] *our militaries cannot be strong if our societies are weak, so our first line of defence must be strong societies* […]" (Jens Stoltenberg, 2020).

A agenda estratégica da UE para 2019-2024, apela ao aumento da resiliência e proteção das sociedades face às AH, salientando a importância da proteção contra os ciberataques e a desinformação (Conselho Europeu, 2019). De acordo com a OTAN (2020b), a resiliência é a capacidade de uma sociedade resistir e recuperar fácil e rapidamente, de choques provocados por AH, entre outras, combinando tanto a preparação civil como a capacidade militar. O conceito de resiliência tem assumido um papel de relevo tanto na OTAN como na UE, pois é o que melhor lida com vulnerabilidades e ameaças que são incertas. Assim, para garantir a dissuasão e resposta face a AH, importa ser resiliente, sendo necessário identificar indicadores que permitam medir a resiliência do Estado face a estas ameaças (Giannopoulos et al., 2020, p. 5).

As AH são impulsionadas pela tecnologia que surge como um elemento multiplicador na dimensão informacional, explorando as vulnerabilidades de uma sociedade em rede, pelo que o objeto de investigação é a resiliência nacional face a AH no domínio informacional.

A investigação foi delimitada no tempo, espaço e conteúdo, sem prejuízo da sua contextualização (Santos & Lima, 2019, p.42). Delimita-se temporalmente desde 2016, ano em que a Comissão Europeia (CE) e a Alta Representante deram um primeiro passo e estabeleceram o Quadro Comum em Matéria de Luta contra as AH (CE, 2016), até ao presente. Quanto ao espaço, é delimitada a Portugal, pois estuda-se a resiliência nacional, e à UE e OTAN, por definirem orientações e recomendações nesta área, relevantes para os Estados-Membros. O conteúdo, foca o estudo das ações e efeitos das técnicas no âmbito das AH no ambiente informacional, bem como as respostas dos visados, à luz da legislação, políticas, ações e quadros de referência.

O objetivo geral (OG) da investigação, bem como os objetivos específicos (OE) necessários para o atingir, estão definidos na Figura 1.

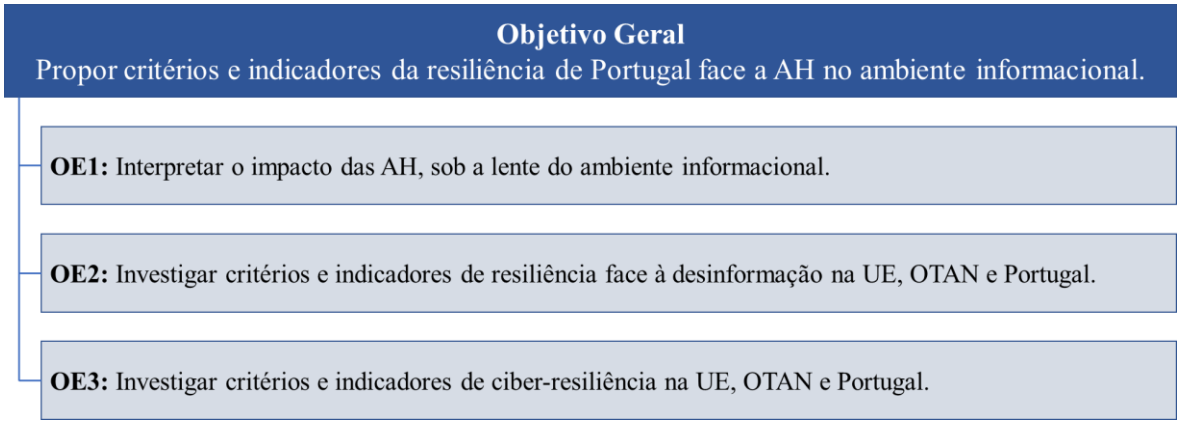

Figura 1 - Objetivos da investigação

A problemática de investigação é formulada pela Questão Central (QC) e pelas Questões Derivadas (QD), definidas na Figura 2.

As QD concorrem diretamente para um OE correspondente, e serviram como elementos orientadores da investigação.

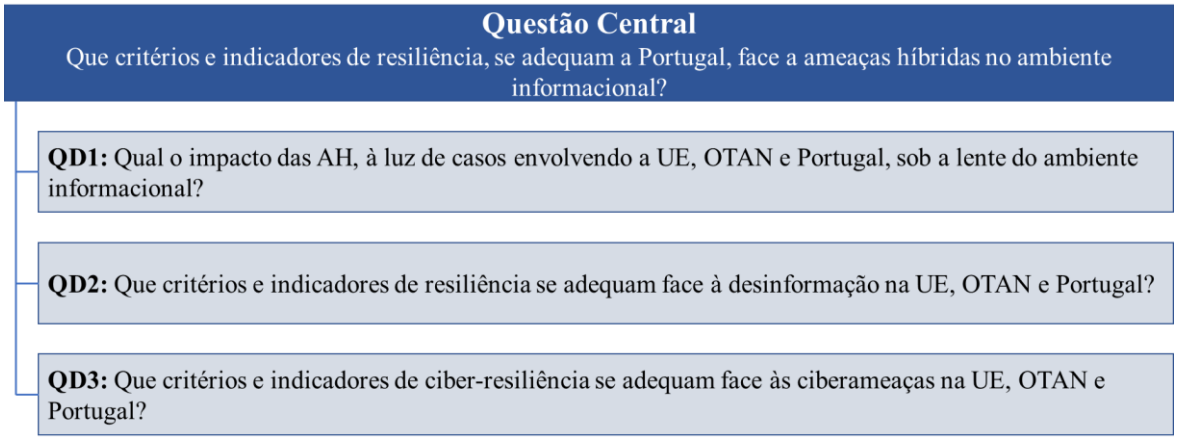

Figura 2 - Questões da investigação

Este estudo está estruturado com este capítulo de introdução mais seis capítulos. O segundo capítulo, apresenta a revisão da literatura, a metodologia e o método. O terceiro, interpreta o impacto das AH sob a lente do ambiente informacional, respondendo à QD1. O quarto e quinto capítulos, materializam a investigação acerca da resiliência face à desinformação e às ciberameaças, no âmbito das AH, procurando responder à QD2 e QD3 respetivamente. O sexto capítulo, transpõe e adequa ao ambiente interno, os indicadores de resiliência obtidos na investigação efetuada em resposta às QD, abordando a validação desses indicadores junto de especialistas entrevistados para esse efeito, respondendo assim à QC. No último capítulo apresentam-se as conclusões.

2. Enquadramento teórico e percurso metodológico

O tema deste Trabalho de Investigação Individual (TII) enquadra-se no ramo do conhecimento das Ciências Militares, reguladas pelo Art.º 5º do Decreto-Lei n.º 249/2015 de 28 de outubro de 2015 (p. 9300), na área de Estudo das Crises e dos Conflitos Armados, no domínio do planeamento estratégico militar.

Neste capítulo apresentam-se os conceitos essenciais e a revisão da literatura focando as AH no domínio informacional, e descreve-se a metodologia adotada.

2.1 Base conceptual

Importa definir o que são AH e a sua conceptualização, a importância do ambiente informacional e o conceito de resiliência.

2.1.1 Ameaças Híbridas

De acordo com a OTAN (2021c), as AH combinam meios militares e não militares, ocultando ações ou não, incluindo desinformação, ciberataques, pressões económicas, utilização de grupos armados irregulares e de forças regulares, para desfocar as linhas entre a guerra e a paz, e tentar semear a dúvida e a incerteza na mente das populações alvo.

A UE, afirma que o conceito de AH é flexível pela sua natureza evolutiva (CE, 2016, p. 2). A mais recente definição de AH, dada pelo Hybrid CoE e abraçada pela UE em vários documentos recentes, é a que se considera neste TII, pois foca as AH nas vulnerabilidades dos sistemas democráticos e no ataque aos seus valores fundamentais, referindo que minam a confiança pública nas instituições democráticas, estimulam a polarização nacional e internacional, afetando a capacidade de tomada de decisões dos líderes políticos (Giannopoulos et al., 2020, p. 6). Este conceito de AH, defende claramente uma abordagem abrangente, incluindo a cooperação civil-militar, conforme referiu Stoltenberg (2015), secretário geral da OTAN, "*Hybrid is the dark reflection of our comprehensive approach. We use a combination of military and nonmilitary means to stabilize countries. Others use it to destabilize them."*

Apesar do foco deste TII ser relativo às AH, importa ressalvar a diferença entre estas e o conceito de Guerra Híbrida (GH). A GH implica violência e um conflito armado, onde um adversário procura contrariar a assimetria de poder com uma combinação de capacidades e métodos, convencionais ou não, por outro lado, as AH procuram ganhos ao mesmo tempo que evitam o escalar do conflito, explorando a *gray zone* (cfr. Figura 3), entre a paz e a guerra (Monaghan, 2019). Numa aproximação à linguagem de Clausewitz, Monaghan (2019) refere que as AH visam principalmente a vontade do povo e a capacidade de decisão

do governo, enquanto a guerra híbrida visa neutralizar a eficácia do instrumento militar na condução de operações.

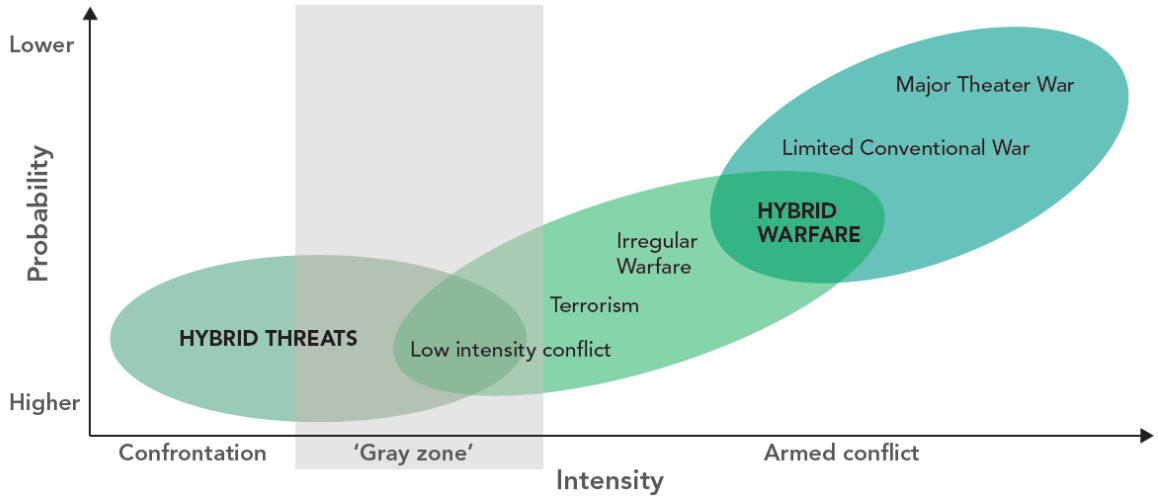

Figura 3 - AH e GH no espetro do conflito

Fonte: Disponível em Monaghan (2019).

2.1.2 Modelos conceptuais de análise das AH

Segundo Giannopoulos et al. (2020), do Hybrid CoE, para compreensão das AH é necessário examinar quatro pilares: (i) os atores e objetivos estratégicos; (ii) as ferramentas utilizadas; (iii) os domínios afetados; e (iv) as fases da campanha híbrida. Um ator, atinge objetivos estratégicos, selecionando uma combinação de ferramentas, em que cada ferramenta aproveita uma oportunidade, explora ou cria vulnerabilidades num ou mais domínios, criando efeitos diretos ou efeitos em cascata. A campanha híbrida normalmente compreende atividades de interferência (e.g., no domínio cognitivo, psicológico) e influência para moldar comportamentos (fase da preparação), podendo evoluir (ou não) para a coerção (GH) (Giannopoulos et al., 2020). O HybridCoE propõe uma representação do modelo (*cfr.* Figura 4) e sugere que este possa ser adaptado a um cenário concreto, permitindo melhorar a resiliência.

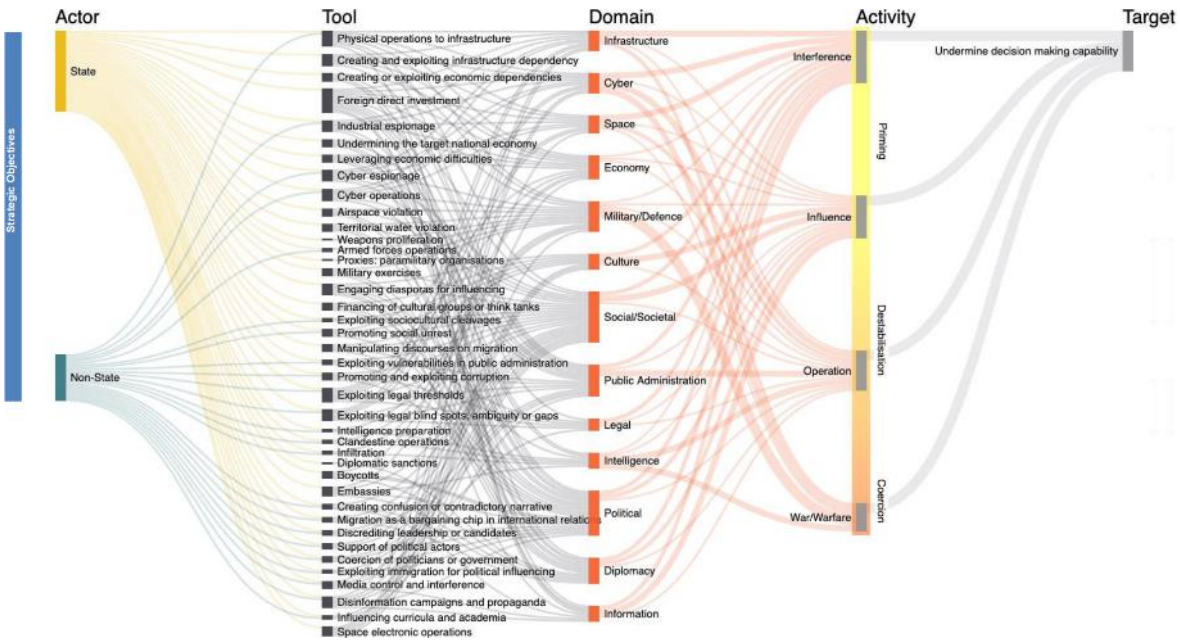

Figura 4 - Visualização do modelo conceptual do HybridCOE

Fonte: Disponível em Giannopoulos et al. (2020).

Outro modelo (cfr. Figura 5), proposto pelo *Multinational Capability Development Campaign* (MCDC) (2019), permite a visualização de um ataque híbrido, focando: (i) as vulnerabilidades das funções críticas; (ii) a capacidade do agressor para sincronizar vários instrumentos de poder; e (iii) os efeitos criados pelas ações.

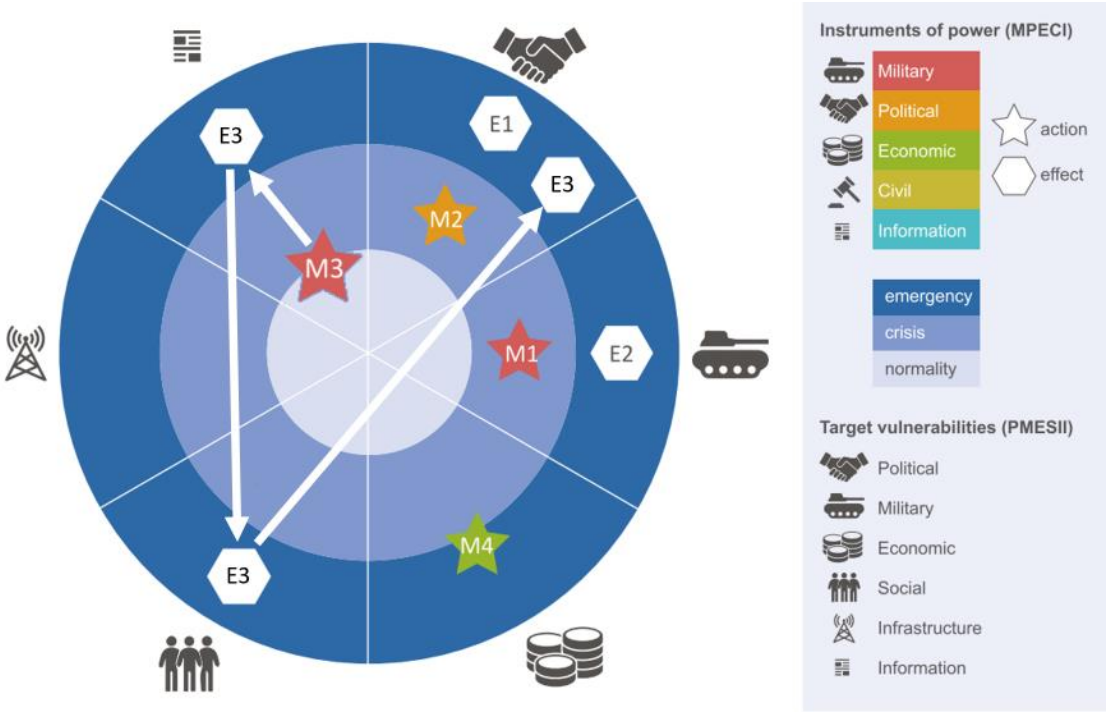

Figura 5 - Visualização do modelo conceptual do MCDC

Fonte: Adaptado a partir de MCDC (2019).

De acordo com a abordagem do MCDC, os instrumentos de poder podem ser de âmbito militar, político, económico, civil e informacional (MPECI) e exploram vulnerabilidades das funções críticas de um Estado no domínio político, militar, económico, social, informacional e das infraestruturas (PMESII).

Como se observa, o modelo do MCDC permite focar as relações entre ações e efeitos, de 1ª ou 2ª ordem. Por exemplo, na Figura 5, em consequência da ação M3 (e.g., ciberespionagem), será divulgada *Informação* para influenciar a opinião pública e as perceções (*Social*), minando a discussão e o processo *Político*.

2.1.3 Ambiente informacional, ciberespaço e desinformação

A Estratégia Nacional de Segurança no Ciberespaço (ENSC), publicada através da Resolução do Conselho de Ministros (RCM) n.º 92/2019, de 05 de junho, no ponto primeiro, define o *ciberespaço* como "[…] um ambiente complexo, de valores e interesses, materializado numa área de responsabilidade coletiva, que resulta da interação entre pessoas, redes e sistemas de informação.". A ENSC define ainda no mesmo ponto, a *cibersegurança* como o "[…] conjunto de medidas e ações de prevenção, monitorização […]" que visam "[…] garantir a confidencialidade, integridade, disponibilidade e não repúdio da informação, das redes e sistemas de informação no ciberespaço, e das pessoas que nele interagem […]", e *ciberdefesa* como a "[…] atividade que visa assegurar a defesa nacional no, ou através do, ciberespaço.".

O *ambiente de informação* permeia todos os domínios físicos e consiste num agregado de indivíduos, organizações, e sistemas que recolhem, processam, divulgam, ou atuam sobre a informação (JP3-12, 2018). Segundo a OTAN (2019, p. A-7), as comunicações estratégicas dirigem, coordenam, e sincronizam o esforço global de comunicação, para moldar o ambiente de informação, e integram as operações psicológicas (PsyOps) e operações de informação (InfoOps), com outras atividades militares. As InfoOps criam efeitos sobre a vontade, compreensão e capacidade dos adversários, as PsyOps são dirigidas a audiências alvo aprovadas, para influenciar perceções, atitudes e comportamentos, que afetam a realização de objetivos políticos e militares (OTAN, 2019).

O ciberespaço, totalmente contido no ambiente de informação, permite executar Operações no Ciberespaço (OpCiber) criando efeitos no ambiente de informação, portanto, com uma forte ligação de apoio às operações no ambiente informacional (JP3-12, 2018). As OpCiber podem ser ofensivas, destinadas a projetar poder no e através do ciberespaço, ou defensivas, para defender a rede de defesa nacional ou outras de ameaças ativas.

A *desinformação*, erradamente reduzida a "*fake news*", segundo Humprecht et al. (2020) é informação falsa estrategicamente partilhada para obter lucros ou causar danos e prejuízo público (ambiente, segurança, processos democráticos, etc.). Os autores definem ainda *misinformation* como a partilha não intencional de conteúdos falsos ou enganosos, e *malinformation* como informação genuína (e.g., privada), partilhada para causar danos. Os conceitos sobrepõem-se (*cfr.* Figura 6), uma vez que os utilizadores em linha partilham involuntariamente informações falsas.

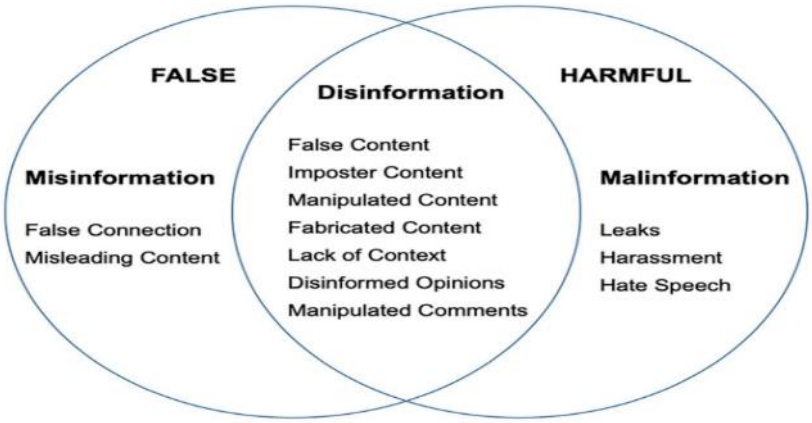

Figura 6 – Tipos de informação no ambiente das redes sociais

Fonte: Disponível em Humprecht et al. (2020).

Propaganda é a persuasão e influência sobre atitudes e opiniões do público-alvo, com fins ideológicos, políticos ou comerciais, através da divulgação de informação parcial (que pode ou não ser factual) (Nelson, 1996).

2.1.4 Resiliência

O conceito de *resiliência*, pode ser interpretado como uma filosofia e metodologia que procura uma melhor preparação de sistemas complexos para uma variedade de ameaças, conhecidas ou não (Linkov et al., 2019). Em vez de especificar medidas contra uma ameaça específica, a abordagem de resiliência prepara os sistemas para um amplo universo de possíveis roturas. No contexto de um Estado, segundo a OTAN (2020b), a resiliência é a capacidade que a sociedade tem para resistir e recuperar com facilidade de choques que causem grande impacto, como é o caso de calamidades, falhas de infraestruturas críticas, um ataque armado, AH, entre outras, combinando tanto a preparação civil (continuidade das funções críticas do Estado) como a capacidade militar.

A ciber-resiliência visa reduzir o risco das funções da organização (e.g., do Estado) dependerem do ciberespaço, procurando reduzir (ou anular) o impacto e a probabilidade de ocorrência de uma ameaça (ciberataques, falhas e outros perigos) no ciberespaço, e continuar a operar as suas funções essenciais nesse ambiente degradado (Ross et al., 2019, p. 78).

2.2 Estado da Arte

Na abordagem clássica da guerra, o instrumento de poder militar é o centro de gravidade, mas hoje, o informacional tem um peso significativo nas novas formas de fazer a guerra (Dodonov et al., 2019). Segundo Nunes (2018, p. 81), a sociedade em rede aumenta as vulnerabilidades e as ameaças. Olhando à trindade de Clausewitz (1984, p. 89) – povo, governo e militares – as AH têm o foco nas duas primeiras, estimuladas por essa sociedade tecnológica. Os analistas russos Chekinov e Bogdanov (2013), descrevem a "Guerra de Nova Geração" com ênfase no seu formato tecnológico e na superioridade da informação.

As AH fundamentam-se em conceitos antigos (Boot, 2013; Fiott & Parkes, 2019, p. 4; Marcuzzi, 2018; Murray & Mansoor, 2012). Por exemplo, Sun Tzu, no século IX a.C., já referia a utilização de uma abordagem indireta (alimentando a discórdia e desconfiança) (Tzu, 1963, p. 77). Liddell Hart, propôs que o inimigo deve ser desequilibrado atacando as suas ligações cognitivas e as suas componentes mais fracas (Hart, 1941). As novas tecnologias proporcionam simplesmente formas mais eficientes de implementar estas ideias estratégicas. Aludindo a Cohen (1999), poderemos estar perante uma revolução em assuntos militares, aproximando a natureza da guerra à população, fazendo uso das novas tecnologias.

Existem diversos livros e artigos que focam a conflitualidade no ciberespaço (Abaimov & Martellini, 2020; Lino Santos & Guedes, 2015; Schreier, 2015; Steffens, 2020) e outros que focam a guerra de informação (Giles, 2016; Whyte et al., 2020).

No âmbito nacional, Nunes (2020) foca a edificação da capacidade de ciberdefesa, enquanto Alves (2020) propõe linhas de ação para as FFAA portuguesas responderem às AH. Quanto aos desafios da desinformação, destaca-se o relatório da Entidade Reguladora para a Comunicação Social (ERC) (2019).

A UE, a OTAN, outras organizações e académicos, têm publicado diversos conteúdos relativos à resposta face a AH, e que citamos ao longo do trabalho. O Hybrid CoE e o MCDC são as referências internacionais no desenvolvimento conceptual e de recomendações na resposta a AH. No que diz respeito à segurança no ciberespaço, destacam-se o Centro de Excelência em Ciberdefesa Cooperativa (CCDCOE) (acreditado pela OTAN) e a Agência da UE para a Segurança das Redes e da Informação (ENISA). Ao nível da desinformação, releva-se o Centro de Excelência em Comunicações Estratégicas (NATO StratCom COE).

A investigação nesta área é muito recente, pelo que ainda não existem estudos científicos e consolidados que abordem a resiliência nacional contra AH, na perspetiva do ambiente informacional, como este TII se propõe fazer.

2.3 Metodologia e método

2.3.1 Modelo de análise e metodologia

A resiliência do instrumento de poder informacional face a AH, foi o conceito de partida, analisado à luz de duas dimensões: a ciber-resiliência e a resiliência face a campanhas de desinformação. A primeira, porque o ciberespaço é o meio primordial para o funcionamento da sociedade em rede, a segunda, porque a desinformação é uma das principais técnicas das AH. Para cada dimensão, analisaram-se variáveis que correspondem às ações-efeitos que materializaram exemplos de AH, bem como as respostas da OTAN, UE e Portugal, à luz das diferentes funções críticas de um Estado (PMESII), permitindo deduzir indicadores de resiliência (ver modelo de análise no Apêndice A).

