A IMPORTÂNCIA DAS INFORMAÇÕES PARA A SEGURANÇA NO CIBERESPAÇO

António Augusto Ramos Carvalho

Dissertação para a obtenção do Grau de Mestre em Segurança da Informação e Direito no Ciberespaço

Mestrado em Segurança da Informação e Direito no Ciberespaço

Orientadores: Professor Doutor Carlos Manuel Costa Lourenço Caleiro

Capitão-de-mar-e-guerra Hélder Fialho de Jesus

Júri

Presidente: Professor Doutor Paulo Alexandre Carreira Mateus

Vogal: Capitão-de-mar-e-guerra Hélder Fialho de Jesus

Vogal: Capitão-de-fragata Fernando Cavaleiro Ângelo

Janeiro 2021

Agradecimentos

Esta dissertação foi o resultado de uma longa jornada, para a qual contribuíram muitas pessoas que pelo apoio, orientação, incentivo, amizade e compreensão tornaram possível levá-la a bom porto.

Assim, começo por agradecer ao meu orientador e coordenador do mestrado do Instituto Superior Técnico, Professor Doutor Carlos Caleiro, por se ter disponibilizado para orientar esta investigação, pelo acompanhamento e disponibilidade permanente e sobretudo pelo incondicional apoio e confiança em que esta investigação chegaria, de facto, a bom porto mesmo após a grande alteração de rumo que, a dada altura, sofreu.

De igual modo, agradeço vivamente ao Capitão-de-mar-e-guerra Hélder Fialho de Jesus, coorientador desta dissertação, pelo incondicional apoio, motivação, recomendações, estímulos e disponibilidade demonstrada ao longo de todas as fases da investigação, bem como pelo empenho e interesse que desde a primeira hora demonstrou nesta orientação. Com efeito, o Senhor Comandante foi o líder e o mentor que, através de todos os aspetos supracitados, garantiu que a investigação não se desviasse da rota traçada e se alcançassem os objetivos traçados.

Agradeço, igualmente, a todos os entrevistados que me concederam um pouco do seu "precioso" tempo, que pela riqueza do saber e das opiniões expressas permitiram aprofundar os temas investigados, enriquecer o trabalho desenvolvido e obter novas perspetivas. Deste modo, manifesto o meu mais elevado apreço e profundo reconhecimento ao Serviço de Informações de Segurança, ao Engenheiro Lino Santos, ao Inspetor Chefe Rogério Bravo, ao Capitão-de-fragata Câmara Assunção, ao Major Pinheiro Rodrigues e ao Major Marques da Silva.

Ao Primeiro-tenente Arrifes Narciso com quem tenho, nos últimos anos, cruzado profissionalmente e contado com o seu apoio. Mais uma vez, não hesitou em se disponibilizar para conceder as suas importantes sugestões e recomendações, além dos pertinentes e relevantes contributos de índole metodológica que em muito melhoram a investigação.

Ao Primeiro-tenente Torpes Limão que fruto da sua longa experiência no Centro de Ciberdefesa, alicerçada na camaradagem existente se disponibilizou, desde a primeira hora para apoiar a investigação. Agradeço as várias recomendações referentes à abordagem ao *Malware Information Sharing Platform* que sedimentados no saber contribuíram, significativamente, para um maior enriquecimento do trabalho.

À Capitão-tenente Marta Gabriel pelo apoio e disponibilidade em contribuir para o enriquecimento deste trabalho concedendo críticas muito construtivas e diferentes perspetivas de análise.

Finalmente, conforme notabilizou o célebre provérbio popular "os últimos são sempre os primeiros", gostaria de agradecer profundamente à minha mulher, Tânia Soares, por toda a compreensão e apoio dado, pois por mais organização e vontade que tivesse, todas as horas dedicadas ao leme deste trabalho só foram possíveis porque aguentas-te o "barco". Termino dedicando este trabalho aos meus filhos Rodrigo e Gonçalo, na certeza que o mesmo implicou uma diminuição do tempo que partilhei momentos convosco, mas ficará como mais um exemplo que o Pai vos demonstra que para tudo na vida é necessário trabalho e dedicação.

Por isso, a todos um grande bem-haja!

Resumo

Atualmente, o ciberespaço assume uma inegável relevância no modo de vida e no bem-estar dos cidadãos, proporcionando grandes oportunidades de progresso, mas acarretando, também, muitos desafios à segurança. Desde logo, assiste-se a um aumento das ameaças neste domínio, por parte de atores estatais e não estatais, que desenvolvem ações, cada vez mais, sofisticadas e disruptivas. Acresce que, nesta era, paradoxalmente, mais informação não significa, necessariamente, mais conhecimento. Ao invés, prolifera no ciberespaço a desinformação, a manipulação, as *fake news*, a propaganda e o anonimato.

Assim, neste ambiente de profunda volatilidade, incerteza, complexidade e ambiguidade as informações, enquanto fonte de conhecimento das ameaças existentes no ciberespaço e da orquestração e condução de ataques, podem contribuir, significativamente, para a antecipação, prevenção e mitigação de ciberataques.

A presente investigação tem como objeto de estudo as "Informações no Ciberespaço", procurando evidenciar o contributo que estas podem desempenhar para a segurança no ciberespaço. Para alcançar este objetivo, caracterizar-se-á o ciberespaço, procurando identificar as principais características deste ambiente e delimitar o espetro de ameaças existentes. Em seguida, abordar-se-ão os principais domínios e entidades que, a nível nacional, contribuem para a segurança no ciberespaço, verificando-se como se articulam operacionalmente. Posteriormente, analisar-se-ão as informações, relevando-se a importância destas, do Conhecimento Situacional no Ciberespaço (CSC) e da partilha de informação para a segurança do ciberespaço.

Por fim, conclui-se que, as informações constituem-se como um ativo essencial para a segurança no ciberespaço, dado que, contribuem para a identificação das pegadas digitais dos agentes maliciosos e das infraestruturas de ataque, concorrem para a construção de um robusto CSC e permitem reduzir a incerteza e apoiar o processo de tomada de decisão.

Palavras-chave: Ciberespaço, Informações, Segurança no Ciberespaço, Conhecimento Situacional e Partilha de Informação.

Abstract

Currently, cyberspace has an undeniable relevance in the way of life and well-being of citizens, providing great opportunities for progress, but also posing many security challenges. First and foremost, there is an increase in threats in this area, by state and non-state actors, which develop increasingly sophisticated and disruptive actions. In addition, in this era, paradoxically, more information does not necessarily mean more knowledge. Instead, disinformation, manipulation, fake news, propaganda, and anonymity proliferate in cyberspace.

Thus, in this environment of deep volatility, uncertainty, complexity and ambiguity, intelligence, as a source of knowledge about the threats that exist in cyberspace and the orchestration and conduction of attacks, can contribute significantly to the anticipation, prevention, and mitigation of cyber-attacks.

The current investigation has as its object of study the “Intelligence in Cyberspace”, seeking to highlight the contribution that intelligence can provide to obtain security in cyberspace. In order to achieve this objective, cyberspace will be characterized, seeking to identify the main characteristics of this environment and the delimitation of the spectrum of existing threats. Then, the main areas and entities that, at national level, contribute to security in cyberspace will be addressed, verifying how they are operationally articulated. Subsequently, the intelligence will be analysed, emphasizing its importance, Situational Awareness in Cyberspace (SAC) and the sharing of information for cyberspace security.

Finally, it concludes that, intelligence is an essential asset for security in cyberspace, since it contributes to the identification of the digital footprints of malicious agents and attack infrastructures, and to the construction of a robust SAC, and it allows to reduce uncertainty and support decision making.

Key words: **Cyberspace**, **Intelligence, Cyberspace Security, Situational Awareness and Sharing Information.**

Índice

Lista de Figuras

Lista de Tabelas

Lista de Siglas e Acrónimos

ACINT	*Acoustic Intelligence*
ACT	*Allied Command for Transformation*
AJP	*Allied Joint Publication*
ANX	Anexo
APD	Apêndice
APDSI	Associação para a Promoção e Desenvolvimento da Sociedade da Informação
API	*Application Programming Interface*
APT	*Advanced Persistent Threats*
AR	Assembleia da República
ARPA	*Advanced Research Projects Agency*
ART.º	Artigo
CAIH	*Cyber Academia and Innovation Hub*
C2	Comando e Controlo
CCD	Centro de Ciberdefesa
CD TEXP	*Cyber Defence Training and Exercise Coordination Platform*
CEDN	Conceito Estratégico de Defesa Nacional
CEMGFA	Chefe do Estado-Maior-General das Forças Armadas
CERT	*Computer Emergency Response Team*
CESEDEN	*Centro Superior de Estudios de la Defensa Nacional*
CIRC	*Computer Incident Response Centre*
CISMIL	Centro de Informações de Segurança Militares
CNCS	Centro Nacional de Cibersegurança
CNA	*Computer Network Attack*
CND	*Computer Network Defense*
CNE	*Computer Network Exploitation*
CNO	*Computer Network Operations*
CP	Código Penal
CPI	Ciclo de Produção de Informações
CPLP	Comunidade dos Países de Língua Portuguesa
CSC	Conhecimento Situacional no Ciberespaço
CSI	Comunicações e Sistemas de Informação
CSIRT	C*omputer Security Incident Response Team*
CTG	*Counter Terrorism Group*
CyDefSIG	*Cyber Defence Signatures*

