INSTITUTO UNIVERSITÁRIO MILITAR
DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS
CURSO DE ESTADO-MAIOR CONJUNTO
2021/2022

TII

CIBERDEFESA – A EVOLUÇÃO E PERTINÊNCIA NO CONTEXTO DA UNIÃO EUROPEIA

Hilário Diogo da Silva Costa
MAJOR, INFANTARIA

INSTITUTO UNIVERSITÁRIO MILITAR
DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

CIBERDEFESA – A EVOLUÇÃO E PERTINÊNCIA NO CONTEXTO DA UNIÃO EUROPEIA

MAJOR, INFANTARIA Hilário Diogo da Silva Costa

Trabalho de Investigação Individual do CEMC

Pedrouços 2022

INSTITUTO UNIVERSITÁRIO MILITAR
DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

CIBERDEFESA – A EVOLUÇÃO E PERTINÊNCIA NO CONTEXTO DA UNIÃO EUROPEIA

MAJOR, INFANTARIA Hilário Diogo da Silva Costa

Trabalho de Investigação Individual do CEMC

Orientador: Major, TRANSMISSÕES
Pedro Manuel Monteiro Fernandes

Pedrouços 2022

Declaração de compromisso Antiplágio

Eu, **Hilário Diogo da Silva Costa**, declaro por minha honra que o documento intitulado **Ciberdefesa – A Evolução e Pertinência no Contexto da União Europeia** corresponde ao resultado da investigação por mim desenvolvida, enquanto auditor do **Curso de Estado-Maior Conjunto 2021/2022** 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**, 04** de **maio** de **2022**

Hilário Diogo da Silva Costa

Agradecimentos

A concretização deste trabalho, só foi possível com o apoio e energia de diversas pessoas, a quem demonstro abertamente o meu sincero e sentido reconhecimento.

Ao meu orientador, Senhor Major Pedro Manuel Monteiro Fernandes, por aceitar em tão boa hora este desafio. Mas também pela partilha de conhecimento e astutas orientações com que me conduziu ao longo da investigação, bem como pelo olho crítico que ensejou nos vários caminhos que segui.

A validação científica desta investigação provém, sobretudo, do contributo de todos os Oficiais que tiveram a gentileza de me conceder uma entrevista e partilhar as suas opiniões e experiência. Como tal, ao Senhor Capitão de Mar e Guerra Fialho de Jesus, Senhor Capitão de Fragata Sérgio Caldeira Carvalho, Senhor Tenente-Coronel David Lopes Antunes, Senhor Tenente-Coronel José Carlos Reimão Teixeira, Senhor Tenente-Coronel Alexandre Miguel Gil Fernandes, Senhor Tenente-Coronel José Manuel Brito Sousa, Senhor Tenente-Coronel Jerome Daes, Senhor Tenente-Coronel Stefan Alois Weiss, Senhor Capitão de Fragata Sérgio Manuel Ferreira Rodrigues e Senhor Major Fábio Vieira da Silva, pela manifesta disponibilidade e pela distinta qualidade das respostas, que muito contribuiram para os resultados alcançados, o meu muito obrigado.

Um agradecimento especial ao Senhor Tenente-Coronel David Lopes Antunes, que para além da entrevista, foi incansável na partilha de conhecimento durante as enumeras conversas efetuadas, bem como pela documentação enquadrante para a lavra deste trabalho. À minha namorada Carina, pelo apoio incondicional e permanente, pelo inabalável e infindável esforço em garantir a estabilidade familiar.

Ao meu filho Diogo, que apesar da tenra idade, tenta compreender a ausência emocional do pai e que espero brevemente poder compensar.

A todos, mais uma vez, o meu sincero Obrigado.

Índice

Índice de Figuras

Índice de Quadros

Resumo

O Ciberespaço constitui-se atualmente, como um desafio à segurança dos Estados e Organizações. Frequentemente, é necessário o emprego de meios militares para exercer a soberania, num espaço caracterizado pela indefinição de fronteiras.

Para neutralizar as ameaças no Ciberespaço, a União Europeia (UE) criou mecanismos de proteção, para garantir segurança e livre uso do Ciberespaço, levando à crescente exploração militar do Ciberespaço, transformando o ambiente estratégico internacional. É nesta envolvente, que o objeto de estudo desta investigação se consubstancia na Ciberdefesa das Operações/Missões militares da UE.

Como tal, efetuou-se um estudo de caso, com um horizonte temporal transversal, recorrendo a um raciocínio dedutivo, numa estratégia qualitativa.

Os principais resultados, sugerem a falta de empenhamento político, da partilha de Informação dos Estados-Membros, doutrina, recursos humanos e meios especializados. Além disso, faltam infraestruturas dedicadas à formação e treino de Ciberdefesa. Estas lacunas, contribuem para a falta de capacidade da UE em garantir uma resposta coordenada credível e eficaz aos incidentes no Ciberespaço.

Como tal, a UE deve empenhar-se na alocação de recursos e meios, que desenvolvam doutrina e infraestruturas para formação e treino de Ciberdefesa, aumentando assim a capacidade de resiliência e dissuasão, na resposta coordenada no Ciberespaço durante as suas Operações/Missões.

Palavras-chave: Ciberdefesa, Ciberespaço, Ciberameaças, incidentes no Ciberespaço, União Europeia.

Abstract

Nowadays, Cyberspace constitute a challenge to the security of States and Organizations. Frequently, the use of military assets is necessary to exercise sovereignty in a space characterized by the undefinition of borders.

To neutralize Cyberthreats, the European Union (EU) has created protection mechanisms to guarantee the security and free use of cyberspace, increasing the military exploitation of Cyberspace, changing the international strategic environment deeply. It´s in this environment that the study object of this investigation lies on the Cyber Defence of EU´s military Operations/Missions.

A case study, with a transversal time horizon, were used to conduct the investigation. It was also used deductive rationality, and a qualitative strategy.

The main results suggests that there is lack of commitment from the Member States, human resources, and specialized assets. In addition, it was identified a lack of dedicated infrastructure´s to Cyber Defence education and training. These lacks are reflecting in EU's incapacity to guarantee a reliable, effective, and coordinated response to Cyberspace´s incidents.

So, EU should have commitment in the attribution of resources and assets, for the development of doctrine and infrastructures for Cyber defence education and training, allowing the increase of resilience and deterrence capacities in Cyberspace during EU's Operations/Missions.

Keywords: *Cyber Defence, Cyberspace, Cyberthreats, Cyberspace incidents, European Union.*

Lista de abreviaturas, siglas e acrónimos

C

CAIH	*Cyber Academia and Innovation Hub*
CIDCC	*Cyber and Information Domain Coordination Center*
CDPF	*Cyber Defence Policy Framework*
CEU	*Council of the European Union*
CNU	Carta das Nações Unidas
CSDN	Conselho Superior de Defesa Nacional
CSDP	*Common Security and Defence Policy*
C2	Comando e Controlo

E

E	Entrevistado
EDA	*European Defence Agency*
EU	*European Union*
EUMS	*European Union Military Staff*

F

FA	Forças Armadas

J

JCU	*Joint Cyber Unit*

M

MDN	Ministério da Defesa Nacional
milCERT	*military Computer Emergency Response Team*

N

NATO	*North Atlantic Treaty Organization*
NCI	NATO *Communications and Information*

O

OCS	Órgãos de Comunicação Social
OE	Objetivo Específico
OG	Objetivo Geral
OHQ	*Operation Headquarters*

P

PESCO	*Permanent Structured Cooperation*
POC	*Point of Contact*

Q

QC	Questão Central
QD	Questão Derivada
QG	Quartel-General

S

SIC	Sistemas de Informação e Comunicações

U

UE	União Europeia

1. Introdução

O Ciberespaço, veio intensificar as transformações sociais nos mais diversos domínios da atividade humana, transformando-a numa sociedade em rede, que é não-presencial e que agrega interações. Porém, o Ciberespaço introduziu um novo desafio à segurança, obrigando a ordem mundial a refletir e a conceber conceitos, estratégias, táticas e sistemas (Rodrigues, 2016). Com este mundo digital advieram grandes benefícios, mas também vulnerabilidades. Os incidentes no Ciberespaço têm aumentando a um ritmo alarmante com impactos cada vez maiores na sociedade, afetando serviços essenciais, como o fornecimento de água, eletricidade ou serviços móveis (Röhrig & Smeaton, 2014).

Atualmente, devido à natureza do Ciberespaço, é possível criar ou aceder facilmente a ferramentas tecnológicas de baixo custo. Estas quando exploradas por atores com más intenções, possibilita-os desenvolver atividades não desejadas à Sociedade, constituindo-se como Ciberameaças. Os Estados e as suas Forças Armadas (FA), tentam com enormes dificuldades, exercer a sua soberania num espaço onde se verifica uma indefinição de fronteiras que não dominam nem controlam (Nunes, 2011, pp. 365-367, 2020, p. 1).

Para neutralizar estas ameaças e tornar o Ciberespaço seguro, a UE, à semelhança de outras organizações, tem vindo a criar mecanismos de proteção do Ciberespaço. Consequentemente, assistiu-se a uma crescente exploração militar do Ciberespaço, transformando profundamente o ambiente estratégico internacional (Kello, 2018).

Neste contexto surge o conceito de Ciberdefesa, que pode ser entendida como uma medida proativa, para detetar ou obter qualquer tipo de informação relativamente a Ciberataques ou impedir uma Ciberoperação (Rocha e Guarda, 2018, p. 14). Prevê-se que a Ciberdefesa assuma uma preponderância cada vez maior, constituindo-se como o mais importante desafio à segurança da primeira metade do século XXI. A abrangência da Ciberdefesa, passa não só pela proteção de um simples computador ou telemóvel e a sua ligação à internet, mas também de infraestruturas fundamentais, como por exemplo as de fornecimento de água e eletricidade (Carayannis et al., 2014, p. 257).

A UE consciente desta realidade, define o seu primeiro conceito para a Ciberdefesa em 2012 através do documento *EU Concept for Cyber Defence for EU-led Military Operations*. Em 2014, cria a *Cyber Defence Policy Framework* (CDPF), com o intuito de auxiliar o desenvolvimento das capacidades de Ciberdefesa dos Estados-Membros, fortalecendo no Ciberespaço, a proteção das infraestruturas afetas à Segurança e à Defesa da UE (Council of the European Union [CEU], 2018, p. 3).

A análise da evolução da capacidade de Ciberdefesa da UE desde 2012 até à atualidade, bem como a análise à Formação, Treino, Exercícios e às respostas aos incidentes no Ciberespaço da UE, julga-se pertinente e relevante, consubstanciando-se como o cerne da presente investigação. Como objeto de estudo, foi identificada a Ciberdefesa das Operações/Missões militares da UE, estando a investigação delimitada na esfera espacial, conceptual e temporal (Santos & Lima, 2019, p. 42).

Temporalmente, o estudo é delimitado ao período compreendido entre os anos de 2012 e a atualidade, coincidindo o início deste período com o surgimento do conceito de Ciberdefesa, que se traduziu num ponto de viragem, relativamente à forma como a UE passou a encarar a proteção do seu Ciberespaço. Ao nível espacial, o estudo foi delimitado à UE, organização na qual recai o objeto de estudo e se pretende no final da investigação propor contributos no âmbito da sua Ciberdefesa. Por fim, no que diz respeito ao conteúdo, o estudo foi delimitado às Operações de Ciberdefesa da UE, analisando a forma como a UE se organiza para defender o seu Ciberespaço, em Operações/Missões de natureza militar.

Considerando o tema proposto, e a sua delimitação, constitui-se como objetivo geral (OG) da investigação, propor contributos para melhorar a Ciberdefesa nas Operações/Missões militares da UE.

Contribuindo diretamente para o OG, foram identificados três Objetivos Específicos (OE):

- OE1 – Analisar a evolução da Ciberdefesa na UE;
- OE2 – Analisar a Formação, Treino e Exercícios de Ciberdefesa na UE;
- OE3 – Analisar a resposta aos incidentes no Ciberespaço da UE.

Por forma a dar resposta ao OG e aos OE, assume-se como fundamental para o desenvolvimento da investigação, a formulação da Questão Central (QC) e as respetivas Questões Derivadas (QD) (Santos & Lima, 2019, pp. 151-157). Assim, para responder ao OG deste estudo, formulou-se a seguinte questão central: De que modo pode ser melhorada a Ciberdefesa das Operações/Missões militares da UE?

A partir do OG e respetivos OE, conjugados com a questão orientadora da pesquisa, foram elencadas as seguintes questões derivadas:

- QD1 (OE1) – De que modo tem evoluído a Ciberdefesa da UE?
- QD2 (OE2) – Como é efetuada a Formação o Treino e Exercícios de Ciberdefesa na UE?
- QD3 (OE3) – De que modo é realizada a resposta aos incidentes no Ciberespaço pela UE?

O estudo encontra-se organizado em cinco capítulos, sendo o primeiro a presente introdução. No segundo, é apresentado o enquadramento teórico e conceptual, onde se aclara o estado da arte e são elencados os conceitos estruturantes, terminando com a apresentação do modelo de análise. No terceiro, é explanada a metodologia e o método que foram seguidos na presente investigação, esclarecendo-se o raciocínio, estratégia de investigação, desenho de pesquisa, participantes e procedimento, bem como os instrumentos e técnicas de recolha de dados utilizados. O quarto capítulo foca-se na investigação propriamente dita, sendo apresentados os dados e discutidos os resultados, com o intuito de se atingir os OE através da resposta às QD e consequentemente, com a resposta à QC atingir o OG. No quinto e último capítulo, são lavradas as conclusões que decorrem do explanado nos capítulos anteriores, pretendendo-se efetuar a súmula dos resultados obtidos, incorporar contributos para o conhecimento, elencar recomendações e propor estudos futuros e concomitantemente apresentar as limitações da investigação.

2. Enquadramento teórico e conceptual

Neste capítulo, é efetuado o enquadramento teórico e conceptual, onde se alumia o estado da arte e a revisão da literatura, espelhando as teorias e conceitos estruturantes, com ênfase para os conceitos de Ciberespaço, Ciberameaças, incidentes no Ciberespaço e Ciberdefesa. O capítulo culmina com a apresentação do modelo de análise.

2.1 Estado da arte/revisão da literatura

Atendendo à temática e o objeto de estudo, foram estudadas as obras de Nunes, (2010, 2011; 2014; 2018; 2020) e Carayannis et al. (2014), que abordam a introdução do Ciberespaço como domínio para as Operações militares e a importância da implementação da Ciberdefesa, para a proteção e liberdade de ação neste domínio. Foram ainda tidos em consideração, os estudos de Trimintzios et al. (2017), Kello (2018) e Röhrig & Smeaton (2014), que analisam a forma como a UE tem vindo a integrar a Ciberdefesa e Cibersegurança, nas suas política para o Ciberespaço. Para a definição dos conceitos estruturantes, cujo contributo foi essencial para o desenvolvimento da investigação, foi estudada a documentação oficial da UE, no âmbito da Ciberdefesa das Missões/Operações da *Common Security and Defence Policy* (CSDP).

A CSDP, é a referência da UE no domínio da defesa e da gestão de crises, incluindo a cooperação e coordenação da defesa entre os Estados-Membros. A CSDP deu origem a estruturas políticas e militares internas da UE (incluindo a Ciberdefesa), que permitiu a realização de Operações/Missões Militares no estrangeiro (Legrand, 2021, p. 1). As Operações/Missões enquadram-se em cenários de manutenção da paz, prevenção de conflitos e fortalecimento da segurança internacional, de acordo com os princípios da Carta das Nações Unidas (CNU). A execução destas tarefas, é realizada com recurso às capacidades fornecidas pelos Estados-Membros e fora da UE (European Union Military Staff [EUMS], 2014, pp. 8–9).

Atualmente, estão em curso três Operações nos Teatros de Operações da Bósnia-Herzegovina, Mar Mediterrâneo e Somália. Quanto às Missões de treino, estão presentes no Mali, Moçambique, Républica Centro-Africana e Somália (European External Action Service [EEAS], 2021).

Seguidamente, serão aflorados os conceitos estruturantes, que contribuíram para a presente investigação.

2.1.1 O Ciberespaço como um domínio de Operações para a UE

A utilização do Ciberespaço, assume atualmente um carácter transversal e multidisciplinar, contribuindo para a definição dos inúmeros tipos de forças tangíveis e intangíveis de uma unidade política (Nunes, 2020, p. 7).

O Ciberespaço pode ser definido como um universo virtual assegurado pelas redes de comunicações, sobretudo pela Internet. Mas também como um novo mundo, um novo espaço, um novo meio de interação, comunicação e de vida em sociedade. Esse universo não é ficcional ou imaginário, é uma realidade que existe num plano essencialmente diferente dos restantes espaços conhecidos (Monteiro, 2007, p. 6).

As conclusões do Conselho Europeu de dezembro de 2013 e junho de 2015 identificaram o Ciberespaço como um domínio de operações para a UE a par dos domínios Terrestre, Marítimo, Aéreo e Espacial (EEAS, 2022, p. 6).

No domínio militar, o Ciberespaço é definido pela *North Atlantic Treaty Organization* (NATO) como um domínio global, que consiste em todas as comunicações interligadas, tecnologias da informação e outros sistemas eletrónicos, redes e dados, incluindo os que estão separados ou independentes, que processam, armazenam ou transmitem dados (2020, p. 4; JP3-12, 2018).