A escolha e construção de conceitos, bem como a identificação de variáveis e indicadores permitiram a formulação das questões iniciais desta investigação (Vilelas, 2009). O modelo de análise, explicitado em dimensões, variáveis e indicadores, foi construído em consonância com os objetivos e questões que esta investigação procura responder, à luz dos conceitos apresentados neste capitulo (Santos & Lima, 2019, pp. 61–62).

Face ao objeto de investigação, adotou-se uma posição ontológica construtivista, segundo a premissa de que o conhecimento é uma construção social (Bryman, 2012, p. 33). Com uma abordagem epistemológica interpretativista, sem recurso a técnicas das ciências naturais, e um raciocínio dedutivo, partiu-se da "[…] lei geral para o particular […]" (Santos & Lima, 2019, pp. 16-18), transpondo as respostas e recomendações da OTAN e da UE para o caso nacional. A estratégia de investigação foi qualitativa, vertida num estudo descritivo, interpretando os fenómenos "[…] a partir de padrões encontrados nos dados […]", sem preocupação com medições e análises estatísticas (Vilelas, 2009, cit. por Santos & Lima, 2019, p. 27). O desenho de pesquisa foi baseado no estudo de casos, num horizonte temporal transversal, pois foram extraídos indicadores observando as recomendações da UE e da OTAN, e adaptados ao contexto nacional.

2.3.2 Método

Na 1ª fase definiu-se o objeto de estudo, delimitou-se o tema, formulou-se o problema de investigação, definiram-se os objetivos, questões de investigação e ainda o procedimento metodológico descrito. Realizaram-se ainda entrevistas exploratórias com especialistas que permitiram desenvolver e definir o modelo de análise.

Na 2ª fase (*cfr.* Figura 7) obtiveram-se as respostas às QD através da revisão da literatura e da análise documental (e.g., legislação, políticas, quadros de referência, estruturas organizacionais) da UE, OTAN e Portugal. O esforço de pesquisa, centrou-se na dedução de indicadores que permitem medir a resiliência nacional face a AH (informacional).

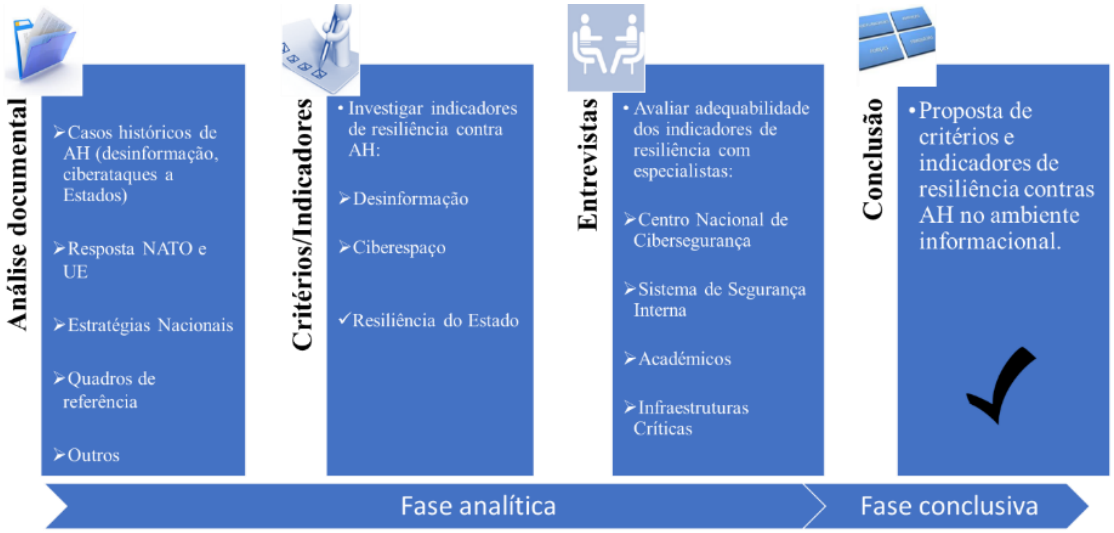

Figura 7 - Esquema síntese da 2ª fase da investigação

Foram realizadas entrevistas semiestruturadas a seis personalidades relevantes no tema em estudo (*cfr.* Apêndice B), por videoconferência e correio eletrónico, que permitiram incluir novos indicadores e validar a adequabilidade e a importância dos indicadores elencados, servindo de suporte para a resposta à QC (Quivy & Campenhoudt, 1998, p. 121). As respostas a quatro das seis questões, foram objeto de tratamento com estatística descritiva, através do *Microsoft Excel* (*cfr.* Apêndice C). O conteúdo das entrevistas, foi analisado utilizando o método das relações por coocorrências (Lúcio Santos & Lima, 2019, p. 120).

3. O impacto das AH

Procura-se neste capítulo, interpretar o impacto das AH, sob a lente do ambiente informacional, e responder à QD1.

3.1 O renascer das técnicas da Guerra Fria

Durante a Guerra Fria, os EUA e a União Soviética (URSS) aperfeiçoaram estratégias indiretas (e.g., guerras por procuração, interferências eleitorais, campanhas de desinformação), em que os EUA visavam denegrir e conter o comunismo, e a URSS o enfraquecimento do Ocidente (Santo, 2009). A investigação de Dov Levin (2019) entre diversas outras (Cull et al., 2017; Hickman et al., 2018; Lucas & Mistry, 2009), ilustra que ambas as superpotências utilizaram a desinformação como tática central para cultivar o apoio ideológico, interna e externamente.

O famoso NSC-68 (1950), um documento estratégico dos EUA, de 1950, refere a utilização da desinformação para combater a expansão comunista. Por outro lado, a doutrina soviética, usava o termo "*Active Measures"*, para agrupar técnicas de desinformação, e.g., agentes de influência, histórias falsas, falsificações (e.g., planos ou cartas forjadas), entre outras (AMWG, 1981; Juurvee, 2018).

Um exemplo de desinformação, foi a alegação dos serviços secretos da URSS (KGB), em jornais soviéticos e internacionais, de que os EUA criaram em laboratório o vírus da SIDA, como arma química (Ward, 2019). Para além da imprensa, o artigo científico (Segal et al., 1987) do professor alemão e agente do KGB, Jakob Segal, deu outra dimensão à história, provocando a desconfiança nas populações (Cull et al., 2017).

Só na administração de Reagan, a partir de 1980, os EUA conseguiram dar uma resposta forte à desinformação soviética, com a criação do *Active Measures Working Group* (AMWG), um grupo interagências (Romerstein, 2001). As principais contramedidas adotadas, segundo Cull et al. (2017), foram o *descrédito vigoroso* (denúncia de falsidades), a ameaça de *sanções* (e.g., cooperação, económicas), uso dos *media internacionais* para denunciar, os *desertores* soviéticos (testemunhos) e a c*oleta de informação* para identificação das campanhas.

3.2 Os novos métodos impulsionados no ciberespaço

Devido à descentralização das fontes de informação que a internet veio proporcionar, aumentou o volume de desinformação bem como os atores envolvidos na sua disseminação. Adicionalmente, a crescente dependência da sociedade moderna no ciberespaço, pode levar

a ciberataques disruptivos com as mesmas consequências de uma guerra convencional (RCM n.º 92, 2019; Steiger et al., 2018; Stiennon, 2015).

Descrevendo exemplos, em 2007, na Estónia, foi lançado um ataque de *negação de serviço* distribuído (DDoS), alegadamente motivado pela Rússia após deslocalização de um memorial soviético, suspendendo as funções do Estado durante duas semanas (Buckland et al., 2010). Na Geórgia, em 2008, a Rússia demonstrou, pela primeira vez, a viabilidade de um ciberataque (também DDoS mas não só) em apoio a uma operação militar convencional (Abaimov & Martellini, 2020, p. 70).

Valeriano e Maness (2015) fizeram um estudo sobre ciberconflitos ocorridos entre 2001 e 2011, com 111 incidentes entre Estados, sendo aproximadamente metade relacionados com *ciberespionagem*. Em 2009, a *Information Warfare Monitor* (2009), revelou a existência de uma rede de ciberespionagem (GhostNet), com alcance a 103 Estados diferentes, incluindo Portugal (duas embaixadas e o CEGER[1]). Desde este incidente, aumentou o foco nos grupos de ciberespionagem, e.g., grupo APT1 alegadamente a cargo da unidade 61398 do Exército de Libertação Popular Chinês (Mandiant, 2013). Ainda no âmbito da ciberespionagem, o recente ataque com impacto ainda desconhecido, que explorou a cadeia de distribuição de atualizações do *software* Solarwinds, é tido como um dos mais sofisticados até agora visto (Menn, 2021). A ciberespionagem é uma ameaça crescente que importa destacar, pois o roubo de segredos de estado e comerciais, direitos de propriedade intelectual e informação proprietária, têm um impacto estratégico difícil de prever (ENISA, 2020a).

Em 2010, no Irão, as centrais de enriquecimento de Urânio fecharam em resultado de uma *cibersabotagem* extremamente sofisticada, através de um código malicioso, i.e., *malware*, designado Stuxnet (Abaimov & Martellini, 2020, p. 71). Outro ciberataque a infraestruturas críticas, ocorreu na Ucrânia em 2015, provocando um corte de energia para 225.000 pessoas durante 3 horas (Lee et al., 2016).

Em 2017, surgiu o WannaCry, o maior de ataque de *ransomware*[2] à escala mundial, encriptando a informação e solicitando o resgate em Bitcoins (Chen & Bridges, 2017). Importa realçar que este ataque foi alavancado por um *zero-day* (explora uma vulnerabilidade desconhecida), uma ciberarma designada EternalBlue, do arsenal da *National Security Agency* dos EUA (NSA), divulgada pelo grupo *Shadow Brokers*,

[1] Centro de Gestão da Rede Informática do Governo.
[2] O *ransomware* é uma classe de *malware* que se autopropaga, encripta os dados de um computador vítima e solicita o resgate, tendo surgido como uma ciberameaça dominante (ENISA, 2020).

relevando os riscos dos arsenais de ciberarmas serem capturados e usados de forma indiscriminada por cibercriminosos como no caso do WannaCry e outros posteriores (Abaimov & Martellini, 2020, p. 12).

Por fim, importa referir o uso do ciberespaço como ferramenta para *influenciar processos eleitorais* em estados democráticos. Destaca-se o caso da empresa Cambridge Analytica, que alegadamente influenciou diversas eleições, como nos EUA em 2016 ou o referendo do Brexit, traçando o perfil psicológico das pessoas através de dados fornecidos pelo Facebook, influenciando os votos com mensagens direcionadas (Isaak & Hanna, 2018). Este ataque demonstrou vulnerabilidades na legislação da privacidade digital e o poder das grandes empresas tecnológicas. Noutro exemplo, em 2017, apenas dois dias antes das eleições presidenciais francesas, sem tempo de resposta foram divulgados 9GB de *e-mails* comprometedores do partido de Emmanuel Macron (Abaimov & Martellini, 2020, p. 14).

3.3 O caso da anexação da Crimeia

Na Ucrânia, as consequências das operações de informação e psicológicas através de campanhas de desinformação no ciberespaço, resultaram no descrédito das FFAA e desconfiança da sociedade em relação às principais autoridades do Estado (Danyk et al., 2017). Foram utilizados conteúdos, nas redes sociais e outros recursos da internet, difundidos como sendo de autores credíveis (e.g., antigos militares patrióticos), replicados em reportagens de televisões públicas na Ucrânia, que utilizaram essas fontes não verificadas (Danyk et al., 2017). A atuação da Rússia, minando a confiança em instituições internacionais e nacionais, é o exemplo de AH impulsionadas no ciberespaço (Atkinson, 2018; Chivvis, 2017).

Esta é a doutrina russa de Gerasimov, que atinge objetivos políticos e estratégicos, com a ênfase no uso dos instrumentos de poder informacional, político, económico, com foco em aumentar o protesto social, agredir e influenciar a consciência pública através da tecnologia e de ciberataques (Galeotti, 2019). Do ponto de vista russo, a guerra é agora conduzida por uma proporção aproximada de 4:1 de medidas não-militares e militares (Bartles, 2016). A transição para o uso explícito da força militar, acontece na fase final do conflito, a coberto do pretexto da manutenção da paz (Dodonov et al., 2019).

A doutrina de Gerasimov é baseada no que a Rússia considera que tem sido a atuação dos EUA, ao provocar instabilidade em países com regimes não-democráticos obtendo o pretexto para intervir militarmente (Bartles, 2016).

3.4 O impacto em Portugal

As AH são também uma preocupação para Portugal. Vejamos a posição da China, como potência emergente, e a sua relação com Portugal. A China fez investimentos críticos em Portugal, designadamente na EDP, na REN ou através da carteira da Fosun (investidor privado chinês), que "[…] vai da saúde à indústria farmacêutica, dos seguros à banca, passando por imobiliário e telecomunicações […]" (Costa, 2021). A persuasão chinesa é tal que impôs censura (preservando o amor à pátria chinesa) aos jornalistas da Rádio Televisão de Macau, contrariando os acordos bilaterais com Portugal e sem que ninguém consiga evitar (Vinagre, 2021). Por outro lado, temos os EUA a pressionar Portugal para "[…] escolher entre os aliados e os chineses […]", referindo-se à tecnologia 5G, tentando condicionar a decisão portuguesa (Jornal SOL, 2020).

O último Relatório Anual de Segurança Interna (RASI 2020), sem atribuir autoria, refere as "[…] ameaças persistentes, tecnologicamente avançadas, de origem estatal […]", especificando a ciberespionagem contra entidades de investigação científica (envolvidas em terapêuticas e vacinas da COVID-19) e "[…] infraestruturas críticas nacionais, com a finalidade de aceder a informação classificada, com valor político e económico […]" (Sistema de Segurança Interna [SSI], 2021, p. 102). Suspeita-se que tanto a China como a Rússia estejam envolvidas nestes ciberataques (Oliveira, 2021).

Relativamente à desinformação, o RASI 2020 refere que as campanhas sobre a origem da COVID-19 e outras questões relacionadas, procuraram "[…] enfraquecer a confiança da sociedade portuguesa na resposta à crise […]". Adicionalmente, o efeito do confinamento social associou-se à crescente disseminação de conteúdos de propaganda e desinformação de movimentos radicais de extrema-direita (SSI, 2021, p. 102). Segundo o RASI, para responder às AH é prioritário combater a desinformação e proteger os processos eleitorais (SSI, 2021, p. 223).

Apesar de "[…] Portugal não ser um alvo significativo de ataques híbridos cinéticos devido à sua dimensão geopolítica […]", não é imune aos crescentes ataques não cinéticos (Alves, 2020, p. 30). De facto, apesar da pandemia ter aumentado a perceção que estamos sujeitos a este tipo de ameaças, Pathe Duarte (2020) demonstrou que Portugal esteve sujeito a pressões económicas, ciberataques e operações de narrativa nas redes sociais e *media*, perpetrados por agentes estatais (China e Rússia) e não-Estatais, muito antes da pandemia (*cfr*. Figura 8).

Hybrid threats in Portugal – 2017/2018						
	Occurrences			Perpetrator		
Type of Threat	Yes	No	Speculative (no factual evidence)	Russia	China	Non-state actor
Kinetic actions						
Proxy wars		×				
Non-declared conflicts		×				
Paramilitary groups		×				
Non-kinetic actions						
Narrative-led operations and weaponization of social media	×		×	×	×	×
Financing	×		×	×	×	
Economic pressure	×				×	
Cyberattacks	×		×	×	×	×

Figura 8 - AH em Portugal entre 2017 e 2018

Fonte: Disponível em Duarte (2020).

Segundo o Centro Nacional de Cibersegurança (CNCS) (2020), os cibercriminosos e agentes estatais agem em colaboração estreita, com ciberataques e desinformação por vezes vendidos como um serviço, dificultando a imputação.

Os incidentes registados pelo CERT.PT[3] têm vindo a aumentar nos últimos anos, não estando imunes setores críticos do Estado (cfr. Figura 9).

RK	Setor e Área Governativa[5]	Nº	%
1º	Outros	251	28
2º	Infraestruturas Digitais	170	19
3º	Prestadores de Serviços de Internet	167	18
4º	Educação, Ciência, Tecnologia e Ensino Superior	81	9
5º	Banca	69	8
6º	Transportes	30	3
7º	Serviços de Computação em Nuvem	26	3
8º	Administração Local	18	2
9º	Saúde	11	1
10º	Infraestruturas do Mercado Financeiro	11	1
11º	Energia	9	1
12º	Defesa Nacional	9	1
13º	Órgãos de Soberania	9	1
14º	Presidência do Conselho de Ministros	9	1
15º	Agricultura	7	0,8

Figura 9 - Incidentes registados pelo CERT.PT, 2019 - *ranking top* 15

Fonte: Disponível em CNCS (2020).

[3] O CERT.PT é a Equipa de Resposta a Incidentes de Segurança Informática Nacional (Lei n.º 46/2018).

3.5 Desafios futuros

Os EUA sugerem que os esforços globais de influência, com ciberataques e desinformação, irão aumentar *(Office of the Director of National Intelligence*, 2021).

A imputação de um ciberataque é essencial para uma eventual resposta, mas implica saber quem o executou e quais as consequências, algo complexo de responder no ciberespaço, tornando-o no local de eleição das AH (Brenner, 2009; Rid & Buchanan, 2015). Muitas das atribuições ao nível Estado, são feitas com base em suposições e não em provas digitais fiáveis, por serem difíceis de obter, principalmente em ataques que recorrem a criptografia e ocultação e ocorrem em múltiplas fases e por diversos locais geográficos e jurisdições (Clark & Landau, 2011; Wheeler et al., 2003). Os *hackers* profissionais encaminham os ataques através de países com os quais a vítima tem más relações diplomáticas dificultando a investigação (Schreier, 2015).

As propostas que visam arquiteturas para a internet, que tornem a imputação mais controlável, conduzirá a um controlo e vigilância governamentais indesejados que chocam com a liberdade e privacidade (Buckland et al., 2010, p. 26). Por exemplo, a Rússia ou a China, mantém enorme censura e restrições nas suas arquiteturas internas (Newman, 2020).

O problema da imputação tem de ser resolvido com capacidades técnicas e diplomacia que garanta colaboração total entre países, empresas e organizações, quer ao nível militar quer civil (Clark & Landau, 2011; Schreier, 2015). Adicionalmente, qualquer pessoa é uma porta de entrada na rede de uma organização (civil ou militar), sendo necessário apostar na educação em cibersegurança e encará-la como uma responsabilidade partilhada (Clarke & Knake, 2010, p. 170).

Os desafios dos sistemas ciber-físicos, e.g., armas autónomas, carros autónomos, internet das coisas (IoT) e o seu uso em *smart cities*[4], trazem novos desafios na área da cibersegurança e potencial para aumentar as AH (Alguliyev et al., 2018). As ferramentas antigas podem ser utilizadas de uma nova forma, ou num contexto diferente do que estamos habituados e podem ser criadas combinações inesperadas (Giannopoulos et al., 2020). Importa realçar o papel disruptivo da inteligência artificial, que é um facilitador dos sistemas ciber-físicos, mas pode também automatizar ciberataques ou criar conteúdos falsos de forma inovadora, e.g., manipulação de imagens ou vídeos (designados *deepfakes*) (Hybrid CoE, 2021). As grandes empresas tecnológicas terão maior influência, passando a ter também um

[4] Cidades sustentáveis e otimizadas devido à tecnologia (Iberdrola, s.d.).

papel cada vez mais relevante para a segurança e defesa, pelo que a regulação e políticas deverão estar sempre a par do desenvolvimento tecnológico (Hybrid CoE, 2021).

No contexto dos desafios elencados, e respondendo à QD1, o uso do instrumento de poder informacional para influenciar o domínio cognitivo (tomada de decisão), é predominante na conflitualidade atual, composta por ameaças permanentes, difíceis de identificar. É necessário criar resiliência não só no domínio tecnológico, mas também no domínio social (dimensão humana, perceção, crenças e raciocínio), pois tal como refere Alex Stamos[5] (2020), estas novas ameaças não são apenas um problema tecnológico, mas fundamentalmente um problema humano.

[5] Antigo responsável da cibersegurança do Facebook e atualmente membro da equipa de combate a fraudes eleitorais dos EUA.

4. Resiliência contra AH com foco na desinformação e propaganda

Este capítulo visa investigar possíveis indicadores de resiliência face à desinformação, à luz das respostas da UE, OTAN e Portugal, e de abordagens de referência, procurando responder à QD2.

4.1 A resposta da UE

Em resposta à desinformação russa, na sequência da anexação da Crimeia, a UE cria a *East StratCom Task Force* (*cfr.* Figura 10), integrada no Serviço Europeu para a Ação Externa (SEAE), reforçando a comunicação estratégica de promoção da UE e apoiando a liberdade de imprensa dos países de leste (CE, 2018b). Um projeto pioneiro do *East StratCom*, foi a divulgação de desinformação pró-Kremlin no sítio em linha EUvsDisinfo[6] ou na conta @EUmythbuster do Twitter, já com mais de 11.535 exemplares de desinformação. (Pamment, 2020). Numa pesquisa efetuada com o filtro *Portugal*, obtêm-se duas notícias falsas em que Portugal é implicado, numa tentativa de dividir e enfraquecer a UE (*cfr.* Figura 11).

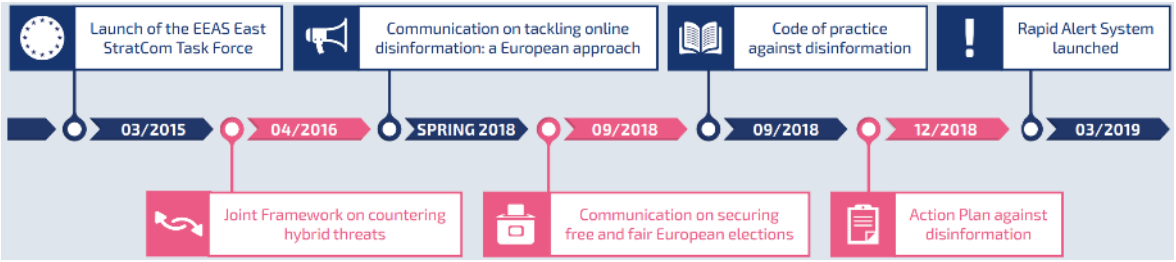

Figura 10 - Ações da UE para combate à desinformação

Fonte: Disponível em *EU vs DISINFORMATION* (s.d.).

DATE	TITLE	OUTLETS	COUNTRY
20.04.2020	Cooperation between the Mediterranean countries threatens Germany's hegemony	News Front - Russian	EU, Portugal, Greece, Spain, Germany
09.09.2019	Italy, Spain, Portugal, and possibly even France are in line to exit the EU	Sonar2050	Portugal, Italy, UK, Spain, France

Figura 11 - Resultado com filtro *Portugal* no sítio EUvsDisinfo

Fonte: Disponível em *EU vs DISINFORMATION* (*op. cit.*).

Num espetro de resposta mais alargado, surge o Quadro Comum em Matéria de Luta contra as AH, onde são propostas 22 ações destinadas a reforçar a resiliência dos Estados-Membros e da UE, com foco no aumento do conhecimento situacional, na comunicação estratégica e na cooperação com a OTAN (CE, 2016). A criação do Hybrid COE a par dos

[6] https://euvsdisinfo.eu/

Exercícios Coordenados e Paralelos (PACE)[7], refletiram essa cooperação (CE, 2017). Na sequência do quadro comum é também criada a Célula de Fusão contra as AH integrada na estrutura de informações (INTCEN) do SEAE, contribuindo para o conhecimento situacional (CE, 2020).

Seguiram-se, em 2018, duas comunicações conjuntas: "Combater a desinformação em linha: uma estratégia europeia" (CE, 2018b), e "Aumentar a resiliência e reforçar a capacidade de enfrentar AH" (CE, 2018c). A primeira, entre outras medidas, aprova o apoio e criação de uma rede europeia independente de verificadores de factos. A segunda, foca a necessidade de aumentar o conhecimento situacional, o esforço dos Estados-Membros, a comunicação estratégica e a ciber-resiliência.

Reconhecendo a necessária colaboração com o setor privado, em outubro de 2018, a UE lançou um Código de Conduta contra a Desinformação juntamente com medidas concretas (e.g., deteção de desinformação, funcionalidade de reporte) para implementação voluntária pela indústria tecnológica (alguns signatários foram a Google, Facebook, Twitter, etc.) (CE, s.d.).

Em dezembro de 2018 foi publicado o Plano de Ação contra a Desinformação, ainda hoje o pilar da abordagem da UE no combate à desinformação (Pamment, 2020). O plano centra-se na cooperação com a OTAN, deteção e exposição da desinformação, literacia mediática, jornalismo de qualidade, comunicação estratégica, sensibilização e resiliência da sociedade. Incentivou ainda as plataformas digitais a aplicarem o Código de Conduta, e estabelece uma abordagem *whole-of-society*, com cooperação entre autoridades públicas, jornalistas, investigadores (meio académico), verificadores de factos, plataformas digitais, setor privado e a sociedade civil em geral. Na sequência do plano, é lançado o Sistema de Alerta Rápido (SAR), para permitir uma consciência situacional comum entre os Estados-Membros, que, no entanto, ainda tem baixos níveis de partilha (Pamment, 2020).

Relativamente à correlação entre segurança interna e externa, deverão ser adotados métodos de trabalho horizontais, numa abordagem *whole-of-government*, com partilha de informações entre as autoridades, formação e exercícios que permitam soluções comuns para combater AH, e particularmente a desinformação (Conselho da UE, 2019).

O recém publicado Plano de Ação para a Democracia Europeia (CE, 2020a), foca-se na promoção de eleições livres, no reforço da liberdade dos *media*, e na luta contra a desinformação. O plano prevê criar instrumentos que permitam impor sanções aos autores

[7] Exercício com foco na gestão e resposta a crises num ambiente de ameaças híbridas.

de desinformação, e transformar o Código de Conduta num quadro de corregulação, em consonância com a nova *Digital Services Act* (DSA), ou Lei dos Serviços Digitais, que permitirá aplicar multas às tecnológicas que não implementem medidas contra a utilização de técnicas manipuladoras (LUSA, 2020).

4.2 A resposta da OTAN

Ao contrário da UE, que vê as AH sem se referir a guerra (e.g., GH), a OTAN, pela sua natureza militar, já em 2010 utilizava ambos os termos mas com a perceção de que a resposta dependia de fatores fora da esfera militar (Uziębło, 2017, p. 14). Assim, a UE tem vindo a liderar o processo na construção de resiliência face a AH, mas a OTAN, um parceiro fundamental, assume-se preparada para apoiar os Estados-Membros a edificarem a sua capacidade de resposta e se necessário dar uma resposta coletiva (OTAN, 2021c).