DIRCSI	Direção de Comunicações e Sistemas de Informação
DDoS	*Distributed Denial of Service*
DR	Decreto Regulamentar
EC3	*European Cybercrime Center*
EMGFA	Estado-Maior-General das Forças Armadas
ENSC	Estratégia Nacional de Segurança do Ciberespaço
EUA	Estados Unidos da América
EU CTC	*EU Counter Terrorism Coordinator*
EUMTG	*EU Military Training Group*
EUROPOL	*European Union Agency for Law Enforcement Cooperation*
FIRST	*Forum of Incident Response and Security Teams*
GB	*Gigabyte*
GEN	Grande Estratégia Nacional
GEOINT	*Geospatial Intelligence*
GNS	Gabinete Nacional de Segurança
IC	Infraestrutura Crítica
IDS	*Intrusion Detection System*
INTCEN	*Intelligence and Situation Centre*
IDN	Instituto de Defesa Nacional
IMINT	*Imagery Intelligence*
INESC	Instituto de Engenharia de Sistemas e Computadores
INTERPOL	*International Criminal Police Organisation*
IOC	*Initial Operational Capability*
IoC	*Indicators of Compromise* – Indicadores de Compromisso
IP	*Internet Protocol*
IPS	*Intrusion Prevention Systems*
IPTO	*Information Processing Techniques Office*
IRF	*Israel Defense Force*
IST	*Instituto Superior Técnico*
HUMINT	*Human Intelligence*
LC	Lei do Cibercrime
MAI	Ministério da Administração Interna
MASINT	*Measurement and Signatures Intelligence*
MDN	Ministério de Defesa Nacional
MISP	*Malware Informational Sharing Plataform*

MIT	*Massachusetts Institute of Technology*
MN CD2	*Multinational Cyber Defence Capability Development*
MN CD E&T	*Multinational Cyber Defence Education & Training*
MNE	Ministério dos Negócios Estrangeiros
Nº	Número
NATO	*North Atlantic Treaty Organization*
NCSC	*National Cyber Security Centre*
NCI	NATO *Communications, Information*
NCIA	*NATO Communications and Information Agency*
NCIRC	*NATO Computer Incident Response Capability*
NIDS	*Network Intrusion Detection System*
NIS	*Network and Information Security*
NSA	*National Security Agency*
OE	Objetivo Específico
OODA	Observar, Orientar, Decidir e Agir
OG	Objetivo Geral
OPC	Orientação Política para a Ciberdefesa
OSINT	*Open-Source Intelligence*
PEC	Parlamento Europeu e do Conselho
PJ	Polícia Judiciária
PM	Primeiro-Ministro
QNRCS	Quadro Nacional de Referência para a Cibersegurança
QC	Questão Central
QD	Questão Derivada
RASI	Relatório Anual de Segurança Interna
RCM	Resolução do Conselho de Ministros
SAC	*Situational Awareness in Cyberspace*
SCADA	*Supervisory Control and Data Acquisition*
SCI	Sistemas de Controlo Industrial
SG	Secretário-Geral
SD	*Smart Defence*
SHAPE	*Supreme Headquarters Allied Powers Europe*
SI	Segurança da Informação
SIED	Serviço de Informações Estratégicas de Defesa
SIEM	*Security Information and Event Management*

SIG	Sistemas de Informações Geográficos
SIGINT	*Signals Intelligence*
SIRP	Sistema de Informações da República Portuguesa
SIS	Serviço de Informações de Segurança
TIC	Tecnologias de Informação e Comunicação
TLP	*Traffic Light Protocol*
TTP	Técnicas, Táticas e Procedimentos
UE	União Europeia
UNICI	Unidade Nacional da Investigação da Criminalidade Informática
UNC3T	Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica
URSS	União das Repúblicas Socialistas Soviéticas
Vd.	Vide
VUCA	*Volatile, Uncertain, Complex and Ambiguous*

1. Introdução

> *"A próxima guerra será precedida de um ciberataque e não por barragens de artilharia nem bombardeamentos aéreos", Engenheiro António Guterres, Secretário-Geral das Nações Unidas (Guterres, 2018).*

1.1. Enquadramento do tema

Ao longo da última metade do século XX, assistiu-se a uma rápida evolução tecnológica, permitindo que as sociedades gerassem elevados índices de crescimento económico e social, desencadeando o desenvolvimento e adoção de novas Tecnologias de Informação e Comunicação (TIC), as quais moldaram a forma como as pessoas vivem e comunicam entre si, sendo atualmente, vitais ao funcionamento das sociedades modernas.

Neste âmbito, a invenção da Internet[1] como uma rede mundial de computadores, desempenhou um papel fundamental na transformação da sociedade, tendo como consequência última, o estímulo e desenvolvimento de um novo espaço que não tem existência física, mas apenas virtual, o qual se denomina de ciberespaço[2] (Schmitt & et al., 2013).

O termo ciberespaço foi utilizado pela primeira vez pelo escritor de ficção científica *Willian Gibson* em 1982[3], para descrever um espaço virtual sustentado na interligação de computadores e pessoas à escala global. Com efeito, mesmo considerando a distância temporal que separa a atualidade, da capacidade visionária de *Gibson* em 1982, constata-se que o ciberespaço intensificou transformações sociais nas diversas esferas de atividade humana. Tal assim se sucedeu porque o ciberespaço permitiu uma troca de informação muito mais célere, global e económica, criando novas acessibilidades e oportunidades para os Estados, organizações e cidadãos, que se tornaram vitais na nossa sociedade (Moniz, 2018).

Na realidade esta grande alteração de comportamentos, em que a conectividade ao ciberespaço é hoje uma necessidade básica para sociedade, é fielmente explanada no crescente número e variedade de equipamentos utilizados no quotidiano, assim como no tempo em que estes se encontram conectados à internet. Neste cenário, sublinham-se os dados apresentados no último relatório *Digital 2020,* da agência criativa global *We Are Social* para a *HootSuite* (We Are Social, 2020) o qual estima

[1] A Origem da internet remonta ao período da presidência de Eisenhower nos Estados Unidos da América (EUA), durante a Guerra Fria. No decurso do lançamento pelos soviéticos do satélite espacial Sputnik, o presidente Eisenhower criou a agência *Advanced Research Projects Agency* (ARPA), em 1957, com o objetivo de juntar um conjunto de cientistas de renome e competência comprovada, para incrementar a tecnologia espacial. A amplitude de matérias coberta pela ARPA levou à criação de vários departamentos especializados. Na área da informática surgiu o *Information Processing Techniques Office* (IPTO). Nestas circunstâncias, um conjunto coincidente de descobertas, desencadeou as fundações da futura internet (Belfiore, 2010).

[2] Importa salientar que, embora a internet tenha sido um dos grandes impulsionadores do ciberespaço, estes dois termos não devem ser confundidos. Deste modo, sucintamente pode referir-se que o ciberespaço é o ambiente e a Internet é uma das suas infraestruturas.

[3] A palavra Ciberespaço foi utilizada pela primeira vez pelo escritor de ficção científica *William Gibson* em 1982, num conto denominado "*Burning Chrome*", publicado na revista *Omni*, para descrever um espaço virtual sustentado na interligação em rede de máquinas e pessoas à escala global, como um "*mass consensual hallucination of computer networks*". O termo viria a ser popularizado mais tarde após a publicação do seu famoso livro "*Neuromancer*" publicado em 1984 (The Guardian, 2014).

que o número de utilizadores ativos na internet em todo o mundo ascenda aos 4.54 mil milhões, cerca de 59 % da população mundial (Figura 1), o que corresponde a um aumento de 7 % face a 2019, sendo previsível que esta tendência de aumento continue nos próximos anos.

Figura 1 - Indicadores estatísticos da utilização da internet à escala mundial no final de 2019 (We Are Social, 2020)

Acresce que, é também no ciberespaço que assentam os sistemas vitais de uma sociedade, os quais se encontram ligados em rede e possibilitam o comando, controlo e monitorização das Infraestruturas Críticas (IC)[4], tais como a rede de água e energia elétrica, as telecomunicações, os transportes, os sistemas financeiros, os serviços de emergência, entre outros (IDN-CESEDEN, 2013).

Neste contexto, perante a criticidade do ciberespaço no mundo global de hoje, não é de admirar que este domínio virtual criado pelo homem, seja tido como um novo *Global Common*[5], isto é, um espaço vital ao funcionamento da sociedade, que sendo partilhado por toda a humanidade não pertence a nenhum Estado em concreto, à semelhança dos mares, do espaço aéreo e do espaço exterior (Barrett, Bedford, Skinner, & Vergles, 2011).