Contudo, na UE é entendido como um domínio virtual, global e comum, inserido no ambiente informacional, constituído por toda a infraestrutura de redes interligadas e interdependentes da informação global, organizacional e nacional, com base nas redes de Internet e telecomunicações, sendo alargada por outras redes, sistemas informáticos e processadores incorporados, contendo ainda sistemas e redes autónomos, sendo como tal a definição adotada neste trabalho (EUMS, 2018, p. 38).

Esta natureza interligada do Ciberespaço, conjugada com digitalização de plataformas militares, sistemas de armas e desenvolvimento de tecnologias, criam ambientes operacionais voláteis, incertos, complexos e ainda mais ambíguos (EEAS 2021, p. 6). O sucesso das Operações Militares nos domínios físicos está cada vez mais dependente da disponibilidade e acesso ao Ciberespaço. As FA são dependentes do Ciberespaço tanto como utilizador como num domínio para concretizar missões de defesa e segurança (Kello, 2018, p. 1). As plataformas militares e os seus sistemas de armas, dependem fortemente de Sistemas de Informação e Comunicações (SIC) através do Ciberespaço, sendo um pré-requisito para garantir o sucesso do cumprimento da missão (EEAS 2022, p. 7) (Figura 1).

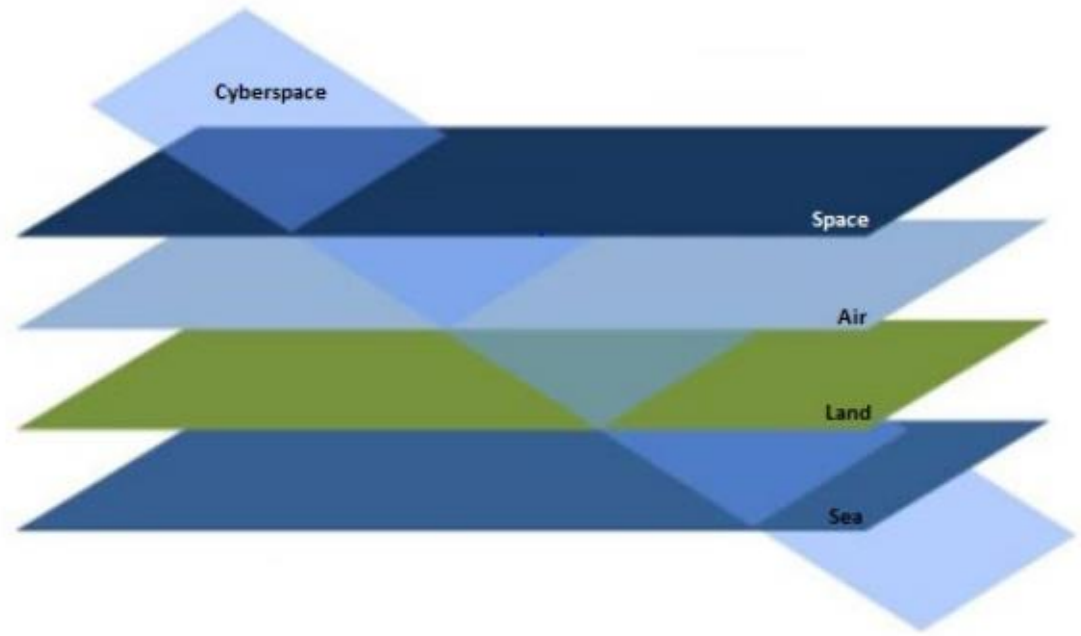

Figura 1– O domínio do Ciberespaço e a sua integração com restantes domínios
Fonte: Disponível EUMS (2021, p. 8).

No Ciberespaço, os comandantes militares terão de considerar as implicações derivadas da compreensão do mesmo, como parte integrante do seu ambiente operacional. Como tal, terão de proteger e defender a sua liberdade de ação no Ciberespaço contra atividades maliciosas, mitigando a perturbação de serviços de infraestruturas críticas, que possam por em causa a confiança do público nas instituições, organismos e agências da UE presentes numa Área de Operações (EEAS 2022, p. 7).

"[…] No ambiente estratégico atual, nenhuma guerra poderá ser ganha exclusivamente com a utilização militar do Ciberespaço (ciberguerra pura). No entanto, também é certo que nenhuma campanha militar conduzida noutro qualquer domínio operacional poderá ser ganha sem o Ciberespaço" (Nunes, 2014, pp. 146–147).

2.1.2 Ciberameaças e os seus Impactos na UE

A complexidade dos Ciberataques tem aumentado consideravelmente, passando a incluir múltiplos vetores para as ameaças, verificando-se uma conjugação entre Operações no Ciberespaço e as Operações nos domínios tradicionais. Estas ameaças são consideradas as mais perigosas. Não obstante, as Ciberameaças podem ser empregues desde o nível político/estratégico da administração da CSDP da UE até ao nível técnico/tático, de forma coerente (campanha organizada) ou não coerente (ataques espontâneos), para alcançar objetivos geopolíticos, económicos e culturais (Figura 2) (Trimintzios et al., 2017, pp. 36–37).

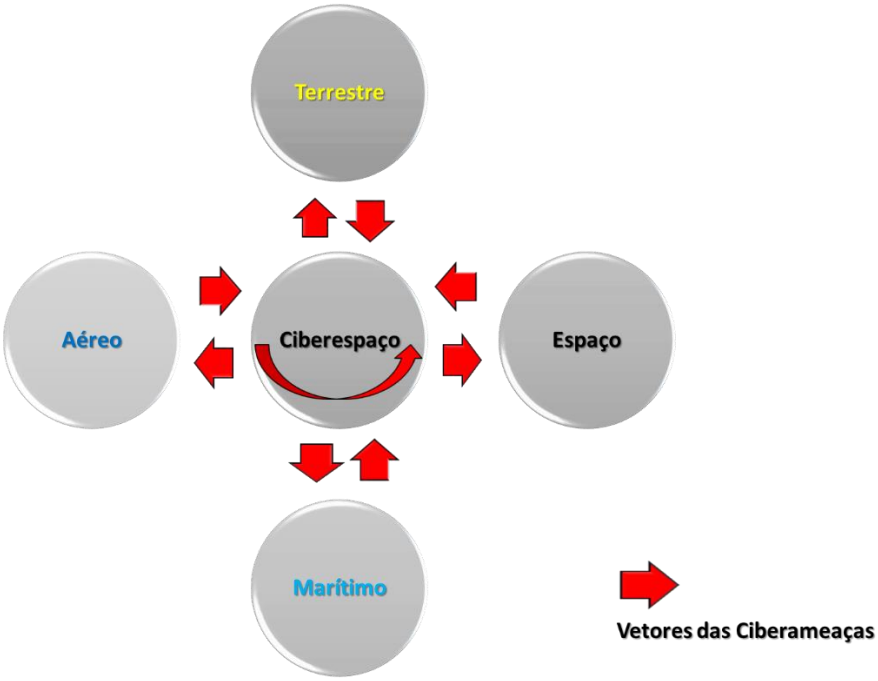

Figura 2– Vetores das Ciberameaças
Fonte: Adaptado a partir de Trimintzios et al. (2017, p. 37).

Segundo a UE, as Ciberameaças são categorizadas em três níveis, (Figura 3). Esta taxonomia foca-se nos atores e respetivas ameaças que atuam no Ciberespaço, bem como as suas intenções e capacidades com aplicação às missões da CSDP nos níveis político, estratégico e operacional (Trimintzios et al., 2017, p. 37).

Origem da Ameaça	Nível da Ameaça	Características
Ciberespaço	A	Explora vulnerabilidades conhecidas pré-existentes
	B	Descobre vulnerabilidades desconhecidas
	C	Cria vulnerabilidades usando todo o espectro

Figura 3– Categorização das Ciberameaças
Fonte: Adaptado a partir de Trimintzios et al. (2017, p. 38).

Estes três níveis de ameaça, estão diretamente ligados às capacidades financeiras dos atores que as executam, que vão desde alguns Euros (Nível A) até vários milhões (Nível C) (Trimintzios et al., 2017, p. 37).

2.1.3 Incidente no Ciberespaço

O eventual impacto disruptivo e consecutivo, de ciberataques para as infraestruturas críticas e serviços vitais de informação, podem majorar um simples incidente, que seria tratado de acordo com os planos da proteção simples e do âmbito criminal, a um estado de sítio ou de emergência, ou em última instância e de acordo com a CNU, relativamente ao uso da força, à necessidade de desenvolver ações ofensivas também no Ciberespaço (Nunes et al., 2018, p. 29).

Neste cenário, a UE tem vindo a promover esforços, para que as FA dos seus Estados-Membros detenham a capacidade de intervir no domínio do Ciberespaço, por forma a garantir em situações de exceção, o regular funcionamento das instituições democráticas e o exercício das funções de soberania dos seus Estados-Membros, através da condução de operações no Ciberespaço (Nunes et al., 2018, p. 30).

Um incidente no Ciberespaço, segundo o EUMS, é definido como uma situação que ameaça ou tem impacto na segurança do pessoal, meios ou Operações/Missões da CSDP, requerendo ação imediata para mitigar ou abordar o impacto. Estes incidentes podem variar consideravelmente quanto à sua aparência, quantidade de sistemas afetados e no potencial impacto nas Operações/Missões. Nas Operações/Missões militares da UE, os incidentes são categorizados e priorizados, para apoiar a avaliação do impacto e facilitar a tomada de decisões (2018, pp. 7–8).

Priorizar o tratamento do incidente, é possivelmente a decisão mais crítica no processo de tratamento. Pois os incidentes que afetam diretamente os sistemas das Operações/Missões, pessoal, meios e atividades, não devem ser tratados pela ordem com que ocorrem, ou com base nos recursos disponíveis para a sua resolução. A priorização deve ser feita com base em fatores relevantes das Operações/Missões, com impacto funcional e nas informações. Concorrentemente, devem ser avaliadas as medidas que devem ser tomadas, para se recuperar desse incidente (EUMS 2018, p. 8).

Os Incidentes segundo o EUMS (2018, p.9), são caracterizados como:

- Negligenciável, caracterizado como um incidente menor, com efeito insignificante nos sistemas das Operações/Missões, pessoal, meios e atividades. sem efeito na capacidade da operação/missão em fornecer todos os serviços aos seus utilizadores;
- Baixo, com impacto marginal nos sistemas das Operações/Missões, pessoal, meios e atividades. Efeito mínimo; a operação/missão ainda é capaz de fornecer todos os serviços críticos a todos os utilizadores, mas perdeu eficiência;

- Médio, identificado como um incidente envolvendo sistemas, pessoal e/ou meios da Operação/Missão, que pode ter um impacto médio nas atividades da mesma e um impacto improvável nos Órgãos de Comunicação Social (OCS). A Operação/Missão, perdeu a capacidade de fornecer um serviço crítico a um subconjunto de utilizadores do sistema;
- Alto, descrito como um incidente grave que envolveu sistemas, pessoal e/ou meios da Missão (lesão ou perda de vida e/ou danos significativos nos meios), que podem ter um alto impacto nas atividades da Operação/Missão com provável impacto nos OCS. A Operação/Missão, torna-se incapaz de fornecer alguns serviços críticos a um subconjunto de utilizadores do sistema ou a qualquer utilizador;
- Crítico, caracterizado como um incidente grave que envolveu sistemas da Operação/Missão, pessoal e/ou meios (perda de vidas e/ou danos significativos ou perda de meios), que tenha um impacto crítico nas atividades da Operação/Missão com impacto relevante nos OCS. A Operação/Missão, é incapaz de fornecer alguns ou mesmo a maioria dos serviços críticos aos utilizadores.

2.1.4 Ciberdefesa

O conceito de Ciberdefesa, desponta pela primeira vez no conceito estratégico da NATO em 2010, aprovado na cimeira de Lisboa (Nunes, 2020, p. 16). Relativamente à UE, esta desenvolveu um conceito de Ciberdefesa, ampliado e aprovado em 2012. Na senda de incrementar a capacidade para enfrentar os Ciberataques, a UE anunciou um conjunto de medidas, incentivando os Estados-Membros a reforçar as suas capacidades de Ciberdefesa, ao submeterem projetos cooperativos no quadro da *Permanent Structured Cooperation* (PESCO) e do Fundo Europeu de Defesa (EC, 2018, p. 3).

Segundo a NATO, a Ciberdefesa são ações defensivas, dentro ou através do Ciberespaço, para preservar a liberdade de ação amigável neste domínio (2020, p. 4).

Em Portugal, a Ciberdefesa é definida como a atividade que visa assegurar a defesa nacional no, ou através do, Ciberespaço (Resolução do Conselho de Ministros n.º 92/2019 de 5 de junho, 2019, p. 2889). Através da aplicação de medidas de segurança, que garantam a salvaguarda da informação e a proteção das infraestruturas dos SIC das FA, contra Ciberataques. No caso de um Ciberataque, proteger e defender as infraestruturas críticas nacionais e do Governo (Nunes, 2020, cit. Conselho Superior de Defesa Nacional [CSDN], 2014, p.15).

Contudo, a definição de Ciberdefesa considerada para esta investigação é a usada pela UE, que define a Ciberdefesa como uma das dimensões da Cibersegurança, (vista principalmente como uma dimensão militar, mas que compreende abordagens militares e civis). É considerada como um conjunto de medidas, que defendem os sistemas de informação críticos, para alcançar a Cibersegurança. A defesa do Ciberespaço, compreende todas as medidas técnicas e não técnicas, para melhorar a resiliência dos sistemas baseados nas tecnologias da informação e comunicação (SIC, Comando e Controlo [C2]) e qualquer sistema, arma ou sensor), apoiando os interesses de defesa e segurança nacional dos Estados-Membros, para prevenir, detetar, reagir e recuperar de um Ciberataque a estes sistemas (EUMS 2021, p. 25).

As Operações Militares de Ciberdefesa, destinam-se a defender todas as redes e SIC relevantes para a missão, bem como as infraestruturas de suporte para a mesma. Através de ferramentas eficazes, Pessoal treinado, processos e perícias adequados, para combater Ciberameaças e mitigar vulnerabilidades, de forma coordenada e sincronizada no Ciberespaço (EUMS 2018, p. 3).

2.2 Modelo de análise

Finda a exposição do estado da arte e da revisão de literatura, ficou aclarado existir conteúdo para a presente investigação, não só por ser uma área com pertinência, mas também por adicionar valor para a comunidade científica, por se tratar de um trabalho nunca antes criado, que se compromete a desenvolver conhecimentos num rumo nunca antes seguido (Phillips & Pugh, 1998). Assim sendo, elaborou-se o modelo de análise[1] onde são apresentados os conceitos estruturantes, bem como as dimensões, variáveis e indicadores estudados.

[1] Ver Apêndice A – Modelo de Análise.

3. Metodologia e método

Enfatizando o relevo que a metodologia tem na investigação científica (Bryman, 2012; Freixo, 2018; Sarmento, 2013; Vilelas, 2009; Yin, 2018), o presente capítulo retrata a metodologia e método empregues neste trabalho.

3.1 Metodologia

A metodologia aplicada à investigação, assim como a estrutura a seguir, regem-se pelas normas em vigor no Instituto Universitário Militar, a que se acrescentam obras de referência relativamente à metodologia de investigação científica (Bryman, 2012; Freixo, 2018; Sarmento, 2013; Vilelas, 2009; Yin, 2018).

Atendendo ao tema em estudo, o raciocínio utilizado é o dedutivo, na medida em que se parte do geral para o particular (Santos & Lima, 2019), decorrente de estudos e conceitos gerais do EEAS, EUMS e CEU, bem como investigadores nacionais e internacionais. Neste processo assegurou-se a fidedignidade das premissas, relacionadas com um raciocínio válido, por forma a que as conclusões fossem igualmente verdadeiras (Freixo, 2018; Santos Santos & Lima, 2019).

Quanto à estratégia adotada, é qualitativa dado existir uma "[…] relação indissociável entre o mundo real e a subjetividade do sujeito que não é passível de ser traduzida em números" (Sousa & Baptista, 2011, p. 55). Por esse motivo a investigação assenta na pesquisa documental e entrevistas, em que a análise é desenvolvida de acordo com os padrões descobertos e de acordo com as experiências dos especialistas estudados (Vilelas, 2009; Santos & Lima, 2019, p. 27), que foram alvo de entrevista.

O desenho de pesquisa utilizado é o estudo de caso, pela sua utilidade na investigação de processos organizacionais (Yin, 2018; Ponte, 2006, cit. por Freixo, 2011, p. 121), com um horizonte temporal transversal, atendo que se pretende recolher informação pormenorizada sobre a Ciberdefesa das Operações/Missões militares da UE, que se constitui como o objeto de estudo previamente selecionado.

3.2 Método

3.2.1 Participantes e procedimento

O percurso metodológico desenrolou-se em duas fases, em que a primeira foi destinada à aclaração do estado da arte e à construção do projeto de investigação. Na segunda fase procedeu-se à elaboração de entrevistas, resposta às QD e QC e à redação do Trabalho de Investigação.