Os esforços da OTAN para lidar com os métodos híbridos, manifestaram-se no relatório anual de 2015, após a anexação da Crimeia (J. Stoltenberg, 2016). O conceito de resiliência, visto como a melhor forma de lidar com AH, foi central na Cimeira de Varsóvia (2016), que inclusivamente proporcionou a declaração conjunta entre a UE e a OTAN (renovada em 2018) visando a cooperação no planeamento civil-militar, ciberdefesa, partilha de informação e comunicação estratégica coordenada (Shea, 2016). Após esse acordo, estabeleceu-se uma proximidade e partilha entre organismos de ambas as partes: o NCIRC[8] da OTAN e o CERT da UE, o HybridCOE e outros[9] da OTAN, a Célula de Fusão da UE e a célula do *Joint Intelligence and Security Division* da OTAN (Conselho da UE, 2019).

A OTAN, vê a desinformação como uma ameaça que procura aprofundar as divisões dentro e entre os aliados (OTAN, 2020a). Alguns dos desafios são o alcance do Russia Today (RT) e Sputnik (*media* controlada pelo Estado), ou a fábrica *troll* (desestabilizadores de discussão) de São Petersburgo - oficialmente chamada *Internet Research Agency* – com recurso a contas falsas ou automatizadas, para difusão de notícias que contêm elementos verdadeiros e falsos, dificultando os filtros de deteção naturais das pessoas (OTAN, 2020a).

A OTAN pauta-se por comunicações baseadas em factos, refutando publicamente as principais narrativas de desinformação destinadas à Aliança, através do sítio em linha "*NATO-Russia: Setting the Record Straight*" (OTAN, 2021a), mas também em relatórios e textos em linha (NATO StratCom COE, 2019; OTAN, 2020a). Outras ações concretas são a intensificação da comunicação digital, a tradução de conteúdos em várias línguas (e.g.,

[8] NATO *Computer Incident Response Capability*.
[9] Como exemplo o NATO StratCom COE ou o CCDCOE.

canal de YouTube da OTAN em russo), informação oportuna aos *media*, ou brífingues aos *media* de países de leste, incluindo a Rússia (OTAN, 2020a).

Em suma, a OTAN, em linha com a UE, defende que a cooperação é fundamental para responder às AH, mas cada país tem de avaliar as suas próprias vulnerabilidades e aumentar a sua resiliência com uma abordagem integrada (*cfr.* Figura 12) (OTAN, 2020a).

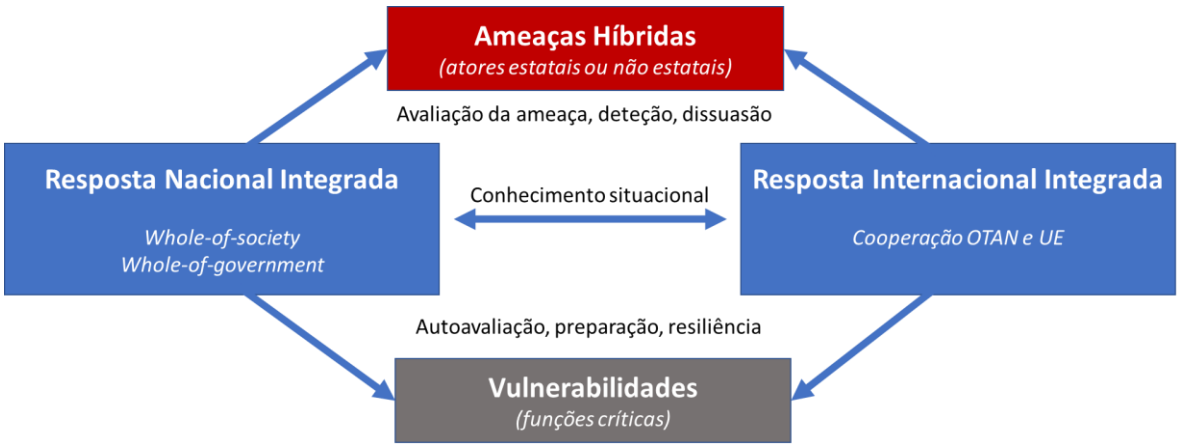

Figura 12 – Abordagem para o combate a AH

Fonte: Adaptado a partir de Giannopoulos et al. (2020).

4.3 A resposta nacional

Sendo as AH um assunto transversal, não existe uma área governativa onde recaia a responsabilidade de resposta, mas todas devem contribuir e tornarem-se resilientes (Alves, 2020). Nesse âmbito, existe uma rede interministerial para as AH, liderada pelo Ministério dos Negócios Estrangeiros, que acompanha e participa no desenvolvimento dos trabalhos sobre as ameaças híbridas.

Relativamente à desinformação, a ERC é a entidade nacional que supervisiona a aplicação do Código de Conduta contra a Desinformação pelas plataformas digitais. Segundo Sousa (2021), embaixador para a ciberdiplomacia e ponto de contato nacional do SAR, "[…] Portugal tem um regulador de uma geração muito avançada […] que se ocupa da regulação da liberdade de informação em todos os domínios […]", incluindo os sítios na internet das televisões e dos jornais, colocando-nos na vanguarda da UE. A ERC preocupa-se com falsos sites de informação (*cfr.* Figura 13) de autoria desconhecida e fins que aparentam ir além do lucro da publicidade, mas também com o combate à desinformação (rigor informativo) que possa provir de órgãos de comunicação social (OCS) (ERC, 2019). Os desafios da ERC neste domínio são muitos e estão detalhados no relatório intitulado "A Desinformação – Contexto Europeu e Nacional" (ERC, 2019).

De facto, o trabalho da ERC não se tem revelado fácil, exemplo disso foi a polémica ao ter registado o sítio "Notícias Viriato" como publicação informativa, quando este tinha sido identificado como sítio de propaganda pelo Medialab do ISCTE/Instituto Universitário de Lisboa e não existindo à data qualquer jornalista associado, condição obrigatória para registo (Câncio, 2020). Apesar deste incidente pontual, a listagem de registos na ERC pode ser consultada no seu sítio oficial, e é uma forma de verificar a credibilidade das fontes de informação em linha.

Figura 13 - Sites de *Fake News* em Portugal

Fonte: Disponível em Os truques da imprensa portuguesa (2018).

Desde 2018, aquando do lançamento do primeiro verificador de factos, intitulado Polígrafo[10], diversos OCS dedicaram-se à mesma causa.

Ao contrário de diversos países da UE, a legislação nacional não determina imputação e sanção à produção e difusão de conteúdos integrados no conceito de desinformação (ERC, 2019, p. 67). Segundo Sousa (2021), dar ao Estado a possibilidade de ajuizar conteúdos pode ser considerado censura, e a desinformação não deve ser considerada crime, devendo-se sim, apostar numa comunicação estratégica eficaz.

De encontro às recomendações da UE para eleições livres e justas, Portugal criou uma rede eleitoral com diversas autoridades responsáveis pelo acompanhamento e execução das regras relativas às atividades em linha, "[…] sendo a ERC um dos seus membros, bem como o MAI, a CNE, a ANACOM, a CNPD, entre outras […], porém os mecanismos existentes são parcos." (ERC, 2019, p. 70).

[10] https://poligrafo.sapo.pt/

A responsabilidade no combate à desinformação recai no cidadão, que deve ser proativo e verificar a veracidade da informação antes de partilhar, para isso é fundamental promover a literacia mediática (ERC, 2019).

4.4 Abordagens de resiliência à desinformação

Na revisão de literatura efetuada, identificámos apenas um trabalho, o de Humprecht et al. (2020), que se adequa a um modelo de resiliência nacional face à desinformação.

Esse modelo identifica indicadores mensuráveis e as métricas que lhes permitiram comparar a resiliência de sociedades de diversos países. Os indicadores, representados na Figura 14, são enquadrados nas dimensões política, informação (*media*) e económica. Salienta-se que as fontes de dados usadas são públicas e permitem uma aplicação imediata da abordagem.

Dimension	Measurable Indicator	Data Source
Political Environment		
Populist Communication	Vote share of populist parties 2018 Change in vote share 2008–2018 Speeches of political leaders	Timbro Authoritarian Populism Index (2019), Aalberg et al. (2016), Van Kessel (2015) Global Populism Database (2019)
Societal Polarization	Polarization of society Online media fractionalization	V-Dem (2019) V-Dem (2019)
Media Environment		
Trust in News Media	Overall trust in news media Trust in news that I use	Digital News Report (2018)
Strength of PSB	Market share of public TV Public revenue (license fee)	Brüggemann et al. (2014)
Shared Media	Share of most used media outlets/ programs	Digital News Report (2019)
Economic Environment		
Size of Online Media Market	No. of online users per country	World Bank Data (2017)
Social Media News Consumption	Social media use for news Sharing news on social media	Digital News Report (2018)
Outcome		
Exposure to Online Disinformation	Reported exposure to dis- and misinformation	Digital News Report (2018)

Note. PSB = public service broadcasting.

Figura 14 - Dimensões, indicadores e fonte dos dados

Fonte: Disponível em Humprecht et al. (2020).

Destaca-se que ao considerarem como indicador, a votação em partidos populistas, assumem que o populismo está associado à desinformação, o que poderá ser verdade, mas pode ser um indicador tendencial (R. Aranha, entrevista via *Microsoft Teams*, 19 de março de 2021).

Em resposta à QD2, com base na investigação e contexto da UE, OTAN e Portugal, e na abordagem de Humprecht et al. (2020), deduziram-se 28 indicadores de resiliência nacional face à desinformação (*cfr.* Quadro 7 do Apêndice B). O nível de polarização da sociedade, o nível de confiança nos *media*, a existência de uma plataforma pública para difundir campanhas de desinformação ou a existência de uma célula de fusão nacional (e.g., integrada nos serviços de informações), são alguns dos indicadores de resiliência elencados. Os indicadores deduzidos, foram submetidos a validação pelos entrevistados (*cfr.* Capítulo 6) e são explicados detalhadamente (descrição e motivação) no Apêndice D.

5. Resiliência do ciberespaço

Este capítulo visa investigar possíveis indicadores de ciber-resiliência, à luz das respostas da UE, OTAN e Portugal, e de abordagens de referência, procurando responder à QD3.

5.1 A resposta da UE

Os incidentes na Estónia (2007) deram um impulso, mas só em 2016 a UE assume uma abordagem holística e um papel centralizador na elaboração de políticas e medidas (visível *cfr*. Figura 15) englobando a proteção de infraestruturas-críticas, cibersegurança, ciberdefesa e a resposta às AH (Beláz, 2019).

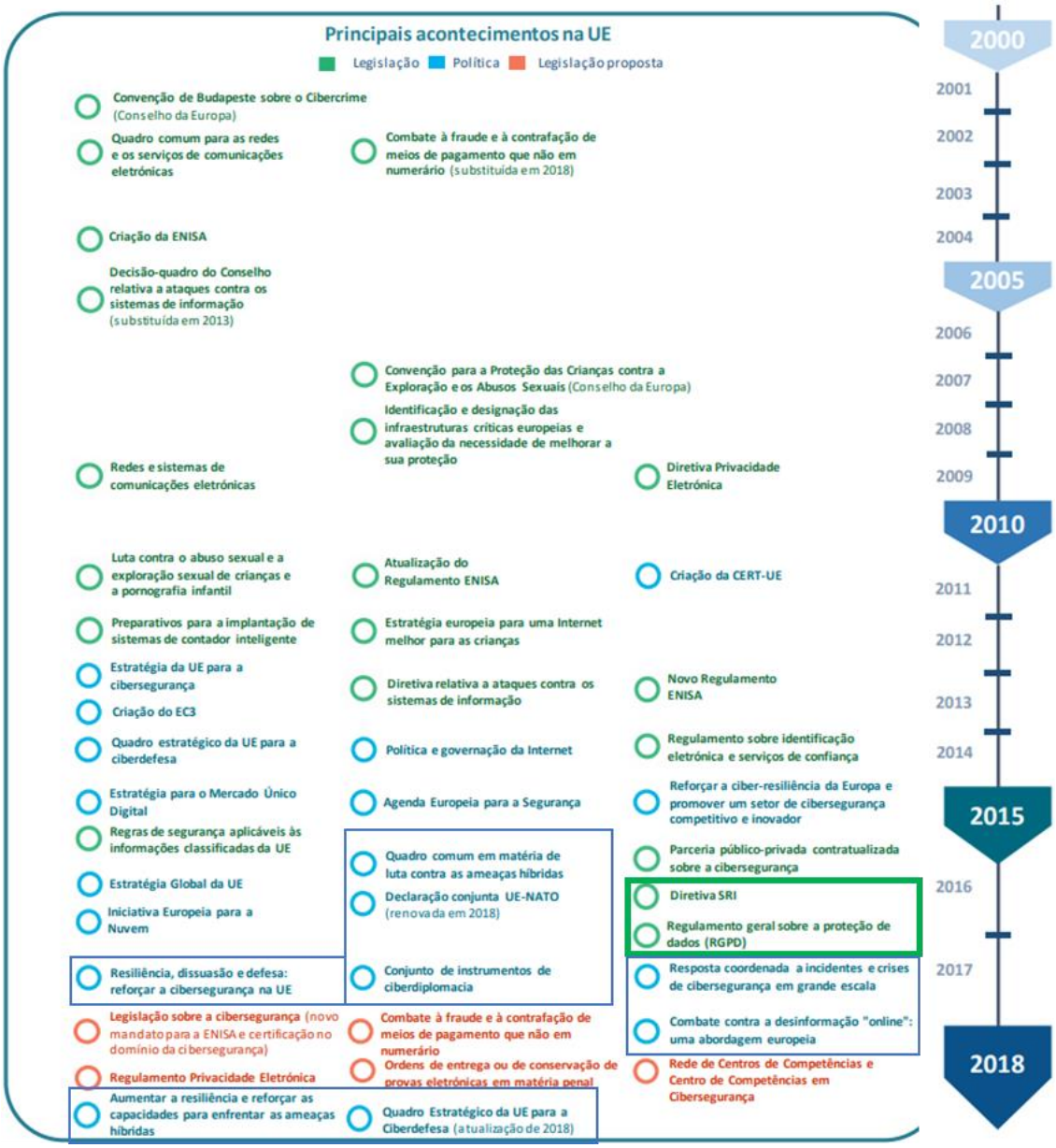

Figura 15 - Políticas e legislação da UE em matéria de cibersegurança

Fonte: Adaptado a partir de Tribunal de Contas Europeu (TCE) (2019).

A Diretiva 2016/1148, de Segurança das Redes e Sistemas de Informação (SRI), obriga os Estados-Membros a adotarem estratégias nacionais e designar autoridades competentes e equipas de resposta a incidentes de segurança informática (CSIRT), bem como a obrigatoriedade de notificação de incidentes.

O Regulamento Geral sobre a Proteção de Dados (RGPD) (2016/679), impôs obrigações com o objetivo de proteger os dados pessoais dos cidadãos.

Em 2017, a UE instituiu um conjunto de instrumentos de ciberdiplomacia, incluindo sanções, já com efeitos práticos, e.g., resposta ao caso WannaCry (Conselho da UE, 2020).

O Regulamento (2019/881) da Cibersegurança (*Cybersecurity Act*), cria um quadro de certificação europeu e reforça as competências da ENISA, focando a redução de vulnerabilidades na origem através da certificação de produtos (e.g., IoT), serviços e processos digitais.

A recente Estratégia Europeia de Cibersegurança de dezembro de 2020, foca que é necessário ultrapassar a falsa dicotomia existente entre «em linha» e «fora de linha» e quebrar uma abordagem compartimentada (CE, 2020b). A nova estratégia apresenta algumas iniciativas centrais (*cfr.* Figura 16), como a criação de um *Cyber Shield* (rede de centros de operações de segurança) e uma *Joint Cyber Unit* (resposta mais eficaz às ciberameaças).

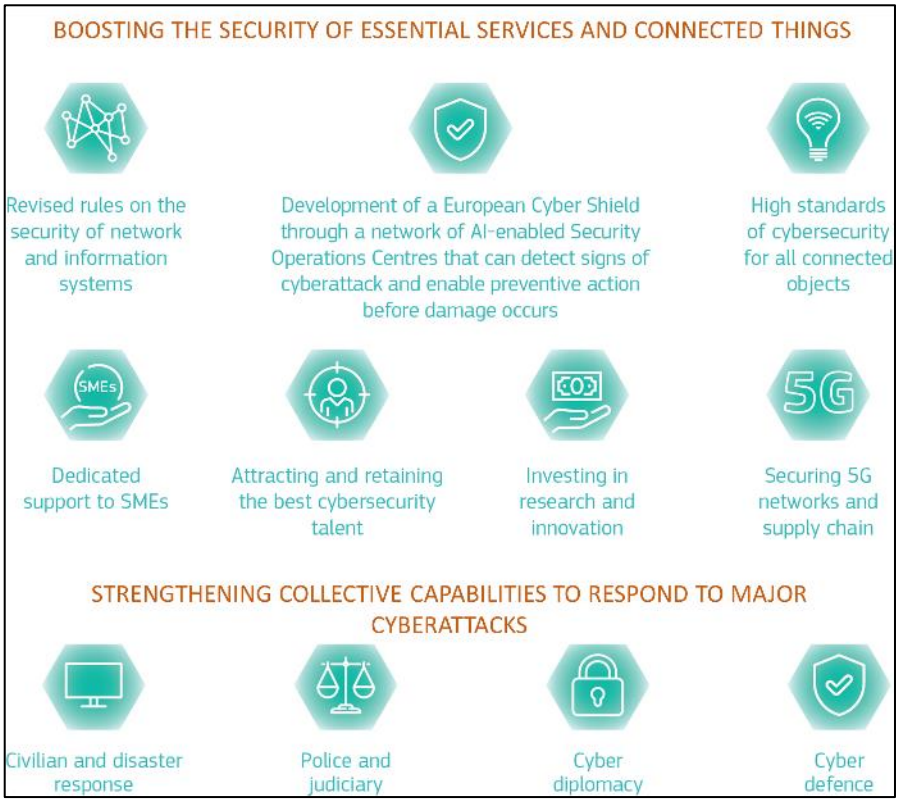

Figura 16 - Medidas da estratégia europeia de cibersegurança para a década digital

Fonte: Adaptado a partir de CE (2020d).

Na nova estratégia é proposta a SRI 2.0, abrangendo mais setores de atividade e promovendo a gestão do risco das cadeias de fornecimento (e.g., 5G) e as ações de supervisão das autoridades nacionais. É também proposta uma nova Diretiva sobre Resiliência das Entidades Críticas nos setores da energia, transportes, banca, infraestruturas dos mercados financeiros, saúde, água potável, águas residuais, infraestruturas digitais, administração pública e espaço, sujeitando-as a avaliações regulares de risco.

Embora a SRI pretenda "[…] atingir um elevado nível de segurança em toda a UE, centra-se explicitamente em alcançar uma harmonização mínima e não máxima […]" (TCE, 2019, p. 23). A SRI 2.0 deverá reforçar esse nível de segurança.

Relativamente à estrutura, destacamos a ENISA enquanto órgão essencialmente consultivo, o Centro Europeu da Cibercriminalidade da Europol (EC3) reforça a resposta à cibercriminalidade, a CERT-UE dá apoio aos órgãos da UE, o SEAE é responsável pela articulação da ciberdefesa e ciberdiplomacia, e alberga os centros de recolha e análise de informações, e por fim, a Agência Europeia de Defesa (EDA) visa desenvolver as capacidades de ciberdefesa (TCE, 2019). Em Bucareste, será o novo Centro Europeu de Competências em Cibersegurança para coordenar a investigação e inovação (Conselho da UE, 2021).

A UE tem apostado na investigação, desenvolvimento e inovação (I&D&I), com incentivos no quadro da *Permanent Structured Cooperation* (PESCO) e do Fundo Europeu de Defesa (FED). Destaca-se a co-liderança de Portugal na Disciplina de Ciberdefesa da UE e a liderança nacional do Projeto *Cyber Academia and Innovation Hub* (CAIH).

Por fim, realça-se a Bússola Estratégica Europeia, a estratégia em estudo que vigorará a partir de 2022, com enfoque na gestão de crises e resiliência (Presidência Portuguesa do Conselho da UE, 2021).

Em perspetiva, o CNCS refere-se à UE como uma entidade reguladora que impede uma digitalização descontrolada, reorientando-a (CNCS, 2021a).

5.2 A resposta da OTAN

O esforço da OTAN nesta matéria começou após os incidentes na Estónia e Geórgia, mas só na cimeira de Varsóvia em 2016, o ciberespaço foi reconhecido como um domínio de operações (OTAN, 2021b). A resiliência foi um conceito central da cimeira, focando a cooperação com a UE e a necessidade de garantir o funcionamento das redes cibernéticas, a capacidade governativa e os serviços críticos, mesmo sob condições de crise (Alves, 2020, p. 7).

Na sequência da cimeira de 2016, Portugal e outros Estados-Membros ratificaram o *Cyber Defence Pledge,* assumindo o compromisso de melhorar a sua resiliência e a capacidade de responder a ciberataques, incluindo aqueles inseridos em campanhas híbridas (OTAN, 2016).

Em 2018, na cimeira de Bruxelas, foi decidido criar um *Cyberspace Operations Centre* (CyOC) para coordenação da atividade operacional da OTAN no ciberespaço, bem como o acordo dos aliados em disponibilizar as suas capacidades nacionais para as operações (OTAN, 2021b). Tendo em conta a dificuldade de imputação dos ciberataques, entende-se a posição cautelosa da OTAN, ao assumir uma postura maioritariamente defensiva e relegando o caráter ofensivo das OpCiber aos designados *Sovereign Cyber Effects Provided Voluntarily by Allies* (SCEPVA) (AJP-3.20, 2020). Adicionalmente, os membros da OTAN têm diferentes visões sobre as OpCiber violarem ou não a soberania nacional, o que torna muito difícil uma resposta coletiva (Pomerleau, 2019).

A OTAN foca a ciberdefesa na proteção das próprias redes (incluindo operações e missões) e no aumento da resiliência em toda a Aliança. (OTAN, 2021b). Para aumento da resiliência, a OTAN tem incentivado projetos de I&D e tem aposta clara na educação e treino, aqui, destaca-se o papel de Portugal, na "[…] liderança do projeto NATO *Smart Defense Multinational Cyber Defence Education and Training* (MNCDE&T) […] e na instalação da NATO *Communications and Information Academy* (NCI *Academy*) em Oeiras." (P. Nunes, 2020, p. 17).

5.3 A resposta nacional

Apesar dos esforços das organizações internacionais a que Portugal pertence, os Estados-Membros são os principais responsáveis pela sua própria cibersegurança.

Na sequência da RCM n.º 26/2013, "Defesa 2020", de 11 de abril, o Ministro da Defesa Nacional (MDN), determinou a criação do Centro de Ciberdefesa (CCD), que surge em 2015 sob a tutela do Estado-Maior-General das Forças Armadas (EMGFA), (RCM n.º 26, 2013). Na diretiva estratégica do EMGFA 2018-2021 (DEEMGFA), é identificado o objetivo estratégico de dinamizar a edificação da capacidade de ciberdefesa nacional, demonstrando que a capacidade (onde se inclui a ofensiva conforme ENSC 2019-2023) está numa fase embrionária, sendo os recursos humanos uma grave limitação (EMGFA, 2018; P. Nunes, 2020).

Aprovado no Decreto-Lei n.º 69/2014 surge o CNCS, com responsabilidade de coordenação operacional e autoridade nacional em matéria de cibersegurança relativamente

ao Estado e operadores de infraestruturas críticas. O CNCS transpôs a Diretiva SRI para a legislação nacional (Lei n.º 46/2018), sendo a entidade que centraliza as notificações de incidentes e comunicação com as demais estruturas nacionais e internacionais. A resposta coordenada aos incidentes de cibersegurança é garantida pelo CERT.PT do CNCS e a rede de CSIRT, bem como o designado "[…] Grupo dos Quatro (G4), composto pelo CNCS, CCD, Unidade Nacional de Combate ao Cibercrime e Criminalidade Tecnológica (UNC3T) e Serviços de Informações de Segurança (SIS)." (P. Nunes, 2020, p. 15). A articulação para a cooperação nacional e internacional está sintetizada na Figura 17.

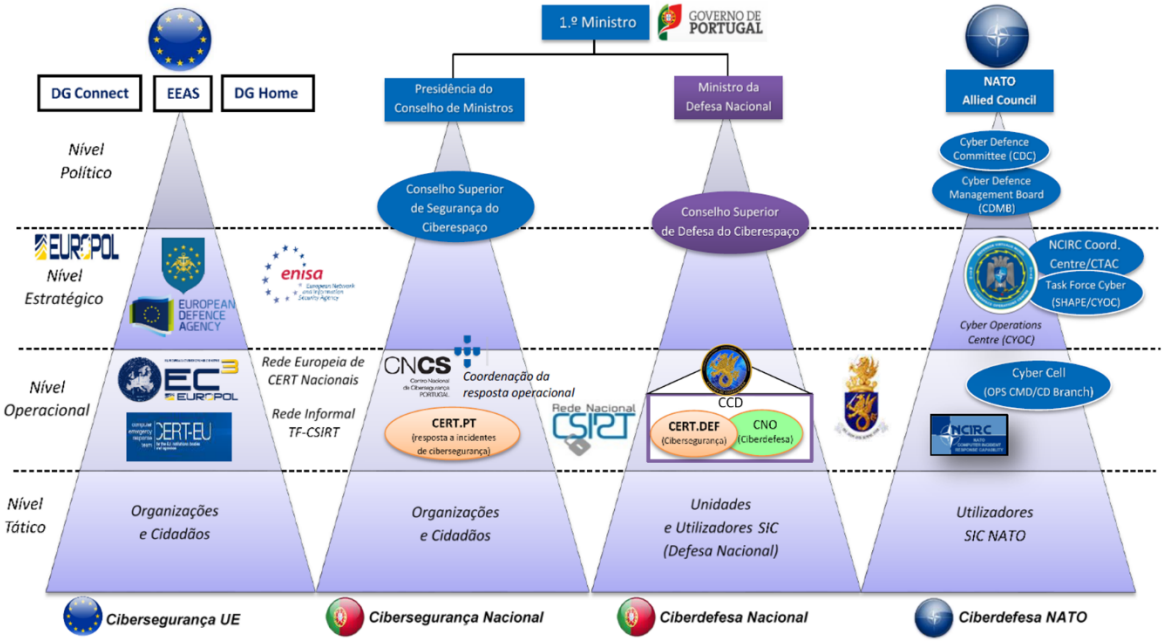

Figura 17 - Articulação da estrutura de ciberdefesa (panorama nacional e internacional)

Fonte: Adaptado a partir de Nunes (2020, p. 33).