Porém, o ciberespaço, enquanto espaço global comum, caracteriza-se pela ausência de fronteiras físicas, não sendo, conforme sublinha Viana (2018, p. 11) "limitado pela esfera pública ou privada, civil ou militar, interna ou externa". De facto, a aspiração e o desejo humano de progresso encontraram no ciberespaço um meio de excelência para atingir esse fim, sem que, no entanto, tivessem sido implementadas as devidas medidas de segurança e regulamentação jurídica adequadas para lidar com este novo paradigma.

[4] São, no geral uma rede de estruturas críticas essenciais ao regular funcionamento da sociedade. Em Portugal, as IC encontram-se definidas na Lei 46/2018, de 13 de agosto, Vd. conceito no Anexo A.

[5] Segundo Barrett *et al.* (2011), os *Global Commons* são espaços ou domínios partilhados pelos diversos Estados da comunidade internacional, não sendo propriedade de nenhum Estado em específico. Neste quadro, os mares e o espaço aéreo foram os primeiros *Global Commons,* unanimemente aceites. Com o progresso tecnológico, têm vindo a ser, igualmente considerados como *Global Common* o espaço exterior, em virtude da proliferação de satélites de comunicações civis e militares à escala global e mais recentemente, o ciberespaço, por sustentar o funcionamento da internet, e por conseguinte a troca de informação e conhecimento a uma escala planetária.

Para além disso, verifica-se que, existe uma perigosa relação de dependência e interdependência entre as IC, o que, conjugado com as diversas vulnerabilidades tecnológicas existentes e com a grande exposição a ações malévolas, tornam o ciberespaço exposto a várias ameaças (Caldas & Freire, 2013). Concretamente, estas ameaças[6] comportam desde ações de cibercrime, ataques de *hackers*[7], atividades de propaganda extremista e crime organizado, mas também, o apoio a ataques terroristas e a ações ilegítimas de outras entidades estatais, como sucedeu nos casos da Estónia em 2007, da Geórgia em 2008 e da Ucrânia em 2014. Com efeito, estes exemplos de ataques demonstram claramente que os Estados terão de assegurar, não só a utilização segura do ciberespaço aos seus cidadãos, como a salvaguarda da sua própria soberania (IDN-CESEDEN, 2013). Assim acontece porque os ciberataques aumentaram significativamente a sua capacidade disruptiva, podendo provocar efeitos e infligir danos cinéticos e/ou materiais, com potencial para afetar gravemente as IC, a segurança e a soberania nacional (Nunes, 2018). Nesta conjuntura, não é de estranhar que o relatório anual publicado pelo *The Economist Intelligence Unit* (2019) considere os ciberataques como um dos 10 maiores riscos para a economia mundial.

Com base nesta realidade, constata-se que existe uma necessidade premente de confrontar os desafios que o ciberespaço impõe à segurança dos cidadãos, das organizações e dos Estados soberanos. Para isso, é crucial que os Estados e as organizações consigam lidar com a permanente incerteza que paira sobre o ciberespaço, inerente às múltiplas ameaças de natureza difusa, limites indefinidos e em constante mutação. Neste quadro, conforme evidencia Silva (2020), "quanto maior a incerteza de um determinado ambiente, mais relevante se torna o apoio e recurso ao processo de informações", uma vez que as informações permitem, por um lado, mitigar a incerteza, e por outro assegurar um apoio clarificado no processo de tomada de decisão. Assim, considera-se que as informações enquanto fonte de conhecimento quer das várias ameaças existentes no ciberespaço, quer da orquestração e condução de ciberataques, além de contribuírem significativamente para a obtenção de um maior CSC[8], poderão desempenhar um papel muito relevante na segurança do ciberespaço.

Concomitantemente, para além da implementação de medidas e procedimentos que permitam a recolha de informações, afigura-se como essencial a existência de mecanismos e procedimentos que possibilitem quer a obtenção de um robusto CSC, quer a célere e eficaz partilha de informação sobre *malware*[9], incidentes e possíveis ameaças, contribuindo assim, significativamente, para a antecipação, defesa e mitigação de ciberataques.

Posto isto, tendo como ponto de partida este panorama, o presente trabalho de investigação tem como objeto de estudo as "Informações no Ciberespaço", visando contribuir para a consciencialização

[6] O quadro das ameaças no ciberespaço é bastante diversificado e complexo, incluindo Estados, serviços de informações de várias nacionalidades, grupos transnacionais de crime organizado, militares, guerreiros cibernéticos, *hackers* atuando sozinhos ou patrocinados por Estados, espiões industriais, entre outros (IDN-CESEDEN, 2013).

[7] Vd. conceito no anexo A.

[8] Tradução do autor do termo anglo-saxónico *Cyber Situation Awareness.* O conceito de CSC será abordado em maior profundidade no capítulo 4 da presente investigação. Não obstante, em traços gerais, o CSC traduz a capacidade de se percecionar, fielmente, o que "ocorre" no ambiente ciberespaço, por forma a prever com maior rigor os acontecimentos futuros e assim responder de forma célere e adequada aos potenciais problemas que possam surgir (NATO, 2020).

[9] Vd. conceito no anexo A.

e relevo da importância que as informações e a sua partilha, em tempo útil e de forma adequada entre os principais atores, desempenha na segurança do ciberespaço.

1.2. Relevância do Estudo

Desde a sua génese, o ciberespaço tem sido bastante vulnerável aos mais variados tipos de ciberataques[10]. Este facto, já por si preocupante, aliado à grande dependência da sociedade atual a este novo domínio, incluindo o militar, potencia em larga escala os riscos decorrentes desses ataques (Monteiro & Pinto, 2016).

Nesta senda, constata-se que o ciberespaço é, cada vez mais, utilizado pelo crime organizado para a concretização de fraudes e extorsões. A título ilustrativo, citam-se os dados expostos no relatório *NortonLifeLock,* sobre a segurança no ciberespaço em 2019, estimando que em 2018 mais de 350 milhões de pessoas, em 10 países[11], foram vítimas de cibercrime (The Harris Poll, 2020). Esta tendência verificou-se também em Portugal, uma vez que, segundo o Relatório Anual da Segurança Interna 2019 (RASI, 2020) os crimes informáticos aumentaram 42,7 % em relação a 2018 (Figura 2).

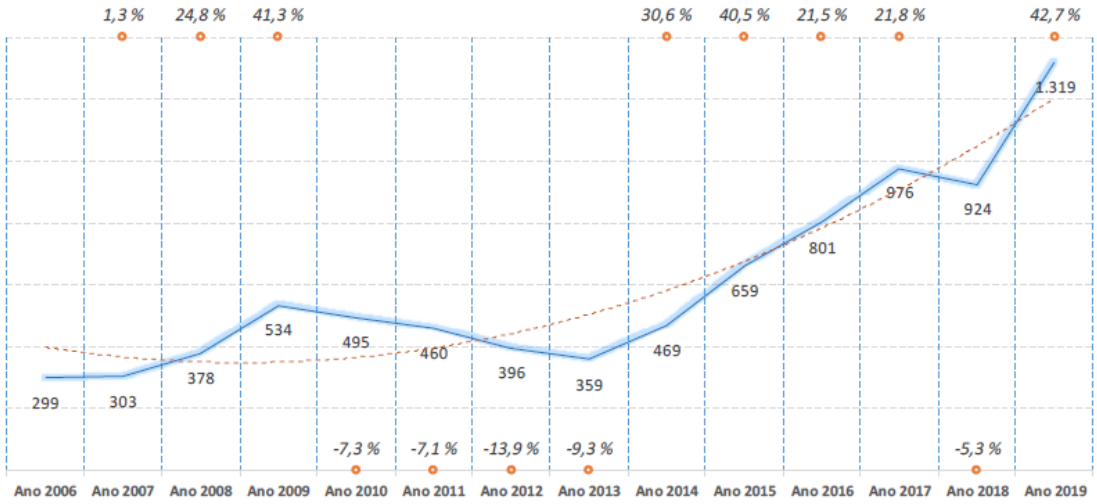

Figura 2 - Número de crimes informáticos participados em Portugal, 2006-2019
(RASI, 2020, p. 47)

Além disso, conforme salienta Nunes (2018), vários ciberataques têm sido utilizados para fins de espionagem e, inclusive, como um meio de coação política contra os Estados. Nesta conjuntura, tome-se, como exemplo, o caso dos alegados ciberataques conduzidos pelos EUA, em Junho de 2019, contra

[10] Segundo Monteiro e Silva (2016), tal assim se sucedeu, porque quando a internet foi originalmente concebida não existiram grandes preocupações de segurança, dado que o objetivo primário assentou na criação de um sistema de comunicação que permitisse a cientistas e investigadores transmitir informação de forma expedita. Por sua vez, Natário (2013) acrescenta que, este facto se encontra fundamentalmente interligado às características particulares deste ambiente, as quais, ao mesmo tempo que lhe conferem um carácter singular, também, têm vindo a ser exploradas de uma forma nociva para a prática de diversos tipos de crimes. Dessas características salientam-se: a quase total ausência de regulação, incitada quer pela defesa exacerbada de liberdade neste meio, quer em virtude da infraestrutura e informação se encontrar no domínio de entidades privadas; a ausência de fronteiras físicas, o que impõe aos Estados dificuldades acrescidas na aplicação da sua jurisdição e soberania; predomínio do anonimato, sendo muito difícil identificar a origem e a autoria das ações, o que dificulta a atribuição de responsabilidades.