Com o intuito de acrescer os conhecimentos do investigador, na primeira fase realizou-se o contacto com diversas entidades, realizando-se enumeras entrevistas exploratórias e

reuniões, merecendo destaque o contacto com o Brigadeiro-General Paulo Fernando Viegas Nunes, antigo coordenador científico do Mestrado em Guerra de Informação e Pós-graduação em Cibersegurança e Ciberdefesa da Academia Militar, tendo publicado diversos livros e artigos neste domínio. Foi também contactado o Tenente-Coronel David Lopes Antunes, *Cyber Defence programe manager da European Defence Agency* com o objetivo de esclarecer a visão e organização da UE relativamente à Ciberdefesa, bem como para a obtenção de documentação. Concomitantemente foi efetuada a leitura de uma extensa bibliografia.

Relativamente à segunda fase da investigação, compôs-se uma amostra não-probabilística intencional (Pardal & Correia, 1995, p. 34), solicitando-se 12 especialistas militares, dos quais dez concordaram em participar no estudo, tendo sido entrevistados. Estes dez especialistas[2] agregam vastos conhecimentos sobre a temática da investigação, fruto da função ou cargo que ocupam, ou ocuparam, bem como das suas competências académicas. Julga-se que a amostra é representativa decorrente da especificidade da temática.

3.2.2 Instrumentos de recolha de dados

Na presente investigação, utilizaram-se como instrumentos de recolha de dados, a entrevista e a análise documental. Foram efetuadas dez entrevistas semiestruturadas[3] (Santos & Lima, 2019; Sarmento, 2013; Quivy & Campenhoudt, 1998, p. 121), constituídas por 12 questões. As primeiras quatro direcionadas para a QD1, a quinta para QD2, e da sexta à décima segunda para a QD3. Foram definidas entrevistas semiestruturadas, para permitir aos entrevistados expressar de forma mais natural as suas opiniões, salvaguardando a hipótese do entrevistador poder instar esclarecimentos adicionais.

A análise documental, baseada mormente em literatura científica e documentos oficiais do EEAS, EUMS, e CEU, possibilitou agregar o conhecimento de base para a realização das entrevistas, mas também para realizar cruzamento e complementaridade de dados.

3.2.3 Técnicas de tratamento de dados

A análise das entrevistas, foi executada em concordância com a metodologia idealizada por Sarmento (2013, pp. 29–63), almejando-se não só "[…] descrever as situações, mas também interpretar o sentido em que foi dito" (Guerra, 2006, p. 69). As

[2] Ver Apêndice B – Lista de Entrevistados.
[3] Ver Apêndice C – Guião das Entrevistas Semiestruturadas.

entrevistas semiestruturadas foram alvo de análise categorial. A referida análise[4] foi realizada para cada uma das questões, de acordo com os seguintes passos:

- Constituição das unidades de contexto;
- Determinação das unidades de registo;
- Elaboração do quadro matriz das unidades de contexto e de registo;
- Elaboração do quadro de análise de conteúdo, por categorias e subcategorias, com a quantificação das unidades de registo, de acordo com as unidades de enumeração;
- Produção de conclusões, "[…] evidenciando os resultados superiores a 50% e enfatizando os resultados maiores ou iguais a 80%" (Sarmento, 2013).

Foram utilizados os programas *Microsoft Excel* e *Microsoft Word*, para apoio à organização e estruturação das unidades de contexto, determinação e quantificação das unidades de registo, e apresentação dos quadros com os resultados.

[4] Ver Apêndice D – Análise de Conteúdo das Entrevistas Semiestruturadas.

4. Apresentação dos dados e discussão dos resultados

No presente capítulo efetua-se a apresentação dos dados e a discussão dos resultados da investigação, que se encontra repartida por quatro pontos. No primeiro, é abordada a evolução da Ciberdefesa na UE, dando-se resposta à primeira QD. O segundo, refere-se à formação, treino e exercícios na UE, respondendo-se à segunda QD. No terceiro, consuma-se uma análise à resposta aos incidentes no Ciberespaço da UE, dando resposta à terceira QD. O final do capítulo culmina com uma síntese conclusiva onde se responde à QC da presente investigação.

4.1 A Ciberdefesa na União Europeia

A origem do conceito de Ciberdefesa da UE, remonta a 2012 aquando da divulgação do *EU Concept for Cyber Defence for EU-led Military Operations*. Nesta publicação, é definida a terminologia e os procedimentos, identificando-se as medidas e capacidades necessárias para combater as Ciberameaças, em operações militares lideradas pela UE (Röhrig & Smeaton, 2014). A Ciberdefesa, veio substituir o conceito de *Computer Network Operations in EU-led military operations*, que era focado na capacidade de desencadear ações para proteger, controlar e otimizar redes de computadores, bem como hardware e software associados, contribuindo para a superioridade da informação, negando ao adversário essa capacidade (EUMS 2014, p. 24).

4.1.1 A Evolução

Fruto das conclusões do Conselho Europeu para a CSDP de 2013, o Conceito de Ciberdefesa da UE desenvolve-se, dando origem a uma estrutura política para a Ciberdefesa, com o intuito de garantir que as capacidades de Ciberdefesa dos Estados-Membros, funcionassem de forma coerente para proteger a Força. Como tal, foi criada em 2014 uma CDPF, para melhorar as capacidades de resiliência e proteção dos SIC e de C2 nas Operações/Missões militares da UE, fornecendo uma estrutura para um trabalho conceptual contínuo, desenvolvimento de capacidades, treino e exercícios, bem como apoiar a cooperação entre os Estados-Membros e outros fornecedores de capacidades (CEU, 2014, p. 2).

Além disso, o referido documento (2014) aponta como prioridades da CSDP para a Ciberdefesa as seguintes áreas (Figura 4):

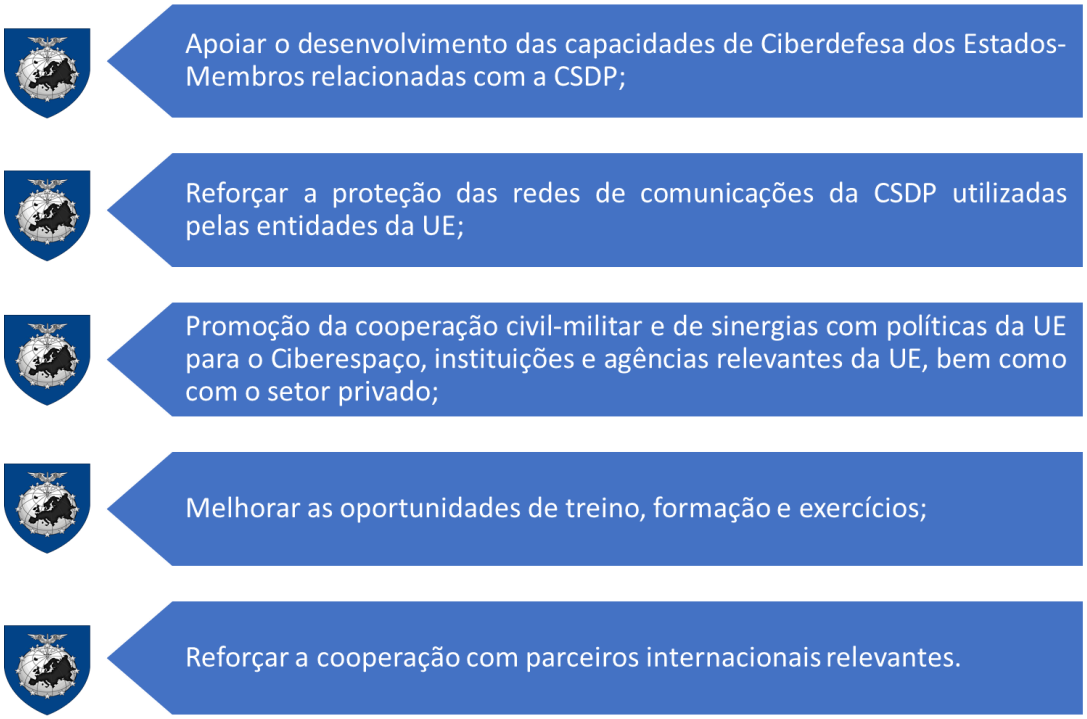

Figura 4– Prioridades da CSDP para a Ciberdefesa
Fonte: Adaptado a partir de CEU (2014, p. 2).

Entretanto, devido ao desenvolvimento da tecnologia militar e do uso do Ciberespaço, surge a necessidade de rever o Conceito de 2012, sendo definidos os aspetos militares dentro deste novo contexto, determinando particularmente a forma da Ciberdefesa ser integrada no planeamento e condução das Operações/Missões militares da UE. Como tal, em 2016 o EEAS publica uma atualização ao Conceito de Ciberdefesa para estas Operações/Missões (EEAS 2016, p. 6).

Esta atualização, salienta a importância de existir *Cyber Intelligence*, avaliação de ameaças e gestão de risco contínuos, bem como a cooperação e partilha de informação entre os Estados-Membros e as instituições da UE (EEAS 2016, p. 7). Fruto dos relatórios de implementação da CDPF e da criação dos Projetos PESCO, os Estados-Membros em 2018, sentiram a necessidade de atualizar a CDPF, acrescentando a Pesquisa e Tecnologia, nas áreas de prioridade para a Ciberdefesa (CEU 2018, pp. 3–8).

Em 2021, o EUMS emana a *European Union Military Vision and Strategy on Cyberspace as a Domain of Operations.* Neste documento são estabelecidas as condições essenciais e descreve os fins, as formas e os meios necessários, para a utilização do Ciberespaço como Domínio de Operações no apoio às Operações/Missões militares da CSDP da UE. Visando a integração do Ciberespaço, em todo o espectro das Operações/Missões militares (EUMS 2021, p. 5). O documento também reconhece, que a atribuição de Ciberataques no e através do Ciberespaço continua a ser uma responsabilidade política, assumida a nível nacional ou por consenso na UE (EUMS 2021, pp. 5–6).

Mais recentemente, com o aparecimento da guerra na Ucrânia e com as consequentes mudanças geopolíticas, assistiu-se a um reforço no empenho da UE em defender os seus interesses. Como tal, na sua Bússola Estratégica para a Segurança e a Defesa, a UE determina que no domínio do Ciberespaço:

> […] as nossas Forças têm de funcionar de forma coordenada, informada e eficiente. Por conseguinte, desenvolveremos e utilizaremos intensivamente novas tecnologias, nomeadamente nos domínios da computação quântica, da inteligência artificial e dos mega dados, a fim de obter vantagens comparativas, inclusive em termos de operações de Ciber-resposta e de superioridade informacional (CEU 2022, p. 32).

Ainda no corrente ano de 2022, encontra-se para aprovação uma atualização do Conceito de Ciberdefesa para as Operações militares lideradas pela UE. Na versão *Draft,* surgem diretrizes para o desenvolvimento e implementação de capacidades de Ciberdefesa para Operações/Missões militares da UE, bem como regras e procedimentos padronizados para o planeamento e execução da Ciberdefesa no apoio à gestão de crises da UE, definindo a terminologia necessária para o efeito (EEAS 2022, pp. 5–6).

A estabelecimento da CDPF, do Conceito de Ciberdefesa para as Operações Militares com as respetivas atualizações, a par da Visão para a Estratégia Militar no Ciberespaço e da Bússola Estratégica para a Segurança e Defesa, demonstram que a UE pretende cumprir com os objetivos no domínio do Ciberespaço para as Operações militares, tão eficazmente como nos outros domínios.

Este desígnio, reúne a concordância dos especialistas entrevistados. Contudo, foi apontado pela maioria dos especialistas, que falta empenhamento político, uma estrutura bem definida de Ciberdefesa, doutrina, pessoal e meios especializados, bem como uma maior partilha da informação entre os Estados-Membros.

Esta integração do Ciberespaço no planeamento das Operações/Missões militares, obriga a que seja estabelecida uma resiliência e dissuasão eficazes, contra potenciais adversários no Ciberespaço. Apesar de todos os entrevistados estarem de acordo com esta integração e com a resiliência, o mesmo não se verifica relativamente à dissuasão. Conforme referido pelo Entrevistado Um (E1) (entrevista por *Zoom,* 28 de março de 2022) "para haver dissuasão têm de existir alterações significativas à lei, respostas ofensivas credíveis e de momento isso apenas existe nos Estados-Membros […]". Que corrobora com as palavras do E2 (entrevista por *Zoom,* 28 de março de 2022) que afirma que "a UE de momento não tem manifestado interesse no desenvolvimento dessa capacidade, pois isso implica ter

capacidade ofensiva residente […]". O E1 (*op. cit*) e o E5 (entrevista por *Zoom*, 05 de abril de 2022), salientam ainda que deve existir uma partilha de informação entre os Estados-Membros da UE para se obter uma *Common Operational Picture* permanente no Ciberespaço.

No que concerne às áreas prioritárias da CDPF:

- Apoiar o desenvolvimento das capacidades de Ciberdefesa dos Estados-Membros, 90% dos entrevistados responderam à questão, dos quais 78% concordam que houve evolução no desenvolvimento;
- Reforço da proteção dos sistemas de comunicação e informação da CSDP utilizados pelas entidades da UE, 80% dos entrevistados responderam à questão, dos quais 75% concordam que existiu evolução no reforço da proteção;
- Promoção da cooperação civil-militar, 80% dos entrevistados responderam à questão, dos quais 75% concordam no evoluir da cooperação civil-militar;
- Investigação e tecnologia, 80% dos entrevistados responderam à questão, dos quais 75% concordam com a evolução nestas áreas;
- Melhorar as oportunidades de educação, formação e exercícios, 90% dos entrevistados responderam à questão, dos quais 65% concordam que houve evolução na educação, formação e exercícios;
- Reforço da cooperação com parceiros internacionais relevantes, 80% dos entrevistados responderam à questão, dos quais 63% concordam que existiu reforço da cooperação.

Como tal, constata-se que a UE tem evoluído em todas as áreas de prioridade. No que toca à questão relacionada com os projetos PESCO, que visam desenvolver capacidades relacionadas com as áreas prioritárias da CDPF, 90% dos entrevistados responderam à questão e 67% concordam fortemente que a criação dos mesmos é essencial, para o desenvolvimento da Ciberdefesa da UE. Usando as palavras do E9 (entrevista por *email*, 11 de abril de 2022), que sintetiza a maioria das opiniões dos restantes especialistas, "não são necessários mais projetos, os Estados-Membros da UE têm é de trabalhar nos projetos existentes que já estão em curso […]".

4.1.2 Resposta à primeira questão derivada

No seguimento do aclarado e respondendo à QD "De que modo tem evoluído a Ciberdefesa da UE?", verifica-se que as atualizações sucessivas da documentação enquadrante, revelam que a UE tem interesse no desenvolvimento das suas capacidades de

Ciberdefesa. Constata-se que, desde 2018 até à atualidade ocorreram evoluções significativas nas áreas da CDPF, impulsionada em parte pela criação dos projetos PESCO. Contudo, continua a faltar o empenhamento e partilha de Informação dos Estados-Membros, bem como, doutrina, recursos humanos e meios especializados. Ademais, a estrutura de Ciberdefesa ainda não se encontra bem consolidada, pelo que não garante uma resposta coordenada e credível da UE no Ciberespaço. Constata-se também, que falta materializar os projetos PESCO em curso, para reforçar a resiliência e dotar a UE com a capacidade de gerar respostas ofensivas credíveis no Ciberespaço.

4.2 Formação e Treino de Ciberdefesa na UE

A crescente complexidade do Ciberespaço, a presença de Ciberameaças e Ciberataques, obriga a que exista pessoal sensibilizado e especializado em Ciberdefesa, para uma resposta credível da UE (EEAS 2022, p. 34).

4.2.1 A Formação

Relativamente à questão da formação, pretendeu-se primariamente analisar, se a UE disponibilizava formação para o Pessoal em cargos e funções de Ciberdefesa. Apuradas as respostas, 89% dos entrevistados que responderam à questão, afirmaram que a formação não é suficiente, faltando sobretudo recursos humanos. Além disso, não se encontra bem organizada, recaindo a responsabilidade de formação nos Estados-Membros. Contudo, esta matéria para além de ser muito sensível, é desenvolvida num círculo muito reservado dentro de cada Estados-Membros. "Apenas algumas nações promovem formação e treino para o exterior, mas a oferta de qualidade reconhecida ainda é reduzida entre os países da UE […]", (E7, entrevista por *email*, 13 de abril de 2022).

Talqualmente importante no âmbito da formação, é não se limitar a mesma a Unidades de Ciberdefesa. "É necessária uma mudança de mentalidade em toda a comunidade operacional, pois no mundo digital o Ciberespaço afeta todos os domínios […]" (E8, entrevista por *email*, 28 de março de 2022). Sendo necessário formar e treinar os utilizadores, mas também os decisores (E9, *op. cit.*).

Numa segunda fase, pretendeu-se analisar a importância alusiva à existência de infraestruturas dedicadas à formação e treino de Ciberdefesa. A opinião dos especialistas foi unânime e 100% dos entrevistados frisaram, que a existência destas infraestruturas é de grande importância. Importa aludir, que 60% dos entrevistados referiu, que a implementação do projeto PESCO *Cyber Academia and Innovation Hub* (CAIH), liderado por Portugal, pode ser a solução para colmatar a falta de infraestruturas de Ciberdefesa na UE.