No âmbito das atribuições do CNCS, foi proposto em 2019 o Quadro Nacional de Referência para a Cibersegurança (QNRCS), com base em normas internacionais de referência, para que qualquer entidade possa cumprir (voluntariamente) os requisitos mínimos de cibersegurança (CNCS, 2019).

É importante destacar que o QNRCS prevê a gestão de cibersegurança como um processo contínuo focando aspetos humanos, tecnológicos, processuais e físicos (e.g., redundância), abordando a gestão do risco e resiliência. Por exemplo, a organização deve identificar os requisitos de resiliência necessários para suportar a prestação de serviços críticos, deve planear a continuidade do negócio (em níveis aceitáveis pré-definidos) na sequência de um incidente disruptivo, entre outras.

Os objetivos do QNRCS estão organizados por categorias (*cfr.* Figura 18) e subcategorias "[…] onde se explanam medidas técnicas e processuais […] que permitam às organizações melhorar a sua capacidade de proteção […]" (CNCS, 2019, p. 15).

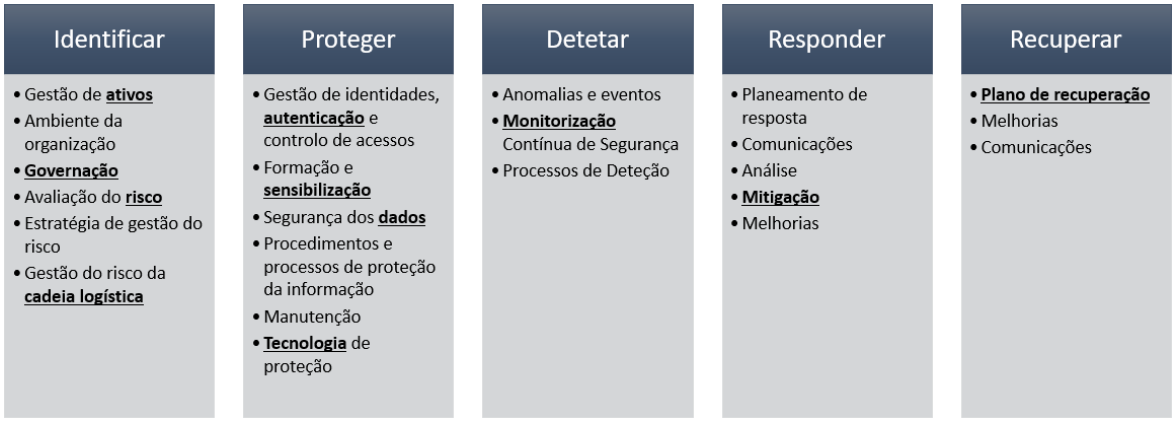

Figura 18 - Objetivos e categorias do QNRCS

Fonte: Adaptado a partir de QRNCS (CNCS, 2019).

Importa referir, de acordo com a Estratégia para a Inovação e Modernização do Estado e da Administração Pública 2020-2023, aprovada na RCM n.º55/2020, 80 % dos organismos da Administração Pública (AP) deverão ser certificados em conformidade com o QNRCS. Este parece ser um passo, em consonância com aquilo que virá a ser espelhado na SRI2.0, em que o CNCS deverá assumir-se como Autoridade Nacional de Certificação da Cibersegurança (CNCS, 2021b). Contudo, resta perceber quais os requisitos de segurança e medidas aplicáveis, pois o art.º 14 da Lei n.º46/2018, define apenas que devem ser "[…] proporcionais para gerir os riscos que se colocam à segurança das redes e dos sistemas de informação que utilizam.".

A preparação civil, é vertida no Sistema Nacional de Planeamento Civil de Emergência (SNPCE) (Decreto-Lei n. º 43/2020, de 21 de julho, 2019), liderado pela Autoridade Nacional de Emergência e Proteção Civil (ANEPC), que integra diversas comissões especializadas, relevando-se a Comissão de Planeamento de Emergência (CPE) da Cibersegurança.

Por fim, importa referir que a ENSC 2019-2023, define como objetivo estratégico "maximizar a resiliência". Os eixos de intervenção, incidem no reforço das estruturas de cibersegurança e ciberdefesa, na educação e sensibilização, proteção e resposta às ameaças, investigação, inovação e cooperação. A ENSC, prevê que é necessário antecipar a emergência e a adoção atempada de ações que acrescentem resiliência. A cooperação (nacional e internacional) e uma resposta em rede integrada entre os vários setores (públicos

e privados), a par de uma sociedade resiliente com competências digitais, são fatores fundamentais para a resiliência.

5.4 Abordagens de ciber-resiliência

O *National Institute of Standards and Technology* (NIST), define ciber-resiliência como a capacidade de "[…] *anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.*" (Ross et al., 2019). Os objetivos de ciber-resiliência são descritos no Quadro 1.

Quadro 1 - Objetivos da ciber-resiliência

Objetivo	Descrição
Antecipar	Estar informado e preparado para a adversidade
Resistir	Continuar as funções essenciais apesar das adversidades
Recuperar	Restaurar todas as funções durante e após a adversidade
Adaptar	Modificar as funções e/ou a capacidade para prever mudanças no ambiente técnico, operacional, ou da ameaça.

Fonte: Adaptado a partir de Ross et al. (2019).

A ciber-resiliência pode aplicar-se a um pequeno aparelho eletrónico, a um sistema complexo de *software* e *hardware*, a uma organização ou a um Estado (Ross et al., 2019, p. 1). Um Estado ciber-resiliente, pode suportar ciberataques ou outros perigos ou falhas no ciberespaço, e continuar a operar nesse ambiente degradado desempenhando as suas funções essenciais.

Ao reduzir o risco das funções da organização (e.g., do Estado) dependerem do ciberespaço, procurando diminuir (ou anular) o impacto e a probabilidade de ocorrência de uma ameaça, aumentamos a ciber-resiliência (Ross et al., 2019, p. 78). As diversas técnicas para aumentar a ciber-resiliência, apesar da maioria se aplicar numa perspetiva de engenharia de sistemas, são detalhadas no documento do NIST da autoria de Ross et al. (2019).

Destacamos também o trabalho de Spidalieri (2015), em que avalia a ciber-resiliência dos EUA, baseado na metodologia *Cyber Readiness Index* (Hathaway, 2015), criada para avaliar a maturidade de um Estado em matéria de cibersegurança (*cfr*. Figura 19).

Figura 19 - Comparação da ciber-resiliência de Estados dos EUA

Fonte: Disponível em Spidalieri (2015).

Na Figura 19, pode ser observado o método utilizado, com critérios que incluem o planeamento estratégico, capacidade de resposta a incidentes, resposta ao cibercrime, partilha de informação e investigação e desenvolvimento.

Outro projeto, do *World Economic Forum* (WEF) por Keys et. al. (2016), propõe uma abordagem baseada no modelo de cibersegurança para infraestruturas críticas do NIST *Cybersecurity Framework* (2014) e no modelo de Linkov (2013). As colunas do Quadro 2 representam os objetivos tradicionais de resiliência a desastres, com a adição do "detect" inspirado na NIST *Cybersecurity Framework* (2014) (Keys et. al., 2016). Nas linhas do Quadro 2 tem-se os domínios da doutrina *Network-Centric Warfare*: físico, informação, cognitivo e social. Os indicadores que completam o quadro, são uma combinação dos indicadores propostos no modelo do NIST e de Linkov, e são detalhados no trabalho de Keys et. al. (2016).

Quadro 2 - Estrutura base do quadro de ciber-resiliência do WEF

	Plan & Prepare	*Detect*	*Absorb*	*Recover from*	*Adapt to*
Physical					
Information					
Cognitive					
Social					

Fonte: Disponível em Brianna Keys et al. (2016).

Em resposta à QD3, com base na investigação e contexto da UE, OTAN e Portugal, e nas abordagens descritas acima, deduziram-se 58 indicadores de ciber-resiliência nacional (*cfr*. Quadro 6 do Apêndice B). A maturidade de cibersegurança (e.g., nível de implementação do QNRCS) das entidades críticas, o nível de risco e evolução das AH no ciberespaço em Portugal, a capacidade das FFAA conduzirem OpCiber (ofensivas e defensivas), a agilidade dos canais de cooperação (internos e externos), são alguns dos indicadores de ciber-resiliência elencados. Os indicadores deduzidos, foram submetidos a validação pelos entrevistados (*cfr*. Capítulo 6) e são explicados detalhadamente (motivação e descrição) no Apêndice D.

6. Critérios e indicadores de resiliência contra AH

Este capítulo responde à QC, com um primeiro subcapítulo onde se faz um enquadramento e explicação da abordagem, e um segundo e terceiro onde se propõem os indicadores de resiliência nacional face à desinformação e indicadores da ciber-resiliência nacional, respetivamente.

6.1 Enquadramento e abordagem

6.1.1 Resiliência e a relação com o modelo conceptual das AH

Os modelos conceituais do HybridCoE (2020) e do MCDC (2019), referem que as AH não são responsabilidade única de uma entidade especifica e é necessário adotar uma abordagem *whole-of-government*, que promove a aproximação, confiança e partilha de informação regular entre organismos do estado (civis e militares), e uma abordagem holística *whole-of-society* (extensível à sociedade e setor privado), reunindo atores civis, militares e políticos num novo ecossistema de segurança preparado para responder a crises de forma mais eficiente. O MCDC (2019) dá como exemplo as abordagens *whole-of-society* espelhada nas estratégias da Suécia ("*Total Defence*"), Noruega ("'*Support and Cooperation*"), Finlândia ("*Comprehensive Security*"), entre outros.

Quanto ao papel da defesa, conforme referiu o secretário-geral da OTAN (2020), "*our militaries cannot be strong if our societies are weak, so our first line of defence must be strong societies*", realçando, por exemplo, a dependência dos militares nas infraestruturas civis ou cadeias de abastecimento, quer para comunicações quer para transporte.

Em Portugal, está sob proposta a criação de um "[…] sistema de resiliência nacional […]" associado a um novo "[…] sistema nacional de gestão de crises […]" que responderá não só a AH como a qualquer outra ameaça ou risco (e.g., sismo), pretendendo-se uma abordagem *whole-of-government,* apoiada em tecnologias de *BigData* e Inteligência Artificial para apoio à decisão e partilha de informação (N.L. Pires, entrevista via *Microsoft Teams*, 09 de março de 2021).

Nesta linha de pensamento, *whole-of-government* e *whole-of-society*, a abordagem de resiliência proposta neste TII, subdivide-se em variáveis que representam as funções críticas de um Estado (PMESII), inspirada no modelo conceptual do MCDC.

6.1.2 Abordagem para a resiliência nacional

A abordagem conceptual relativa à resiliência social dos Estados-Membros da UE, desenvolvida por Manca et. al. (2017), propõe um processo genérico que compreende a obtenção de indicadores, o processo analítico (métricas e processamento) e a visualização

(e.g., *dashboard*), para que se possa monitorizar a resiliência e identificar pontos de melhoria. Num processo continuo de lições aprendidas, devemos perceber quais os indicadores que mais contribuem ou quais devem ser removidos e substituídos por outros, para melhor aferir a resiliência (Manca et al., 2017).

Com base na abordagem descrita, destacam-se os trabalhos com a mesma coautora, Manca et al. (2020) e (CE, 2020c), que propõe um conjunto de indicadores para as variáveis sociais, económicas e de saúde, que resultam num protótipo de *dashboard* (cfr. Figura 20) para comparar países da UE.

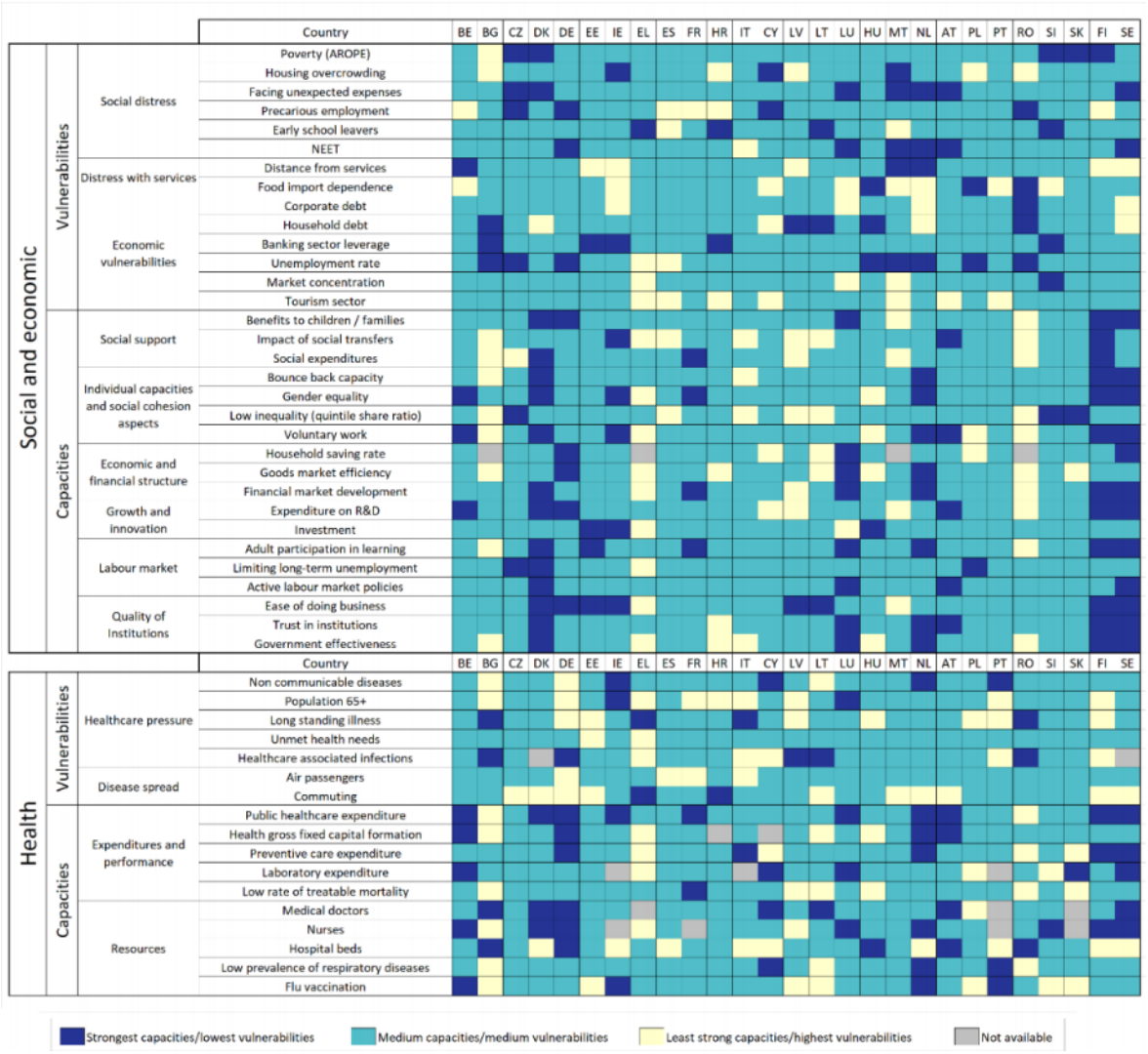

Figura 20 - Protótipo de *dashboard* de resiliência económica, social e de saúde da UE

Fonte: Disponível em CE (2020c).

No presente TII, focou-se a identificação de indicadores. O processo analítico e a visualização, não sendo objeto deste estudo, terão que ser analisadas em trabalhos futuros para materializar a abordagem numa ferramenta prática que permita monitorizar e melhorar a resiliência nacional.

Por dedução, através da análise das ações e respostas face a AH (descritas nos Capítulos 4 e 5) da UE, OTAN e Portugal, foram obtidos os indicadores inicialmente propostos e exarados no guião de entrevista (*cfr.* Apêndice B). Os indicadores, inspirados na revisão de literatura e adequados ao contexto nacional, têm como requisito serem mensuráveis (e.g. uma percentagem, variação, sim/não).

Através das entrevistas a seis especialistas, validaram-se alguns dos indicadores propostos e incluíram-se outros (*cfr.* Apêndice C). A inclusão de novos indicadores, foi efetuada após análise do conteúdo das entrevistas, utilizando o método das relações por coocorrências (Lúcio Santos & Lima, 2019, p. 120). Assim, considerou-se um indicador válido (i.e., indicador selecionado) desde que tivesse duas ou mais ocorrências, com avaliação média igual ou superior a 3,5 (numa escala de 1 - pouco importante a 5 - muito importante). A decisão de optar pelo valor 3.5, surge na sequência do contributo de Miguel Correia (entrevista via correio eletrónico, 09 de março de 2021) que sugeriu priorizar indicadores, potenciando a aplicabilidade prática dos mesmos. No caso da resiliência nacional face à desinformação selecionaram-se 23 de um total de 52 indicadores. No caso da ciber-resiliência selecionaram-se 54 de um total de 114 indicadores.

6.2 Indicadores de resiliência nacional contra a desinformação

Conforme referido, optou-se por identificar indicadores associados a cada uma das funções críticas do Estado (PMESII). No entanto, importa salientar a importância do domínio Social, pois as campanhas de desinformação e outros métodos híbridos interligados, procuram afetar a homogeneidade da cultura e da sociedade do Estado alvo. Contudo, existe uma clara ligação entre domínios, por exemplo, a ciberespionagem pode ser o primeiro passo para obter *Informação* para influenciar a opinião pública (*Social*), as perceções e o discurso, minando a discussão e o processo *Político* no Estado alvo.

Importa também realçar, que o combate à desinformação é um tema sensível devido ao direito à liberdade de expressão, ou seja, é necessário evitar que os mecanismos se tornem em censura ou controle da opinião pública (O. Rocha, entrevista via correio eletrónico, 10 de março de 2021).

Os indicadores selecionados, estão espelhados naquilo que designamos de matriz de resiliência nacional face à desinformação (cfr. Quadro 3). O farol dos indicadores propostos, são os quatro pilares do plano de ação da UE para combate à desinformação (CE, 2018a): melhorar a deteção e denúncia, reforçar a coordenação, mobilizar o setor privado e sensibilizar as pessoas.

Apesar dos indicadores serem autoexplicativos, no Apêndice D, encontra-se informação detalhada sobre a motivação e definição dos mesmos.

Quadro 3 - Proposta de matriz da resiliência nacional face à desinformação (AH)

	Indicadores de resiliência nacional face à desinformação no âmbito das ameaças híbridas
Ações / Domínios	Melhorar (detetar, analisar, denunciar); Reforçar coordenação; Mobilizar o setor privado; Sensibilizar as pessoas
Político	**P.1.** Está definida a coordenação entre instituições e uma definição clara dos fluxos de partilha de informação e colaboração? **P.2.** Existe uma estratégia nacional que contemple resposta à desinformação no âmbito das AH? **P.3.** Existe uma estratégia de comunicação para preparar a população ou contrariar narrativas de desinformação? **P.4.** Existem mecanismos de cooperação internacional no domínio político-diplomático para responder à desinformação no âmbito das AH?
Militar	**M.1.** Agilidade na partilha, cooperação e coordenação com as autoridades civis **M.2.** Capacidades para detetar, analisar e denunciar desinformação ao nível militar **M.3.** Exercícios militares que contemplem o combate à desinformação (que vise denegrir a instituição ou liderança militar) **M.4.** Existe um plano de comunicação estratégico que reforce a união e prestígio da instituição militar e vise anular efeitos de desinformação?
Económico	**E.1.** Investimento em I&D para criação de mecanismos de combate à desinformação
Social	**S.1.** Nível de polarização da sociedade (e.g. V-Dem https://www.v-dem.net/) **S.2.** Nível de confiança nos media (e.g. digitalnewsreport.org/interactive/) **S.3.** Percentagem de cidadãos que usa redes sociais como fonte de notícias (e.g. digitalnewsreport.org/interactive/) **S.4.** Existem mecanismos para identificação de audiências alvo mais vulneráveis às campanhas de desinformação?
Informação	**I.1.** Quantidade de mecanismos (e.g. *fact checks*), por OCS, para detetar, analisar e denunciar as fontes de desinformação? **I.2.** Existe um sistema de informação comum para conhecimento situacional da desinformação aos diferentes níveis e entre as diferentes instituições? **I.3.** Nível de risco e registos da evolução da desinformação em Portugal **I.4.** Existe uma plataforma pública centralizada para difundir campanhas de desinformação (e.g. https://euvsdisinfo.eu/)? **I.5.** Existem mecanismos para certificação de órgãos de comunicação social na internet? **I.6.** Variação do volume de ações de sensibilização - comunicação estratégica e educação (literacia mediática) **I.7.** Ações de formação para jornalistas
Infraestruturas	**II.1.** Existe um gabinete de comunicação estratégica? **II.2.** Existe uma Célula de Fusão Nacional para aumentar o conhecimento situacional? **II.3.** Existem recursos e infraestruturas dedicadas à deteção de campanhas de desinformação no ciberespaço (inclui deteção de redes de distribuição com *bots* ou *trolls*)?

6.3 Indicadores de ciber-resiliência nacional

No Quadro 4 está esquematizada a matriz de ciber-resiliência com os indicadores selecionados e adequados ao contexto nacional, inspirada nos modelos propostos por Keys et al. (2016) e Spidalieri (Spidalieri, 2015), apresentados anteriormente. Pretende-se que a matriz proposta, possa vir a contribuir para uma visão da ciber-resiliência nacional face a AH (ou outras) no ciberespaço, num processo dinâmico de adaptação da mesma.

Na matriz, o domínio Infraestruturas integra o conjunto de entidades abrangidas pela Lei n.º 46/2018, de 13 de agosto, embora estas sejam transversais aos outros domínios (e.g., autarquias são também do domínio Político).

Quadro 4 - Proposta de matriz da ciber-resiliência nacional face a AH

		Indicadores de ciber-resiliência face a ameaças híbridas					
Objetivos resiliência ->		**Antecipar**			**Resistir**	**Recuperar**	**Adaptar**
Domínios	**Objetivos cibersegurança**	**1. Identificar/Planear**	**2. Proteger**	**3. Detetar**	**4. Responder**	**5. Recuperar**	**6. Adaptar**
CS	**Infraestruturas** Operadores Infraestruturas críticas e Svc. essenciais Administração Pública Prestadores de Serviços Digitais	**CS.1.1.** Maturidade QNRCS (Identificar) **CS.1.2.** Foco em ativos críticos **CS.1.3.** Assume ataques com sucesso no planeamento **CS.1.4.** Certifica ativos críticos **CS.1.5.** Exercícios e treinos	**CS.2.1.** Maturidade QNRCS (Proteger) **CS.2.2.** Foco em ativos críticos	**CS.3.1.** Maturidade QNRCS (Detetar) **CS.3.2.** Agilidade na partilha e colaboração **CS.3.3.** Deteção de redes de distribuição de desinformação	**CS.4.1.** Maturidade QNRCS (Responder) **CS.4.2.** Capacidade de coordenação da resposta **CS.4.3.** Colaboração	**CS.5.1.** Maturidade QNRCS (Recup.) **CS.5.2.** Foco nos ativos críticos **CS.5.3.** Agilidade	**CSD.6.1.** Rever e corrigir configurações/ procedimentos **CSD.6.2.** Melhorar partilha de informação
CD	**Militar** (Forças Armadas)	**CD.1.x=CS.1.x** **CD.1.6.** Garante diversidade (fornecedores, arquitetura) **CD.1.7.** Projeção de poder	**CD.2.x=CS2.x** **CD.2.3.**Projeção de poder e Dissuasão	**CD.3.x.=CS.3.x.**	**CD.4.x.=CS.4.x.** **CD.4.4.** Capacidade de OpCiber (ofensivas e defensivas)	**CD.5.x.=CS.5.x**	
S	**Social**	**S.1.** Oferta formativa em cibersegurança **S.2.** Níveis de ensino onde se ministram conteúdos de cibersegurança **S.3.** Observação de atitudes e comportamentos (e.g., fonte observatório do CNCS) **S.4.** Campanhas de sensibilização para a cibersegurança nacional					
E	**Económico**	**E.1.** Investimento privado e público em cibersegurança incluindo I&D&I (e.g., fonte observatório do CNCS) **E.2.** Mercado de trabalho de cibersegurança (e.g., fonte observatório do CNCS)					
P	**Político**	**P.1.** Existe uma estratégia de segurança no ciberespaço que contemple resposta a AH? **P.2.** Existe atribuição de competências na resposta a AH? **P.3.** Políticas de investimento em cibersegurança e ciberdefesa **P.4.** O regime jurídico da segurança do ciberespaço impõe obrigatoriedade de certificação ou requisitos de segurança suficientes (e.g., requisitos QNRCS pelo CNCS)? **P.5.** Existe um planeamento civil de emergência para fazer face a AH no ciberespaço? **P.6.** Existem autoridades nacionais competentes em matéria eleitoral com recursos adequados para responder a AH no ciberespaço?					
I	**Informação** (partilha)	**I.1.** Existe uma Célula de Fusão para AH ao nível nacional e interoperável com o da UE? **I.2.** Existe coordenação entre instituições e uma definição clara dos fluxos de partilha de informação e colaboração? **I.3.** Existe um sistema de informação comum para conhecimento situacional de AH aos diferentes níveis e entre as diferentes instituições? **I.4.** Nível de risco e registos da evolução das AH no ciberespaço em Portugal					

Nos domínios Infraestruturas e Militar, propõe-se como indicadores de resiliência, os níveis de maturidade das organizações em matéria de cibersegurança, de acordo com o QNRCS. Assim, para obter uma visão mais granular, optou-se por subdividir a matriz, para esses dois domínios, de acordo com os objetivos de segurança do QNRCS (identificar, proteger, detetar, responder e recuperar), aninhados dentro dos objetivos da *framework* de sistemas ciber-resilientes do NIST, que pressupõe ataques com sucesso (antecipar, resistir, recuperar e adaptar) (CNCS, 2019; Ross et al., 2019).

No âmbito Militar, acrescem aos indicadores de cibersegurança, os indicadores específicos que evidenciem a maturidade da capacidade de ciberdefesa, conforme salientado por Paulo Nunes (entrevista via mail, 08 de março de 2021).

As restantes dimensões PMESII, para além da Infraestruturas e Militar já referidas, são analisadas à luz da influência que possam ter na ciber-resiliência.

Por fim, importa referir que se assume o pressuposto que é ou será possível aferir a maturidade de cibersegurança das diferentes organizações, por exemplo, através de auditorias, reporte, questionários, ou exigência de eventuais certificações QNRCS ou equivalentes (e.g., ISO 27001), caso contrário, a medição da ciber-resiliência será sempre falaciosa e só será efetivamente aferida após um ciberataque.