[11] Os 10 países alvos desta investigação foram: a Austrália, a França, a Alemanha, a Índia, o Japão, a Holanda, a Nova Zelândia, o Reino Unido e os EUA (The Harris Poll, 2020).

os sistemas de mísseis iranianos em consequência do abate de um *drone* americano por parte das Forças Armadas iranianas (Nakashima, 2019). E desenganem-se os mais céticos que possam acreditar que Portugal se encontra imune ou excluído destas ameaças. Pelo contrário, conforme alertou o Chefe do Estado-Maior-General das Forças Armadas (CEMGFA), Portugal sofreu em novembro de 2018, um ataque aos sistemas de informação das Forças Armadas e Defesa Nacional, do tipo *Spear-phishing*[12], habitualmente, conotados a ações de espionagem atribuídos a grupos denominados de *Advanced Persistent Threats* (APT), tendo sido furtados cerca de 3GB de dados (Ribeiro, 2019).

Consequentemente, estes tipos de ataques podem afetar em larga escala a relação entre os Estados, tendo potencial para se tornarem uma arma de elevado impacto na segurança do próprio sistema internacional (Nunes, 2018). Adicionalmente, os ciberataques, independentemente do seu grau de sofisticação, usufruem de uma natureza assimétrica consubstanciada na desigualdade originada pelo baixo custo de operação e o elevado potencial de impacto (Marques, 2019).

É nesta sequência que se considera que as informações referentes ao conhecimento dos atores existentes no ciberespaço capazes de conduzirem ataques e ao seu planeamento e execução podem contribuir, significativamente, para a antecipação, proteção e mitigação dos ciberataques. Neste âmbito, um exemplo inequívoco desta asserção foi demonstrado publicamente por Israel, após as *Israel Defense Force* (*IDF*) terem executado um ataque aéreo contra um prédio localizado na Faixa de Gaza, por existirem informações que indiciavam a orquestração de um ciberataque contra este Estado, por alegados *hackers* pertencentes ao *Hamas* (Figura 3). No seguimento deste ataque as IDF afirmaram, inclusive, na sua página oficial da rede social *Twitter* que tinham "impedido uma tentativa de uma ofensiva [no ciberespaço] do Hamas contra alvos Israelitas. Após a nossa bem-sucedida operação de defesa [no ciberespaço], atacamos um prédio onde os operacionais do Hamas trabalhavam. O *HamasCyberHQ.exe* foi removido" (IDF, 2019).

Figura 3 - Ataque aéreo conduzido pela IDF contra um alegado centro de operações no ciberespaço do Hamas (IDF, 2019)

[12] Ataque de *phishing* direcionado especificamente a um alvo concreto e estudado. Vd. conceito Anexo A.

Por fim, para além do processo de informações, conceitua-se que complementarmente a obtenção de um robusto CSC e a partilha de informação entre os principais atores com responsabilidade no ciberespaço, a nível nacional e internacional, são aspetos fundamentais na segurança deste ambiente que devem ser investigados, desenvolvidos e promovidos.

1.3. Enquadramento Teórico e Conceptual

1.3.1. Conceito de Ciberespaço

Após o conceito de ciberespaço[13] ter sido apresentado por Willian Gibson em 1982, constata-se que proliferaram várias definições até ao presente. Nesta conjuntura David Clark (2010), do *Massachusetts Institute of Technology* (MIT), avança com uma definição próxima da utilizada por Gibson (1984), ao considerar o ciberespaço como "um conjunto de computadores ligados em rede, na qual é eletronicamente armazenada e utilizada informação, onde há lugar à comunicação" (Clark, 2010, p. 1). Por sua vez, a NATO (2019), recorre a um conceito mais abrangente de ciberespaço definindo-o como um domínio global constituído pela interligação dos sistemas de comunicação, sistemas de informação e outros sistemas eletrónicos, bem como pela sua interação e informação que neles é armazenada, processada ou transmitida. Já em Portugal, o conceito de ciberespaço encontra-se sintetizado e delimitado na Estratégia Nacional de Segurança do Ciberespaço (ENSC) 2019-2023, definindo-o como um "ambiente complexo, de valores e interesses, materializado numa área de responsabilidade coletiva, que resulta da interação entre pessoas, redes e sistemas de informação" (GOV-PT, 2019, p. 2889).

1.3.2. Conceito de Cibercrime

A ENSC 2019-2023 considera que por cibercrime "entendem-se os factos correspondentes a crimes previstos na Lei do Cibercrime (LC)[14] e ainda a outros ilícitos penais praticados com recurso a meios tecnológicos, nos quais estes meios sejam essenciais à prática do crime em causa" (GOV-PT, 2019, p. 2890).

De igual modo, Venâncio (2011, p. 16) acrescenta ainda que o cibercrime compreende toda a atividade criminosa que pode ser executada "por meios informáticos, ainda que estes não sejam mais que um instrumento para a sua prática, mas que não integra o seu tipo legal, pelo que o mesmo crime poderá ser praticado por recurso a outros meios". Neste âmbito, estes crimes podem ser divididos, de acordo com a opinião de Grabosky (2004), em três grupos: crimes convencionais realizados através de um computador; crimes convencionais em que o computador não é o objeto essencial à sua prática,

[13] Em traços gerais, constata-se que, a palavra ciberespaço resulta da junção da palavra mãe *espaço* com o seu prefixo *ciber*, proveniente do prefixo anglo-saxónico *cyber*. Adicionalmente, verifica-se que, o prefixo *cyber*, deriva do termo *cybernetics,* ou em língua portuguesa *cibernética*, a qual é definida como a "ciência e técnica do funcionamento e do controlo dos comandos eletromagnéticos e das transmissões eletrónicas nas máquinas de calcular e nos autómatos modernos", e ainda como "a ciência que estuda os mecanismos de comunicação de controlo nas máquinas e nos seres vivos. (Dicionário infopédia da Língua Portuguesa, 2003-2019).

[14] Lei do Cibercrime, Lei nº 109/2009, de 15 de setembro, disponível em: http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1137&tabela=leis (Consultado em 3-5-2020)

mas no qual o meio de obtenção de prova é realizado sobre a forma digital; e os crimes em que o alvo são os sistemas informáticos.

1.3.3. Conceito de Ciberespionagem

No contexto da segurança nacional, o SIS (2020a) define espionagem como sendo a atividade que se dedica à obtenção de informação, que pelo seu valor e importância para a segurança e interesses nacionais se encontra protegida. Assim, o acesso ilícito a esta informação é realizado através da exploração de métodos encobertos com o recurso a meios técnicos sofisticados ou a agentes e fontes humanas que estão ao serviço de países estrangeiros.

A ciberespionagem assume-se como uma variante da espionagem tradicional, consistindo na obtenção de conhecimento e informações sensíveis ou classificadas sobre indivíduos, organizações, Estados e competidores e/ou inimigos, que possam conceder uma vantagem económica, política ou militar. Estas informações são, por norma, obtidas com recurso à utilização de métodos de exploração ilegais da internet, das redes, de *software* e/ou de computadores. Importa ressalvar que a diferença entre a espionagem tradicional e a ciberespionagem se traduz, essencialmente, no espaço onde as ações são desencadeadas. Com efeito, a primeira é conduzida no meio físico, enquanto a segunda é concretizada através do ciberespaço (ENISA, 2013).

1.3.4. Conceito de Ciberterrorismo

No que concerne ao Ciberterrorismo, este resulta, segundo Denning (2000a), da convergência entre o terrorismo e o ciberespaço consubstanciando-se na condução de ataques ou tentativas de ataques contra redes de comunicação, computadores e informação neles armazenada, com a finalidade de atemorizar ou persuadir um governo ou o seu povo, a fim de materializar objetivos de ordem política ou sociais. Esclarece ainda que para um ciberataque ser considerado um ato de ciberterrorismo, deverá da execução deste resultar violência contra pessoas ou propriedade, ou no mínimo provocar danos significativos capazes de instigar medo. Por conseguinte, enquadram-se neste tipo de ataques, os que provoquem: morte ou dano físico; explosões; queda de aviões; contaminação de água; grandes perdas económicas. Pelo contrário, excluiu-se do âmbito do ciberterrorismo os ataques que apenas causem disrupção de serviços não essenciais ou que provoquem perdas financeiras insignificantes – situações que podem ser enquadradas no âmbito do cibercrime.

Neste contexto, ao analisar-se a definição de ciberterrorismo supracitada, infere-se que para que uma ação no ciberespaço seja considerada como ciberterrorismo, esta tem de respeitar dois critérios em simultâneo, nomeadamente: o de apresentar uma motivação política; o de provocar danos significativos capazes de instigar medo. Por sua vez, no que concerne aos alvos mais prováveis de serem objeto de ataque, constata-se que neste campo existe unanimidade ao reconhecerem-se as IC como os alvos mais prováveis.