O CAIH foi desenvolvido com a missão de promover a Formação, Treino e Exercícios, Investigação, Desenvolvimento e Inovação e o Desenvolvimento da Indústria no domínio do Ciberespaço, para apoiar o desenvolvimento das capacidades de Ciberdefesa e Cibersegurança. O CAIH, ambiciona constituir-se num Centro de Excelência de nível internacional de Ciberdefesa e Cibersegurança (Ministério da Defesa NacionaL [MDN], 2021, p. 4). Bem como, aproveitar as sinergias com a NATO *Communications and Information* (NCI) *Academy* localizada em Oeiras, estabelecendo a ponte entre a NATO e a UE, colocando Portugal num papel de destaque na comunidade de Ciberdefesa internacional (E1, *op. cit*).

4.2.2 O Treino e Exercícios

O treino e a realização de exercícios, devem ocorrer de forma regular, contemplando todos os níveis de comando e acompanhado de avaliações regulares (EEAS 2022, p. 34).

Relativamente ao treino, investigou-se a realização do mesmo e a sua regularidade em Unidades com elementos ou Células de Ciberdefesa. Apuradas as respostas dos entrevistados, verifica-se que 85%[5] confirmam a existência de treinos de forma regular na sua Unidade. Registou-se também, alguma disparidade na regularidade, que varia entre treinos diários e trimestrais. Outro ponto elencado, refere que as atividades de treino são conduzidas apenas "entre os elementos intrinsecamente dedicados a essas funções […]" (E7, *op. cit.*).

Quanto aos exercícios, procurou-se perceber se estes são uma ferramenta eficaz no combate às Ciberameaças e Ciberataques. Analisadas as respostas dos especialistas, constata-se que 80% considera os exercícios eficazes. Devendo-se inclusivamente integrar o Ciberespaço, no cenário dos exercícios dos restantes domínios (E9, *op. cit.*). Todavia, devido à frequência com que são realizados, não tem existido oportunidade para retirar as lições apreendidas no final dos mesmos (E1, *op. cit.*). Além disso, os exercícios têm sido idênticos aos realizados pela NATO. Esta situação deve ser evitada, pois o Pessoal que participa nos exercícios da UE e da NATO, tendem a ser os mesmos (E2, *op. cit.*).

Foi também elencado, que devem ser melhorados "os aspetos relacionados às ferramentas de combate à intrusão nos sistemas […]" (E5, *op. cit.*). Bem como, a relutância na partilha de informação e de perícias por parte dos participantes (E7, *op. cit.*).

[5] A percentagem supracitada, advém das funções dos entrevistados. Apenas setes pertencem, ou pertenceram a Unidades com elementos ou Células de Ciberdefesa, portando deve-se considerar sete e não dez unidades de enumeração.

4.2.3 Resposta à segunda questão derivada

Destarte e em resposta à QD "Como é efetuada a Formação o Treino e Exercícios de Ciberdefesa na UE?", assinala-se que:

- A formação, não se encontra organizada, sendo ministrada pelos Estados-Membros, que revelam alguma relutância na partilha da mesma. Além disso, verifica-se que os recursos humanos são escassos, faltando também uma mudança na mentalidade dos militares, para evitar limitar a formação apenas a elementos afetos à Ciberdefesa, formando e treinando utilizadores e decisores.
- No que toca à importância da criação de infraestruturas dedicadas à formação e treino de Ciberdefesa, a implementação do CAIH pode ser a solução para a Ciberdefesa na UE. Através do CAIH, a UE pode assegurar um Centro de Excelência de Ciberdefesa e Cibersegurança. Por estar localizado em Portugal, poderão ser criadas sinergias com a NCI *Academy*.
- Quanto ao treino, apesar de se verificar que este existe, a regularidade com que se realiza varia consideravelmente, constata-se que certas Unidades apenas efetuam treinos trimestrais. Ademais estes treinos tendem a abranger apenas os elementos colocados em funções dedicadas à Ciberdefesa.
- Relativamente aos exercícios, apurou-se que apesar de serem eficazes, ainda existe uma reserva na partilha de informação e de perícias. Além disso, devido à sua regularidade, não tem sido possível identificar as devidas lições apreendidas. Constatou-se também, que existe pouca diversidade dos cenários, pois os exercícios têm-se mostrado idênticos aos realizados pela NATO. Acresce ainda referir, que relativamente a cenários, estes deveriam contemplar sempre o Ciberespaço, mesmo quando o exercício visa o treino nos outros domínios. Por fim, foi apontado que os aspetos relacionados às ferramentas de combate à intrusão nos sistemas necessitam de ser melhorados.

4.3 A Resposta aos Incidentes no Ciberespaço da UE

Com o intuito de garantir o regular funcionamento das redes das Instituições, inclusivamente as militares, é necessário implementar mecanismos, procedimentos e recursos aprimorados, que permitam a proteção, deteção, resposta, mitigação, relatórios e a recuperação de incidentes que afetam redes e sistemas, recursos e serviços de apoio.

Os mecanismos de resposta, formam um ciclo continuo insistindo na preparação como pré-requisito para tornar mais eficientes as etapas do processo (Figura 5). (EEAS 2022, p. 29; EUMS 2018, p. 7).

Figura 5– Ciclo de Resposta a incidentes no Ciberespaço
Fonte: Adaptado a partir de EUMS (2018, p. 7).

Paralelamente, é vital estabelecer relações com recurso a meios de comunicação adequados, com outras partes interessadas (outras equipes de resposta a incidentes e de aplicação da lei). Como tal, encontram-se em desenvolvimento dois projetos. *O Cyber and Information Domain Coordination Center* (CIDCC) e uma rede especifica para as *military Computer Emergency Response Team* (milCERT).

O CIDCC é um projeto da PESCO, que fornecerá uma análise holística do Ciberespaço, do ambiente eletromagnético e do domínio cognitivo, conectando diferentes fontes de informação, para os níveis estratégico e operacional. Proporcionará a capacidade de sincronizar efeitos e realizar o planeamento e condução de Operações/Missões relacionadas com o domínio do Ciberespaço, contribuindo para a resiliência militar da UE (Figura 6) (EEAS 2022, p. 11).

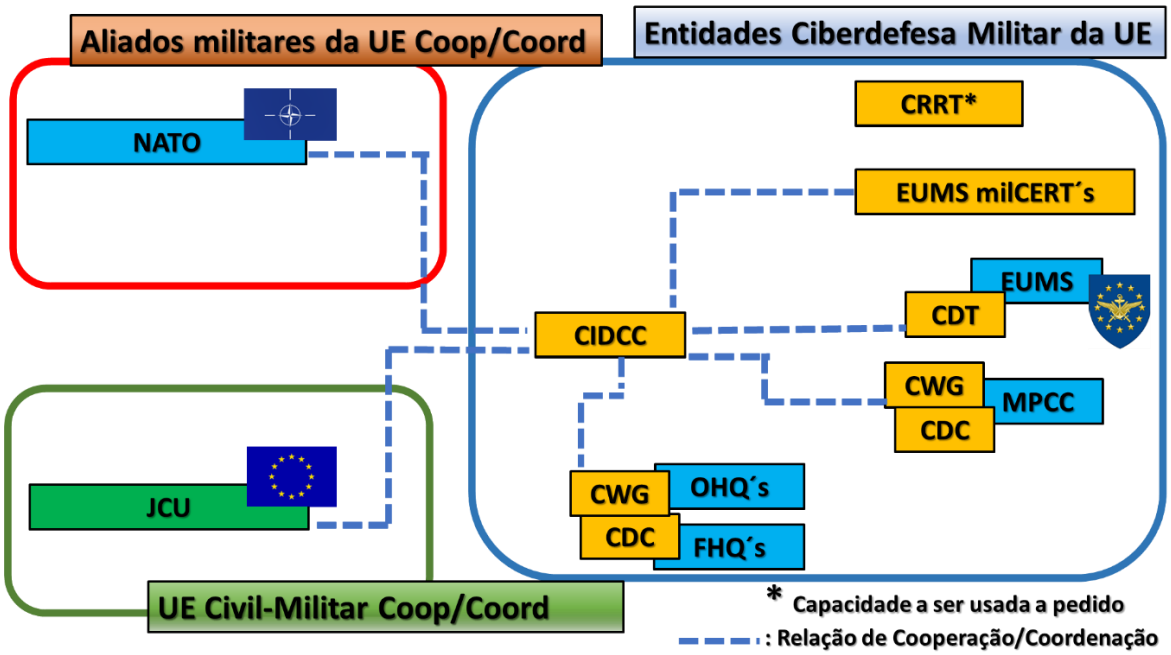

Figura 6– Relações previstas da Ciberdefesa das Operações/Missões militares da UE
Fonte: Adaptado a partir de EEAS (2022, p. 15).

Questionados os entrevistados sobre a importância da inserção do CIDCC na estrutura de Ciberdefesa da UE, 90% dos entrevistados concordaram fortemente com essa inserção. Destacando-se a resposta do E1:

> "faz falta uma estrutura física de coordenação para a informação no Ciberespaço, fazendo a ligação dos milCERT dos Centros de Ciberdefesa Nacionais (CCDN), com a comunidade de Cibersegurança, via *Joint Cyber Unit* (JCU), bem como na parte operacional, ligar os *Operation Headquarters* (OHQ) às suas células *Cyber* e à comunidade de Intel para tratar as Informações deste domínio e eventualmente à comunidade de Ciberdefesa dos Estados-Membros […]." *(op. cit.)*

Relativamente à rede para as milCERT, foi identificada a sua falta na CDPF de 2014. A criação de uma rede de milCERTs poderá facilitar a troca de informações, promovendo uma resposta mais forte às Ciberameaças, na defesa das estruturas da UE e dos Estados-Membros, incluindo Operações/Missões militares lideradas pela UE. Além disso, essa resposta poderá ser ampliada quando usada de forma complementar com as entidades de Cibersegurança da UE e com a NATO (European Defence Agency [EDA], 2021).

Na opinião dos entrevistados, 90% concorda ou concorda fortemente com a criação da rede. Constata-se que, a existência da rede permitirá reagir rapidamente e evitar consequências, de um eventual Ciberataque em larga escala (E7, op. cit.), ligando as milCERT da UE entre si, através da JCU (E1, op. cit.). A melhoria na cooperação entre as

milCERT da UE beneficiará as Operações/Missões militares da UE. Esta cooperação na comunidade *Cyber* militar é essencial para implementar e usar o Ciberespaço como domínio de Operações na UE (E8, op. cit.).

Passando à análise do Processo de Resposta aos Incidentes no Ciberespaço, interrogou-se os entrevistados, averiguando se atualmente o processo garante uma resposta eficaz. Responderam à questão 80% dos entrevistados, em que 50% respondeu que o sistema era eficaz e os restantes 50% responderam negativamente. Das respostas negativas, foi apontado o facto do CIDCC ainda não estar implementado, como sendo um dos motivos para a UE não deter a capacidade para dar uma resposta coordenada e eficaz no Ciberespaço, cabendo aos Estados- Membros a resolução do incidente (E1, *op. sit*.; E8, *op. sit*.).

Seguidamente, nas seções do presente subcapítulo, será efetuada a análise das quatro fases que compõem o processo de resposta aos incidentes no Ciberespaço.

4.3.1 A Preparação

A fase de preparação visa a prevenção de incidentes, criando antecipadamente, resiliência e medidas de proteção, através de controlos de segurança. A Preparação, é uma tarefa para quase todos os elementos de um Quartel-General (QG) e fundamental para o sucesso de qualquer resposta a incidentes no Ciberespaço (EUMS 2018, p. 9).

Questionados os especialistas sobre a existência de medidas e estruturas que contribuem para a Preparação nos QG a que pertencem, responderam à questão 60% dos entrevistados, tendo-se obtido as seguintes respostas:

- 83% confirmaram a existência de Células de Ciberdefesa;
- 83% atestaram a existência de um *Security Operation Center*;
- 83% confirmaram possuir uma *Incident Handling Team*;
- 67% refere ter utilizado uma plataforma de partilha de informação com outras Nações ou outras entidades sobre incidentes de Ciberdefesa;
- 83% afirmaram dispor de um Plano de Ciberdefesa;
- 83% confirmaram executar Treinos regulares de Ciberdefesa.

É relevante referir, que apenas 40% dos entrevistados comprovaram a existência de todas as medidas e estruturas elencadas.

4.3.2 Deteção e Análise

A fase de Deteção e Análise, consiste num conjunto de atividades que visam identificar e analisar incidentes (vetores) que constituem ameaças aos SIC (EUMS 2018, p. 11).

Relativamente à existência da capacidade de Deteção e Análise, 60% dos entrevistados atestaram deter esta capacidade. Contudo, foi referido que "Estas duas áreas, embora planeadas, ainda não se podem considerar realmente operacionais. Falta formação e treino dos poucos operacionais existentes […]" (E7, *op. cit.*).

4.3.3 Resposta e Reporte do Incidente

O objetivo geral desta fase, é negar ao adversário o sucesso das Operações ofensivas no Ciberespaço direcionadas aos sistemas das Nossa Forças, mitigando eventuais danos que daí possam advir. A resposta a incidentes, é um conjunto de medidas e ações defensivas ou de mitigação, que são desencadeadas em reação ao apurado na fase anterior, incluindo medidas técnicas internas, bem como ações de Ciberdefesa fora dos próprios SIC, em apoio a outras atividades militares (EUMS 2018, p. 13).

Para esta fase, confirmou-se junto dos entrevistados a existência de mecanismos e capacidades nos QG e Unidades a que pertencem. Responderam à questão 60% dos entrevistados, tendo-se obtido, sobre essa percentagem, os seguintes resultados:

- 100% afirmaram deter a capacidade de aplicar medidas contenção;
- 67% confirmaram a capacidade forense;
- 100% atestaram possuir a capacidade de erradicação;
- 100% afirmaram ter um *Point of Contact* (POC) para o reporte de incidentes internos e externos;
- 100% confirmou a existência de capacidade de recuperação.

Apesar de todos os entrevistados confirmarem a existência de um POC para reporte de incidentes, importa salientar que 67% dos entrevistados afirmou que nunca tinham sido estabelecidos contactos externos com a UE.

4.3.4 Atividade após o incidente

O objetivo desta fase é aprender com os incidentes, refletir e rever o acontecimento, como é que o incidente foi gerido e o que pode ser melhorado (EUMS 2018, p. 17).

Relativamente à última fase do ciclo, apurou-se através dos entrevistados, a existência de determinadas ações e medidas, que devam fazer parte da Atividade após o incidente. Responderam à questão 50% dos entrevistados, tendo-se obtido, os seguintes resultados:

- 100% confirmaram fazer o registo de lições apreendidas para melhorar o treino;
- 100% atestaram a realização de reuniões após o incidente;
- 100% afirmaram existir um *sharepoint* de informação e relatórios.

Importa referir que, apesar da confirmação destas ações e medidas, os entrevistados também referiram que as mesmas nunca foram desenvolvidas no âmbito da UE. Tendo sido desenvolvidas a nível interno, nacional ou com a NATO.

4.3.5 Resposta à terceira questão derivada

No seguimento do referido e respondendo à QD "De que modo é realizada a resposta aos incidentes no Ciberespaço pela UE?", importa referir que:

As Instituições, inclusive as Militares, requerem mecanismos de resposta, procedimentos e recursos aprimorados de Ciberdefesa, para o regular funcionamento das suas redes. Estes mecanismos formam um ciclo continuo composto de quatro etapas, dando origem a um processo. Concomitantemente, é essencial conceber e coordenar relações com recurso a meios de comunicação adequados, com outras partes interessadas.

O CIDCC poderá proporcionar a sincronização de efeitos e realizar o planeamento e condução de Operações/Missões no Ciberespaço, aumentando a resiliência militar da UE. A existência desta estrutura física, irá garantir a ligação dos milCERT/CCDN com a comunidade de Cibersegurança e na parte operacional ligar os OHQ e as células *Cyber* da UE.

Quanto aos meios de comunicação adequados, a criação de uma rede de milCERTs poderá promover a troca de informações e uma resposta mais forte às Ciberameaças, na defesa das estruturas da UE e das Operações/Missões militares lideradas pela UE, permitindo reagir rapidamente e evitar um eventual Ciberataque em larga escala.

Consequentemente, a não implementação destes dois projetos, sobretudo do CIDCC, inviabiliza um processo de resposta a incidentes no Ciberespaço eficaz, obrigando a UE a recorrer às capacidades dos seus Estado-Membros.

Na fase da Preparação do referido processo, verificou-se que as Células, Centros e elementos de QG com responsabilidades na Ciberdefesa, não detêm a totalidade das medidas e estruturas analisadas. Além disso, aferiu-se que existe pouca afluência no uso de plataformas de partilha de informação com outras Nações, ou entidades sobre incidentes de Ciberdefesa.

Quanto à capacidade de Deteção e Análise, apesar da sua existência, foi apontado que falta alocar recursos humanos, formados e treinados.

Relativamente à Resposta e Reporte do Incidente, inferiu-se que a capacidade forense não se encontra plenamente desenvolvida e que a maioria das entidades de Ciberdefesa não têm um POC para reporte de incidentes na UE.

Por último, na Atividade após o incidente, constatou-se que as ações e medidas não têm sido desenvolvidas com a UE, sendo realizadas ao nível interno, nacional ou com a NATO.

4.4 Síntese Conclusiva

No seguimento das respostas às QD, cumpre responder à QC "De que modo pode ser melhorada a Ciberdefesa das Operações/Missões da UE?"

Fruto da análise efetuada, propõe-se que para evolução da Ciberdefesa na UE, é necessário um maior empenhamento político e de partilha de Informação dos Estados-Membros. Ademais, propõe-se a criação de doutrina conjunta e alocação de recursos humanos e meios especializados. Simultaneamente, propõe-se a criação de uma estrutura bem definida de Ciberdefesa, podendo ser materializada através dos projetos PESCO.