Não será certamente simples verificar ou exigir a todas as entidades críticas que sejam certificadas de acordo com o QNRCS na sua plenitude, mas será possível mapear os controlos e processos de cibersegurança através de vários níveis de maturidade, a atingir de acordo com a dimensão, função, ou análise de risco de cada entidade ou setor. Por exemplo, o departamento de defesa dos EUA requer certificação de cibersegurança às empresas privadas que façam contratos de defesa, de acordo com um *Cybersecurity Maturity Model Certification* (CMMC) que se subdivide em 5 níveis de maturidade, sendo que o mais básico é tão simples como perguntar se a empresa tem software de antivírus, faz *updates* ao software de antivírus, ou se tem política de passwords (Todd Lopez, 2020). A framework de segurança do NIST também prevê diferentes níveis de maturidade (*tiers*) que refletem uma progressão de respostas (NIST, 2018). O QNRCS sugere que o "[…] documento seja interiorizado com espírito crítico […]" e cada organização deve adaptar o QNRCS face às suas especificidades (CNCS, 2019, p. 10). Contudo, seria muito útil haver a predefinição de um *perfil* de maturidade (i.e., controlos ou medidas técnicas e processuais a implementar) desejável para as organizações dos vários setores, em sintonia com regras emanadas pelos reguladores setoriais (e.g., Entidade Reguladora dos Serviços Energéticos).

A tendência será que a certificação em cibersegurança seja um processo natural no futuro, tal como é a higiene e segurança do trabalho atualmente (G. Marques, entrevista via *Microsoft Teams*, 11 de março de 2021).

Um tópico de discussão interessante seria a "[…] obrigatoriedade de as empresas realizarem ações de formação de cibersegurança (e.g., *e-learning*) utilizando, por exemplo, os cursos disponibilizados pelo CNCS." (R. Aranha, entrevista via *Microsoft Teams*, 19 de março de 2021).

7. Conclusões

As novas tecnologias vieram alavancar e potenciar as AH, um conceito antigo com nova designação. Por um lado, temos o problema da dependência tecnológica que aumenta as vulnerabilidades exploradas através de ciberataques. Por outro lado, temos as redes sociais e outros meios de comunicação, que permitem a comunicação em massa e a qualquer indivíduo ser uma fonte de notícias, potenciando a propaganda e a desinformação fácil.

As AH permitem atingir objetivos estratégicos sem ultrapassar o limiar da guerra convencional, quer seja porque os efeitos gerados não justificam uma resposta militar convencional, quer porque há ambiguidade em aspetos legais ou é impossível provar a imputação. Contudo, o assunto continua a ser também do foro militar, não só porque as AH podem combinar as técnicas do instrumento militar, mas também porque colocam em causa a soberania das nações.

A UE e a NATO despertaram para o problema após a anexação da Crimeia, onde a Rússia demonstrou como acentuar fracionamentos culturais e sociais com recurso a campanhas de desinformação. A pandemia veio acentuar as AH, com a ciberespionagem em torno de entidades que investigam terapêuticas, ou com a desinformação em torno das vacinas ou da origem do vírus COVID-19, criando a desconfiança em torno da eficácia das instituições e organizações.

Neste contexto, a resiliência surge como a melhor resposta para fazer face a vulnerabilidades e ameaças que são incertas. Assim, torna-se basilar propor critérios e indicadores da resiliência de Portugal face a AH no ambiente informacional.

O Hybrid CoE e a UE referem que as campanhas de desinformação e os ciberataques fazem frequentemente parte do ambiente das AH. O ciberespaço é um meio privilegiado para as AH (permite alcance, velocidade, ocultação, e a imputação é difícil) e sendo o próprio ciberespaço um domínio contido no ambiente informacional, optou-se por analisar duas dimensões: (i) ciber-resiliência; e (ii) a resiliência face à desinformação.

Face ao objeto de investigação, adotou-se um raciocínio dedutivo, assente numa estratégia de investigação qualitativa, consubstanciada num desenho de pesquisa baseado no estudo de casos, transpondo e contextualizando as respostas e recomendações da OTAN e da UE, bem como de outras abordagens de referência, para o caso nacional.

Através da revisão da literatura e da análise documental, para resposta às QD, o esforço de pesquisa centrou-se em perceber o fenómeno das AH e em deduzir indicadores que permitissem medir a resiliência nacional face a AH (informacional). Para resposta à QC,

foram realizadas entrevistas semiestruturadas a especialistas reconhecidos, que permitiram validar a adequabilidade e a importância dos indicadores deduzidos previamente.

Relativamente ao impacto das AH sob a lente do ambiente informacional, foi possível observar o seu uso desde a Guerra Fria aos novos métodos alavancados no ciberespaço. Portugal não é imune e está sujeito a ciberataques e desinformação. Os esforços globais de influência tendem a aumentar e é necessário criar resiliência não só no domínio tecnológico, mas também no domínio social. A dificuldade de imputação persiste como a grande dificuldade na resposta. Esse problema, só pode ser resolvido com a regulação, o reforço de competências, tecnologia, diplomacia, colaboração total (externa e interna, civil e militar), e com a aposta na educação e consciencialização, fomentando a cibersegurança como uma responsabilidade partilhada.

Relativamente aos critérios e indicadores de resiliência nacional face à desinformação, deduziram-se 28 indicadores. Como exemplo de alguns dos indicadores elencados temos a existência de um gabinete de comunicação estratégica, o nível de polarização da sociedade, o nível de confiança nos *media*, a existência de uma plataforma pública para difundir campanhas de desinformação, ou a existência de uma célula de fusão nacional (e.g., integrada nos serviços de informações).

Quanto aos critérios e indicadores de ciber-resiliência nacional, deduziram-se 58 indicadores. Alguns exemplos dos indicadores elencados são a maturidade de cibersegurança (e.g., nível de implementação do QNRCS) das entidades críticas, a certificação de ativos críticos, o nível de investimento privado e público em cibersegurança, a existência de uma definição clara dos fluxos de partilha de informação e colaboração ente instituições, ou a capacidade das FFAA conduzirem OpCiber (ofensivas e defensivas).

A resposta às AH não são responsabilidade única de uma entidade especifica e torna-se necessário adotar abordagens holísticas. Assim, os indicadores deduzidos nas respostas às QD2 e QD3, refletem uma perspetiva *whole-of-government* em que se deve promover a partilha de informações, a formação e exercícios de forma integrada (organismos do Estado), permitindo soluções comuns para obter resiliência face às AH, e uma perspetiva *whole-of-society*, que estende a cooperação ao setor privado, jornalistas, investigadores (meio académico), verificadores de factos, plataformas digitais, e a sociedade civil em geral. Neste sentido, os indicadores forma subdivididos em variáveis que representam as funções críticas de um Estado (PMESII).

Os indicadores deduzidos nas respostas à QD2 e QD3, foram submetidos à apreciação dos entrevistados. As entrevistas permitiram também que os entrevistados sugerissem novos indicadores. Como resultado, aplicando o critério de seleção descrito no sexto capítulo, no caso da resiliência nacional face à desinformação selecionaram-se 23 de um total de 52 indicadores, e no caso da ciber-resiliência selecionaram-se 54 de um total de 114 indicadores. Os indicadores selecionados (i.e., adequados ao contexto nacional) constituem a resposta à QC e a materialização do OG (*Propor critérios e indicadores da resiliência de Portugal face a AH no ambiente informacional*).

Como principais contributos para o conhecimento, este TII propõe um conjunto de indicadores de resiliência nacional face a AH, no ambiente informacional, enquadrados por uma abordagem alinhada com as recomendações da UE e da OTAN, colhendo o melhor de outras abordagens relacionadas com resiliência (ainda que noutros âmbitos).

Elenca-se como possível limitação da investigação, o facto de não existir um leque mais alargado de especialistas entrevistados, para complementar a validação e adição de novos indicadores. Do total de entrevistas planeadas (e.g., a membros da rede interministerial para AH) só seis corresponderam. Salienta-se que sendo as AH um tópico recente, o conhecimento nesta área ainda não está consolidado de forma transversal, em especial quando restrito ao ambiente informacional.

Quanto a estudos futuros, sugere-se o desenvolvimento das métricas para o processo analítico e a visualização, para materializar a abordagem proposta numa ferramenta prática que permita monitorizar e melhorar a resiliência nacional.

Referências bibliográficas

Abaimov, S., & Martellini, M. (2020). *Cyber Arms - Security in Cyberspace*. Boca Raton: CRC Press.

AJP-3.20. (2020). Allied Joint Doctrine for Cyberspace Operations. Bruxelas: NATO Standardization Office.

Alessi, L., Benczur, P., Campolongo, F., Cariboni, J., Manca, A. R., Menyhert, B., & Pagano, A. (2020). The Resilience of EU Member States to the Financial and Economic Crisis. *Social Indicators Research*, *148*(2), pp. 569–598. doi:10.1007/s11205-019-02200-1

Alves, A. J. F. M. (2020). *A prevenção e o combate às ameaças híbridas: impacto para as Forças Armadas Portuguesas*. Trabalho de Investigação Individual do CPOG 2019/2020. Lisboa: Instituto Universitário Militar.

AMWG. (1981). Forgery, Disinformation, Political Operations. *United States Department of State Bureau of Public Affairs*, *88*, 4.

Atkinson, C. (2018). Hybrid Warfare and Societal Resilience: Implications for Democratic Governance. *Information & Security: An International Journal*, *39* (1), pp. 63–76.

Bartles, C. K. (2016). Getting Gerasimov Right. *Military Review*, (February), pp. 30–38.

Beláz, A. (2019). The changing role of the EU in Cybersecurity. *Biztonságtudományi Szemle*, *1*(1-2.), pp. 17–30.

Boot, M. (2013). *Invisible Armies: An Epic History of Guerrilla Warfare from Ancient Times to the Present*. New York, NY: Liveright Publishing.

Brenner, S. (2009). *Cyberthreats: The Emerging Fault Lines of the Nation State*. Nova Iorque: Oxford University Press.

Brianna Keys, Aashish Chhajer, Zilong Liu, Daniel Horner, & Stuart Shapiro. (2016). *A framework for assessing cyber resilience*. Retirado de http://bloustein.rutgers.edu/wp-content/uploads/2016/05/2016_WEF.pdf

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

Buckland, B. S., Schreier, F., & Winkler, T. H. (2010). *Democratic governance challenges of cyber security*. Génova: DCAF.

Câncio, F. (2020). ERC regista como ″informativo″ site de desinformação e propaganda. [Página *online*]. Retirado de https://www.dn.pt/edicao-do-dia/27-jan-2020/erc-regista-como-informativo-site-de-desinformacao-e-propaganda-11751353.html

Centro Nacional de Cibersegurança. (2020). *Relatório de Cibersegurança em Portugal* -

Riscos & Conflitos.

Chekinov, S. G., & Bogdanov, S. A. (2013). The Nature and Content of a New-Generation War. *Military Thought*, *4*, pp. 12–23.

Chen, Q., & Bridges, R. A. (2017). Automated behavioral analysis of malware: A case study of wannacry ransomware. *Proceedings - 16th IEEE International Conference on Machine Learning and Applications, ICMLA 2017*, *2017-Decem*, pp. 454–460.

Chivvis, C. (2017). Understanding Russian "Hybrid Warfare": And What Can Be Done About It. *Rand Corporation*.

Clark, D., & Landau, S. (2011). Untangling attribution. *Harvard National Security Journal*, *2*(February 2010), pp. 323-352.

Clarke, R. A., & Knake, R. K. (2010). *Cyber war: the next threat to national security and what to do about it*. Nova Iorque: HarperCollins e-books.

Clausewitz, C. Von, Howard, M., & Paret, P. (1984). *On War*. Princeton, N.J: Princeton University Press.

CNCS. (2019). *Quadro Nacional de Referência para Cibersegurança*. Lisboa: Autor.

CNCS. (2021a). *Boletim nº1/2021 do Observatório Nacional de Cibersegurança*. Lisboa: Autor.

CNCS. (2021b). Projeto de decreto-lei regulamenta o Regime Jurídico da Segurança do Ciberespaço e define as obrigações em matéria de certificação da cibersegurança. [Página *online*]. Retirado de https://www.cncs.gov.pt/recursos/noticias/projeto-de-decreto-lei-regulamenta-o-regime-juridico-da-seguranca-do-ciberespaco-e-define-as-obrigacoes-em-materia-de-certificacao-da-ciberseguranca/.

Comissão Europeia. (n.d.). Code of Practice on Disinformation | Shaping Europe's digital future. [Página *online*]. Retirado de https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation.

Comissão Europeia. (2016). Comunicação conjunta ao parlamento europeu e ao conselho - Quadro comum em matéria de luta contras as ameaças híbridas - uma resposta da UE. [Página *online*]. Retirado de https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52016JC0018&from=PT

Comissão Europeia. (2017). Relatório Conjunto ao Parlamento Europeu e ao Conselho relativo à aplicação do Quadro comum em matéria de luta contra as ameaças híbridas - uma resposta da União Europeia. [Página *online*]. Retirado de https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52017JC0030&from=PT

Comissão Europeia. (2018a). Action Plan against Disinformation. Joint communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions. [Página *online*]. Retirado de *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018JC0036&from=en*

Comissão Europeia. (2018b). Comunicação aa Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões - Combater a desinformação em linha: uma estratégia europeia. [Página *online*]. Retirado de https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52018DC0236&from=PT

Comissão Europeia. (2018c). Comunicação conjunta ao parlamento europeu, ao conselho europeu e ao conselho - Aumentar a resiliência e reforçar a capacidade de enfrentar ameaças híbridas. [Página *online*]. Retirado de https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52018JC0016&from=PT

Comissão Europeia. (2018d). Uma Europa que protege: UE intensifica medidas contra a desinformação. [Página *online*]. Retirado de https://ec.europa.eu/commission/presscorner/detail/pt/IP_18_6647

Comissão Europeia. (2020a). Comunicação da comissão ao parlamento europeu, ao conselho, ao comité económico e social europeu e ao comité das regiões sobre o plano de ação para a democracia europeia. [Página *online*]. Retirado de https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52020DC0790&from=PT

Comissão Europeia. (2020b). Nova Estratégia da UE para a Cibersegurança e novas regras para aumentar a resiliência das entidades críticas físicas e digitais. [Página *online*]. Retirado de https://ec.europa.eu/commission/presscorner/detail/pt/IP_20_2391. https://ec.europa.eu/commission/presscorner/detail/pt/IP_20_2391

Comissão Europeia. (2020c). Prototype Dashboard for Monitoring the Social and Economic Dimension of Resilience. [Página *online*]. Retirado de https://ec.europa.eu/info/sites/default/files/social_and_economic_dashboard_asfr_background_en.pdf

Comissão Europeia. (2020d). The EU's Cybersecurity Strategy in the Digital Decade | Shaping Europe's digital future. [Página *online*]. Retirado de https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade.

Conselho da UE. (2019). Conclusões do Conselho sobre os esforços complementares para

aumentar a resiliência e combater as ameaças híbridas. [Página *online*]. Retirado de https://data.consilium.europa.eu/doc/document/ST-14972-2019-INIT/pt/pdf

Conselho da UE. (2020). UE impõe primeiras sanções contra ciberataques. [Página *online*]. Retirado de https://www.consilium.europa.eu/pt/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/.

Conselho da UE. (2021). Conselho dá luz verde ao Centro de Competências em Cibersegurança, com sede em Bucareste - Consilium. [Página *online*]. Retirado de https://www.consilium.europa.eu/pt/press/press-releases/2021/04/20/bucharest-based-cybersecurity-competence-centre-gets-green-light-from-council/.

Conselho Europeu. (2019). A New Strategic Agenda 2019-2024. [Página *online*]. Retirado de https://www.consilium.europa.eu/media/39914/a-new-strategic-agenda-2019-2024.pdf

Costa, F. S. (2021). A "guerra fria" com a China está a aquecer. [Página *online*]. Retirado de https://eco.sapo.pt/especiais/a-guerra-fria-com-a-china-esta-a-aquecer/. https://eco.sapo.pt/especiais/a-guerra-fria-com-a-china-esta-a-aquecer/

Cull, N. J., Gatov, V., Pomerantsev, P., Applebaum, A., & Shawcross, A. (2017). Soviet Subversion, Disinformation and Propaganda: How the West Fought Against it: An Analytic History, with Lessons for the Present. [Página *online*]. Retirado de https://www.lse.ac.uk/iga/assets/documents/arena/2018/Jigsaw-Soviet-Subversion-Disinformation-and-Propaganda-Final-Report.pdf

Danyk, Y., Maliarchuk, T., & Briggs, C. (2017). Hybrid War: High-tech, Information and Cyber Conflicts. *Connections: The Quarterly Journal*, *16*(2), pp. 5–24.

Dodonov, R., Dodonova, V., & Mozgovoy, L. (2019). Polemological Paradigm of Comprehension of Essence of Hybrid War. pp. 7–17. doi: 10.31865/2520-684292018157445.

Estado-Maior-General das Forças Armadas. (2018). *Diretiva Estratégica do EMGFA 2018-2021, de 18 abril de 2018*. Lisboa: Chefe do Estado-Maior-General das Forças Armadas.

ENISA. (2020). *ENISA Threat Landscape 2020 - Main Incidents in the EU and Worldwide*. Retirado de https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-main-incidents/at_download/fullReport

Entidade Reguladora Para a Comunicação Social. (2019). *A Desinformação - Contexto Europeu e Nacional*. Retirado de

https://www.parlamento.pt/Documents/2019/abril/desinformacao_contextoeuroeunacional-ERC-abril2019.pdf

EU vs DISINFORMATION. (n.d.). [Página *online*]. Retirado de https://euvsdisinfo.eu/

Fiott, D., & Parkes, R. (2019). Protecting Europe: The EU's response to hybrid threats. *Chaillot Paper*, Vol. 151, Issue April. Retirado de https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_151.pdf

Galeotti, M. (2019). The mythical 'Gerasimov Doctrine' and the language of threat. *Critical Studies on Security*, *7*(2), pp. 157–161. doi: 10.1080/21624887.2018.1441623

Giannopoulos, G., Smith, H., & Theocharidou, M. (2020). The Landscape of Hybrid Threats: A Conceptual Model Public Version. *Comissão Europeia, Ispra, PUBSY No. JRC123305*. Retirado de https://publications.jrc.ec.europa.eu/repository/bitstream/JRC123305/conceptual_framework-reference-version-shortened-good_cover_-_publication_office.pdf

Giles, K. (2016). *Handbook of Russian Information Warfare.* (Fellowship Monograph). NATO Defence College, Roma.

Gunneriusson, H. (2019). Hybrid Warfare and Deniability as Understood by the Military. *Polish Political Science Yearbook*, *48*(2).

Hart, B. H. L. (1941). *The strategy of indirect approach*. Londres: Faber and Faber Limited.

Hathaway, M. (2015). Cyber Readiness Index 2.0. [Página *online*]. Retirado de https://www.belfercenter.org/publication/cyber-readiness-index-20

Hickman, K., Weissmann, M., Nilsson, N., Bachman, S., Gunneriusson, H. & Thunholm, P. (2018). Hybrid Threats and Asymmetric Warfare: What to do? Em: Swedish Defence University. *Conference proceeding (February).* Conferência organizada pela Universidade de Defesa Sueca, Estocolmo.

Humprecht, E., Esser, F., & Van Aelst, P. (2020). Resilience to Online Disinformation: A Framework for Cross-National Comparative Research. *The International Journal of Press/Politics*, *25*(3), pp. 493–516. doi:10.1177/1940161219900126

Hybrid CoE. (n.d.). Hybrid threats as a concept - Hybrid CoE - The European Centre of Excellence for Countering Hybrid Threats [Página *online*]. Retirado de https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/

Hybrid CoE. (2021). The future of cyberspace and and hybrid threats. [Página *online*]. Retirado de https://www.hybridcoe.fi/wp-content/uploads/2021/04/20210407_Hybrid_CoE_Trend_Report_6_The_future_of_cy

berspace_and_hybrid_threats_WEB.pdf

Iberdrola. (n.d.). Smart cities: a transformação digital das cidades. [Página *online*]. Retirado de https://www.iberdrola.com/inovacao/smart-cities

Isaak, J., & Hanna, M. J. (2018). User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection. *Computer*, *51*(8), pp. 56–59.

Jakovljevic, M., Bjedov, S., Jaksic, N., & Jakovljevic, I. (2020). Covid-19 pandemia and public and global mental health from the perspective of global health security. *Psychiatria Danubina*, *32*(1), pp. 6–14.

Jens Stoltenberg. (2020). Keynote speech by NATO Secretary General Jens Stoltenberg at the Global Security 2020 (GLOBSEC) Bratislava Forum, 07-Oct.-2020. [Página *online*]. Retirado de https://www.nato.int/cps/en/natohq/opinions_178605.htm?selectedLocale=uk

Jornal SOL. (2020). Marcelo responde a "ameaça" do embaixador dos EUA. [Página *online*]. Retirado de https://sol.sapo.pt/artigo/710015/marcelo-responde-a-ameaca-do-embaixador-dos-eua

JP3-12. (2018). *Joint Publication 3-12 - Cyberspace Operations*. Washington: Joint Chiefs of Staff.

Juurvee, I. (2018). The resurrection of ' active measures ': Intelligence services as a part of Russia ' s influencing toolbox. [Página *online*]. Retirado de https://www.hybridcoe.fi/wp-content/uploads/2020/07/Strategic-analysis-7-April.pdf

Lee, R. M., Assante, M. J., & Conway, T. (2016). Analysis of the Cyber Attack on the Ukrainian Power Grid. *White Paper*. Retirado de https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2016/05/20081514/E-ISAC_SANS_Ukraine_DUC_5.pdf

Levin, D. H. (2019). Partisan electoral interventions by the great powers: Introducing the PEIG Dataset. *Data Feature Conflict Management and Peace Science*, *36*(1), pp. 88–106.

Linkov, I., Baiardi, F., Florin, M. V., Greer, S., Lambert, J. H., Pollock, M., Rickli, J. M., Roslycky, L., Seager, T., Thorisson, H., & Trump, B. D. (2019). Applying Resilience to Hybrid Threats. *IEEE Security and Privacy*, *17*(5), pp. 78–83.

Linkov, I., Eisenberg, D. A., Plourde, K., Seager, T. P., Allen, J., & Kott, A. (2013). Resilience metrics for cyber systems. *Environment Systems and Decisions*, *33*(4), pp. 471–476. doi:10.1007/s10669-013-9485-y

Lucas, S., & Mistry, K. (2009). Illusions of Coherence: George F. Kennan, U.S. Strategy and Political Warfare in the Early Cold War, 1946–1950. *Diplomatic History*, *33*(1), pp. 39–66.

LUSA. (2019). Governo quer plano nacional para combater desinformação e ciberataques - Combate às Fake News, uma questão democrática. [Página *online*]. Retirado de https://combatefakenews.lusa.pt/fake-news-governo-quer-plano-nacional-para-combater-desinformacao-e-ciberataques-c-audio/

LUSA. (2020). Fake News. UE vai dizer às plataformas como devem eliminar desinformação e pode multá-las. [Página *online*]. Retirado de https://www.dinheirovivo.pt/empresas/fake-news-ue-vai-dizer-as-plataformas-como-devem-eliminar-desinformacao-e-pode-multa-las-13101588.html

Manca, A. R., Benczur, P., & Giovannini, E. (2017). *Building a Scientific Narrative Towards a More Resilient EU Society - Part 1: A Conceptual Framework*. Luxembourg: União Europeia, Joint Research Centre.

Mandiant. (2013). *APT1 Exposing One of China's Cyber Espionage Units*. Retirado de https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

Marcuzzi, S. (2018). Hybrid Warfare in Historical Perspectives. *Max Weber International Workshop*. Retirado de http://www.natofoundation.org/wp-content/uploads/2018/06/NDCF_StefanoMarcuzzi_Paper.pdf

Menn, J. (2021). U.S. intelligence agencies say Russia likely behind hacking of government agencies. [Página *online*]. Retirado de https://www.reuters.com/world/us/us-intelligence-agencies-say-russia-likely-behind-hacking-government-agencies-2021-01-05/

Monaghan, S. (2019). Hybrid Warfare and Hybrid Threats Are Different Things. *Prism*, *8*(2), pp. 82–99.

Monitor, I. W. (2009). Tracking GhostNet: Investigating a Cyber Espionage Network. *Think Tank White Paper*, *March 29*, 1–53.

Multinational Capability Development Campaign (2019). *Countering Hybrid Warfare Project.* Retirado de https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/784299/concepts_mcdc_countering_hybrid_warfare.pdf

Murray, W., & Mansoor, P. R. (2012). *Fighting Complex Opponents from the Ancient World*.

New York: Cambridge University Press.

NATO StratCom COE. (2019). Hybrid Threats - A Strategic Communications Perspective. *Encyclopedia of Creativity, Invention, Innovation and Entrepreneurship*. doi.org: 10.1007/978-3-319-15347-6_300702

Nelson, R. A. (1996). *A Chronology and Glossary of Propaganda in the United States*. Londres: Greenwood.

Newman, L. H. (2020). Russia Takes a Big Step Toward Internet Isolation. [Página *online*]. Retirado de https://www.wired.com/story/russia-internet-control-disconnect-censorship/.

NIST. (2014). *Framework for improving critical infrastructure cybersecurity: Version 1.0*. National Institute of Standards and Technology. Retirado de https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

NIST. (2018). Cybersecurity Framework. [Página *online*]. Retirado de https://www.nist.gov/cyberframework/framework.

NSC-68. (1950). National Security Council Report: United States Objectives and Programs for National Security. *History and Public Policy Program Digital Archive*.

Nunes, P. (2020). *A Edificação da Capacidade de Ciberdefesa Nacional*. Trabalho de Investigação Individual do CPOG 2019/2020. Lisboa: Instituto Universitário Militar.

Nunes, P. V., Mendes, C. P., Santos, J. R. L., Santos, L. C. dos, Moniz, P., & Casimiro, S. de V. (2018). *Contributos para uma Estratégia Nacional de Ciber Defesa*.

Office of the Director of National Intelligence. (2021). *Annual Threat Assessment of the US Intelligence Community*. Retirado de https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf

Oliveira, M. (2021). China e Rússia suspeitas de fazerem ciberespionagem a Portugal. [Página *online*]. Retirado de https://www.publico.pt/2021/04/06/sociedade/noticia/china-russia-suspeitas-fazerem-ciberespionagem-portugal-1957275

Os truques da imprensa portuguesa. (2018). Sites de fake news em Portugal – Comunidade Cultura e Arte. [Página *online*]. Retirado de https://www.comunidadeculturaearte.com/sites-de-fake-news-em-portugal/

Organização do Tratado do Atlântico Norte. (2016). Cyber Defence Pledge. [Página *online*] Retirado de https://www.nato.int/cps/en/natohq/official_texts_133177.htm

Organização do Tratado do Atlântico Norte. (2019). *NATO Standard AJP-3 Allied Joint Doctrine for the Conduct of Operations* (C version). NATO Standartization Office (NSO).