1.3.5. Conceito de Ciberguerra

Efetivamente, existem várias definições de Ciberguerra[15], as quais, conforme evidencia Santos (2011), se diferenciam, essencialmente, nos tipos de ação e nos atores considerados. Num quadro mais geral, o IDN-CESEDEN (2013, p. 23) considera que a "Ciberguerra, pode ser definida como uma luta ou conflito entre duas ou mais nações ou entre diferentes fações dentro de uma nação onde o ciberespaço é o campo de batalha".

Numa vertente mais operacional, tomando por referência o memorando de padronização da terminologia conjunta dos EUA para as operações no ciberespaço (Department of Defense, 2010), poder-se-á delimitar a Ciberguerra como um conflito armado conduzido em parte, ou totalmente, por meios cibernéticos. Neste contexto, as operações militares são conduzidas com a finalidade de negar à força opositora a utilização eficaz dos seus sistemas no ciberespaço e das suas armas no conflito. Inclui a condução de operações defensivas, operações ofensivas e operações de exploração da utilização do ciberespaço.

1.3.6. Segurança das Redes e dos Sistemas de Informação e a Estratégia Nacional de Segurança no Ciberespaço

No quadro específico das redes e dos sistemas de informação, conforme delimitado no Regime Jurídico da Segurança do Ciberespaço, Lei nº 46/2018, segurança significa:

> "a capacidade das redes e dos sistemas de informação para resistir, com um dado nível de confiança, a ações que comprometam a confidencialidade, integridade, disponibilidade, autenticidade e o não repúdio dos dados armazenados, transmitidos ou tratados, ou dos serviços conexos oferecidos por essas redes ou por esses sistemas de informação, ou acessíveis através dos mesmos". (AR, 2018, p. 4032)

No que concerne à segurança no ciberespaço, em 2019, foi aprovada a nova ENSC[16] com um horizonte temporal compreendido entre 2019-2023 tendo por base três objetivos estratégicos, designadamente: maximizar a resiliência; promover a inovação; garantir recursos. Para além disso, a ENSC 2019-2023, tem como finalidade:

> "aprofundar a segurança das redes e sistemas de informação, como forma de garantir a proteção e defesa do ciberespaço de interesse nacional e potenciar uma utilização livre, segura e eficiente do mesmo por parte de todos os cidadãos, das empresas e das demais entidades públicas e privadas". (GOV-PT, 2019, p. 2889)

As implicações e necessidades relativas a cada um dos objetivos estratégicos identificados permitem delinear e articular linhas de ação concretas, dirigidas a reforçar o potencial estratégico

[15] Termo que deriva do anglo-saxónico "*cyber warfare*". Segundo Arquilla e Ronfeldt (1997), o termo foi originalmente exposto por Thomas Rona em 1979, em *Weapon Systems and Information War*.

[16] A primeira ENSC foi promulgada em 2015, através da RCM nº 36/2015, e teve como finalidade "aprofundar a segurança das redes e dos sistemas de informação e potenciar uma utilização livre, segura e eficiente do ciberespaço, por parte de todos os cidadãos e das entidades públicas e privadas" (GOV-PT, 2019, p. 2888).

nacional no ciberespaço, através do incremento da segurança. A estas linhas de ação dá-se o nome de eixos de intervenção. Neste âmbito, a ENSC 2019-2023 elenca e sobreleva seis eixos prioritários de intervenção, a saber: Eixo 1 – Estrutura de segurança do ciberespaço; Eixo 2 – Prevenção, educação e sensibilização; Eixo 3 – Proteção do ciberespaço e das infraestruturas; Eixo 4 – Resposta às ameaças e combate ao Cibercrime; Eixo 5 – Investigação, desenvolvimento e inovação; Eixo 6 – Cooperação nacional e internacional" (GOV-PT, 2019, p. 2889).

1.3.7. Conceitos de Cibersegurança e Ciberdefesa

Segundo a ENSC 2019-2023, a cibersegurança:

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

Assim, facilmente se infere que compete a diversas entidades garantir a sua cibersegurança[17], tendo as organizações e os cidadãos um importante papel a desempenhar neste desiderato. Não obstante, Santos (2020) corroborar com esta definição de cibersegurança, o mesmo esclarece que, o conceito de cibersegurança, fruto da própria noção de transformação digital, tem sido ao longo dos tempos alvo de diversas interpretações, inclusive no seio da academia. Neste contexto, Santos (2020), acrescenta que a cibersegurança também pode ser, simplesmente, entendida como "o sentimento percecionado pelas pessoas quando usam a tecnologia".

Por sua vez, a ENSC 2019-2023 define a ciberdefesa[18] como a "atividade que visa assegurar a defesa nacional, no, ou através do, ciberespaço" (GOV-PT, 2019, p. 2889).

Além do ponto de vista conceptual, considera-se que a distinção entre cibersegurança e ciberdefesa também pode ser exposta com base no grau de ameaça que um Estado tem necessidade de prevenir ou enfrentar. Assim, a cibersegurança inclui as atividades de prevenção, monitorização e resposta às ameaças que "coloquem em risco o bem-estar e a salvaguarda dos direitos dos cidadãos ou organizações" (Moniz, 2018, p. 23). Por seu turno, a ciberdefesa centrar-se-á nas "ameaças que coloquem em risco a soberania nacional" (Moniz, 2018, p. 23).

1.3.8. Conceito de Informações

A doutrina *North Atlantic Treaty Organization* (NATO) define informações como sendo "o produto resultante da recolha direta e do processamento de dados sobre o ambiente, e as capacidades e intenções dos atores, por forma a identificar as ameaças e proporcionar oportunidades a serem exploradas pelos decisores" (NATO, 2019b).

[17] No nosso país, a responsabilidade pela cibersegurança nacional encontra-se formalmente atribuída a um conjunto variado de entidades, que inclui as Forças e Serviços de Segurança, o CNCS e a ANPC.

[18] Em Portugal, compete às Forças Armadas assegurar a missão de ciberdefesa.

A nível nacional as informações, tradução técnica do inglês *intelligence*, são entendidas como sendo o conhecimento que resulta de um processo denominado de "ciclo de informações" que compreende a recolha de dados e factos através de meios humanos, tecnológicos e documentais, e a organização, análise e avaliação com recurso a técnicas e metodologias específicas (SIRP, 2020).

Neste sentido, ao analisarem-se estas duas definições elencadas, infere-se que por um lado, a doutrina NATO, certamente influenciada pela sua natureza, realça a importância das informações para a identificação das ameaças e proporcionar oportunidades, enquanto a nacional destaca sobretudo os métodos e os meios através dos quais o conhecimento é produzido. Não obstante, ambas deixam à evidência que, conforme se abordará em maior detalhe no Capítulo 4, para se entender o que são informações dever-se-á realizar uma análise holística e global que examine o processo, o produto e a organização (Lowenthal, 2006).

Ao efetuar-se uma revisão da literatura verifica-se que existe uma grande pluralidade de definições sobre o conceito de informações. Segundo Romana as informações são "um processo de obtenção de conhecimento fundamental à tomada de decisão quanto à salvaguarda dos interesses permanentes ou conjunturais dos Estados, assumindo natureza e finalidade ofensiva e defensiva" (2008, p. 98). Por sua vez, Breakspear (2013) tem uma visão mais operacional do conceito defendendo que as informações se traduzem na capacidade de prever alterações no futuro, permitindo reagir em tempo. Refere, ainda, que esta capacidade envolve análise e previsão por forma a identificar mudanças iminentes.

Não obstante a panóplia de definições existentes, releva-se que as informações, na sua essência, visam apoiar o processo de tomada de decisão e têm como objetivo último a obtenção de uma vantagem sobre um competidor, adversário ou contrário (Ribeiro, 2020). É em concordância com esta asserção que Silva (2020) reitera que "importa compreender que as informações não são um fim em si mesmo, elas pretendem sempre assegurar o apoio à tomada de decisão".

1.4. Objeto, objetivos e delimitação da investigação

A presente investigação tem como objeto de estudo as "Informações no Ciberespaço", procurando evidenciar a importância que estas e a sua partilha, entre os principais atores, desempenham na segurança do ciberespaço.

Devido à abrangência do tema, existe a necessidade de o limitar em três dimensões, nomeadamente: conteúdo, temporal e espacial (Santos, et al., 2019).

Quanto ao conteúdo, após a necessária caracterização do ambiente ciberespaço, o foco centrar-se-á na doutrina de informações da NATO, complementada pela opinião de vários especialistas nacionais e internacionais, com vista à obtenção de um robusto CSC e na partilha de informação eficiente entre as principais entidades com responsabilidade na segurança do ciberespaço. A investigação a nível espacial tem sobretudo por base a ENSC 2019-2023 e incide, maiormente, sobre as principais entidades que, a nível nacional, possuem responsabilidade na segurança no ciberespaço. Por sua vez, em termos temporais o estudo centra-se, essencialmente entre 2007, ano em que ocorreram os ciberataques em larga escala à Estónia e o mundo, sobretudo o ocidental, "despertou" para a criticidade da necessidade de garantir a segurança no ciberespaço, e a atualidade.