No que tange à formação, propõe-se que esta seja organizada e que deixe de estar dependente dos Estados-Membros, promovendo assim a partilha da informação.

Paralelamente, propõe-se também uma maior alocação de recursos humanos, bem como a implementação de ações de sensibilização para o Ciberespaço, com o intuito de mudar a mentalidade dos militares, alargando a formação para além dos elementos afetos à Ciberdefesa. Quanto a infraestruturas dedicadas à formação e treino de Ciberdefesa, propõe-se a implementação do CAIH como Centro de Excelência de Ciberdefesa e Cibersegurança para a UE, a sua localização em Portugal, permite criar sinergias com a NCI *Academy*. Relativamente ao treino, propõe-se que este seja feito com regularidade e que abranja o maior número possível de utilizadores das redes da UE e não apenas os elementos colocados em funções dedicadas à Ciberdefesa.

Relativamente aos exercícios, propõe-se a incrementação da partilha de informação e de perícias entre os participantes. Propõe-se também a criação de plataformas de partilha de lições apreendidas. Propõe-se ainda a criação de novo cenários para evitar cenários idênticos aos de outras Organizações, incluindo o Ciberespaço nos exercícios, mesmo quando estes se desenrolam noutro(s) domínio(s). Finalmente propõe-se melhorar os aspetos relacionados às ferramentas de combate à intrusão nos sistemas.

Quanto à resposta aos incidentes no Ciberespaço, de acordo com a investigação, propõe-se a implementação do CIDCC, dotando a UE com a capacidade de sincronizar efeitos e realizar o planeamento e condução de Operações/Missões militares no Ciberespaço. Propõe-se também a criação de uma rede, ou utilizar uma já existente, possibilitando a troca de informações entre as milCERTs, garantindo uma resposta mais forte às Ciberameaças, na defesa das estruturas da UE e das Operações/Missões lideradas militares pela UE.

No âmbito do processo de resposta aos incidentes, propõe-se para a fase da Preparação, que as entidades com responsabilidade da Ciberdefesa nas Operações/Missões militares da UE, implementem todas as capacidades necessárias para a execução desta fase. Além disso, propõe-se a criação de plataformas de partilha de informação com outras Nações ou entidades sobre incidentes no Ciberespaço. Quanto à Deteção e Análise, propõe-se mais uma vez a alocação de recurso humanos com formação e treino. Relativamente à fase de Resposta e Reporte do Incidente, propõe-se o reforço na capacidade forense e a criação/difusão de POC para reporte de incidentes na estrutura de Ciberdefesa da UE. Quanto à Atividade após o incidente, propõe-se que a UE desenvolva os procedimentos relativos a esta fase, envolvendo todos os elementos da estrutura de Ciberdefesa da UE.

5. Conclusões

As sociedades modernas, manifestam atualmente uma grande dependência do Ciberespaço, que assume uma função de agregação de interações.

A internet reduziu as distâncias, criou redes e deu origens a interações ao nível global, social, económico e indubitavelmente ao nível militar. Como consequência, os sistemas de C2 e a forma de fazer a guerra, mudaram drasticamente. O emprego das FA, depende funcionalmente da disponibilidade e fiabilidade dos seus SIC. Considerando que os sistemas de armas tendem a ser cada vez mais sofisticados, um ataque lançado através do Ciberespaço pode causar um efeito disruptivo e/ou destrutivo com implicações nos outros domínios.

Atualmente existem ferramentas tecnológicas de fácil acesso e de baixo custo. Quando exploradas com más intenções, podem desencadear atividades não desejadas, constituindo-se como Ciberameaças. Os ciberataques poderão assim ser considerados uma ameaça, com impacto profundo e consistente, constituindo-se como uma ferramenta de excelência para o terrorismo transnacional, ou para a projeção de Poder dos Estados através do Ciberespaço.

A UE e os seus Estados-Membros, sentiram a necessidade de neutralizar/mitigar estes ataques e tornar o Ciberespaço mais seguro e resiliente. Como tal, foi solicitado às FA dos vários Estados-Membros, a criação de mecanismos de proteção do Ciberespaço, assistindo-se a uma crescente exploração militar deste Domínio e uma alteração profunda no ambiente estratégico internacional.

Nesta conjuntura, em 2012 surge o conceito de Ciberdefesa da UE, como dimensão militar da Cibersegurança, compreendendo também abordagens civis, destinada a defender sistemas e informações críticos, a fim de alcançar a Cibersegurança. A Ciberdefesa visa compreender todas as medidas técnicas e não técnicas para melhorar a resiliência dos sistemas baseados nas tecnologias da informação e comunicação, C2 e qualquer sistema, arma ou sensor, apoiando os interesses de defesa e segurança da UE e dos seus Estados-Membros, na prevenção, deteção, reação e recuperação de um Ciberataque a esses sistemas.

Prevê-se que a Ciberdefesa assuma cada vez mais preponderância, assumindo-se como um importante desafio à segurança nos próximos tempos. O alcance da Ciberdefesa não passará apenas pela proteção de um computador ou telemóvel ligado à internet, mas também de infraestruturas fundamentais, tais como estações de fornecimento de água e eletricidade.

A pertinência e relevância desta investigação, assenta na análise da evolução da capacidade de Ciberdefesa da UE desde 2012 até à atualidade, bem como na análise à Formação, Treino, Exercícios e nas respostas aos incidentes no Ciberespaço da UE.

Atendendo à metodologia e com o objetivo de propor contributos para Ciberdefesa das Operações/Missões militares da UE, desenvolveu-se um estudo de caso, com um horizonte temporal transversal, recorrendo a um raciocínio dedutivo, numa estratégia qualitativa.

Com o propósito de aprimorar os conhecimentos do investigador, foram contactados diversos especialistas, realizando-se profusas entrevistas exploratórias. Paralelamente, foi efetuada a leitura de uma extensa bibliografia. Posteriormente, constituiu-se uma amostra não-probabilística intencional, com dez especialistas detentores de conhecimentos alargados na temática em apreço, decorrente do cargo em que estão ou estiveram colocados, a par das suas qualificações académicas. Constituída a amostra, procedeu-se à realização de entrevistas semiestruturadas que através de uma análise categorial concorreram para as respostas às QD. A análise documental, baseada sobretudo em documentos oficiais do EEAS, EUMS e CEU, serviu de base para a realização das entrevistas, bem como para efetuar cruzamento e complementaridade de dados.

Como principais conclusões, constatou-se que desde 2018 até à atualidade desenrolaram-se evoluções significativas nas áreas da CDPF, impulsionada sobretudo pela criação dos projetos PESCO. Todavia, constatou-se que continua a faltar o empenhamento e partilha de Informação dos Estados-Membros, a par da doutrina, recursos humanos e meios especializados. Ademais, a estrutura de Ciberdefesa não se encontra consolidada e como tal, não garante uma resposta coordenada e credível da UE no Ciberespaço. Constata-se também que falta concretizar os projetos PESCO que estão em curso, essenciais para dotar a UE com resiliência e capacidade de dissuasão credíveis no Ciberespaço.

No campo da formação, conclui-se que a mesma não se encontra organizada, sendo ministrada pelos Estados-Membros, que revelam alguma resistência na sua partilha. Além disso, constatou-se que os recursos humanos são escassos e urge fazer-se uma mudança na mentalidade dos militares, alargando a formação para além dos elementos afetos à Ciberdefesa, incluindo utilizadores e decisores.

Relativamente à existência de infraestruturas dedicadas à formação e treino de Ciberdefesa, constatou-se que a implementação CAIH pode ser uma solução viável para a Ciberdefesa na UE. O CAIH pode constituir-se como um Centro de Excelência de Ciberdefesa e Cibersegurança. Exponenciando a sua localização em Portugal, para criar sinergias com a NCI *Academy*.

No treino, constatou-se que certas Unidades apenas efetuam treinos trimestrais e que estes tendem a abranger meramente os elementos colocados em funções dedicadas à Ciberdefesa. Quanto aos exercícios, apurou-se que apesar de serem eficazes, existe uma

reserva na partilha de informação e de perícias. Ademais, fruto da sua regularidade, não tem sido possível identificar lições apreendidas. Paralelamente, verificou-se que existe pouca diversidade dos cenários e que os mesmos têm sido idênticos aos realizados por outras Organizações. Constatou-se também, que os aspetos relacionados às ferramentas de combate à intrusão nos sistemas necessitam de ser melhorados.

Quanto à resposta a incidentes no Ciberespaço, averiguou-se que o CIDCC, quando implementado, proporcionará a capacidade de sincronizar efeitos e realizar o planeamento e condução de Operações/Missões no Ciberespaço, exponenciando a resiliência militar da UE. Através do CIDCC será possível estabelecer a ligação dos milCERT/CCDN com a comunidade de Cibersegurança e na parte operacional, ligar os OHQ às células *Cyber* da UE. No que toca aos meios de comunicação adequados, apurou-se que a criação de uma rede de milCERTs poderá proporcionar a troca de informações e uma resposta mais musculada às Ciberameaças, aquando da defesa das estruturas da UE e das Operações/Missões militares lideradas pela UE.

Analisado o processo de resposta a incidentes, conclui-se que na fase da preparação as entidades com responsabilidade na Ciberdefesa, não possuem a totalidade das medidas e estruturas que foram alvo da análise. Além disso, constatou-se que existe pouca afluência no uso de plataformas de partilha de informação com outras Nações ou entidades sobre incidentes de Ciberdefesa.

No âmbito da capacidade de Deteção e Análise, apurou-se que falta formar, treinar e alocar recursos humanos. Relativamente à Resposta e Reporte de Incidentes, inferiu-se que a capacidade forense não se encontra plenamente desenvolvida. Talqualmente, apurou-se que a maioria das entidades estudadas não têm um POC para reporte de incidentes na UE. No respeitante à Atividade após o incidente, constatou-se que as ações e medidas não têm sido desenvolvidas com a UE, mas sim realizadas ao nível interno, nacional ou com a NATO.

Em resultado dos contributos para o conhecimento deste estudo, propõe-se, que no âmbito da evolução da Ciberdefesa na UE, exista um maior empenhamento político e partilha de Informação dos Estados-Membros. Concomitantemente, propõe-se a criação de uma doutrina conjunta e alocação de recursos humanos e meios especializados, a par da criação de uma estrutura bem definida de Ciberdefesa, que poderá ser materializada através dos projetos PESCO. Deste modo, poderá ser assegurada a resiliência e uma resposta coordenada e credível da UE no Ciberespaço.

Como contributos para a formação, propõe-se que esta seja organizada, saindo da dependência dos Estados-Membros, viabilizando a partilha da informação. Paralelamente

propõe-se uma vez mais o incremento na alocação de recursos humanos, a par da implementação de ações de sensibilização para o Ciberespaço, estendendo a formação para além dos elementos de Ciberdefesa, contribuindo para uma mudança de mentalidades. Quanto às infraestruturas para a formação e treino de Ciberdefesa, recomenda-se a consolidação da implementação do CAIH como Centro de Excelência de Ciberdefesa e Cibersegurança para a UE. Relativamente ao treino, sugere-se que este seja feito com mais regularidade e que abranja o maior número possível de utilizadores das redes da UE e não apenas os elementos em funções dedicadas à Ciberdefesa.

Nos exercícios, propõe-se que se incremente a partilha de informação e de perícias entre os participantes. Propõe-se também que se criem plataformas de partilha de lições apreendidas. Propõe-se ainda a criação de novo cenários, incluindo o Ciberespaço sempre que possível, mesmo nos exercícios dos restantes domínios. Finalmente propõe-se melhorar os aspetos relacionados às ferramentas de combate à intrusão nos sistemas.

Quanto à resposta aos incidentes no Ciberespaço, propõe-se como contributos, a implementação do CIDCC e a criação de uma rede, ou uso de uma existente, para as milCERTs, promovendo a troca de informações e uma resposta mais forte às Ciberameaças, na defesa das estruturas da UE e das Operações/Missões militares lideradas pela UE.

Relativamente ao processo de resposta aos incidentes, propõe-se na fase da Preparação, que as entidades de Ciberdefesa envolvidas nas Operações/Missões militares da UE, adquiram todas as capacidades necessárias para a execução desta fase. Propõe-se também a operacionalização de plataformas de partilha de informação com outras Nações ou entidades, sobre incidentes de Ciberdefesa. No respeitante à Deteção e Análise, propõe-se uma vez mais, a alocação de recursos humanos formados e treinados. No que toca à fase de Resposta e Reporte do Incidente, propõe-se como contributos o reforço na capacidade forense e a criação/difusão de POC para reporte de incidentes na estrutura de Ciberdefesa da UE. Quanto à Atividade após o incidente, propõe-se que a UE desenvolva os procedimentos relativos a esta fase, envolvendo os elementos das Operações/Missões militares da UE e os CCDN.

Apesar dos resultados alcançados, considera-se que a presente investigação apresenta duas limitações. A primeira prende-se com a indisponibilidade na resposta às entrevistas, dos oficiais a desempenhar funções nos QG das Missões da UE na Somália e República Centro-Africana, o que poderá enviesar o estudo para a visão dos especialistas portugueses. A segunda está relacionada com a temática do trabalho. A escolha de realizar um estudo não classificado, para que se mantivesse a abrangência de divulgação e o interesse académico,

impediu o acesso a estudos e relatórios classificados com o detalhe do estado atual da Ciberdefesa das Operações/Missões militares da EU.

Como estudos futuros afetos a esta temática, vislumbra-se a importância de estudar o grau de maturação dos projetos PESCO, bem como estudar o impacto que a atual guerra na Ucrânia poderá ter, na forma como a UE prevê organizar a defesa do seu Ciberespaço. Considera-se de igual modo importante, efetuar este estudo com matérias classificadas de modo a obter uma análise plena dos factos, pesa embora a perda de abrangência de divulgação.

Em termos práticos, considera-se que Portugal deve tirar partido da sua posição como membro da NATO e da UE e constituir-se como uma referência na formação e treino da Ciberdefesa, criando sinergias entre o CAIH e a NCI *Academy*.

Referências bibliográficas

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

Carayannis, E. G., Campbell, D. F. J., & Efthymiopoulos, M. P. (2014). *Cyber-Development, Cyber-Democracy and Cyber-Defense*. New York: Springer New York Heidelberg Dordreacht London.

Conselho da União Europeia. (2022). *Bússola Estratégica para a Segurança e a Defesa – Por uma União Europeia que protege os seus cidadãos, os seus valores e os seus interesses e contribui para a paz e a segurança internacionais*. Bruxelas: Autor.

Council of the European Union. (2014). *EU Cyber Defence Policy Framework*. Bruxelas: Autor.

Council of the European Union. (2018). *EU Cyber Defence Policy Framework (2018 update)*. Bruxelas: Autor.

European Defence Agency. (2021). *CYBER DEFENCE Built on European cooperation* [Página *online*]. Retirado de http://www.eda.europa.eu.

European External Action Service. (2016). *EU Concept on Cyber Defence for EU-led military Operations and Missions*. Bruxelas: Autor.

European External Action Service. (2021). *EU missions and operations* [Página *online*]. Retirado de http://www.eeas.europa.eu/csdp/missions-and-operations/index_en.htm.

European External Action Service. (2022). *Draft Concept on Cyber Defence for EU-led military operations and missions*. Bruxelas: Autor.

European Union Military Staff. (2014). *European Union Concept for EU-led Military Operations and Missions* [Página *online*]. Retirado de https://data.consilium.europa.eu/doc/document/ST-17107-2014-INIT/en/pdf.

European Union Military Staff. (2018). *European Union Cyber Defense SOP for European Union HQ*. Brussels: Autor.

European Union Military Staff. (2021). *European Union Military Vision and Strategy on Cyberspace as a Domain of Operations*. Bruxelas: Autor.

Freixo, M. J. V. (2011). *Metodologia Científica: Fundamentos, Métodos e Técnicas (4.ª Edição)*. Lisboa: Instituto Piaget.

Freixo, M. J. V. (2018). *Metodologia Científica Fundamentos Métodos e Técnicas*. 5.ª Ed. Lisboa: Instituto Piaget.

Guerra, I. (2006). *Pesquisa Qualitativa e Análise de Conteúdo. Sentidos e formas de uso*. Lisboa: Princípia.

JP3-12. (2018). *Joint Publication 3-12 - Cyberspace Operations*.

Kello, L. (2018). Cyber Defence [Página *online*]. *The Handbook of European Defence Policies and Armed Forces*. Retirado de https://www.eda.europa.eu.

Legrand, J. (2021). *Common Security and Defence Policy* [Página *online*]. Retirado de https://www.europarl.europa.eu/ftu/pdf/en/FTU_5.1.2.pdf.

Ministério da Defesa Nacional. (2021). *Cyber Academia and Innovation Hub - CAIH CALL para a sua implementação*. Lisboa: Autor.

Monteiro, S. D. (2007). O Ciberespaço: o termo, a definição e o conceito. *DataGramaZero - Revista de Ciência Da Informação*, *8* n.*3*.

North Atlantic Treaty Organization. (2020). *Allied Joint Publication-3.20*. Bruxelas: NATO STANDARDIZATION OFFICE [NSO].