Organização do Tratado do Atlântico Norte. (2020a). NATO's approach to countering disinformation. [Página *online*]. Retirado de https://www.nato.int/cps/en/natohq/177273.htm.

Organização do Tratado do Atlântico Norte. (2020b). Resilience and Article 3. [Página *online*]. Retirado de https://www.nato.int/cps/en/natohq/topics_132722.htm. https://www.nato.int/cps/en/natohq/topics_132722.htm

Organização do Tratado do Atlântico Norte. (2021a). NATO-Russia: setting the record straight. [Página *online*]. Retirado de https://www.nato.int/cps/en/natohq/115204.htm.

Organização do Tratado do Atlântico Norte. (2021b). *NATO - Cyber defence*. [Página *online*]. Retirado de https://www.nato.int/cps/en/natohq/topics_78170.htm. https://www.nato.int/cps/en/natohq/topics_78170.htm

Organização do Tratado do Atlântico Norte. (2021c). *NATO - Topic: NATO's response to hybrid threats*. [Página *online*]. Retirado de https://www.nato.int/cps/en/natohq/topics_156338.htm

Pamment, J. (2020). *The EU's Role in Fighting Disinformation: Taking Back the Initiative*. [Página *online*]. Retirado de https://carnegieendowment.org/2020/07/15/eu-s-role-in-fighting-disinformation-taking-back-initiative-pub-82286

Patel, S. S., Moncayo, O. E., Conroy, K. M., Jordan, D., & Erickson, T. B. (2020). The landscape of disinformation on health crisis communication during the COVID-19 pandemic in Ukraine: hybrid warfare tactics, fake media news and review of evidence. *Journal of Science Communication 19(05)(2020)A02*.

Pathe Duarte, F. (2020). Non-kinetic hybrid threats in Europe – the Portuguese case study (2017-18). *Transforming Government: People, Process and Policy*, *14*(3), pp. 433–451. doi: 10.1108/TG-01-2020-0011

Pomerleau, M. (2019). When do cyberattacks deserve a response from NATO? [Página *online*]. Retirado de https://www.fifthdomain.com/international/2019/12/03/when-do-cyberattacks-deserve-a-response-from-nato/

Presidência Portuguesa do Conselho da UE. (2021). Workshop de Ministros da Defesa da UE sobre a Bússola Estratégica. [Página *online*]. Retirado de https://www.defesa.gov.pt/pt/comunicacao/noticias_fa/Paginas/Workshop-de-

Ministros-da-Defesa-da-UE-sobre-a-Bussola-Estrategica.aspx

Quivy, R., & Campenhoudt, L. Van. (1998). *Manual de Investigação em Ciências Sociais*. Lisboa: Gradiva.

RCM n.º 26, 11 de abril. (2013). *Aprova a reforma "Defesa 2020."* Diário da República, 1.ª Série, 77, 2285–2289. Lisboa: Presidência do Conselho de Ministros.

RCM n.º 92. (2019). *Aprova a Estratégia Nacional de Segurança do Ciberespaço 2019-2023*. Diário da República, 1.ª Série, 108.

Rid, T., & Buchanan, B. (2015). Attributing Cyber Attacks. *Journal of Strategic Studies*, *38*(January 2015), 4–37.

Romerstein, H. (2001). Disinformation as a KGB Weapon in the Cold War. *Journal of Intelligence History*, *1*(1), pp. 54–67. doi: 10.1080/16161262.2001.10555046

Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., & Mcquaid, R. (2019). Developing Cyber Resilient Systems: A Systems Security Engineering Approach. *NIST Special Publication 800-160 Volume 2*, *2*, 224. Retirado de https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2.pdf

Santo, G. E. (2009). A NATO numa Perspectiva Militar: entre o Sonho e as Realidades. *Nação e Defesa*, *123*, Lisboa: IDN, pp. 31–39.

Santos, Lino, & Guedes, A. M. (2015). Breves reflexões sobre o poder e o ciberespaço. *RDeS – Revista de Direito e Segurança*, *III*(6), pp. 189–209.

Santos, Lúcio, & Lima, J. (2019). *Orientações metodológicas para a elaboração de trabalhos de investigação* (2ª ed.). Cadernos do IUM, 8. Lisboa: Instituto Universitário Militar.

Schreier, F. (2015). On Cyberwarfare. *DCAF HORIZON*, *7*.

Segal, J., Segal, L., & Dehmlow, R. (1987). AIDS: Its nature and origin. *Bertrand Russell Peace Foundation, Australian Branch*.

Shea, J. (2016). Resilience: a core element of collective defence. [Página *online*]. Retirado de https://www.nato.int/docu/review/articles/2016/03/30/resilience-a-core-element-of-collective-defence/index.html

Sistema de Segurança Interna. (2021). *Relatório Anual de Segurança Interna 2020*. Lisboa: Sistema de Segurança Interna. Retirado de http://www.ansr.pt/InstrumentosDeGestao/Documents/Relatório Anual de Segurança Interna (RASI)/RASI 2016.pdf

Sousa, L. B. de. (2021). Portugal nunca foi alvo de uma campanha de desinformação externa.

[Página *online*]. Retirado de https://www.dn.pt/edicao-do-dia/05-mar-2021/portugal-nunca-foi-alvo-de-uma-campanha-de-desinformacao-externa--13420138.html

Spidalieri, F. (2015). State of the States on Cybersecurity. *Pell Center for International Relations and Public Policy*, *November*. doi: 10.1016/j.jacc.2018.01.032

Stamos, A. (2020). Realistic Threats and Realistic Users: Lessons from the Election. [Página *online*]. Retirado de https://www.sigsac.org/ccs/CCS2020/keynotes.html.

Steffens, T. (2020). *Attribution of Advanced Persistent Threats*. Berlim: Springer Vieweg.

Steiger, S., Harnisch, S., Zettl, K., & Lohmann, J. (2018). Conceptualising conflicts in cyberspace. *Journal of Cyber Policy*, *3*(1), pp. 77–95.

Stiennon, R. (2015). *There Will Be Cyberwar: How the Move to Network-centric Warfighting Set the Stage for Cyberwar*. Birmingham: IT-Harvest Press.

Stoltenberg, J. (2016). *The Secretary General's Annual Report 2015*. Bruxelas: NATO. doi: 10.1353/bmc.2015.0008

Stoltenberg, Jens. (2015). Keynote speech by NATO Secretary General Jens Stoltenberg at the opening of the NATO Transformation Seminar , 25-Mar.-2015. [Página *online*]. Retirado de https://www.nato.int/cps/en/natohq/opinions_118435.htm. https://www.nato.int/cps/en/natohq/opinions_118435.htm

Todd Lopez. (2020). DOD to Require Cybersecurity Certification in Some Contract Bids. [Página *online*]. Retirado de https://www.defense.gov/Explore/News/Article/Article/2071434/dod-to-require-cybersecurity-certification-in-some-contract-bids/

Tribunal de Contas Europeu. (2019). *Desafios à eficácia da política de cibersegurança da UE*. Luxemburgo: Autor.

Tzu, S. (1963). The Art of War. In *Sun Tzu On The Art Of War*. Traduzido por Samuel B. Griffith. Oxford: Oxford University Press. doi: 10.4324/9781315030081

Uziębło, J. J. (2017). United in ambiguity? EU and NATO approaches to hybrid warfare and hybrid threats. *EU Diplomacy Papers*, *5*, 38. Retirado de https://www.coleurope.eu/research-paper/united-ambiguity-eu-and-nato-approaches-hybrid-warfare-and-hybrid-threats

Valeriano, B., & Maness, R. C. (2015). *Cyber War versus Cyber Realities, Cyber Confict in the International System*. Oxford: Oxford University Press.

Vilelas, J. (2009). *Investigação – o processo de construção do conhecimento*. Lisboa: Edições Sílabo.

Vinagre, A. (2021). Jornalistas de Macau denunciam pressões sobre as redacções. [Página *online*]. Retirado de https://www.publico.pt/2021/03/20/mundo/noticia/jornalistas-macau-denunciam-pressoes-redaccoes-1955270

Ward, M. (2019). *Formative Battles: Cold War Disinformation Campaigns and Mitigation Strategies*. Washington: Wilson Center.

Wheeler, D. A. D. A., Larsen, G. N., & Leader, T. (2003). *Techniques for cyber attack attribution* (Issue October). IDA Paper P-3792. Institute for Defense Analysis.

Whyte, C., Thrall, A. T., & Mazanec, B. M. (2020). *Information warfare in the age of cyber conflict.* Oxfordshire: Routledge.

William Sebastian Cohen. (1999). *Annual Report to the President and the Congress*. Washington, DC: US Government Printing Office.

Apêndice A — Modelo de análise

Quadro 5 –Modelo de análise

Tema: A Prevenção e o Combate de ameaças Híbridas: Identificar instrumentos de medida: variáveis e indicadores de resiliência nacionais face às ameaças híbridas. (Informacional)				
Conceito	**Dimensões**	**Variáveis**	**Indicadores**	**Observações**
Resiliência do Instrumento de poder Informacional face a Ameaças Híbridas	Resiliência face à Desinformação e Propaganda	Ação – Efeito	- Respostas a campanhas de desinformação e propaganda ao nível da UE, OTAN e Portugal - Desinformação em Portugal	Interpretar e investigar as dimensões em análise com foco na procura de critérios e indicadores de resiliência face a ameaças híbridas (informacional). A pesquisa foi suportada em análise documental e os critérios/variáveis e indicadores obtidos foram validados através de entrevistas semiestruturadas a especialistas.
		Resiliência do Estado Funções críticas: Político Militar Social Económico Infraestruturas Informacional	- Resiliência social (dimensão humana, perceção, crenças e raciocínio) - Comunicação interna e externa - Medidas de controlo e mitigação - Legislação, Políticas, Estrutura Organizacional	
	Resiliência no Ciberespaço (ciber-resiliência)	Ação - Efeito	- Respostas a campanhas ofensivas no ciberespaço (e.g., ciberespionagem, cibersabotagem)	
		Resiliência do Estado Funções críticas: Político Militar Social Económico Infraestruturas Informacional	- Ciber-resiliência (dimensão tecnológica, humana e física) - Quadros de referência para a segurança da informação - Funções críticas do Estado garantidas - Legislação, Políticas, Estrutura Organizacional	

Apêndice B — Lista de entrevistados e guião de entrevista

Lista de entrevistados

ID	Cargo	Título/Posto Nome
N1	Diretor do Gabinete Nacional de Segurança	Contra-Almirante Gameiro Marques
N2	Subdiretor-Geral da Direção-Geral de Política de Defesa Nacional	Major General Nuno Lemos Pires
N3	Assessor no Gab. da Secretária-Geral do Sist. de Seg. Interna	Coronel Óscar Rocha
N4	Ex-Diretor da Escola Comunicações e Sist. de Inf. da OTAN	Coronel Tirocinado Paulo Viegas Nunes
N5	Docente especialista em Segurança de Informação do IST	Prof. Doutor Miguel Pupo Correia
N6	Diretor de cibersegurança da REN	Engº Rafael Aranha

Guião de entrevista

TEMA: A prevenção e o combate de ameaças híbridas: identificar instrumentos de medida (variáveis e indicadores) da resiliência nacional face às ameaças híbridas, no domínio informacional.

Identificação do entrevistado:

Função do entrevistado:

ENQUADRAMENTO GERAL

O objetivo geral deste estudo é **propor critérios e indicadores de resiliência nacional, face a ameaças híbridas com recurso ao instrumento informacional.** Estudos paralelos a este vão analisar os outros instrumentos de poder (Militar, Económico e Diplomático).

Os ciberataques a infraestruturas-críticas e operadores de serviços essenciais, a ciberespionagem, a influência em eleições, a instrumentalização política e desinformação (e.g., em torno do vírus Covid-19), fazem parte do ambiente das ameaças híbridas[11]. O Centro de Excelência Europeu para o Combate a Ameaças Híbridas (Hybrid CoE)[12], do qual fazem parte Portugal e outros membros da EU e da NATO, define ameaça híbrida como uma ação coordenada e sincronizada, conduzida por atores estatais ou não estatais, cujo objetivo é minar ou prejudicar um alvo, influenciando a sua tomada de decisões a nível local, regional, estatal ou institucional. Estas ameaças visam deliberadamente as vulnerabilidades dos estados democráticos e das instituições, utilizando uma vasta gama de meios e concebidas para se manterem abaixo do limiar de deteção e imputação. Contudo, nem todas as combinações de meios nem o uso desses meios isoladamente, constituem uma ameaça híbrida[1].

A agenda estratégica da UE para 2019-2024, apela à proteção contra ameaças híbridas com origem em atores hostis, estatais e não estatais[13]. Para garantir a dissuasão e resposta, importa ser resiliente, sendo necessário identificar indicadores de medida que permitam medir a resiliência do Estado face a estas ameaças[1]. De acordo com a NATO, a resiliência é a capacidade de uma sociedade resistir e recuperar fácil e rapidamente de choques provocados por ameaças híbridas, entre outras, combinando tanto a preparação civil como a capacidade militar[14]. Falamos de resiliência porque as vulnerabilidades e ameaças são incertas.

O Hybrid CoE[1], e a UE[15], referem que as campanhas de desinformação, fazem frequentemente parte do ambiente das ameaças híbridas, envolvendo também ciberataques. De facto, o ciberespaço é um meio privilegiado para as ameaças híbridas (permite alcance, velocidade, ocultação, e a imputação é difícil), e sendo o próprio ciberespaço um domínio contido no ambiente informacional, optou-se por analisar duas dimensões ao nível nacional: (i) **ciber-resiliência**; (ii) a **resiliência face à desinformação**.

[11] https://euhybnet.eu/wp-content/uploads/2021/01/Conceptual-Framework-Hybrid-Threats-HCoE-JRC.pdf
[12] https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/
[13] https://www.consilium.europa.eu/en/eu-strategic-agenda-2019-2024/
[14] https://www.nato.int/cps/en/natohq/topics_132722.htm
[15] https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52018JC0036&from=en

Parte 1 – Ciber-resiliência nacional

Enquadramento para as 3 questões:

Pretende-se que a matriz de ciber-resiliência idealizada neste trabalho (ver Quadro 6), possa contribuir para uma visão da ciber-resiliência nacional face a ameaças híbridas (instrumento informacional). Considerámos as diferentes funções críticas de um Estado, representadas pelos **domínios** Político, Militar, Económico, Social, Informação e Infraestruturas (PMESII)[16].

A dimensão Infraestruturas integra um conjunto de entidades fundamentais para o Estado, embora estas sejam transversais aos outros domínios (e.g., câmaras municipais do domínio Político, ou operadores de telecomunicações do domínio Informacional). Nos domínios Infraestruturas e Militar, pretende-se focar a avaliação da maturidade da cibersegurança, de acordo com o nível de aplicação das **medidas**[17] do Quadro Nacional de Referência para a Cibersegurança (QNRCS)[18], ou equivalente, adicionando outros indicadores específicos de resiliência. No âmbito Militar, acrescem as especificidades da ciberdefesa. De notar, que o QNRCS prevê a gestão de cibersegurança como um processo contínuo focando aspetos humanos, tecnológicos, processuais e físicos (e.g., redundância), abordando a gestão do risco e resiliência. As restantes dimensões PMESII são analisadas à luz da influência que possam ter na ciber-resiliência.

Salienta-se que na matriz proposta, as medidas do QNRCS são aninhadas dentro dos **objetivos** de sistemas ciber-resilientes[19], que pressupõe ataques com sucesso: Antecipar, Resistir, Recuperar e Adaptar.

Por fim, importa referir que se assume o pressuposto que é/será possível aferir a maturidade de cibersegurança das diferentes organizações, por exemplo, através de auditorias, reporte, ou exigência de eventuais certificações QNRCS ou equivalentes (e.g., ISO 27001), caso contrário, a medição da ciber-resiliência será sempre falaciosa.

Nota: O objetivo das questões incide sobre a pertinência dos indicadores elencados na matriz e na proposta de novos indicadores, que terão de ser mensuráveis, e.g., CS.1.5. percentagem de organizações que certificam ativos críticos, CS.2.1. nível de maturidade das organizações relativamente à medida "Detetar" do QNRCS.

Questão 1. Analise a matriz e se considerar pertinente, proponha/adicione outros indicadores (**na própria matriz**) que considere relevantes para a ciber-resiliência. Nota: por favor, não desative o modo de revisão do documento para ser fácil identificar as alterações sugeridas à posteriori.

Questão 2. Numa escala entre 1 (pouco importante) a 5 (muito importante), indique na matriz a importância que atribui a todos os indicadores (como no exemplo à direita - a amarelo).

Medidas	1. Identificar/Planear
críticas	5 CS.1.1. Maturidade QNRCS (Identificar) 3 CS.1.2. Foco em ativos críticos
Pública	

Questão 3. Identifica comentários/contributos para melhoria da abordagem relativa à construção da matriz de ciber-resiliência?

Nota: Algumas referências que abordam em detalhe, a ciber-resiliência ao nível Estado:

Spidalieri, F. (2015). State of the States on Cybersecurity. *Pell Center for International Relations*.

Keys, B., Chhajer, A., Liu, Z. and Horner, D., (2016). *A Framework for Assessing Cyber Resilience*. World Economic Forum.

16 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/784299/concepts_mcdc_countering_hybrid_warfare.pdf

17 Identificar, Proteger, Detetar, Responder, Recuperar (medidas QNRCS) + Adaptar (objetivo de resiliência)

18 https://www.cncs.gov.pt/content/files/cncs_qnrcs_2019.pdf

19 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2.pdf

Quadro 6 - Proposta de indicadores da ciber-resiliência nacional face a AH

		Indicadores de ciber-resiliência face a ameaças híbridas					
Objetivos ->		Antecipar			Resistir	Recuperar	Adaptar
Domínios \ Medidas		1. Identificar/Planear	2. Proteger	3. Detetar	4. Responder	5. Recuperar	6. Adaptar
CS	Infraestruturas críticas Administração Pública Operadores de Serviços Essenciais Prestadores de Serviços Digitais	CS.1.1. Maturidade QNRCS (Identificar) CS.1.2. Foco em ativos críticos CS.1.3. Assume ataques com sucesso no planeamento CS.1.4. Garante diversidade (fornecedores, arquitetura) CS.1.5. Certifica ativos críticos CS.1.6. Exercícios e treinos …	CS.2.1. Maturidade QNRCS (Proteger) CS.2.2. Foco em ativos críticos …	CS.3.1. Maturidade QNRCS (Detetar) CS.3.2. Agilidade na partilha e colaboração CS.3.3. Capacidade deteção de redes de distribuição de desinformação	CS.4.1. Maturidade QNRCS (Responder) CS.4.2. Capacidade de coordenação da resposta CS.4.3. Colaboração …	CS.5.1. Maturidade QNRCS (Recuperar) CS.5.2. Foco nos ativos críticos CS.5.3. Agilidade …	CSD.6.1. Documentar incidente CSD.6.2. Rever e corrigir configurações/ procedimentos CSD.6.3. Melhorar partilha de informação CSD.6.4. Testar resiliência contra ameaças similares CSD.6.5. Agilidade …
CD	Militar (Forças Armadas)	CD.1.1. Maturidade QNRCS ou equivalente CD.1.2… CD.1.3… CD.1.4… CD.1.5… CD.1.6… CD.1.7. Projeção de poder …	CD.2.1. … ou equiv. CD.2.2… CD.2.3. Projeção de poder e Dissuasão …	CD.3.1. … ou equiv. CD.3.2. … CS.3.3. Capacidade deteção de redes de distribuição de desinformação …	CD.4.1. … ou equiv. CD.4.2. … CD.4.3. … CD.4.4. Capacidade OpCiber (ofensivas e defensivas) …	CD.5.1. … ou equiv. CD.5.2. … CD.5.3. … …	
S	Social	S.1. Oferta formativa em cibersegurança S.2. Níveis de ensino onde se ministram conteúdos de cibersegurança S.3. Observação de atitudes e comportamentos (e.g., Observatório do CNCS) …					
E	Economico	E.1. Investimento privado e público em cibersegurança incluindo I&D (e.g., Observatório do CNCS) E.2. Mercado de trabalho de cibersegurança (e.g., Observatório do CNCS) …					
P	Político	P.1. Existe uma estratégia de segurança no ciberespaço que contemple resposta a ameaças híbridas? P.2. Existe atribuição de competências na resposta a ameaças híbridas? P.3. Políticas de investimento em cibersegurança e ciberdefesa P.4. O regime jurídico da segurança do ciberespaço impõe obrigatoriedade de certificação (e.g., ISO27001 ou eventual certificação QNRCS pelo CNCS)? P.5. Existe um planeamento civil de emergência para fazer face a ameaças híbridas no ciberespaço? P.5. Existem autoridades nacionais competentes em matéria eleitoral com recursos adequados para responder a ameaças híbridas no ciberespaço? …					
	Informação (partilha)	I.1. Existe uma Célula de Fusão para Ameaças Híbridas ao nível nacional? I.2. Existe coordenação entre instituições e uma definição clara dos fluxos de partilha de informação e colaboração? I.3. Existe um sistema de informação comum para conhecimento situacional de ameaças híbridas aos diferentes níveis e entre as diferentes instituições? I.4. Nível de risco e registos da evolução das ameaças-híbridas no ciberespaço em Portugal …					

Parte 2 – Resiliência nacional face à desinformação

Enquadramento para as 3 questões:

Pretende-se que a matriz do Quadro 7, possa contribuir para uma visão da resiliência nacional face à desinformação no âmbito das ameaças híbridas (instrumento informacional).

Considerámos a análise da resiliência mediante as diferentes funções críticas de um Estado, representadas pelos **domínios** PMESII[20]. No entanto, importa salientar a importância do domínio Social, pois as campanhas de desinformação e outros métodos híbridos interligados, procuram afetar a homogeneidade da cultura e da sociedade do Estado alvo. Contudo, existe uma clara ligação entre domínios, por exemplo, através de ciberespionagem ou de espionagem tradicional, pode ser obtida e divulgada Informação para influenciar a opinião pública, as perceções e o discurso, minando a discussão e o processo Político no Estado alvo.

Nota: O objetivo das questões incide sobre a pertinência dos indicadores elencados na matriz e na proposta de novos indicadores, que terão de ser mensuráveis (e.g., resposta direta, percentagem, taxa).

Questão 1. Analise a matriz e proponha/adicione outros indicadores (**na própria matriz**) que considere relevantes para avaliar a resiliência. Se necessário coloque um comentário a descrever com mais detalhe o indicador adicionado. Nota: por favor, não desative o modo de revisão do documento para ser fácil identificar as alterações sugeridas à posteriori.

Questão 2. Numa escala entre 1 (pouco importante) a 5 (muito importante), indique na matriz a importância que atribui a todos os indicadores (como no exemplo à direita - a amarelo).

Informação	2 I.1. Quantic 5 I.2. Existe c 3 I.3. Existe u 1 I.4. Nível de 5 I.5. Nível de

Questão 3. Identifica comentários/contributos para melhoria da abordagem relativa à construção da matriz de resiliência?

Nota: Referência que aborda em detalhe, a resiliência face à desinformação ao nível Estado:

Humprecht, Edda & Esser, Frank & Aelst, Peter. (2020). *Resilience to Online Disinformation: A Framework for CrossNational Comparative Research* . *The International Journal of Press/Politics.*

20 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/784299/concepts_mcdc_countering_hybrid_warfare.pdf

Quadro 7 - Proposta de indicadores da resiliência nacional à desinformação (AH)

	Indicadores de resiliência nacional face à desinformação (foco nas ameaças híbridas)
Ações[11] / Domínios	Melhorar (detetar, analisar, denunciar); Reforçar coordenação; Mobilizar o setor privado; Sensibilizar as pessoas
Político	P.1. Existem autoridades nacionais competentes em matéria eleitoral com recursos adequados para responder a ameaças híbridas? P.2. Está definida a coordenação entre instituições e uma definição clara dos fluxos de partilha de informação e colaboração? P.3. A legislação em vigor permite o combate eficaz à desinformação no âmbito das ameaças híbridas? P.4. Existe uma estratégia nacional que contemple resposta à desinformação no âmbito das ameaças híbridas? P.5. Existe uma estratégia de comunicação para preparar a população ou contrariar narrativas de desinformação? …
Militar	M.1. Agilidade na partilha, cooperação e coordenação com as autoridades civis M.2. Capacidades para detetar, analisar e denunciar desinformação ao nível militar M.3. Exercícios militares que contemplem o combate à desinformação (e.g., que vise denegrir e enfraquecer a instituição ou a liderança militar) M.4. Existe um plano de comunicação estratégico que reforce a união e prestígio da instituição militar e vise anular efeitos de desinformação? …
Económico	E.1. Investimento em I&D para criação de mecanismos de combate à desinformação …
Social	S.1. Percentagem de votos em partidos populistas (e.g., *Timbro Authoritarian Populism Index*) S.2. Variação de votos (e.g., mapas oficiais de eleições) S.3. Variação de discursos populistas em Portugal (e.g., *Global Populism Database*) S.4. Nível de polarização da sociedade (e.g., V-Dem https://www.v-dem.net/) S.5. Monitorização do nível de influência política no meio académico (e.g., questionários aos alunos) … S.6. Nível de confiança nos media (digitalnewsreport.org/interactive/) S.7. Percentagem de uso de redes sociais para ver notícias (digitalnewsreport.org/interactive/) … S.8. Mecanismos para identificação de audiências alvo mais vulneráveis às campanhas de desinformação …
Informação	I.1. Quantidade de mecanismos (e.g., *fact checks*), por cada órgão de comunicação social, para detetar, analisar e denunciar as fontes e combater a desinformação I.2. Existe um sistema de informação comum para conhecimento situacional da desinformação aos diferentes níveis e entre as diferentes instituições? I.3. Nível de risco e registos da evolução da desinformação em Portugal I.4. Existe uma plataforma pública centralizada para difundir campanhas de desinformação (e.g., https://euvsdisinfo.eu/)? I.5. Existem mecanismos para certificação de órgãos de comunicação social na internet? I.6. Variação do volume das ações de sensibilização (inclui comunicação estratégica e educação) I.7. Ações de formação para jornalistas …
Infraestruturas	II.1. Existe um gabinete de comunicação estratégica? II.2. Existe uma Célula de Fusão Nacional para aumentar o conhecimento situacional? II.3. Existem recursos e infraestruturas dedicadas à deteção de campanhas de desinformação no ciberespaço (inclui deteção de redes de distribuição com *bots* ou *trolls*)? …

Apêndice C — Análise de conteúdo das respostas

Tabela 1 - Análise das respostas de validação (Ciber-resiliência)

Questão 1. Analise a matriz e proponha/adicione outros indicadores (**na própria matriz**) que considere relevantes para avaliar a resiliência. Se necessário coloque um comentário a descrever com mais detalhe o indicador adicionado.