Neste quadro, o Objetivo Geral (OG) desta investigação consiste em **analisar o contributo e a importância que as informações podem desempenhar para a obtenção da segurança no ciberespaço.** Com vista à prossecução deste OG, foram, complementarmente, estabelecidos os sequentes Objetivos Específicos (OE) de investigação expostos na Tabela 1.

Tabela 1 – Objetivos Específicos da investigação

OE1	Caracterizar o ambiente ciberespaço.
OE2	Descrever os principais domínios e entidades que a nível nacional contribuem para a segurança no ciberespaço.
OE3	Com base na análise das informações identificar aspetos em que estas poderão contribuir para a segurança no ciberespaço.

1.5. Questão Central e Questões Derivadas

Tendo por base o objeto de estudo, a delimitação do tema e de forma a alcançar o OG estabelecido, e definir o fio condutor da presente investigação, foi identificada a seguinte **Questão Central (QC)** – **Como poderão as informações contribuir para a segurança no ciberespaço**?

Em resposta a esta QC emergiram e foram definas as Questões Derivadas (QD) apresentadas na Tabela 2.

Tabela 2 - Questões Derivadas da investigação

QD1	Como se caracteriza o atual ambiente ciberespaço?
QD2	Quais são os principais domínios e entidades nacionais que contribuem para a segurança no ciberespaço e como se articulam?
QE3	De que forma as informações poderão contribuir para a segurança no ciberespaço?

1.6. Metodologia da Investigação

A presente investigação assentou numa filosofia ontológica construtiva, uma vez que, conforme expõem Santos *et al.* (2019), os fenómenos sociais e as suas interpretações são obtidos através da própria interação social e encontram-se em permanente evolução. Ora, esta é a própria natureza do ciberespaço o qual alicerçado na transformação digital e na interação humana se encontra em permanente mudança.

De igual modo, a investigação tem como fio condutor a abordagem epistemológica "interpretativista", respeitando a missiva elencada por Santos *et al.* (2019, p. 18), ao referirem que "compete ao investigador não só verificar os fenómenos, mas também compreender os significados subjetivos desses fenómenos sociais". Assim, tendo por base esta premissa as conclusões foram obtidas quer através da interpretação da doutrina, legislação e documentação, bem como recorrendo à opinião de peritos e especialistas na área.

Recorreu-se ainda ao raciocínio dedutivo, dado que se partiu do geral para o particular, não se assumindo como sendo a verdade dos factos, mas sim da sua validade, combinado com a utilização de um pensamento crítico (Santos, et al., 2019). Com efeito, ao visar-se relevar e evidenciar a

importância das informações na antecipação, defesa e mitigação dos ciberataques e na segurança do ciberespaço a investigação desenvolveu-se procurando validar e atestar esta hipótese.

No que concerne à metodologia científica utilizada na elaboração da presente investigação utilizou-se uma estratégia qualitativa pois "procurou-se alcançar um entendimento mais profundo e subjetivo do objeto de estudo" (Vilelas, 2009, p. 108), designadamente sobre as informações no ciberespaço, sem se atender a medições e análises estatísticas. Neste âmbito, a recolha de dados foi efetuada através da análise documental, de âmbito legal, doutrinário e produzida por especialistas, bem como por intermédio da observação e de entrevistas estruturadas a peritos na matéria.

O percurso metodológico da investigação desenvolveu-se em três fases, nomeadamente: exploratória; analítica; conclusiva. Na fase exploratória começou-se por determinar o "Estado da Arte" através da revisão da legislação enquadrante, da doutrina, de artigos de especialistas e de entrevistas exploratórias com vista ao enquadramento do tema, ao relevo da investigação, à definição dos objetivos e à formulação inicial das questões de investigação. Na fase analítica, procurou-se através do complemento entre a recolha da informação em diversas fontes e a realização de entrevistas estruturadas a especialistas em cibersegurança, ciberdefesa, combate ao cibercrime e informações, alcançar os OE definidos. Na fase conclusiva foram avaliados e discutidos os resultados obtidos de modo a responder à QC e às QD. Por fim, foram apresentadas as conclusões e os contributos para o conhecimento, bem como identificadas limitações, recomendações e sugestões para futuras investigações. A Figura 4 apresenta o percurso metodológico que ligou as três fases da investigação seguidas.

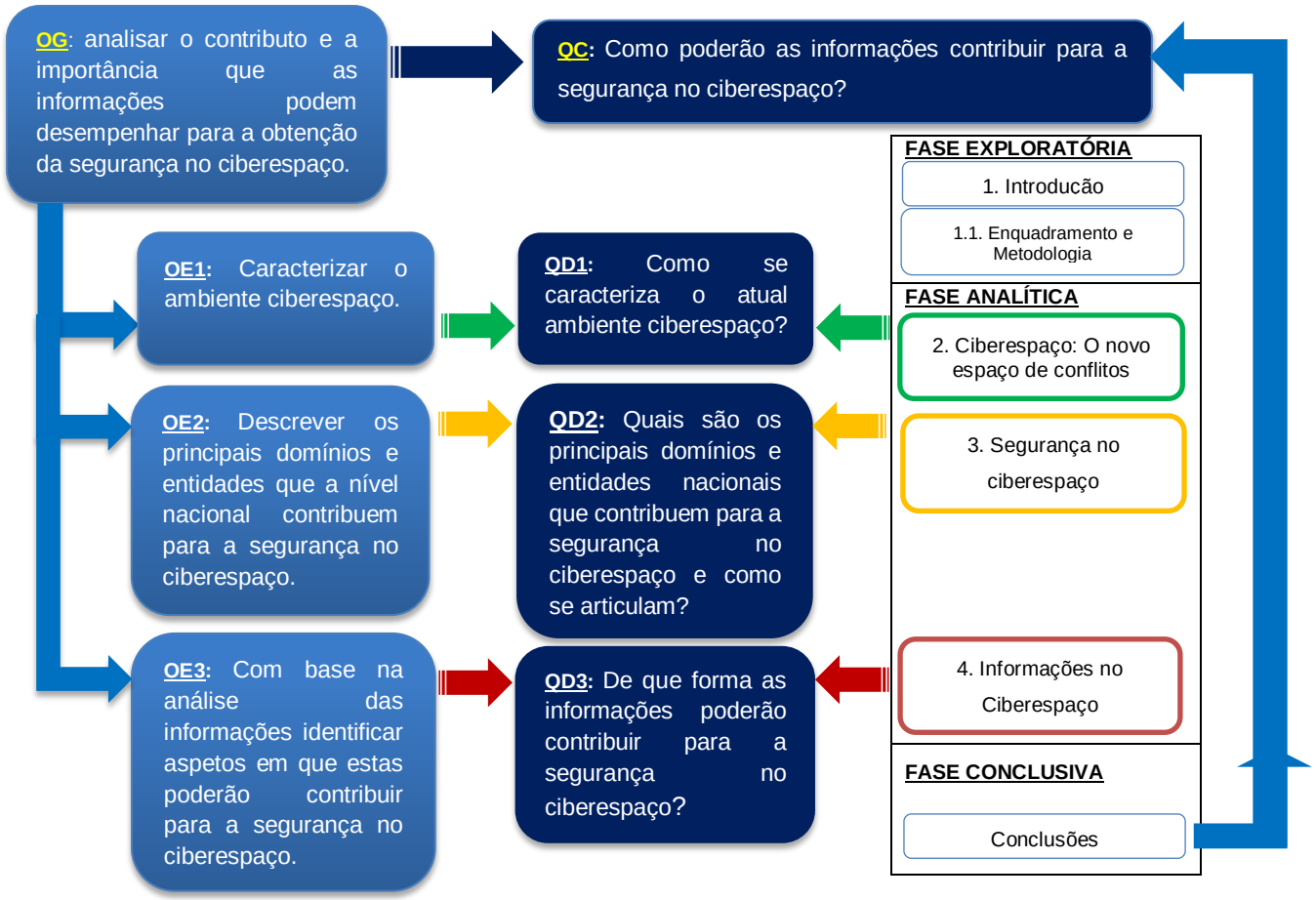

Figura 4 – Percurso metodológico da investigação

1.7. Estrutura do Estudo

O presente trabalho está organizado em cinco capítulos. Após a introdução, onde foi apresentado o tema, a relevância do estudo, o enquadramento concetual, o objeto, os objetivos, as questões e a metodologia da investigação, procurar-se-á no segundo capítulo, caracterizar o ciberespaço. Para esse efeito, serão identificadas algumas das principais características deste ambiente singular, bem como exposto de que forma se constitui como um novo domínio para a condução de operações militares e desafia os conceitos tradicionais de soberania e fronteira. Ainda neste capítulo, analisar-se-ão as ameaças presentes no ciberespaço tendo por base a motivação e o perfil dos autores.

Posteriormente, no terceiro capítulo serão descritos os principais domínios e entidades que, a nível nacional, contribuem para a segurança no ciberespaço. Em concreto, caracterizar-se-á de um modo geral o domínio da cibersegurança, do combate ao cibercrime, da ciberdefesa, das informações e da ciberdiplomacia e cooperação, expondo-se de que forma os principais atores intervenientes se articulam operacionalmente.