Nunes, P. F. V. (2010). Mundos virtuais, riscos reais: fundamentos para a definição de uma estratégia da informação nacional. *Revista Militar*, *2506*, 1169–1198. https://www.revistamilitar.pt/artigo/608

Nunes, P. F. V. (2011). *Estratégia, Volume XX - 2011*. Lisboa: ACAMA - Unip.Lda.

Nunes, P. F. V. (2020). *A Edificação da Capacidade de Ciberdefesa Nacional: Contributos para a Definição de uma Estratégia Militar para o Ciberespaço*. Lisboa: Instituto Universitário Militar.

Nunes, P. V. (2014). Ciberespaço, ciberviolência e o uso organizado da força. *JANUS 2014 - Metamorfoses Da Violência (1914-2014)*, 146–147. http://repositorio.ual.pt/handle/11144/2902

Nunes, P. V., Mendes, C. P., Ralo, J., Santos, L., Santos, L. C. dos, Moniz, P., & Casimiro, S. de V. (2018). *Contributos para uma Estratégia Nacional de Ciberdefesa*. Lisboa: Instituto de Defesa Nacional.

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*.

Pardal, L. A., & Correia, E. (1995). *Métodos e técnicas de investigação social*. Porto:Areal.

Phillips, E. M., & Pugh, D. S. (1998). *Como preparar um Mestrado ou Doutoramento: um manual prático para estudantes e seus orientadores*. Mem Martins: Lyon Edições.

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

Resolução do Conselho de Ministros n.º 92/2019 de 5 de junho. (2019). *ESTRATÉGIA NACIONAL DE SEGURANÇA DO CIBERESPAÇO 2019 -2023*. Diário da República, 1.ª série, 1, 2889-2895. Lisboa: Assembleia da República.

Rocha, Á., & Guarda, T. (2018). *Developments and Advances in Defense and Security*.

Coimbra: SpringerInternational Publishing AG.

Rodrigues, J. C. (2016). *O ciberespaço e a ordem mundial* [Página *online*]. Retirado de https://observador.pt/opiniao/o-ciberespaco-e-a-ordem-mundial/.

Röhrig, W., & Smeaton, R. (2014). *Cyber Security and Cyber Defence in the European Union. Opportunities, Synergies and Challenges* [Página *online*]. Retirado de https://eda.europa.eu/docs/default-source/documents/23-27-wolfgang-r%C3%B6hrig-and-j-p-r-smeaton-article.pdf?msclkid=cf8eb66abde511ec9bd642282f61fe52.

Santos, L. A. B., Lima, J. M. M. V, Garcia, F. M. G. P. P., Monteiro, F. T., Silva, N. M. P., Silva, J. C. V. F., Santos, R. J. R. P., Afonso, C. F. N. L. D., & Piedade, J. C. L. (2019). *Orientações metodológicas para a elaboração de trabalhos de investigação* (Cadernos d). (2.ª Ed., revista e atualizada). Cadernos do IUM, 8. Lisboa: Instituto Universitário Militar.

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

Sarmento, M. (2013). *Metodologia científica para a elaboração, escrita e apresentação de teses*. Lisboa: Universidade Lusíada Editora.

Sousa, M. J., & Baptista, C. S. (2011). *Como fazer investigação, dissertações, teses e relatórios segundo Bolonha*. Lisboa: Lidel.

Trimintzios, P., Chatzichristos, G., Portesi, S., Drogkaris, P., Palkmets, L., Liveri, D., & Dufkova, A. (2017). *Cybersecurity in the EU Common Security and Defence Policy Challenges and risks for the EU*. Bruxelas: European Parliamentary Research Service Scientific Foresight Unit.

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

Yin, R. K. (2018). *Case study research and applications design and methods*. (6.ª Ed.). Los Angeles: SAGE Publications Ltd.

Apêndice A – Modelo de Análise

Quadro 1- Modelo de análise

TEMA		**Ciberdefesa – A evolução e pertinência no contexto da UE**							
Objeto de estudo		Ciberdefesa das Operações/Missões militares da UE							
Delimitação		Temporal	De 2012 até ao presente.						
		Espacial	União Europeia.						
		Conteúdo	A Ciberdefesa da UE						
Objetivo Geral		Propor contributos para melhorar a Ciberdefesa nas Operações/Missões militares da UE.							
Questão Central		De que modo pode ser melhorada a Ciberdefesa das Operações/Missões militares da UE?							
Objetivos Específicos		**Questões derivadas**		**Conceitos**	**Dimensões**	**Variáveis**	**Indicadores**	**Técnicas de recolha de dados**	**Estrutura**
OE1	Analisar evolução da Ciberdefesa na UE	**QD1**	De que modo tem evoluído a Ciberdefesa da UE?	Ciberespaço Ciberdefesa	Ciberespaço da UE Ciberdefesa da UE	Componente militar de Ciberdefesa da UE	- Criação da Visão para a estratégia de Ciberdefesa da UE; - Integração do Ciberespaço no planeamento e operações militares das missões da UE, estabelecendo uma resiliência e dissuasão eficazes e consistentes; - Áreas prioritárias da política de Ciberdefesa da UE; - Projetos PESCO.	Análise documental Entrevistas	Capítulo 4
OE2	Analisar a Formação, Treino e Exercícios de Ciberdefesa na UE	**QD2**	Como é efetuada a Formação o Treino e Exercícios de Ciberdefesa na UE?	Ciberdefesa da UE	Formação Treino e Exercícios	Recursos Humanos da UE para a Ciberdefesa	- Existência de formação em Ciberdefesa adequada; - Existência regular de treinos do Pessoal de Ciberdefesa; - Existência de exercícios de Ciberdefesa ajustados aos desafios do Ciberespaço.	Análise documental Entrevistas	Capítulo 4
						Infraestruturas de Formação e Treino de Ciberdefesa da UE	- Existência de infraestruturas dedicadas à Formação e Treino na UE;		
OE3	Analisar a resposta aos	**QD3**	De que modo é	Ciberdefesa	Processo de resposta a	Preparação	- Existência de uma *Cyber Defence Cell*;	Análise documental	Capítulo 4

	incidentes no Ciberespaço da UE		realizada a resposta aos incidentes no Ciberespaço pela UE?	Incidentes de Ciberdefesa	incidentes de Ciberdefesa nas Estruturas Militares da UE		- Existência de uma *Security Operation Center*; - Existência de uma *Incident Handling Team*; - Partilha de informação com outras nações ou outras entidades; - Existência de um *Cyber Defence Plan*; - Treinos regulares de Ciberdefesa nos HQs.	Entrevistas	
						Deteção e Análise	- Capacidade de deteção de precursores e indicadores e do incidente; - Capacidade de Análise do incidente.		
						Resposta e Reporte	- Capacidade de aplicar medidas contenção; - Capacidade forense; - Capacidade de erradicação; - Estabelecimento de POC para o reporte de incidentes internos e externos; - Existência de centro de coordenação de Ciberdefesa p/ reporte de incidentes; - Existência de uma rede específica de reporte para os MCERTs dos MS ou dos EU HQ; - Capacidade de recuperação.		
						Atividade após o incidente	- Registo de lições apreendidas para melhorar o treino; - Realização de reuniões; - Existência de *sharepoint* de informação e relatórios.		

Estratégia	Qualitativa	**Raciocínio**	Dedutivo	**Desenho de Pesquisa**	Estudo de Caso / com horizonte temporal transversal

Apêndice B – Lista de Entrevistados

Quadro 2– Lista de entrevistados

Cargos na UE	**Posto/Título e Nome**
Cyber Defence programe manager da *European Defence Agency*	Tenente-Coronel David Lopes Antunes
Chefe do J6 da EUTM Mali	Tenente-Coronel Alexandre Miguel Gil Fernandes
EUMS Seconded National Expert / Action officer Cyber and SATCOM	Tenente-Coronel Jerome Daes
MPCC Chief Cyber Ops, Head of Cyber Defence Cell	Tenente-Coronel Stefan Alois Weiss
Chefe do J6 da EUTM Moçambique	Major Fábio Vieira da Silva
Cargos Nacionais	**Posto/Título e Nome**
Ex-Chefe do Centro de Ciberdefesa do Nacional	Capitão de Mar e Guerra Fialho de Jesus
Chefe da Divisão de Planos do Centro de Ciberdefesa Nacional	Capitão de Fragata Sérgio Caldeira Carvalho
Chefe do Centro de Ciberdefesa Nacional	Tenente-Coronel José Carlos Reimão Teixeira
Antigo Diretor de Curso de Planeamento de Operações de Ciberdefesa – IUM	Tenente-Coronel José Manuel Brito Sousa
Coordenador do Programa FMN / MG Rep / CWIX NL (DIRCSI) EMGFA	Capitão de Fragata Sérgio Manuel Ferreira Rodrigues

Apêndice C – Guião da Entrevista Semiestruturada

Cabeçalho

Excelentíssimo Senhor,

O meu nome é Hilário Diogo da Silva Costa, sou Major de Infantaria, e encontro-me a frequentar o Curso de Estado-Maior Conjunto 2021/2022, que decorre no Instituto Universitário Militar. Durante este curso os auditores elaboram vários trabalhos, nos quais se abordam questões relevantes e importantes para o futuro das Forças Armadas Portuguesas. Neste âmbito, encontro-me a realizar um Trabalho de Investigação Individual, intitulado "Ciberdefesa – A Evolução e Pertinência no Contexto da União Europeia"

O objetivo geral deste trabalho, consiste em propor contributos para Ciberdefesa das Operações/Missões da UE, estando delimitado temporalmente desde 2012 até à atualidade e à UE. Em termos de conteúdo está limitado às operações de Ciberdefesa. No sentido de alcançar o objetivo geral foram levantados três objetivos específicos, sendo eles:

Analisar a evolução da Ciberdefesa na UE; Analisar a Formação, Treino e Exercícios de Ciberdefesa na UE; analisar o processo de resposta de incidentes no Ciberespaço da UE. Pelo que as respostas às seguintes questões, são fundamentais para os contributos que se pretende apresentar para a resposta da UE na defesa dos incidentes no Ciberespaço.

Solicito a sua autorização para gravar a presente entrevista e para referir no trabalho o conteúdo da mesma associado ao seu nome. Caso não seja essa a sua vontade, garanto a sua confidencialidade e tratarei a informação recolhida de forma anónima. Estimo que a entrevista dure um máximo de 45 minutos.

O seu conhecimento e experiência são essenciais para a qualidade e relevância deste trabalho, pelo que, agradeço a sua disponibilidade para a prossecução da presente investigação.

Caraterização do entrevistado

Nome do Entrevistado:
Posto:
Cargo/Função:
Data da entrevista:
Local: Plataforma

Questões

1. Concorda que a UE deva ser capaz de cumprir os seus objetivos no domínio do Ciberespaço tão eficazmente como nos outros domínios, a fim de executar Operações/Missões Militares da UE?
Use uma das seguintes opções:
1- Discordo fortemente; 2- Discordo; 3- Indiferente; 4- Concordo; 5- Concordo Fortemente
Se sim, oque falta fazer para atingir esse objetivo?

2. É da opinião que a UE integre o Ciberespaço no planeamento e operações militares das suas missões, estabelecendo uma resiliência e dissuasão eficazes e consistentes contra potenciais adversários no Ciberespaço, incluindo a cooperação internacional com parceiros de apoio à Ciberdefesa da *Common Security and Defence Policy* (CSDP) da UE? Que medidas necessitam de ser implementadas para o efeito?

3. A *Cyber Defence Policy Framework* (CDPF) de 2018 determina seis áreas como prioritárias:
- Apoiar o desenvolvimento das capacidades de Ciberdefesa dos Estados-Membros;
- Reforço da proteção dos sistemas de comunicação e informação da CSDP utilizados pelas entidades da UE;
- Promoção da cooperação civil-militar;
- Investigação e tecnologia;
- Melhorar as oportunidades de educação, formação e exercícios;
- Reforço da cooperação com parceiros internacionais relevantes;

Classifique de acordo com os valores abaixo a evolução que houve destas áreas? (coloque o número à frente de cada área)
1- Discordo fortemente; 2- Discordo; 3- Indiferente; 4- Concordo; 5- Concordo Fortemente

4. Concorda que a criação dos projetos da *Permanent Structure* (PESCO) da UE são essenciais para o desenvolvimento das capacidades de Ciberdefesa da UE?
Use uma das seguintes opções:
1- Discordo fortemente; 2- Discordo; 3- Indiferente; 4- Concordo; 5- Concordo Fortemente
Considera que falta desenvolver algum projeto? Se sim qual?

5. Uma resposta eficaz às Ciberameaças e Ciberataques, requer a existência de pessoal sensibilizado e especializado em Ciberdefesa. Como tal a sua formação e treino revela-se fundamental para uma defesa eficaz do Ciberespaço da UE.

5.1. Considera que a formação em Ciberdefesa disponível na UE é suficiente para o desempenho de funções em Unidades de Ciber? Existe a possibilidade de ser melhorada?

5.2. São conduzidos treinos das tarefas críticas de Ciberdefesa na sua Unidade? Com que regularidade?

5.3. Considera que os Exercícios de Ciberdefesa da UE são eficazes na preparação contra as Ciberameaças e Ciberataques? Considera que podem ser melhorados em alguns aspetos?

5.4. Na sua Opinião considera importante existirem infraestruturas dedicadas à Formação e Treino da Ciberdefesa na UE? Que tipo de infraestruturas julga pertinente existirem?

6. O *Cyber and Information Domain Coordination Center* (CIDCC) é um projeto PESCO, que como o próprio nome indica visa a criação de um centro de coordenação para os domínios do Ciber e da Informação. Considera ser importante a inserção do CIDCC na arquitetura da Ciberdefesa da UE, por forma a garantir uma resposta conjunta e eficaz aos incidentes no Ciberespaço?

Use uma das seguintes opções:

1- Discordo fortemente; 2- Discordo; 3- Indiferente; 4- Concordo; 5 - Concordo Fortemente

7. Concorda que a criação de uma rede especifica para a comunidade de *Computer Emergency Response Team* (CERT) militares da UE é essencial para a implantação de uma defesa comum do Ciberespaço Europeu?

Use uma das seguintes opções:

1- Discordo fortemente; 2- Discordo; 3- Indiferente; 4- Concordo; 5- Concordo Fortemente

Se sim, porquê?

8. O processo de resposta aos incidentes no Ciberespaço é composto pelas fases de Preparação, Deteção e Análise, Resposta e Reporte do incidente e Atividade após o incidente. Na sua opinião, o sistema atualmente garante uma resposta eficaz? Se não porquê?

9. Relativamente à fase da Preparação no processo de resposta aos incidentes na Ciberdefesa confirma a existência das seguintes medidas ou estruturas no QG a que pertence?

- Célula de Ciberdefesa;
- *Security Operation Center*;
- *Incident Handling Team*;
- Plataforma de partilha de informação com outras nações ou outras entidades sobre incidentes de Ciberdefesa;
- Plano de Ciberdefesa;
- Treinos regulares de Ciberdefesa;

10. No seu QG no caso da Deteção e Análise de um incidente, existe a capacidade de deteção de precursores e indicadores do incidente, bem como a capacidade de Análise do incidente? Se não, porquê?

11. A fase de Resposta e Reporte no processo de resposta aos incidentes na Ciberdefesa contempla, entre outras, a existência das seguintes capacidades e estruturas:

- Capacidade de aplicar medidas contenção;
- Capacidade forense;
- Capacidade de erradicação;
- Estabelecimento de POC para o reporte de incidentes internos e externos;
- Existência de centro de coordenação de Ciberdefesa p/ reporte de incidentes;
- Existência de uma rede específica de reporte para os milCERTs dos Estados-Membros ou dos QG da UE;
- Capacidade de recuperação.

No seu QG confirma a existência destas capacidades ou mecanismos previstos para estabelecimento do contacto com alguma entidade que as detivesse da UE?

12. Após a ocorrência do incidente inicia-se a fase da Atividade após o incidente, confirma que estão previstas as seguintes ações?

- Registo de lições apreendidas para melhorar o treino
- Realização de reuniões
- Existência de *sharepoint* de informação e relatórios

Em alguma situação desenvolveu este tipo de ações no âmbito da UE?

Agradecimento

Agradeço mais uma vez a sua disponibilidade e contributos para a prossecução da presente investigação.

Muito obrigado.