Questão 2. Numa escala entre 1 (pouco importante) a 5 (muito importante), indique na matriz a importância que atribui a todos os indicadores

Domínio	Indicadores Nota: as unidades de registo são identificadas entre aspas e ID de entrevistado. Só os indicadores predefinidos e as unidades de registo com 2 ou mais coocorrências, com avaliação média igual ou superior a "3.5", são contabilizadas como indicador válido (a verde)	Relevância de 1 a 5 Respostas dos entrevistados N1	N2	N3	N4	N5	N6	Média
Cibersegurança das: Infraestruturas críticas Administração Pública Operadores de Serviços Essenciais Prestadores de Serviços Digitais	Identificar/Planear							
	CS.1.1. Maturidade QNRCS (Identificar)	5	-	3	4	5	5	4.4
	CS.1.2. Foco em ativos críticos	4	-	5	5	4	5	4.6
	CS.1.3. Assume ataques com sucesso no planeamento	3	-	3	4	4	5	3.8
	CS.1.4. Garante diversidade (fornecedores, arquitetura)	3	-	5	4	3	1	3.2
	CS.1.5. Certifica ativos críticos	4	-	5	5	4	1	3.8
	CS.1.6. Exercícios e treinos	3	-	4	4	4	3	3.6
	"Análise risco, ameaça e vulnerabilidades"N3	-	-	5	-	-	-	5
	"Inventário/documentação de infraestruturas, instalações e pontos de contacto"N5	-	-	-	-	5	-	5
	"Análise de risco de cada infraestrutura / organização / serviço"N5	-	-	-	-	5	-	5
	"Modelação de ameaças"N5	-	-	-	-	4	-	4
	"Análise de Interdependências entre infraestruturas"N5	-	-	-	-	4	-	4
	"Existência de um plano de continuidade de negócio"N6	-	-	-	-	-	3	3
	Proteger							
	CS.2.1. Maturidade QNRCS (Proteger)	5	-	3	4	5	4	4.2
	CS.2.2. Foco em ativos críticos	4	-	5	5	4	4	4.4
	"Proteção multinível/camada."N4	-	-	-	5	-	-	5
	"Pen testing (testar proteção)"N4	-	-	-	4	-	-	4
	"Simulação/Treino (modelo capture the flag)"N4	-	-	-	4	-	-	4
	"Existência planos de segurança"N3	-	-	5	-	-	-	5
	"Existência diretor segurança"N3	-	-	5	-	-	-	5
	"Mecanismos de proteção ciber (firewalls, controle de acesso,...)"N5	-	-	-	-	5	-	5
	"Redundâncias (replicação, backups,...)"N5	-	-	-	-	4	-	4
	"Segurança da supply chain"N5	-	-	-	-	4	-	4
	Detetar							
	CS.3.1. Maturidade QNRCS (Detetar)	5	-	3	4	5	4	4.2
	CS.3.2. Agilidade na partilha e colaboração	3	-	5	5	5	4	4.4
	CS.3.3. Capacidade deteção de redes de distribuição de desinformação	4	-	5	4	5	2	4
	"Implementação de rede de sensores/sondas"N4	-	-	-	4	-	-	4
	"Capacidade de conhecimento situacional agregada (COP Cyber)"N4	-	-	-	5	-	-	5
	"Monitorização de redes e equipamentos ciber"N5	-	-	-	-	5	-	5
	"Correlação de eventos"N5	-	-	-	-	5	-	5
	"Auditorias / scans / testes de penetração periódicos para detetar APTs"N5	-	-	-	-	4	-	4
	Responder							
	CS.4.1. Maturidade QNRCS (Responder)	4	-	3	4	5	3	3.8
	CS.4.2. Capacidade de coordenação da resposta	3	-	5	5	5	3	4.2

	CS.4.3. Colaboração	5	-	4	4	4	3	4
	"Colaboração Nacional (G4)"N4	-	-	-	4	-	-	4
	"Cooperação Internacional (e.g. Rede Europeia CERT)"N4	-	-	-	4	-	-	4
	"Equipas de resposta a incidentes"N5	-	-	-	-	5	-	5
	"Exercícios de preparação"N5	-	-	-	-	5	-	5
	Recuperar							
	CS.5.1. Maturidade QNRCS (Recuperar)	4	-	3	4	5	3	3.8
	CS.5.2. Foco nos ativos críticos	4	-	5	5	4	3	4.2
	CS.5.3. Agilidade	3	-	5	4	4	3	3.8
	"Exercícios de preparação"N5	-	-	-	-	5	-	5
Ciberdefesa Capacidade Militar (FFAA)	Identificar/Planear							
	CD.1.1. Maturidade QNRCS (Identificar) ou equivalente	5	-	3	4	-	-	4
	CD.1.2. Foco em ativos críticos	4	-	5	5	-	-	4.7
	CD.1.3. Assume ataques com sucesso no planeamento	3	-	4	4	-	-	3.6
	CD.1.4. Garante diversidade (fornecedores, arquitetura)	3	-	5	4	-	-	4
	CD.1.5. Certifica ativos críticos	4	-	5	5	-	-	4.7
	CD.1.6. Exercícios e treinos	3	-	4	4	-	-	3.7
	CD.1.7. Projeção de poder	5	-	-	5	-	-	5
	"Segurança da Suply Chain Management"N4	-	-	-	4	-	-	4
	"Certificação de Sistemas e Entidades"N4	-	-	-	5	-	-	5
	"Mecanismos de degradação graciosa"N4	-	-	-	4	-	-	4
	"Segurança multi-nível"N4	-	-	-	5	-	-	5
	Proteger							
	CD.2.1. Maturidade QNRCS (Proteger) ou equivalente	5	-	3	4	-	-	4.7
	CD.2.2. Foco em ativos críticos	4	-	5	5	-	-	3.7
	CD.2.3. Projeção de poder e Dissuasão	5	-	-	5	-	-	5
	"Proteção multinível/camada"N4	-	-	-	5	-	-	4
	"Pen testing (testar proteção)"N4	-	-	-	4	-	-	5
	"Simulação/Treino (modelo red and blue)"N4	-	-	-	4	-	-	4
	Detetar							
	CD.3.1. Maturidade QNRCS (Detetar/ "infiltrar"N4) ou equivalente	5	-	3	4	-	-	4
	CD.3.2. Agilidade na partilha e colaboração	3	-	5	5	-	-	4.3
	CS.3.3. Capacidade deteção de redes de distribuição de desinformação	5	-	5	4	-	-	4.7
	"Implementação de rede de sensores/sondas"N4	-	-	-	5	-	-	5
	"Capacidade de conhecimento situacional agregada (COP Cyber)"N4	-	-	-	5	-	-	5
	Responder							
	CD.4.1. Maturidade QNRCS (Responder/"defender/neutralizar"N4) ou equivalente	4	-	3	4	-	-	3.7
	CD.4.2. Capacidade de coordenação da resposta	3	-	5	5	-	-	4.3
	CD.4.3. Colaboração	5	-	4	4	-	-	4.3
	CD.4.4. Capacidade OpCiber (ofensivas e defensivas)	5	-	-	4	-	-	4.5
	"Regras de empenhamento"N4	-	-	-	5	-	-	5
	"Enquadramento legal (uso da força)"N4	-	-	-	5	-	-	5
	"Capacidade de condução de operações Ciber multidomínio"N4	-	-	-	5	-	-	5
	"Colaboração Nacional (G4)"N4	-	-	-	4	-	-	4
	"Cooperação Internacional (e.g. NATO)"N4	-	-	-	4	-	-	4
	Recuperar							
	CD.5.1. Maturidade QNRCS (Recuperar) ou equivalente	4	-	3	4	-	-	3.7
	CD.5.2. Foco "na capacidade de garantir operação"N4 dos ativos críticos	4	-	5	5	-	-	4.7
	CD.5.3. Agilidade	3	-	5	4	-	-	4
	"Resiliência das Forças Armadas (visão multidomínio)"N4	-	-	-	5	-	-	5

Cibersegurança e Ciberdefesa	Adaptar							
	CSD.6.1. Documentar incidente	3	-	3	4	4	2	3.2
	CSD.6.2. Rever e corrigir configurações/ procedimentos	3	-	5	4	4	2	3.6
	CSD.6.3. Melhorar partilha de informação	4	-	5	5	4	2	4
	CSD.6.4. Testar resiliência contra ameaças similares	3	-	4	4	4	2	3.4
	CSD.6.5. Agilidade	3	-	5	4	3	2	3.4
	"Ajustar Regras de empenhamento"N4	-	-	-	5	-	-	5
	"Melhorar processos de colaboração (nacional)"N4	-	-	-	5	-	-	5
	"Melhorar processos de cooperação (internacional)"N4	-	-	-	5	-	-	5
	"Ajustar enquadramento legal de Ciberdefesa e Cibersegurança"N4	-	-	-	5	-	-	5
	"Exercícios de preparação"N5	-	-	-	-	4	-	4
Social	S.1. Oferta formativa em cibersegurança	4	-	4	5	5	3	4.2
	S.2. Níveis de ensino onde se ministram conteúdos de cibersegurança	3	-	4	4	4	5	4
	S.3. Observação de atitudes e comportamentos (e.g., Observatório do CNCS)	3	-	4	4	3	4	3.6
	"Campanhas de sensibilização para a cibersegurança nacional"N4,N5	-	-	-	5	3	-	4
	"Índice de produção científica na área da cibersegurança/defesa (não só tecnológica mas em áreas transversais)"N1	4	-	-	-	-	-	4
Económico	E.1. Investimento privado e público em cibersegurança incluindo I&D"&inovação"N1 (e.g., Observatório do CNCS)	4	-	5	5	4	5	4.6
	E.2. Mercado de trabalho de cibersegurança (e.g., Observatório do CNCS)	3	-	4	4	4	4	3.8
	"Quadro de competências-base em cibersegurança e utilização de tecnologias digitais (acesso ao mercado de emprego)"N4	-	-	-	5	-	-	5
Político	P.1. Existe uma estratégia de segurança no ciberespaço que contemple resposta a ameaças híbridas?	4	-	3	4	5	5	4.2
	P.2. Existe atribuição de competências na resposta a ameaças híbridas?	5	-	5	5	5	4	4.8
	P.3. Políticas de investimento em cibersegurança e ciberdefesa	4	-	4	4	4	4	4
	P.4. O regime jurídico da segurança do ciberespaço impõe obrigatoriedade de certificação/"requisitos ao invés de certificação"N1 (e.g., ISO27001 ou eventual certificação QNRCS pelo CNCS)?	4	-	4	4	4	5	4.2
	P.5. Existe um planeamento civil de emergência para fazer face a ameaças híbridas no ciberespaço?	5	-	5	5	5	3	4.6
	P.6. Existem autoridades nacionais competentes em matéria eleitoral com recursos adequados para responder a ameaças híbridas no ciberespaço?	4	-	4	5	4	3	4
	"Existe um sistema nacional de gestão de crises para responder a ameaças híbridas no ciberespaço?"N4	-	-	-	5	-	-	5
	"Existem processos de cooperação internacional neste domínio?"N4	-	-	-	5	-		5
	"Existe um planeamento de intervenção das Forças e Serviços de Segurança?"N3	-	-	5	-	-	-	5
	"Existe um planeamento de intervenção de capacidades civis com capacidades militares?"N3	-	-	5	-	-	-	5
	"A estratégia de cibersegurança está materializada em medidas concretas e mensuráveis?"N5	-	-	-	-	3	-	3
	"Análise de risco (quem pode ter interesse em realizar ataques híbridos? Qual a probabilidade de acontecer?	-	-	-	-	4	-	4

	Quais os grupos sociais mais vulneráveis a serem influenciados?)"N5							
	"Os reguladores de setores identificados no DL 46/18 produziram regulação apropriada?"N6	-	-	-	-	-	5	5
	"O regime jurídico existente é eficaz na identificação de regras que as as entidades críticas deveam cumprir?"N6	-	-	-	-	-	5	5
Informação (partilha)	I.1. Existe uma Célula de Fusão para Ameaças Híbridas ao nível nacional "e interoperável com o da UE"N1?	4	-	5	5	5	3	4.4
	I.2. Existe coordenação entre instituições e uma definição clara dos fluxos de partilha de informação e colaboração?	5	-	5	5	5	4	4.8
	I.3. Existe um sistema de informação comum para conhecimento situacional de ameaças híbridas aos diferentes níveis e entre as diferentes instituições?	4	-	4	5	4	5	4.4
	I.4. Nível de risco e registos da evolução das ameaças-híbridas no ciberespaço em Portugal	4	-	3	4	4	4	3.8
	"Existem sistemas e processos de troca de informação de forma a viabilizar a cooperação internacional neste domínio?"N4	-	-	-	5	-	-	5
	"Exercícios de treino para resposta a ataques híbridos"N5	-	-	-	-	4	-	4

Tabela 2 - Análise das respostas de validação (resiliência à desinformação)

Questão 1. Analise a matriz e proponha/adicione outros indicadores (**na própria matriz**) que considere relevantes para avaliar a resiliência. Se necessário coloque um comentário a descrever com mais detalhe o indicador adicionado.

Questão 2. Numa escala entre 1 (pouco importante) a 5 (muito importante), indique na matriz a importância que atribui a todos os indicadores

Domínio	Indicador Nota: as unidades de registo são identificadas entre aspas e ID de entrevistado. Só os indicadores predefinidos e as unidades de registo com 2 ou mais coocorrências, com avaliação média igual ou superior a "3.5", são contabilizadas como indicador válido (a verde)	Relevância de 1 a 5 Respostas dos entrevistados N1	N2	N3	N4	N5	N6	Média
Político	P.1. Existem autoridades nacionais competentes em matéria eleitoral com recursos adequados para responder a ameaças híbridas?	3	-	4	4	4	2	3.4
	P.2. Está definida a coordenação entre instituições e uma definição clara dos fluxos de partilha de informação e colaboração?	4	-	5	5	5	3	4.4
	P.3. A legislação em vigor permite o combate eficaz à desinformação no âmbito das ameaças híbridas?	3	-	3	4	4	3	3.4
	P.4. Existe uma estratégia nacional que contemple resposta à desinformação no âmbito das ameaças híbridas?	4	-	5	3	5	4	4.2
	P.5. Existe uma estratégia de comunicação para preparar a população ou contrariar narrativas de desinformação?	3	-	5	4	5	5	4.4
	"Existem mecanismos de cooperação internacional no domínio político-diplomático para responder à desinformação no âmbito das ameaças híbridas?"N4,N6	-	-	-	5	-	5	5
	"Existem códigos de conduta para as plataformas sociais que permitam a remoção de conteúdos desinformativos ou de informação falsa?"N3	-	-	5	-	-	-	5
	"Existe uma autoridade nacional que determine a remoção de conteúdos desinformativos ou de informação falsa?"N3	-	-	5	-	-	-	5
	"Existe um regime sancionatório para punir a não remoção ou a publicação dolosa de conteúdos desinformativos ou de informação falsa?"N3	-	-	5	-	-	-	5
	"Os partidos políticos têm líderes com capacidade para compreender o problema das ameaças híbridas e de dar resposta legislativa adequada?"N5	-	-	-	-	4	-	4

	"Mecanismos de controle dos mecanismos de controle de desinformação, pois podem ser usados em sentido inverso (Quem guarda os guardas?)"N5	-	-	-	-	5	-	5
	"Existe uma coordenação entre entidades públicas e privadas (e.g. órgãos de comunicação social) para contrariar narrativas de desinformação?"N6	-	-	-	-	-	5	5
Militar	M.1. Agilidade na partilha, cooperação e coordenação com as autoridades civis	3	-	-	4	4	4	3.75
	M.2. Capacidades para detetar, analisar e denunciar desinformação ao nível militar	3	-	-	5	5	4	4.25
	M.3. Exercícios militares que contemplem o combate à desinformação (e.g., que vise denegrir e enfraquecer a instituição ou a liderança militar)	3	-	-	5	5	3	4
	M.4. Existe um plano de comunicação estratégico que reforce a união e prestígio da instituição militar e vise anular efeitos de desinformação?	4	-	-	4	4	5	4.25
	"As Forças Armadas têm capacidade para desenvolver operações de informação (defensivas/ofensivas) para fazer face a ataques de desinformação?"N4	-	-	-	5	-	-	5
	"Existem mecanismos de planeamento e coordenação de operações de informação?"N4	-	-	-	5	-	-	5
	"Uma vez que as *Computer Network Operations* fazem parte das operações de informação, existe um planeamento integrado com as operações no ciberespaço?"N4	-	-	-	5	-	-	5
	"Mecanismos de controle dos mecanismos de controle de desinformação, pois podem ser usados em sentido inverso (Quem guarda os guardas?)"N5	-	-	-	-	5	-	5
Econ.	E.1. Investimento em I&D para criação de mecanismos de combate à desinformação	3	-	4	4	5	4	4
	"Campanhas de sensibilização para a proteção de patentes e segredo industrial (proteção contra-espionagem e contra-desinformação)"N4	-	-	-	5	-	-	5
	"Criar um observatório de atividades de "guerra económica" (ver caso francês), de forma a identificar campanhas de desinformação no domínio económico."N4	-	-	-	4	-	-	4
	"Existem Órgãos de Comunicação Social manipuláveis por falta de capacidade económica?"N3	-	-	5	-	-	-	5
Social	S.1. Percentagem de votos em partidos populistas (e.g., *Timbro Authoritarian Populism Index*)	4	-	1	3	3	-	2.75
	S.2. Variação de votos (e.g., mapas oficiais de eleições)	3	-	1	4	2	-	2.5
	S.3. Variação de discursos populistas em Portugal (e.g., *Global Populism Database*)	4	-	1	3	3	-	2.75
	S.4. Nível de polarização da sociedade (e.g., V-Dem https://www.v-dem.net/)	4	-	3	4	4	-	3.75
	S.5. Monitorização do nível de influência política no meio académico (e.g., questionários aos alunos)	3	-	3	3	3	-	3
	S.6. Nível de confiança nos *media* (digitalnewsreport.org/interactive/)	3	-	4	4	3	4	3.6
	S.7. Percentagem de uso de redes sociais como fonte de notícias (digitalnewsreport.org/interactive/)	4	-	4	4	3	4	3.8
	S.8. Mecanismos para identificação de audiências alvo mais vulneráveis às campanhas de desinformação	3	-	4	5	4	5	4.2
	"Identificação de "fake news" e de narrativas destinadas a manipular a informação"N4	-	-	-	5	-	-	5
	"Índice de produção cientifica na resposta à desinformação"N1	3	-	-	-	-	-	3
	"Nível de literacia digital e comunicacional da população"N3	-	-	5	-	-	-	5
	"Existência de mecanismos independentes (opinion makers) de verificação de informação (polígrafo)?"N3	-	-	5	-	-	-	5
	"Sensibilização da opinião pública"N5	-	-	-	-	4	-	4
	"Monitorização de redes sociais, meios de comunicação social (jornais, TV,...), blogs, etc."N5	-	-	-	-	5	-	5

	"Existência de canais para dar resposta entre a opinião pública (e.g., *Fact Check* Observador, Polígrafo da SIC,... e canais em redes sociais)"N5	-	-	-	-	4	-	4
Inform.	I.1. Quantidade de mecanismos (e.g., *fact checks*), por cada órgão de comunicação social, para detetar, analisar e denunciar as fontes e combater a desinformação	4	-	5	4	4	3	4
	I.2. Existe um sistema de informação comum para conhecimento situacional da desinformação aos diferentes níveis e entre as diferentes instituições?	3	-	3	4	4	5	3.8
	I.3. Nível de risco e registos da evolução da desinformação em Portugal	3	-	4	4	4	4	3.8
	I.4. Existe uma plataforma pública centralizada para difundir campanhas de desinformação (e.g., https://euvsdisinfo.eu/)?	4	-	5	4	4	5	4.4
	I.5. Existem mecanismos para certificação de órgãos de comunicação social na internet?	3	-	4	5	3	4	3.8
	I.6. Variação do volume das ações de sensibilização (inclui comunicação estratégica e educação)	3	-	4	4	4	3	3.6
	I.7. Ações de formação para jornalistas	4	-	5	4	3	3	3.8
	"Existem processos e organizações responsáveis pelo desenvolvimento de Cyber Intel /Media Intel?"N4	-	-	-	5	-	-	5
	"Existem organizações nacionais (civis e militares) responsáveis pela condução de operações de informação?"N2	-	-	-	5	-	-	5
	"Existência de códigos de conduta e regras de utilização das redes sociais e dos Órgãos de Comunicação Social para combater a desinformação"N3	-	-	5	-	-	-	5
Infraest.	II.1. Existe um gabinete de comunicação estratégica?	4	-	5	4	-	3	4
	II.2. Existe uma Célula de Fusão Nacional para aumentar o conhecimento situacional?	4	-	5	5	-	4	4.5
	II.3. Existem recursos e infraestruturas dedicadas à deteção de campanhas de desinformação no ciberespaço (inclui deteção de redes de distribuição com *bots* ou *trolls*)?	4	-	5	4	-	5	4.5

Quadro 8 - Respostas integradas à questão 3 da parte 1 e parte 2

Questão 3. Identifica comentários/contributos para melhoria da abordagem relativa à construção da matriz de resiliência?

ID	Ideias-Chave
N1	"A **matriz necessita ser convertida numa ferramenta que ajude a monitorizar e melhorar a resiliência nacional**" "Existem planos para a criação de uma **Autoridade Nacional de Certificação de Cibersegurança** através do CNCS […] que permitirá a atribuição de um **selo digital com 3 níveis (bronze, prata ouro)**." "**A certificação em Segurança da Informação" será um processo** tal como o de "certificação RGPD" ou outro como "certificação ambiental, habitabilidade ou acessibilidade".
N2	**"Já existe uma proposta de sistema de resiliência nacional (classificado)** […] associada a uma **nova proposta sobre o sistema nacional de gestão de crises** que é o que lida com o **fenómeno das ameaças híbridas e com outras crises… como um terramoto**". "A resiliência nacional contra ameaças híbridas deve ser vista numa **preceptiva integrada com a NATO (resiliência na estratégia 2030) e a UE (5ª componente é o sistema de resiliência na bússula estratégica)".** O **"plano de recuperação económica proposto pelo governo**, diz que devemos desenvolver (nós Portugal e nós as alianças) **sistemas de resiliência** que nos permitam fazer face a qualquer tipo de ameaça … como? sistema integrado de resposta ***whole-of-society approach* (abrangente) e *whole-of-government approach* (integrada)"** "Este futuro Sistema deve permitir **monitorização constante** de **qualquer tipo de ameaça e riscos de um país**" e deve poder **dar uma proposta de solução/resposta** … "**através de inteligência**

	artificial, computação quântica e *bigdata* […] será um género de **centro de comando operacional *whole-of-government***"
N3	"A revisão da Diretiva em vigor centra a sua abordagem na **resiliência das entidades críticas, ao invés da proteção de infraestruturas críticas** […] aproximando-se da futura "**Diretiva NIS 2, em que a resiliência física e a resiliência cibernética das entidades se aproximam**." "A questão da **desinformação** é um tema que exige um grande equilíbrio" devido ao direito à "**liberdade de expressão**, pelo que nesta matéria se trilham **linhas muito ténues** e as medidas se estendem por um limbo difícil de definir."
N4	"existe valor acrescentado em incluir a visão de especialistas dos diversos vetores do poder nacional" "o ciberespaço interseta transversalmente todos" os domínios PMESII, "afetando também, por essa razão, a ciber-resiliência nacional de uma forma agregada." "**A CD e CS** […] **sobrepõe-se no que à CS diz respeito**", portanto, **a CD deve focar-se no "acréscimo de capacidades nos vários domínios apresentados** […] decorrente da especificidade do emprego da força" para a "salvaguarda da soberania nacional […] a **própria resiliência das Forças Armadas e do Estado depende disso**" Na resiliência face à **desinformação** "assume especial acuidade estabelecer a relação doutrinaria com as **INFO OPS**, **responsáveis pela coordenação e integração das CNO** no contexto do desenvolvimento de operações defensivas e ofensivas."
N5	"A matriz proposta **corre o risco de ser uma *wishlist* de métricas que é desejável maximizar,** mas que é **demasiado longa para ser útil na prática**, ou seja, para dela extrair medidas concretas passíveis de serem implementadas e de terem impacto… **será útil definir quais são os N indicadores mais prioritários** que permitem reduzir o problema em X% […] Além das prioridades, outro aspeto a considerar é o balanço com a facilidade de implementação." Quanto à desinformação, "os mecanismos são importantes para o combate às ameaças híbridas, mas corre-se o risco de se tornarem em mecanismos de censura ou controle da opinião pública"
N6	Um tópico de discussão interessante seria a "**obrigatoriedade de as empresas realizarem ações de formação de cibersegurança** (e.g. e-learning) utilizando, por exemplo, os cursos disponibilizados pelo CNCS" "os indicadores relativos ao QNRCS devem ter por base **níveis diferentes de maturidade** … pois é muito difícil todas as organizações conseguirem implementar o mesmo nível de maturidade, tendo em **conta diferentes capacidades e criticidade**." "A **diversidade de fornecedores e arquiteturas** não é necessariamente bom pois acarreta **custos acrescidos e aumenta a superfície de ataque**." "A Lei nº46/18 que estabelece o **regime jurídico da segurança do ciberespaço é insuficiente para que possa impor medidas**. Este regime, transposto da Diretiva NIS, obriga, em alto-nível, a que algumas entidades tenham a obrigação de ter uma resposta a incidentes coordenada com o CNCS. **Será necessário que haja um regime jurídico mais efetivo e eficaz."** "Quanto aos indicadores de desinformação, os que são associados ao populismo ou variação dos votos […] podem estar enviesados pois está-se a fazer uma associação que os partidos populistas são por si só fontes de desinformação, poderá ser verdade, mas pode tornar tendencial o indicador."