Em seguida, no quarto capítulo analisar-se-ão as informações relevando-se a importância destas, do CSC e da partilha de informação para a segurança do ciberespaço. Neste âmbito, abordar-se-á, igualmente, o *Malware Information Sharing Plataform* (MISP), como evidência da relevância da existência de sistemas que permitam a partilha de informação e de indicadores de compromisso associados a ciberataques, possibilitando realizar uma avaliação precoce de ameaças. Ainda neste capítulo, realizar-se-á a discussão da investigação, analisando-se os contributos explanados pelos peritos nas entrevistas realizadas, constatando-se a importância das informações e a premência da sua partilha no ciberespaço.

Finalmente, no último capítulo serão apresentadas as conclusões da investigação.

2. Ciberespaço: O novo espaço de conflitos

> *"O ciberespaço é o campo de batalha do futuro", Leon Panetta, Secretário da Defesa dos EUA* (Ravindranath, 2014).

2.1. Principais características do ciberespaço

Em primeiro lugar, ao analisar-se o ciberespaço, constata-se que, existem e sobressaem um conjunto muito particular de características, intrínsecas à natureza e utilização deste ambiente, que importa elencar por forma a serem compreendidos os desafios que o ciberespaço impõe à segurança e defesa dos Estados. Neste sentido, identificam-se, em seguida, algumas dessas particularidades tendo como fio orientador a investigação conjunta realizada pelo IDN-CESEDEN (2013), complementada pela opinião dos especialistas que participaram no presente estudo.

Neste quadro, começa-se por evidenciar o **carácter dinâmico** do ciberespaço, subjacente aos sistemas que o integram serem alvo de constantes modificações, impulsionadas pela descoberta de novas ameaças e vulnerabilidades (IDN-CESEDEN, 2013). O dinamismo do ciberespaço é, igualmente, realçado por Assunção (2020), ao afirmar que por ter sido "pensado e edificado pelo Homem (…) pode sofrer transformações muito rápidas".

Simultaneamente, é um domínio dotado de um **enorme potencial de crescimento**, tanto nas funcionalidades, como na velocidade comunicacional dos fluxos de informação (IDN-CESEDEN, 2013).

Possui, igualmente, uma **elevada capacidade de processamento e armazenamento** de grandes quantidades de informação (IDN-CESEDEN, 2013). Nesta senda, Rodrigues (2020) destaca também esta característica, referindo-se em concreto à grande velocidade de geração de efeitos que, conforme esclarece, "cria enormes desafios sociais, e torna necessário criar canais de comunicação entre instituições, e/ou Estados que não se coadunam com os métodos de comunicação tradicionais". Da mesma forma, Assunção (2020) reitera que, esta grande velocidade de propagação de efeitos no ciberespaço "pode ser catalisado pelos atores em proveito próprio, trazendo para a esfera da segurança uma necessidade de monitorização constante dos sistemas para uma resposta eficaz". Com o mesmo entendimento, mas com outro ângulo de análise, o SIS (2020b) sublinha o facto de o ciberespaço conferir um elevado grau de "imediatismo de atuação aos seus intervenientes". Por sua vez, Bravo (2020) realça sobretudo a grande capacidade de armazenamento, alertando para a particularidade do ciberespaço "ter efeito de eco e permitir memória persistente de factos contrafeitos, como os '*deep fakes'* e a contra-informação Estatal ou originada noutros interesses difusos".

Para além disso, o ciberespaço apresenta um **carácter assimétrico**, uma vez que é possível concretizar ações de grande magnitude com relativamente poucos recursos (IDN-CESEDEN, 2013). Neste enquadramento, Silva (2020) alerta que, a "severidade de que parcos recursos humanos e materiais podem causar, veio necessariamente transfigurar as prioridades ao nível pessoal, das comunidades, das nações e consequentemente da sociedade mundial".

Outro aspeto muito importante que o ciberespaço confere é o **relativo grau de anonimato**, uma vez que é muito difícil determinar a origem de um ciberataque (IDN-CESEDEN, 2013). Esta

circunstância é reconhecida por, praticamente, todos os especialistas entrevistados, como sendo uma das que cria maiores desafios à segurança, pois conforme esclarece Santos (2020) "o relativo grau de anonimato impõe grandes dificuldades à investigação criminal e à atribuição de ações no ciberespaço". Neste âmbito, o SIS (2020b) esclarece que o "anonimato é tanto decorrente do uso de técnicas, táticas e de ferramentas próprias de anonimização pelo agente de ameaça, como da ausência de observância de políticas e de procedimentos de rastreio de atividade tanto dos operadores como dos próprios alvos dessas ações". Complementarmente, Rodrigues (2020) identifica, como uma das grandes brechas de segurança nesta matéria, a anonimização realizada através de *proxys* e por intermédio de infraestruturas de rede desprotegidas.

Em linha com o anonimato surge uma outra característica muito similar, mas de âmbito mais delituoso, a **mistificação**. Para Assunção (2020) é relativamente fácil atores maliciosos mistificarem a sua presença no ciberespaço causando grandes dificuldades na capacidade das autoridades conseguirem identificar e atribuir a autoria dos ciberataques.

O ciberespaço é, também, **transversal** a todos os sectores da sociedade, visto que uma ação ou um evento desencadeado neste ambiente poderá ter impacto em todos os outros domínios de atividade[19] (IDN-CESEDEN, 2013). Este aspeto engloba o que Santos (2020) denomina de "simultaneidade e multiplicidade de efeitos", e ao consubstanciar-se, segundo Bravo (2020), como um domínio interdependente, promove o "surgimento dos fenómenos voláteis, incertos, complexos e ambíguos, o que é compatível com o 'novo conceito' de ameaças híbridas".

A **ausência de regulação** é outra característica valorizada por Santos (2020) e por Assunção (2020) sublinhando este último que a "ausência de um entendimento à escala global sobre a governação e regulação da internet caracteriza este espaço virtual como o "*digital far west*"".

Por sua vez, Santos (2020) releva também a **capacidade de amplificação** do ciberespaço, na medida em que este ambiente se fundamenta num meio extraordinariamente eficaz para a exploração da vulnerabilidade humana. Na sua perspetiva, o ciberespaço potencializa este facto, "seja porque facilita a cooptação, associação e a mobilização para a ação coletiva, seja porque permite a manipulação e a polarização da sociedade" Santos (2020).

Ademais, a investigação conjunta do IDN-CESEDEN (2013) elenca, ainda, mais dois atributos do ciberespaço, nomeadamente: o **custo reduzido de acesso**; e a **alta capacidade para produzir efeitos físicos.**

Por outro lado, o SIS (2020b) destaca a particularidade de o ciberespaço assentar em **infraestruturas geograficamente dispersas**, o que impõe grandes desafios à segurança, dado que estas se encontram "cometidas a diferentes quadros legislativos e à intervenção de inúmeras entidades internacionais". A mesma entidade reitera que este facto obriga "em termos de resposta securitária a um elevado trabalho de *intelligence* bem como de cooperação internacional, nem sempre profícuo em termos de capacidade atempada de resposta".

Por fim, importa referir que o ciberespaço se caracteriza, segundo Assunção (2020), por ser um "**espaço sem limites físicos de fronteiras**". Este relevante aspeto, a que Santos (2020) denomina de "aterritorialidade", está intimamente ligado, quer à indefinição dos limites das fronteiras no ciberespaço

[19] Tais como a área política, económica, social ou até, a segurança e defesa dos Estados

- tais como, se conhecem na sua expressão geográfica -, quer à sua própria natureza, onde a crescente interdependência resultante da globalização e a elevada velocidade de comunicação dos fluxos de informação debelam as fronteiras físicas instituídas. Nesta senda, o SIS (2020b) enfatiza que este aspeto conjugado com a característica do anonimato confere aos cibercriminosos "tanto impunidade de conduta como de segurança operacional elevada pela não exposição física das suas ações". Este aspeto, face à sua relevância, será abordado em maior detalhe no Subcapítulo 2.5.

Tabela 3 – Quadro resumo das principais características do ciberespaço identificadas na investigação.

Característica	Breve Descrição	Autores
Carácter dinâmico	• Os vários sistemas que compõem o ciberespaço alteram e modificam-se frequentemente, sobretudo as suas interligações; • Subjacente a ser uma dimensão criada pelo homem.	• IDN-CESEDEN (2013); • SIS (2020b). • Assunção (2020).
Enorme potencial de crescimento	• Patente nas funcionalidades que disponibiliza e na velocidade da troca de informação.	• IDN-CESEDEN (2013).
Elevada capacidade de processamento e armazenamento	• De grandes quantidades de informação; • Desencadeia uma grande velocidade de geração de efeitos; • Velocidade de propagação; • Imediatismo de atuação; • Ter efeito de eco e permitir memória persistente de factos contrafeitos.	• IDN-CESEDEN (2013); • Rodrigues (2020); • Assunção (2020); • SIS (2020b); • Bravo (2020).
Carácter assimétrico	• Desequilíbrio entre a capacidade de provocar ações hostis de grande impacto e os reduzidos recursos necessários; • Severidade de que parcos recursos humanos e materiais podem causar.	• IDN-CESEDEN (2013); • Silva (2020).
Relativo grau de anonimato	• Difícil detetar a origem de um ataque, impondo grandes dificuldades à investigação criminal e à atribuição de ações no ciberespaço.	• IDN-CESEDEN (2013); • Santos (2020); • Bravo (2020); • Rodrigues (2020); • Silva (2020); • SIS (2020b).
Mistificação	• Capacidade para atores maliciosos dissimularem a sua presença no ciberespaço.	• Assunção (2020).
Transversalidade	• Uma ação ou evento ocorrido no ciberespaço pode afetar um ou mais domínios de atividade das sociedades modernas; • Simultaneidade e multiplicidade de efeitos; • Domínio interdependente.	• IDN-CESEDEN (2013); • Santos (2020); • Bravo (2020).
Ausência de regulação	• Espaço de utilização livre, com muito pouca regulação; • Ausência de mediação.	• Assunção (2020); • Santos (2020).
Capacidade de amplificação	• Meio extremamente eficaz para a exploração da vulnerabilidade humana.	• Santos (2020).