Apêndice D – Análise de Conteúdo das Entrevistas Semiestruturadas[6]

Quadro 3- Matriz das unidades de contexto e de registo da primeira questão

Entrevistado	Unidade de Contexto	Unidade de Registo
1	- "Concordo fortemente, apesar de existir empenhamento político, falta uma estrutura de Ciberdefesa, doutrina, pessoal e meios especializados sobretudo no MPCC."	1.1.1
2	- "Concordo fortemente, mas a UE apenas está interessada em garantir a liberdade de movimentos e a capacidade de resposta a incidentes no Ciberespaço."	1.1.1
3	- "Concordo fortemente, falta existir uma política de segurança clara para o Ciberespaço, alinhada com os restantes domínios."	1.1.1
4	- "Concordo fortemente, falta haver uma maior partilha da informação entre os Estados-Membros e a UE assumir-se como uma organização militar."	1.1.1
5	- "Concordo fortemente, faltam recursos humanos especializados, doutrina, formação e treino eficazes."	1.1.1
6	- "Concordo fortemente, a otimização passará pelo desenvolvimento e estabelecimento de prioridades dos domínios DOTMLPF-I e pelo desenvolvimento de projetos e iniciativas, contribuindo para se alcançar, deste modo, o Nível de Ambição da EU."	1.1.1
7	- "Concordo fortemente, existe necessidade de reunir dados e informação de que habilite o C2 e o apoio à decisão, numa plataforma ou sistema de informação conjunto e interoperável com os sistemas em operação nos Estados-Membros."	1.1.1
8	- "Concordo fortemente, contudo faltam edificar as capacidades elencadas na Visão Estratégica de setembro de 2021, reforçar a cooperação entre os Estados-Membros, recrutar pessoal especializado, maior eficácia nos projetos PESCO	1.1.1
9	- "Concordo fortemente, contudo falta um empenhamento político e recursos humanos especializados."	1.1.1
10	- "Concordo fortemente, contudo deve existir numa primeira fase um investimento na formação especializada para depois colocar em prática o conhecimento adquiro em exercícios dedicados, neste âmbito, entre os membros da EU. Por fim, englobar no planeamento o domínio do Ciberespaço para criar efeitos no Ciberespaço ou, através deste, nos outros domínios	1.1.1

[6] De modo a garantir a confidencialidade das respostas dos entrevistados, a ordem dos entrevistados no presente apêndice não corresponde à ordem apresentada no apêndice C.

Quadro 4- Análise de conteúdo da primeira questão

Categorias	Subcategorias	Unidades de registo	Entrevistados										Unidades de enumeração	Resultados (%)
			1	2	3	4	5	6	7	8	9	10		
Estruturas militares da UE para a Ciberdefesa	----------	1.1.1 Criação da Visão para a estratégia de Ciberdefesa da UE	x	x	x	x	x	x	x	x	x	x	10	100

Quadro 5- Matriz das unidades de contexto e de registo da segunda questão

Entrevistado	Unidade de Contexto	Unidade de Registo
1	- "Concordo na parte da resiliência, não na parte da dissuasão, para haver dissuasão têm de existir alterações significativas à lei, respostas ofensivas credíveis e de momento isso apenas existe nos Estados-Membros." - "Há que existir uma partilha de informação com a comunidade ciber da UE, falta de capacidades para obter uma *Common Operational Picture* constante no Ciberespaço, capacidade de Ciberdefesa nos HQ e que seja projetável para o terreno, em estreita ligação com a comunidade de Cibersegurança dos Estados-Membros e a *Host Nation*."	2.1.1
2	- "Sim, mas apenas para a resiliência, mas para a dissuasão não, pois a UE de momento não tem manifestado interesse no desenvolvimento dessa capacidade, pois isso implica ter capacidade ofensiva residente."	2.1.1
3	- "Sim, falta definir e atribuir tarefas, bem como depois coordenar entre as partes envolvidas."	2.1.1
4	- "sim, é necessário traduzir para diretivas Operacionais e táticas oque está vertido na visão e conceito estratégico da Ciberdefesa da UE	2.1.1
5	- "Sim, relativamente à cooperação com parceiros esta tem que ser feita com transparência, pois existe relutância dos países em partilhar informação sobre as suas capacidades no Ciberespaço.	2.1.1
6	- "Sim, é necessário o estabelecimento de produtos coerentes ao nível do processo de planeamento de operações. Na garantia da complementaridade. Na prevenção da sobreposição e duplicação de esforços. No estabelecimento de relações de proximidade ao nível do planeamento."	2.1.1
7	- "Sim. A EU tem já em curso algumas iniciativas para o desenvolvimento de capacidades para a EU e para os Estados-Membros no âmbito dos sistemas de C2 *multi-layer*, para os vários domínios das operações militares, incluindo o Ciberespaço, que denotam uma clara intenção nesse sentido."	2.1.1
8	- "Sim. O Comitê Militar da UE aprovou em 15 de setembro de 2021, a Visão Estratégica Militar da UE em que o Ciberespaço é o 5º domínio de operações. Com esta visão a UE visa integrar o Ciberespaço em todos os aspetos das Operações/Missões Militares da CSDP da UE, desenvolvendo as capacidades necessárias consoante os níveis de autoridade, de forma permanente ou de acordo como a missão ou operação."	2.1.1

9	- "Sim, há que desenvolver as capacidades espelhadas na visão estratégica e alocar recursos sobretudo na estrutura de comando."	2.1.1
10	- "Sim, deve ser criada uma estrutura orgânica robusta para apoiar e colaborar, juntamente com as outras áreas de EM, durante o planeamento e também na condução das operações. Esta estrutura vai interligar o Ciberespaço com os outros domínios, aumentando os efeitos pretendidos.	2.1.1

Quadro 6- Análise de conteúdo da segunda questão

Categorias	Subcategorias	Unidades de registo	Entrevistados										Unidades de enumeração	Resultados (%)
			1	2	3	4	5	6	7	8	9	10		
Estruturas militares da UE para a Ciberdefesa	----------	2.1.1 Integração do Ciberespaço no planeamento e operações militares das missões da UE, estabelecendo uma resiliência e dissuasão eficazes e consistentes	x	x	x	x	x	x	x	x	x	x	10	100

Quadro 7- Matriz das unidades de contexto e de registo da terceira questão

Entrevistado	Unidade de Contexto	Unidade de Registo
1	- "Discordo que houve o apoio o desenvolvimento das capacidades de Ciberdefesa dos Estados-Membros, pois os Estados-Membros não gostam de partilhar informação." - "Discordo que houve reforço da proteção dos sistemas de comunicação e informação da CSDP utilizados pelas entidades da UE, falta da existência de um mecanismo que verifique a qualidade do serviço prestado." - "Concordo que houve promoção da cooperação civil-militar; Investigação e tecnologia; - "Concordo que houve melhoramento das oportunidades de educação, formação e exercícios, mas existe alguma duplicação com os exercícios da NATO, o que causa uma sobrecarga no pessoal." - "Discordo fortemente que houve reforço da cooperação com parceiros internacionais relevantes, não se fez praticamente nada	3.1.1
2	- "Concordo, existe uma grande tentativa em apoiar o desenvolvimento das capacidades de Ciberdefesa dos Estados-Membros, na Educação e Treino também sobretudo com o aparecimento do EU CAIH português. As restantes áreas estão dependentes da concretização dos projetos PESCO. Quanto à cooperação com parceiros internacionais resume-se praticamente à NATO."	3.1.1
3	- "Sim, todas as aéreas têm projetos PESCO em desenvolvimento com vista a cumprir com a CSDP."	3.1.1
4	- "Concordo fortemente que houve desenvolvimento das capacidades de Ciberdefesa dos Estados-Membros."	3.1.1

	- "Concordo que houve reforço da proteção dos sistemas de comunicação e informação da CSDP, mas problema é o investimento que é necessário fazer para que haja esse reforço e isso tem ficado um pouco aquém." - "Concordo fortemente que houve promoção da cooperação civil-militar; Investigação e tecnologia, sobretudo com o desenvolvimento dos projetos PESCO." - "Concordo fortemente que houve melhorias nas oportunidades de educação, formação e exercícios, sobretudo na educação e formação." - "Concordo que houve reforço da cooperação com parceiros internacionais relevantes, sobretudo com a NATO.	
5	- "Concordo que houve desenvolvimento das capacidades de Ciberdefesa dos Estados-Membros, com repercussões no reforço das capacidades dos HQ nas missões não executivas da UE." - "Concordo fortemente que houve melhorias nas oportunidades de educação, formação e exercícios, sobretudo na formação e exercícios." - "Desconheço o estado de maturação das restantes áreas."	3.1.1
6		
7	- "Concordo que houve apoio no desenvolvimento das capacidades de Ciberdefesa dos Estados-Membros;" - "Foi indiferente o reforço da proteção dos sistemas de comunicação e informação da CSDP utilizados pelas entidades da UE;" - "Concordo que houve promoção da cooperação civil-militar; Investigação e tecnologia;" - "Foi indiferente a melhoria das oportunidades de educação, formação e exercícios;" - "Foi indiferente o reforço da cooperação com parceiros internacionais relevantes;"	3.1.1
8	- "Concordo, processo de revisão da Política de Ciberdefesa está em andamento. A Bússola Estratégica destacou a importância do desenvolvimento de uma nova CDP para abordar os desafios em constante mudança do Ciberespaço. Mas tem havido falta de empenho dos Estados-Membros e falta de recursos humanos."	3.1.1
9	- "Concordo que houve evolução todas as áreas, contudo ainda existe um longo caminho a percorrer, pois tem que haver mais empenhamento por parte dos Estados-Membros."	3.1.1
10	- "Concordo que houve o apoio o desenvolvimento das capacidades de Ciberdefesa dos Estados-Membros." - "Concordo que houve reforço da proteção dos sistemas de comunicação e informação da CSDP." - "Concordo fortemente que houve promoção da cooperação civil-militar; Investigação e tecnologia." - "Concordo fortemente que houve melhoramento das oportunidades de educação, formação e exercícios." - "Indiferente relativamente ao reforço da cooperação com parceiros internacionais relevantes."	3.1.1

Quadro 8- Análise de conteúdo da terceira questão

Categorias	Subcategorias	Unidades de registo	Entrevistados										Unidades de enumeração	Resultados (%)
			1	2	3	4	5	6	7	8	9	10		
Estruturas militares da UE para a Ciberdefesa	----------	3.1.1 Áreas prioritárias da política de Ciberdefesa da UE	x	x	x	x	x		x	x	x	x	10	90

Quadro 9- Matriz das unidades de contexto e de registo da quarta questão

Entrevistado	Unidade de Contexto	Unidade de Registo
1	- "Concordo, contudo falta estruturar, integrar e sincronizar todos os projetos. Falta desenvolver o projeto de *Cyber defense deploy teams* para garantir capacidade de Ciberdefesa nas missões da UE	4.1.1
2	- "Indiferente, pois falta apresentar os resultados desses projetos. Existem os programas suficientes, falta é materializar os mesmos, pois estes têm ficado apenas pelos conceitos teóricos."	4.1.1
3	- "Concordo Fortemente, não falta desenvolver mais projetos, mas sim concretizar os projetos existentes."	4.1.1
4	- "É indiferente, pois embora haja investimento, não tem existido a concretização dos projetos, pois não tem havido resultados práticos dos mesmos. Não falta desenvolver novos projetos, há é que concretizar os projetos existentes."	4.1.1
5	- "Desconheço os programas da PESCO".	
6	- "Concordo fortemente, falta desenvolver mais projetos no âmbito da cooperação com outras instituições da EU e outros parceiros, nomeadamente com a NATO."	4.1.1
7	- "Concordo fortemente, nesta fase não identifico uma área especifica em falta."	4.1.1
8	- "Concordo fortemente, de acordo com a Bússola Estratégica os Estados-Membros da UE têm de gastar mais e melhor na defesa e melhorar o desenvolvimento e planeamento de capacidades para melhor responder às realidades operacionais e às novas ameaças e desafios. Não são necessários mais projetos, os Estados-Membros da UE têm é trabalhar nos projetos existentes que já estão em curso. Os Estados-Membros da UE têm que deixar de o estatuto de observadores, passando a ser Estados contribuintes.	4.1.1
9	- "Concordo fortemente, os Projetos PESCO são capazes de preencher lacunas, potenciando as capacidades das Operações Ciber, permitindo partilhar o fardo do desenvolvimento pelos Estados-Membros. Não existe necessidade de desenvolver novos projetos, mas sim concretizar os existentes."	4.1.1
10	- "Concordo fortemente, falta organizar e sincronizar os projetos existentes."	4.1.1

Quadro 10- Análise de conteúdo da quarta questão

Categorias	Subcategorias	Unidades de registo	Entrevistados										Unidades de enumeração	Resultados (%)
			1	2	3	4	5	6	7	8	9	10		
Estruturas militares da UE para a Ciberdefesa	----------	4.1.1 Projetos PESCO	x	x	x	x		x	x	x	x	x	10	90

Quadro 11- Matriz das unidades de contexto e de registo da quinta questão

Entrevistado	Unidade de Contexto	Unidade de Registo
1	- "Não é suficiente e não está estruturada, o projeto de *Cyber Dicipline* liderado por Portugal levantou uma *Trainnig Need Analysis* apontando as falhas existentes na Formação e treino. Pode ser melhorada através do EU CAIH liderado por Portugal, aproveitar as sinergias com a NCI *Agency - NATO Communications and Information Agency* em Oeiras, estabelecendo a ponte entre a NATO e a UE, revelendo o papel importante de Portugal em estabelecer esta ponte". - "Considero que têm sido pouco eficazes, além disso como são feitos em elevado número, depois não são retirados os devidos ensinamentos e lições apreendidas dar mais importância aos pós exercício." - "Sim, utilizando o que está previsto no EU CAIH, infelizmente Portugal não está a aproveitar esta oportunidade e existe demora na concretização do projeto"	5.1.1; 5.1.3; 5.2.1
2	- "Desconheço o tipo de formação dada pela UE, com exceção ao ministrado no EU CAIH." - "Existe treino interno, mas não existe partilha de informação com a UE." - "Sim são eficazes. Mas os exercícios têm sido idênticos aos da NATO, pois a empresa que os vendou ser a mesma que prestou esse serviço à NATO, pelo que a empresa devia criar novos cenários em exclusivo para a UE." - "Sim, e o EU CAIH vai ter um papel fundamental, existindo um grande esforço de Portugal, carece de adesão dos outros Estados-Membros."	5.1.1; 5.1.2; 5.1.3; 5.2.1
3	- "A formação não é suficiente, porque faltam sobretudo recursos humanos, e como tal há sempre margem para melhorar." - "Sim, era feito muito treino e com bastante regularidade." - "A maior incidência de exercícios na UE é de Cibersegurança, e os militares são audiência secundária de treino, deve haver maior integração dos CERT militares nos exercícios da UE." - "Sim é importante, o CAIH visa precisamente isso existindo um protocolo de cooperação com a NATO."	5.1.1; 5.1.2; 5.1.3; 5.2.1
4	- "Não existe formação em Ciberdefesa na UE, apenas existe nos Estados-Membros, pelo que há que criar essa formação."	5.1.1; 5.1.2; 5.1.3; 5.2.1

	- "Sim são feitos treinos, são feitos cerca de cinco exercícios por ano e existem treinos que são feitos diariamente." - "Não, a UE tem exercícios de planeamento de operações no Ciberespaço e de partilha de informação, deve cooperar mais nos exercícios da NATO, sem contudo, repetir os exercícios para não sobrecarregar o pessoal. - "Sim, deve existir uma escola centralizada para a formação e uma infraestrutura para o treino."	
5	- "Considero que a formação na UE não é suficiente, pelo que a formação tem sido feita com cooperação de outras entidades, devia existir uma escola de Ciberdefesa que acompanhasse a evolução das ferramentas, da doutrina e das técnicas, táticas e procedimentos." - "Sim são, com treinos trimestrais." - "Sim são eficazes, contudo podem ser melhorados nos aspetos relacionados às ferramentas de combate à intrusão nos sistemas." - "Sim considero, deve existir uma escola conjunta e as Nações devem potenciar a sua capacidade Nacional em conjunto com esta estrutura transnacional, e a criação de uma comunidade de CERT que permita criar e uniformizar a doutrina."	5.1.1; 5.1.2; 5.1.3; 5.2.1
6	- "Não é suficiente, deve ser priorizada a aposta na CAIH, no sentido de estimular a Educação, Formação, Pesquisa, a Inovação e o Desenvolvimento." - "Sim são, podem ser melhorados com a criação de modelos de desenvolvimento sustentáveis. Disponibilidade de instalações seguras para a formação, treino, pesquisa e operações; Estabelecimento de projetos de formação e treino imersivos, relevantes e flexíveis; Estabelecimento de Pesquisa, Desenvolvimento, Testagem e Avaliação de novas soluções e tecnologias; Promoção da cooperação Civil-Militar." -"Sim é importante, a criação do CAIH por forma a tornar-se num centro de excelência para Cyber formação e treino em Segurança e Defesa Cibernética, capaz de fomentar a cooperação e a inovação entre os seus membros."	5.1.1; 5.1.3; 5.2.1
7	- "Esta matéria é sempre muito sensível e desenvolvida num círculo muito reservado em cada Estado-Membro. Apenas algumas nações promovem formação e treino para o exterior, mas a oferta de qualidade reconhecida ainda é reduzida entre os países da EU." - "São conduzidas diversas atividades de treino no âmbito da Ciberdefesa, mas apenas entre os elementos intrinsecamente dedicados a essas funções." - "Nesta matéria não tenho experiência concreta, no entanto tem havido progresso no que refere ao número de iniciativas/exercícios promovidos. É notória uma clara reserva na partilha de informação e de perícias já que se trata de uma área em clara ascensão de desenvolvimento cuidadoso." - Concordo claramente. É necessário partilhar conhecimento e perícias, realizar treino e exercícios conjuntos para desenvolver uma base de atuação comum capaz de reagir ou antecipar crises, de forma coordenada e colaborativa. Devem existir escolas de Ciberdefesa, academias, *CyberRanges* e realização de exercícios regulares	5.1.1; 5.1.2; 5.1.3; 5.2.1