Apêndice D — Informação sobre os indicadores de resiliência

Quadro 9 – Descrição dos indicadores de resiliência face à desinformação

Indicador	Motivação	- Definição - Sugestão de avaliação do indicador
Domínio Político		
P.1. Está definida a coordenação entre instituições e uma definição clara dos fluxos de partilha de informação e colaboração?	O plano de ação contra a desinformação da UE (PADUE) prevê o reforço das respostas coordenadas (perspetiva abrangente). O plano de ação para a democracia europeia (PADE) convida os Estados-Membros a investir na coordenação integrada entre entidades relevantes.	Existência de legislação nacional que defina a coordenação entre instituições e os fluxos de partilha relativo à desinformação. Avaliação qualitativa (sim/parcial/não) ou quantitativa (e.g., % de instituições com canais de coordenação).
P.2. Existe uma estratégia nacional que contemple resposta à desinformação no âmbito das AH?	O conceito estratégico de defesa nacional (2013) em vigor, não refere a desinformação como risco. A atualização da estratégia permitirá medidas subsequentes e resolver lacunas identificadas. Conforme recomendação do NATO StratCom COE (2019, p. 10)	Existência de uma estratégia nacional que inclua o tema das AH e da desinformação. Avaliação qualitativa (sim/parcial/não).
P.3. Existe uma estratégia de comunicação para preparar a população ou contrariar narrativas de desinformação?	A comunicação conjunta para aumentar a resiliência e reforçar a capacidade de enfrentar AH, refere que é fundamental reforçar a comunicação estratégica, para sensibilizar e educar o público geral a distinguir a desinformação.	Existência de uma estratégia de comunicação eficaz para sensibilizar a população e contrariar as narrativas de desinformação. Avaliação qualitativa (sim/parcial/não).
P.4. Existem mecanismos de cooperação internacional no domínio político-diplomático para responder à desinformação no âmbito das AH?	No âmbito da operacionalização do SAR, o PADUE pede aos Estados-Membros que designem um ponto de contato, para partilhar alertas e assegurar a coordenação interna e externa, incluindo o suporte a sanções.	Existência de mecanismos de cooperação (incluindo um ponto de contato) internacional no domínio político-diplomático para responder à desinformação no âmbito das AH. Avaliação qualitativa (sim/parcial/não).
Domínio Militar		
M.1. Agilidade na partilha, cooperação e coordenação com as autoridades civis	O NATO StratCom COE (2019, p. 22) refere que as autoridades nacionais devem partilhar informação com agilidade, permitindo responder às AH. Na abordagem *whole-of-government* a interação civil- militar é fundamental.	Nível de interação entre militares e civis, garantindo a agilidade na partilha, cooperação e coordenação face a AH. Avaliação qualitativa (sim/parcial/não) ou quantitativa (e.g., % de instituições que têm interação com a militar).
M.2. Capacidades para detetar, analisar e denunciar desinformação ao nível militar	O caso da Crimeia revelou os efeitos da desinformação na instituição militar. Deve haver uma capacidade militar para o combate à desinformação, em linha com o pilar um do PADUE.	Existência de capacidade militar para detetar, analisar e denunciar desinformação. Avaliação qualitativa (sim/parcial/não).
M.3. Exercícios militares que contemplem o combate à desinformação (e.g., que vise denegrir a instituição ou a liderança militar)	Em linha com o desenvolvimento de exercícios internacionais, e.g., PACE (NATO-UE), é necessário não só promover a participação nacional nesses exercícios, como também integrar nos exercícios nacionais, objetivos de treino que lidem com a desinformação.	Participação das FFAA em exercícios que contemplem o combate à desinformação. Avaliação qualitativa (sim/parcial/não) ou quantitativa (e.g., #exercícios de treino da resposta à desinformação).

M.4. Existe um plano de comunicação estratégico que reforce a união e prestígio da instituição militar e vise anular efeitos de desinformação?	O PADUE refere na página 7, que para combater a desinformação é fundamental uma comunicação efetiva e regular. A ERC (2019) refere que a desinformação é diluída com informação de qualidade. Um plano de comunicação estratégico é assim fundamental para reforçar e credibilizar as FFAA.	Existência de um plano de comunicação estratégico que reforce a união e prestígio da instituição militar e vise anular efeitos de desinformação. Avaliação qualitativa (sim/parcial/não).
Domínio Económico		
E.1. Investimento em I&D para criação de mecanismos de combate à desinformação	O PADUE, no âmbito do pilar 4, refere que os Estados-Membros devem suportar a I&D no combate à desinformação, para identificação de estruturas e mecanismos de disseminação, no ambiente de informação nacional.	Nível de investimento em I&D para criação de mecanismos de combate à desinformação. Avaliação quantitativa (e.g., % do investimento em I&D dedicado ao combate à desinformação).
Domínio Social		
S.1. Nível de polarização da sociedade	A falta de coesão social pode ser explorada (NATO StratCom COE, 2019, p. 30). Quanto maior a polarização menor será a resiliência à desinformação (Humprecht et al., 2020). O PADE diz que é fundamental fomentar a confiança na democracia (p. 12).	Nível de polarização da sociedade e confiança na democracia. Avaliação quantitativa - resultado de sondagens sobre o estado da democracia (e.g. https://www.v-dem.net/).
S.2. Nível de confiança nos *media*	A resiliência à desinformação é menor nas sociedades onde a desconfiança nos OCS oficiais é elevada (Humprecht et al., 2020). A credibilidade da informação é fundamental (CE, 2018b).	Nível de confiança nos OCS oficiais. Avaliação quantitativa - resultado de sondagens sobre a exposição à desinformação nos OCS (e.g. digitalnewsreport.org/interactive/)
S.3. Percentagem de cidadãos que usa redes sociais como fonte de notícias	Segundo o PADUE, p. 4, as redes sociais tornaram-se importantes meios de difusão da desinformação. Níveis baixos de utilização das redes sociais proporcionam melhores condições para a resiliência e menor exposição à desinformação (Humprecht et al., 2020).	Percentagem de cidadãos que usa redes sociais como fonte de notícias. Avaliação quantitativa (e.g., % de cidadãos que usa redes sociais como fontes de notícias) (e.g. digitalnewsreport.org/interactive/)
S.4. Existem mecanismos para identificação de audiências alvo mais vulneráveis às campanhas de desinformação?	Compreender a lógica adversária, conduz à identificação de vulnerabilidades e audiências alvo, permitindo uma comunicação coerente e eficaz para manter a confiança e a coesão nessas audiências (NATO StratCom COE, 2019, pp. 12-13).	Existência de mecanismos para identificação de audiências alvo mais vulneráveis às campanhas de desinformação. Avaliação qualitativa (sim/parcial/não).
Domínio Informação		
I.1. Quantidade de mecanismos (e.g. *fact-checks*), por OCS, para detetar, analisar e denunciar as fontes e combater a desinformação	Os *fact-checkers* são fundamentais para o combate à desinformação (NATO StratCom COE, 2019, p. 31). O PADE prevê intensificar a verificação dos factos (CE, 2020a, p. 27).	Quantidade de mecanismos (e.g. *fact-checks*), por OCS, para detetar, analisar e denunciar as fontes e combater a desinformação. Avaliação quantitativa (e.g., %OCS com mecanismos para deteção, análise e denúncia de desinformação)
I.2. Existe um sistema de informação comum para conhecimento situacional da desinformação aos	O PADUE previu o SAR, para partilha de informações (entre Estados-Membros NATO e UE) sobre campanhas de desinformação em curso. Na mesma linha, é fundamental um	Existência um sistema de informação comum para conhecimento situacional da desinformação aos diferentes níveis e entre as diferentes instituições (*whole-of-government*).

diferentes níveis e entre as diferentes instituições?	sistema de informação (interno), com foco no ambiente de informação nacional, numa abordagem *whole-of-government*.	Avaliação qualitativa (sim/não).
I.3. Nível de risco e registos da evolução da desinformação em Portugal	Compreender as ameaças, os seus objetivos e modo de atuação, permite antecipar futuros desenvolvimentos e ajustar a preparação e resposta (NATO StratCom COE, 2019, p. 12).	Nível de risco e registos da evolução da desinformação em Portugal. Avaliação qualitativa (Risco baixo/médio/alto). Avaliação qualitativa (atores, incidentes, ameaças, prospetivas, táticas, técnicas e procedimentos do adversário)
I.4. Existe uma plataforma pública centralizada para difundir campanhas de desinformação (e.g. https://euvsdisinfo.eu/)?	Tal como a inciativa do *East StratCom* ao criar o euvsdisinfo.eu, considera-se importante uma plataforma pública nacional que denuncie campanhas de desinformação que prejudiquem o processo de decisão, funções críticas do estado e a coesão social.	Existência de uma plataforma pública centralizada para difundir campanhas de desinformação que visem que prejudicar o processo de decisão, funções críticas do estado e a coesão social. Avaliação qualitativa (sim/não).
I.5. Existem mecanismos para certificação de órgãos de comunicação social na internet?	Os OCS - rádio, televisão ou imprensa - independentemente da plataforma utilizada, são sujeitos a supervisão da ERC, obrigando-os a registo junto da mesma (ERC, 2019, p. 31). Seria útil ter esse registo sempre visível (nas plataformas em linha) e legislação que sancione quem não o tiver (ERC, 2019, p. 32).	Existência de mecanismos para certificação de OCS na internet. Avaliação qualitativa (sim/não).
I.6. Variação do volume das ações de sensibilização (inclui comunicação estratégica e educação) (i.e., literacia mediática)	A sensibilização da sociedade para valores democráticos e para a necessidade de avaliar e cruzar de forma crítica conteúdos e fontes (literacia mediática), deve ser contínua e inclusiva *whole-of-society* (CE, 2020a, p. 28).	Variação do volume das ações de sensibilização, por jornalistas a docentes ou público em geral, ou integrada nos planos curriculares Avaliação quantitativa (e.g., taxa de crescimento anual de ações de sensibilização)
I.7. Ações de formação para jornalistas	Qualificação dos jornalistas e promoção dos valores fundamentais do jornalismo, em ambientes em linha (ERC, 2019, p. 52)	Quantidade de formação para jornalistas focada na desinformação em linha. Avaliação quantitativa (e.g., #ações de formação do Cenjor)
Domínio Infraestruturas		
II.1. Existe um gabinete de comunicação estratégica?	O PADUE prevê o reforço das estruturas de *StratCom* da UE e que o ponto de contato para o SAR, de preferência, pertença a um departamento de comunicação estratégica nacional.	Existência de um gabinete (departamento ou estrutura) de comunicação estratégica. Avaliação qualitativa (sim/não).
II.2. Existe uma Célula de Fusão Nacional para aumentar o conhecimento situacional?	Tal como a UE tem uma Célula de Fusão integrada no INTCEN, ao nível nacional, deverá existir uma Célula de Fusão nos serviços de informações, para integrar contributos internos.	Existência de uma Célula de Fusão Nacional para aumentar o conhecimento situacional. Avaliação qualitativa (sim/não).
II.3. Existem recursos e infraestruturas dedicadas à deteção de campanhas de desinformação no ciberespaço (inclui deteção de redes de distribuição com *bots* ou *trolls*)?	O pilar 3 do PADUE refere a mobilização das plataformas em linha para deteção de redes de distribuição com *bots* e contas falsas. Contudo, é necessária a colaboração com investigadores, verificadores de factos, sociedade civil e autoridades nacionais com competências no ciberespaço (*whole-of-society*).	Existência de recursos e infraestruturas dedicadas à deteção de campanhas de desinformação no ciberespaço (inclui deteção de redes de distribuição com *bots* ou *trolls*). Avaliação qualitativa (sim/não).

Quadro 10 – Descrição dos indicadores de ciber-resiliência

Indicador	Motivação	- Definição - Sugestão de avaliação do indicador
Domínio Infraestruturas (cibersegurança)		
CS.1.1. Maturidade QNRCS (Identificar)	A RCM n.º55/2020, prevê que 80 % dos organismos da AP deverão ser certificados em conformidade com o QNRCS. A maturidade da postura de cibersegurança é um indicador de resiliência.	Nível de maturidade de cibersegurança das entidades críticas, no objetivo Identificar do QNRCS. Avaliação quantitativa por setor de atividade (e.g., % de medidas implementadas - Identificar do QNRCS - de acordo com o perfil/setor)
CS.1.2. Foco em ativos críticos	O foco nos ativos críticos é um princípio no desenho de resiliência (Ross et al., 2019, 99). Apesar da gestão de ativos (críticos ou não) fazer parte do QNRCS (indicador CS.1.1), o foco nos ativos críticos é tão importante que deve ter um indicador dedicado.	As entidades críticas identificam os ativos críticos (humanos, tecnológicos, dispositivos, dados, tempo e aplicações) e meios primários e redundantes ou secundários. Avaliação qualitativa por setor de atividade (sim/parcial/não de acordo com o perfil/setor)
CS.1.3. Assume ataques com sucesso no planeamento	A resiliência lida com ameaças incertas e vulnerabilidades desconhecidas. O processo de avaliação e gestão do risco (previsto no indicador CS.1.1) deve prever mitigar essas disrupções, mas devem ser definidos critérios de resiliência (previsto no CS.1.1) e haver um indicador dedicado.	As entidades críticas assumem a existência de ameaças incertas e vulnerabilidades desconhecidas e preveem requisitos de resiliência para suportar a prestação de serviços críticos. Avaliação qualitativa por setor de atividade (sim/parcial/não de acordo com o perfil/setor).
CS.1.4. Certifica ativos críticos	A diretiva SRI2.0 irá prever a certificação e o CNCS será a autoridade nacional de certificação. Os ativos críticos (*hardware/software*) deverão ser submetidos a certificação.	Percentagem de ativos críticos certificados por cada entidade crítica. Avaliação quantitativa por setor de atividade (e.g., % de ativos críticos certificados de acordo com o perfil/setor)
CS.1.5. Exercícios e treinos	Os exercícios e treinos permitem formar, avaliar, praticar e melhorar o desempenho de uma organização (ISO 22301).	Percentagem entidades críticas que participam em exercícios de CS. Avaliação quantitativa por setor de atividade (e.g., % de entidades críticas que participam em exercícios de cibersegurança)
CS.2.1. QNRCS (Proteger)	Equivalente ao indicador CS.1.1	Equivalente ao indicador CS.1.1 mas para objetivo Proteger.
CS.2.2. Foco em ativos críticos	Os recursos para implementar medidas de proteção podem ser escassos e a priorização das mesmas devem em primeiro lugar salvaguardar os ativos críticos.	As entidades críticas priorizam as medidas de proteção nos ativos críticos. Avaliação qualitativa por setor de atividade (sim/parcial/não de acordo com o perfil/setor).
CS.3.1. QNRCS (Detetar)	Equivalente ao indicador CS.1.1	Equivalente ao indicador CS.1.1 mas para objetivo Detetar.
CS.3.2. Agilidade na partilha e colaboração	Devem estar estabelecidos canais de comunicação com o CNCS e rede CSIRT para partilha imediata.	Percentagem de entidades críticas que têm um ponto de contato com o CNCS. Avaliação quantitativa (e.g., % de entidades com ponto de contacto).
CS.3.3. Deteção de redes de distribuição de desinformação	As entidades críticas podem estar sujeitas a desinformação, com variados fins, por exemplo, económicos, destabilização, etc. É importante terem capacidade de detetar quando são alvo de desinformação.	Percentagem de entidades críticas têm capacidade de detetar desinformação e contribuir para a deteção de redes de distribuição de desinformação.

		Avaliação quantitativa por setor de atividade (e.g., % de entidades com capacidade para detetar desinformação).
CS.4.1. QNRCS (Responder)	Equivalente ao indicador CS.1.1	Equivalente ao indicador CS.1.1 mas para objetivo Responder.
CS.4.2. Capacidade de coordenação da resposta	A coordenação da resposta com partes interessadas deve ocorrer conforme planos de resposta previsto no indicador CS.4.1. Contudo, este indicador reforça a importância do plano de resposta a incidentes.	Percentagem de entidades críticas que têm um plano de resposta a incidentes. Avaliação quantitativa por setor de atividade (e.g., % de entidades com plano de resposta a incidentes).
CS.4.3. Colaboração	A colaboração com outras entidades e organizações é muito importante. A adesão à rede nacional CSIRTs é um bom princípio, contudo, implica requisitos que nem todas as entidades conseguem cumprir.	Percentagem de entidades críticas que fazem parte da rede nacional de CSIRT. Avaliação quantitativa por setor de atividade (e.g., % de entidades membros da rede nacional de CSIRT).
CS.5.1. QNRCS (Recup.)	Equivalente ao indicador CS.1.1	Equivalente ao indicador CS.1.1 mas para objetivo Recuperar.
CS.5.2. Foco nos ativos críticos	A alocação de recursos necessária no processo de recuperação, deve priorizar a continuidade de operação dos ativos críticos.	As entidades críticas priorizam as medidas de recuperação nos ativos críticos. Avaliação qualitativa por setor de atividade (sim/parcial/não de acordo com o perfil/setor).
CS.5.3. Agilidade	A agilidade na recuperação deve ser medida e testada com simulações e exercícios dos planos de recuperação e resposta.	Percentagem de entidades críticas que testam a agilidade na implementação do plano de continuidade de negócio. Avaliação quantitativa por setor de atividade (e.g., % de entidades que testam e registam implementação de um plano de recuperação).
CSD.6.1. Rever e corrigir configurações/ procedimentos	É fundamental rever os planos de recuperação de acordo com as lições aprendidas (previsto no CS.5.1).	Percentagem de entidades críticas que reviram os planos de recuperação e as configurações/procedimentos após incidente. Avaliação quantitativa por setor de atividade (e.g., % de entidades que reviram os planos de recuperação e processos após incidente).
CSD.6.2. Melhorar partilha de informação	Os processos de partilha de informação são normalmente postos à prova em situações de crise. Importa rever e melhorar os canais de comunicação.	Percentagem de entidades críticas que reviram os processos e canais de partilha de informação após incidente. Avaliação quantitativa por setor de atividade (e.g., % de entidades que reviram os processos e canais de partilha de informação após incidente).
Domínio Militar		
CD.[1…5].x=CS.[1…5].x	Equivalente ao indicador CS.[1…5].x A ciberdefesa e a cibersegurança sobrepõe-se no que à cibersegurança diz respeito.	Equivalente ao indicador CS.[1…5].x Avaliação das FFAA
CD.1.6. Garante diversidade (fornecedores, arquitetura)	A diversidade é uma das técnicas de ciber-resiliência, em conjunto com a redundância (duplicação de ativos) (Ross et al., 2019, 12). Consiste em usar heterogeneidade nos sistemas para minimizar impacto de vulnerabilidades comuns ou eliminar a dependências. Contudo, tem custo alto e aumenta a superfície.	As FFAA garantem diversidade: (i) dos seus fornecedores; (ii) de troços de comunicações; (iii) de arquitetura (e.g., uso de mais que um Sistema Operativo) Avaliação qualitativa por abordagem de diversidade (sim/parcial/não de acordo com o perfil/setor).

CD.1.7. Projeção de poder	A capacidade de planear e conduzir OpCiber (ofensivas) é fundamental para projetar poder (AJP-3.20, 2020).	As FFAA têm capacidade de planear a condução de operações ofensivas no ciberespaço. Avaliação qualitativa (sim/parcial/não).
CD.2.3. Projeção de poder e Dissuasão	A capacidade de conduzir OpCiber (ofensivas e defensivas) é fundamental para dissuadir um adversário.	As FFAA têm capacidade de conduzir operações ofensivas e defensivas no ciberespaço. Avaliação qualitativa (sim/parcial/não).
CD.4.4. Capacidade de OpCiber (ofensivas e defensivas)	No âmbito das AH, é ainda importante a capacidade de integrar as OpCiber no âmbito das *InfoOps* (entrevista via mail, 08 de março de 2021).	As FFAA têm capacidade de conduzir operações ofensivas no ciberespaço e integrar as *InfoOps*. Avaliação qualitativa (sim/parcial/não).
Domínio Social		
S.1. Oferta formativa em cibersegurança	O eixo 2 da ENSC visa a prevenção, educação e sensibilização através da formação técnica avançada em segurança do ciberespaço no ensino superior universitário. É também importante a formação especializada e sensibilizar decisores, gestores públicos, etc.	Existência de formação técnica avançada e de formação especializada na área da cibersegurança no ensino superior. Avaliação quantitativa formação especializada (e.g., % de universidades com unidades curriculares de cibersegurança). Avaliação quantitativa formação técnica avançada (e.g., # cursos de formação avançada em cibersegurança).
S.2. Níveis de ensino onde se ministram conteúdos de cibersegurança	O eixo 2 da ENSC visa a prevenção, educação e sensibilização com a incluisão destas temáticas na estrutura curricular dos ensinos básico, secundário e superior.	Existência de formação obrigatória na área da cibersegurança nos diferentes níveis de ensino. Avaliação qualitativa por nível de ensino (sim/parcial/não).
S.3. Observação de atitudes e comportamentos (e.g., fonte observatório do CNCS)	O "Relatório de Cibersegurança em Portugal – Sociedade 2020" do observatório do CNCS, contém indicadores sobre atitudes e comportamentos individuais, na organização e em relação à educação e sensibilização na cibersegurança.	Ver indicadores do "Relatório de Cibersegurança em Portugal – Sociedade 2020": Atitudes, Comportamentos Individuais, Comportamentos Organizacionais, Educação e Sensibilização
S.4. Campanhas de sensibilização para a cibersegurança nacional	Sensibilização para a temática da cibersegurança, através de campanhas patrocinadas pelo Estado, nos OCS ou nas escolas, ou outros (e.g., tal como se fez para a prevenção da droga ou para reduzir acidentes rodoviários).	Existência de ações de sensibilização à escala nacional nos OCS ou escolas. Avaliação quantitativa (e.g., # campanhas de sensibilização nacional).
Domínio Económico		
E.1. Investimento privado e público em cibersegurança incluindo I&D&I	O observatório do CNCS tem uma linha de observação (ainda sem relatórios) da economia da cibersegurança.	Nível de investimento (privado e público) em cibersegurança (incluindo I&D&I). Avaliação quant. por setor/entidade (e.g., % do orçamento gasto CS).
E.2. Mercado de trabalho de cibersegurança (e.g., fonte observatório do CNCS)	O observatório do CNCS tem uma linha de observação (ainda sem relatórios) da economia da cibersegurança, incluindo mercado em termos de oferta e procura.	Quantidade de ofertas de emprego na área da cibersegurança. Avaliação quantitativa (#ofertas de emprego e taxa de variação anual).
Domínio Político		

P.1. Existe uma estratégia de segurança no ciberespaço que contemple resposta a AH?	A ENSC já refere ameaças como a desinformação, ciberespionagem, etc. É importante conforme recomendação do NATO StratCom COE (2019, p. 10)	Existência de uma estratégia de segurança no ciberespaço que inclua o tema das AH e da desinformação. Avaliação qualitativa (sim/parcial/não).
P.2. Existe atribuição de competências na resposta a AH?	As AH não são responsabilidade de uma única entidade. Contudo, é necessário definir um sistema de resposta a crises que contemple a resposta de forma coordenada.	Existência de um sistema nacional de gestão de crises com atribuição de responsabilidades e competências na resposta a AH. Avaliação qualitativa (sim/parcial/não).
P.3. Políticas de investimento em cibersegurança e ciberdefesa	O observatório do CNCS tem uma linha de observação (ainda sem relatórios) das políticas públicas. O Plano de Recuperação e Resiliência de Portugal (2021) prevê investimento em cibersegurança/ciberdefesa que importa monitorizar.	Nível de investimento em CS e CD (incluindo I&D&I). Avaliação quantitativa (e.g., evolução investimento em cibersegurança e ciberdefesa).
P.4. O regime jurídico da segurança do ciberespaço impõe obrigatoriedade de certificação ou requisitos de segurança suficientes?	A atual Lei n.º 46/2018 não prevê obrigatoriedade para além da notificação de incidentes. A nova SRI2.0 irá impor novas medidas para aumentar a ciber-resiliência. Importa monitorizar se as medidas do regime jurídico que esteja em vigor são eficazes.	Existência de um regime jurídico da segurança do ciberespaço eficaz com obrigatoriedade de certificação e requisitos de segurança suficientes (e.g., requisitos QNRCS pelo CNCS). Avaliação qualitativa (sim/parcial/não).
P.5. Existe um planeamento civil de emergência para fazer face a AH no ciberespaço?	O SNPCE, já contempla a Comissão de Planeamento de Emergência da Cibersegurança que representa o sistema nacional em grupos congéneres no âmbito da OTAN.	Existência de um Sistema Nacional de Planeamento Civil de Emergência para fazer face a AH. Avaliação qualitativa (sim/parcial/não).
P.6. Existem autoridades nacionais em matéria eleitoral com recursos para responder a AH no ciberespaço?	A EU recomenda cada Estado-Membro ter autoridades competentes em matéria eleitoral e pelo acompanhamento das atividades em linha no contexto eleitoral, mas os recursos nacionais são parcos (ERC, 2019, p. 70)	Existência de autoridades nacionais competentes em matéria eleitoral com recursos adequados para responder a AH no ciberespaço. Avaliação qualitativa (sim/parcial/não).
Domínio Informação		
I.1. Existe uma Célula de Fusão nacional para AH e interoperável com o da UE?	Tal como a UE tem uma Célula de Fusão integrada no INTCEN, ao nível nacional, deverá existir uma Célula de Fusão, para integrar contributos internos.	Existência de uma Célula de Fusão Nacional, interoperável com o da UE, a fim de aumentar o conhecimento situacional. Avaliação qualitativa (sim/parcial/não).
I.2. Existe coordenação entre instituições e uma definição clara dos fluxos de partilha de informação e colaboração?	Para a resposta a ciberataques, a partilha de informação entre instituições é fundamental. No mínimo o G4 - Grupo dos Quatro devem ter canais perfeitamente estabelecidos, numa abordagem *whole-of-government*.	Existência de coordenação entre instituições e uma definição clara dos fluxos de partilha de informação e colaboração. Avaliação qualitativa (sim/parcial/não)
I.3. Existe um sistema de informação comum para conhecimento situacional de AH aos diferentes níveis e entre as diferentes instituições?	Na mesma linha do SAR previsto no PADUE, é fundamental um sistema de informação (interno), para conhecimento das ameaças no ciberespaço, numa abordagem *whole-of-government*.	Existência um sistema de informação comum para conhecimento situacional das ameaças no ciberespaço, aos diferentes níveis, e entre as diferentes instituições (*whole-of-government*). Avaliação qualitativa (sim/não).
I.4. Nível de risco e registos da evolução das AH no ciberespaço em Portugal	O observatório do CNCS tem uma linha de observação de Riscos e Conflitos, essencial para desenvolver estratégias de proteção.	Nível de risco e registos da evolução das ciberameaças (no âmbito das AH) em Portugal. Avaliação qualitativa (Risco baixo/médio/alto).