8	-"Não é suficiente, há espaço para melhorar. Todos os Estados-Membros, instituições, organismos e agências da UE enfrentam um desafio de recursos humanos neste domínio que é necessário formar e treinar desde os utilizadores aos decisores." - "Não. O EUMS atua como um órgão consultivo para o EUMC e o EEAS, não sendo realizadas tarefas críticas de Ciberdefesa no mesmo." - "Sim. Os exercícios de Ciberdefesa devem ser planeados regularmente (como o Cyber Phalanx). - "Sim concordo, mas não devem ser criadas novas infraestruturas para não duplicar esforços, deve existir cooperação com o centro de excelência de Ciberdefesa da NATO com a NCI *Agency* – NATO (Oeiras) e o projeto CAIH."	5.1.1; 5.1.3; 5.2.1
9	- "Não é suficiente e não está bem organizada. A formação em Ciberdefesa não se deve limitar a Unidades de Ciberdefesa. É necessária uma mudança de mentalidade em toda a comunidade operacional, pois no mundo digital o Ciberespaço afeta todos os domínios." - "Sim são eficazes. Sempre que existirem exercícios mesmo nos outros domínios, a Ciberespaço deve fazer parte do cenário." - "Sim devem existir infraestruturas dedicadas, sobretudo *Cyber Ranges*.	5.1.1; 5.1.3; 5.2.1
10	- "Considero que sim, contudo o efetivo que desempenha funções nesta área é bastante reduzido para conseguir englobar as diversas áreas da Ciberdefesa." - "São realizadas principalmente ações de sensibilização dos utilizadores da rede IP e, internamente dentro do meu *Branch*, ações para incrementar as configurações de segurança e de monitorização do tráfego." - "Nunca participei em exercícios de Ciberdefesa da EU." - "Claro que sim. Considero que iniciativas como a criação *EU Cyber Academia and Innovation Hub* são excelentes para aumentar o conhecimento/formação."	5.1.1; 5.1.2; 5.2.1

Quadro 12- Análise de conteúdo da quinta questão

Categorias	Subcategorias	Unidades de registo	Entrevistados										Unidades de enumeração	Resultados (%)
			1	2	3	4	5	6	7	8	9	10		
Recursos Humanos da UE para a Ciberdefesa	----------	5.1.1 Existência de formação em Ciberdefesa adequada	x		x	x	x	x	x	x	x	x	10	90
		5.1.2 Existência regular de treinos do Pessoal de Ciberdefesa		x	x	x	x		x			x	10	60
		5.1.3 Existência de exercícios de Ciberdefesa ajustados aos desafios do Ciberespaço	x	x	x		x	x	x	x	x		10	80
Infraestruturas de Formação e Treino de Ciberdefesa da UE	----------	5.2.1 Existência de infraestruturas dedicadas à Formação e Treino na UE	x	x	x	x	x	x	x	x	x	x	10	100

Quadro 13- Matriz das unidades de contexto e de registo da sexta questão

Entrevistado	Unidade de Contexto	Unidade de Registo
1	- "faz falta uma estrutura física de coordenação para a informação no Ciberespaço, fazendo a ligação dos milCERT/CCDN, com a comunidade de Cibersegurança, via Joint Cyber Unit (JCU), bem como na parte operacional, ligar os OHQ às suas células Cyber e à comunidade de Intel para tratar as Informações deste domínio e eventualmente à comunidade de Ciberdefesa dos Estados-Membros."	6.1.1
2	- "Concordo fortemente, é essencial para coordenar as operações no Ciberespaço da UE."	6.1.1
3	- "Concordo fortemente, o CIDCC permite garantir uma resposta coordenada ao nível da UE."	6.1.1
4	- "Concordo fortemente, a sua implementação vai ser muito importante para a UE atuar de forma coordenada no Ciberespaço."	6.1.1
5	- "Concordo fortemente, haver um centro de coordenação é essencial para a proteção dos nossos sistemas de informação no Ciberespaço."	6.1.1
6	- "Concordo fortemente "	6.1.1
7	- "Concordo, deve existir um "centro" para esse efeito na perspetiva da coordenação, mas entendo que deva ser conjunto com os restantes domínios."	6.1.1
8	- "Concordo fortemente, o CIDCC vai ser fundamental para colocar a comunidade Ciber dos Estados-Membros em contacto e a partilhar informação."	6.1.1

9	- "Concordo fortemente, o CIDCC será essencial para coordenar a informação no Ciberespaço, ligando as CERT militares dos Estados-Membros."	6.1.1
10	- "Concordo fortemente, o domínio do Ciberespaço deve estar interligado com os outros ambientes/operações e especificamente com as operações de informação, no sentido de criar efeitos neste ambiente/operações."	6.1.1

Quadro 14- Análise de conteúdo da sexta questão

Categorias	Subcategorias	Unidades de registo	Entrevistados										Unidades de enumeração	Resultados (%)
			1	2	3	4	5	6	7	8	9	10		
Processo de resposta a incidentes de Ciberdefesa nas Estruturas Militares da UE	Resposta e Reporte	6.1.1 Existência de centro de coordenação de Ciberdefesa p/ reporte de incidentes	x	x	x	x	x	x	x	x	x	x	10	100

Quadro 15- Matriz das unidades de contexto e de registo da sétima questão

Entrevistado	Unidade de Contexto	Unidade de Registo
1	- "Concordo, para aquando da criação da *Joint Cyber Unit* a UE estar preparada para uma resposta a um eventual Ciberataque em larga escala, ligando os CERT militares entre eles."	7.1.1
2	- "Concordo com o uso de uma rede específica, mas deve-se utilizar uma rede própria já existente e não criar uma nova, contudo existe resistência na partilha de Informação entre os Estados.	7.1.1
3	- "Concordo fortemente, para que possa existir uma resposta interligada da UE e os seus Estados-Membros."	7.1.1
4	- "Discordo, deve é ser utilizada uma rede classificada já existente que ligue os diferentes Centros e se criem plataformas para a partilha de informação."	
5	- "Concordo, pois, uma rede especifica requer que todos os Estados-Membros tenham todos os primariamente mesmos padrões de doutrina e só depois é possível criar e usar eficazmente uma rede de CERTs."	7.1.1
6	- "Concordo fortemente, a criação desta rede permite estabelecer sinergias, conhecer e interagir com os parceiros dentro e fora de uma Operação, valores que, a par da confiança, são necessários para a implementação eficaz de uma defesa comum no domínio do Ciberespaço."	7.1.1
7	- "Concordo fortemente. Essa é a forma de reagir rapidamente e de evitar consequências de maior escala. À semelhança do que já se verifica no âmbito civil e empresarial, uma rede CERT militar é critica para a defesa comum do Ciberespaço Europeu	7.1.1

8	- "Concordo fortemente, a bússola estratégica da UE refere isso. O melhoramento da cooperação entre as CERT militares da UE beneficiará as Operações/Missões Militares da CSDP da UE. A cooperação na Comunidade Ciber militar da UE é identificada como um meio necessário para implementar e usar o Ciberespaço como domínio de operações.	7.1.1
9	- "Concordo fortemente, a rede permite ligar os CERT militares entre eles, o MPCC deve estar incluído nessa rede para uma resposta credível da UE a um eventual Ciberataque em larga escala."	7.1.1
10	- "Concordo fortemente a partilha de informação na rede fortalece a defesa comum e diminui as vulnerabilidades pontuais que podem pôr em causa toda EU"	7.1.1

Quadro 16- Análise de conteúdo da sétima questão

Categorias	Subcategorias	Unidades de registo	Entrevistados										Unidades de enumeração	Resultados (%)
			1	2	3	4	5	6	7	8	9	10		
Processo de resposta a incidentes de Ciberdefesa nas Estruturas Militares da UE	Resposta e Reporte	7.1.1 Existência de uma rede específica de reporte para os milCERTs dos Estados-Membros ou dos QQ da UE	x	x	x		x	x	x	x	x	x	10	90

Quadro 17- Matriz das unidades de contexto e de registo da oitava questão

Entrevistado	Unidade de Contexto	Unidade de Registo
1	- "Não temos uma resposta eficaz a nível da UE, apenas existe resposta eficaz nos Estados-Membros, falta sobretudo uma capacidade de resposta credível, o CIDCC quando implementado vai poder coordenar uma resposta credível com recurso aos seus Estados-Membros."	8.1.1
2	- "Sim é eficaz, mas ao nível dos Estados-Membros, não da UE."	8.1.1
3	- "O processo é eficaz pois garante uma resposta para a organização continuar a operar."	8.1.1
4	- "Sim garante."	8.1.1
5	- "Sim é bastante eficaz nas três primeiras fases, desconheço a eficácia da atividade após incidente, pois estamos a aguardar relatórios relativos aos incidentes sofridos."	
6		
7	- "Ainda não temos edificada uma capacidade realmente eficaz de resposta a incidentes. O vetor do pessoal me parece ser o mais difícil de edificar, quer pela dificuldade em formar pessoal, quer para assegurar condições de retenção e progresso de carreira, devido à excecional oferta do mercado externo (civil) em comparação com os incentivos que as carreiras de âmbito militar podem oferecer."	8.1.1

8	- "De momento não é eficaz, o processo necessita de ser desenvolvido, caso exista um incidente no Ciberespaço da UE, visto o CIDCC ainda não estar implementado para dar uma resposta coordenada e eficaz, o incidente terá que ser resolvido com recurso das capacidades dos Membros-Estados."	8.1.1
9	- "Sim o processo é eficaz."	8.1.1
10	- "Nunca vivenciei esse processo de resposta a incidentes."	

Quadro 18- Análise de conteúdo da oitava questão

Categorias	Subcategorias	Unidades de registo	Entrevistados										Unidades de enumeração	Resultados (%)
			1	2	3	4	5	6	7	8	9	10		
Processo de resposta a incidentes de Ciberdefesa nas Estruturas Militares da UE	Preparação	8.1.1 - Existência de uma *Incident Handling Team*	x	x	x	x	x		x	x	x		10	80

Quadro 19- Matriz das unidades de contexto e de registo da nona questão

Entrevistado	Unidade de Contexto	Unidade de Registo
1		
2	- "Confirmo a existência de tudo."	9.1.1; 9.1.2; 9.1.3; 9.1.4; 9.1.5
3	- "Sim confirmo a existência de tudo."	9.1.1; 9.1.2; 9.1.3; 9.1.4; 9.1.5
4	- "Sim confirmo a existência de tudo, contudo não existe ligação com a UE".	9.1.1; 9.1.2; 9.1.3; 9.1.4; 9.1.5
5	- "Apenas confirmo a existência de um Plano de Ciberdefesa e de treinos regulares de Ciberdefesa."	9.1.4; 9.1.5
6		
7	- "Confirmo a existência de tudo, mas Célula de Ciberdefesa é mínima. E o Plano de Ciberdefesa e os Treinos regulares são rudimentares"	9.1.1; 9.1.2; 9.1.3; 9.1.4; 9.1.5
8		
9		
10	- "Na unidade estão definidas apenas as estruturas: Célula de Ciberdefesa e *Security Operation Center*.	9.1.1; 9.1.2;

Quadro 20- Análise de conteúdo da nona questão

Categorias	Subcategorias	Unidades de registo	Entrevistados										Unidades de enumeração	Resultados (%)
			1	2	3	4	5	6	7	8	9	10		
Processo de resposta a incidentes de Ciberdefesa nas Estruturas Militares da UE	Preparação	9.1.1 Existência de uma Célula de Ciberdefesa		x	x	x			x			x	10	50
		9.1.2 Existência de uma *Security Operation Center*		x	x	x			x			x	10	50
		9.1.3 Partilha de informação com outras nações ou outras entidades		x	x	x			x				10	40
		9.1.4 Existência de um Plano de Ciberdefesa		x	x	x	x		x				10	50
		9.1.5 Treinos regulares de Ciberdefesa nos HQs		x	x	x	x		x				10	50

Quadro 21- Matriz das unidades de contexto e de registo da décima questão

Entrevistado	Unidade de Contexto	Unidade de Registo
1		
2	- “Sim temos essa capacidade.”	10.1.1; 10.1.2
3	- “sim existe a capacidade, pois temos bons equipamentos.”	10.1.1; 10.1.2
4	- “Existe essa capacidade”	10.1.1; 10.1.2
5	- “sim, foram recentemente adquiridas essas a capacidades, sobretudo ao nível do correio eletrónico.”	10.1.1; 10.1.2
6		
7	- “Estas duas áreas, embora planeadas, ainda não se podem considerar realmente operacionais. Falta formação e treino dos poucos operacionais existentes e espera-se recrutar o pessoal necessário, o quanto antes.”	10.1.1; 10.1.2
8		
9		
10	- “Encontra-se implementada na arquitetura CSI uma firewall com a capacidade de monitorização do tráfego, bem como gerar logs que contem informação para a análise dos incidentes.”	10.1.1; 10.1.2

Quadro 22- Análise de conteúdo da décima questão

Categorias	Subcategorias	Unidades de registo	Entrevistados										Unidades de enumeração	Resultados (%)
			1	2	3	4	5	6	7	8	9	10		
Processo de resposta a incidentes de Ciberdefesa nas Estruturas Militares da UE	Deteção e Análise	10.1.1. Capacidade de deteção de precursores e indicadores e do incidente		x	x	x	x		x			x	10	60
		10.1.2. Capacidade de Análise do incidente		x	x	x	x		x			x	10	60

Quadro 23- Matriz das unidades de contexto e de registo da décima primeira questão

Entrevistado	Unidade de Contexto	Unidade de Registo
1		
2	- "Confirmo a existência de todas as capacidades, com limitações na capacidade forense por falta de pessoal e formação, nunca foi estabelecido nenhum contacto com a UE."	11.1.1; 11.1.2; 11.1.3; 11.1.4; 11.1.5
3	-"Confirmo a existência de todas as capacidades. Nunca foram estabelecidos contactos com a UE".	11.1.1; 11.1.2; 11.1.3; 11.1.4; 11.1.5
4	- "Confirmo a existência de todas as capacidades, contudo não existe uma rede especifica de ligação com a UE e contactos externos que existem são com a NATO e os países membros da NATO."	11.1.1; 11.1.2; 11.1.3; 11.1.4; 11.1.5
5	- "Confirmo a existência da capacidade de aplicar medidas contenção, a capacidade reduzida de erradicação, a capacidade de estabelecer POC para o reporte de incidentes internos e externos através de uma célula de *Network surveillance* e a capacidade de recuperação. São estabelecidos contactos com a célula de Ciberdefesa do MPCC."	11.1; 11.1.3; 11.1.4; 11.1.5
6		
7	- "Confirmo a existência de todas as capacidades à exceção da capacidade forense. As Capacidades de erradicação e de recuperação são rudimentares. Desconheço se há POC's estabelecidos com a EU no âmbito militar (EUMS)."	11.1.1; 11.1.3; 11.1.4; 11.1.5
8		
9		
10	- "Existem processos e procedimentos para reagir e recuperar de incidentes de Ciberdefesa, sendo sempre uma ação conjunta com o escalão superior."	11.1.1; 11.1.2; 11.1.3; 11.1.4; 11.1.5

Quadro 24- Análise de conteúdo da décima primeira questão

Categorias	Subcategorias	Unidades de registo	Entrevistados										Unidades de enumeração	Resultados (%)
			1	2	3	4	5	6	7	8	9	10		
Processo de resposta a incidentes de Ciberdefesa nas Estruturas Militares da UE	Resposta e Reporte	11.1.1. Capacidade de aplicar medidas contenção		x	x	x	x		x			x	10	60
		11.1.2. Capacidade forense		x	x	x						x	10	40
		11.1.3. Capacidade de erradicação		x	x	x	x		x			x	10	60
		11.1.4. Estabelecimento de POC para o reporte de incidentes internos e externos		x	x	x	x		x			x	10	60
		11.1.5. Capacidade de recuperação		x	x	x	x		x			x	10	60

Quadro 25- Matriz das unidades de contexto e de registo da décima segunda questão

Entrevistado	Unidade de Contexto	Unidade de Registo
1		
2	- "Sim confirmo a existência, estas ações nunca foram desenvolvidas no âmbito da UE."	11.1.1; 11.1.2; 11.1.3
3	- "Sim estão previstas todas as ações e ainda eram efetuados brífingues. As ações não eram desenvolvidas no âmbito da UE. Em Portugal quem responde à UE é o Centro Nacional de Cibersegurança."	11.1.1; 11.1.2; 11.1.3
4	- "Fazemos todas as ações, contudo nunca foi feito no âmbito da UE apenas no âmbito da NATO.	11.1.1; 11.1.2; 11.1.3
5	- "A atividade após o incidente ainda não se encontra implementada em pleno, mas estas três áreas estão a ser trabalhadas para que sejam materializadas em breve, sobretudo na parte das lições apreendidas."	
6		
7	- "Sim confirmo a existência destas ações. Desconheço se são desenvolvidas no âmbito da UE."	11.1.1; 11.1.2; 11.1.3
8		
9		
10	- "sim. Durante as minhas funções felizmente não existiram incidentes de Ciberdefesa."	11.1.1; 11.1.2; 11.1.3

Quadro 26- Análise de conteúdo da décima segunda questão

Categorias	Subcategorias	Unidades de registo	Entrevistados										Unidades de enumeração	Resultados (%)
			1	2	3	4	5	6	7	8	9	10		
Processo de resposta a incidentes de Ciberdefesa nas Estruturas Militares da UE	Atividade após o incidente	11.1.1. Registo de lições apreendidas para melhorar o treino		x	x	x			x			x	10	50
		11.1.2. Realização de reuniões		x	x				x			x	10	50
		11.1.3. Existência de *sharepoint* de informação e relatórios		x	x	x			x			x	10	50