Custo reduzido de acesso	• Nos dias de hoje, o custo económico de acesso ao ciberespaço é reduzido.	• IDN-CESEDEN (2013).
Alta capacidade para produzir efeitos físicos	• Embora seja um espaço virtual os seus efeitos repercutam-se no mundo físico amplificados na possibilidade de atingir um vasto conjunto de equipamentos e indústrias.	• IDN-CESEDEN (2013).
Infraestruturas geograficamente dispersas	• Submetidas a diferentes quadros legislativos e à intervenção de inúmeras entidades internacionais, aspeto que é amplamente explorado pelos agentes de ameaça.	• SIS (2020b).
Indefinição de fronteiras	• Indefinição dos limites das fronteiras no ciberespaço; • Ausência de delimitação geográfica de ação; • Gera dificuldades em determinar a forma como um Estado poderá exercer a sua soberania sobre uma área ou ambiente que não domina e não controla.	• Assunção (2020); • SIS (2020b); • Santos (2020).

2.2. Um novo domínio das operações

A importância do ciberespaço, incluindo para as operações militares, é atualmente inquestionável facto que levou os militares a reconsiderarem os tradicionais conceitos de operação. Neste campo, salienta-se a publicação da doutrina conjunta americana para a condução de Operações no Ciberespaço (JP 3-12), que descreve o ciberespaço através de uma conceptualização de três camadas inter-relacionadas, nomeadamente: Física; Lógica; e Pessoa *Ciber*[20] (USJCS, 2018)). Esta representação encontra-se esquematizada na Figura 5.

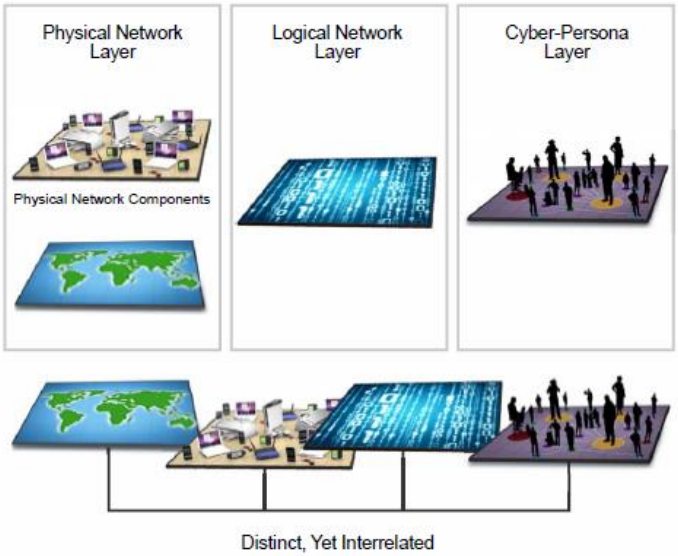

Figura 5 - Conceptualização do ciberespaço em três camadas inter-relacionadas (USJCS, 2018, p. I-3)

A camada Física representa a camada tangível do ciberespaço, constituída pelas redes físicas de computadores e sistemas. Com efeito, apesar de o ciberespaço ser um domínio global e virtual, o seu funcionamento exige sempre uma ligação ao mundo físico onde se encontram instalados os

[20] Tradução adotada para a expressão *Cyber-Persona* (USJCS, 2018).

componentes da rede (*hardware*, equipamentos, cabos, *routers*, *switchs*, servidores, transmissores). Quanto à camada Lógica é constituída pelas ligações que são estabelecidas entre os vários nós da rede. Esta camada engloba a informação em si mesmo e o respetivo suporte[21], possibilitando a ligação de diferentes componentes, tais como, os computadores, *tablets*, *smartphones* ou outros equipamentos que tenham o seu endereço *Internet Protocol* (IP)[22] na rede. Por sua vez, a camada referente à Pessoa *ciber* relaciona os aspetos humanos e cognitivos realizando a separação entre a pessoa física e a pessoa *ciber*. Esta camada toma em linha de conta, quer as características que determinam a pessoa enquanto elemento incorporada na rede por meio de uma identificação[23], quer a pessoa como utilizadora dos serviços e aplicações da rede (USJCS, 2018).

O ciberespaço, perante este conceito multidimensional, face à sua intrínseca ligação às IC e em virtude da grande preocupação com o impacto deste ambiente no sistema de segurança internacional, levou a que o mesmo seja atualmente definido e comummente aceite como um domínio das operações à semelhança do Mar, da Terra, do Ar e do Espaço[24]. Facto que a própria Aliança Atlântica reconheceu formalmente na Cimeira de Varsóvia de 2016 (NATO, 2016). Em específico, o ciberespaço emerge como um domínio que possibilita a interdependência entre todos os restantes domínios, através da existência de nós e *links* (USJCS, 2018). Esta interdependência entre os cincos domínios encontra-se exemplificada na Figura 6, com destaque ainda para o espectro eletromagnético.

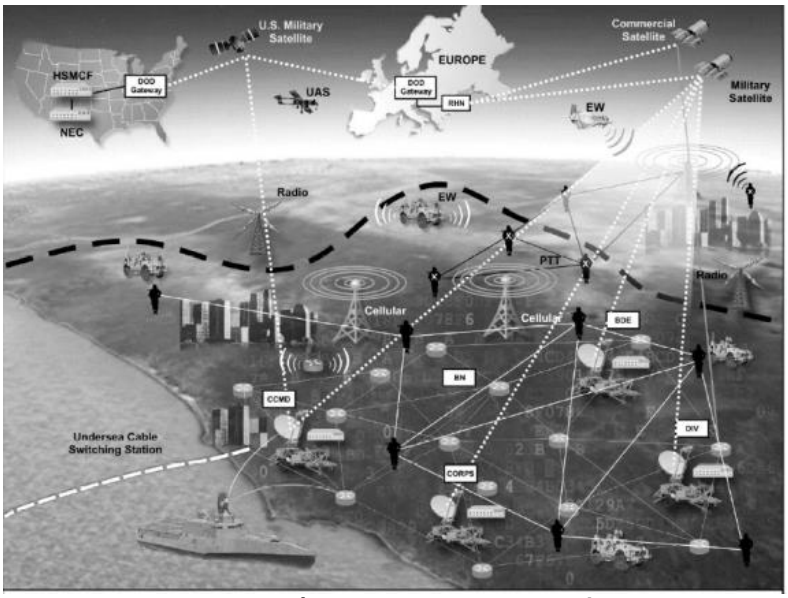

Figura 6 – Exemplo da interdependência entre os cinco domínios para a condução de operações militares e o espetro eletromagnético (U.S. Army, 2017, pp. 1-3)

Em suma, verifica-se que, no ciberespaço são conduzidas operações militares específicas cada vez mais importantes ao suporte e concretização das operações militares levadas a cabo nos domínios físicos.

[21] Em mais detalhe, na camada Lógica realiza-se o processamento, armazenamento, disseminação, divulgação e proteção da informação. Nesta camada, além da informação, inclui-se ainda os algoritmos, o *software*, o *firmware* e os processos automáticos de decisão (USJCS, 2018).

[22] É uma das características mais importantes da internet, responsável pela identificação das máquinas e redes e pelo encaminhamento das mensagens até ao seu destino. Vd. conceito no anexo A.

[23] Através, por exemplo, de um endereço IP, de um endereço de *email* ou do nome de utilizador.

[24] Face à importância que os sistemas espaciais atualmente representam para a Defesa, a NATO reconheceu formalmente o Espaço como um domínio para a condução de operações, à semelhança do Mar, Terra, Ar e Ciberespaço, na reunião que decorreu em Londres, nos dias 3 e 4 de dezembro de 2019 (NATO, 2019).

2.3. Caracterização das ameaças no ciberespaço

A correta identificação e catalogação do conjunto de ameaças existentes no ciberespaço, capazes de conduzir ataques deliberados[25], é um fator essencial para se poderem definir e implementar estratégias adequadas para a proteção do ciberespaço. Visando a prossecução deste objetivo afigura-se como importante determinar numa primeira análise, as possíveis fontes de ameaças no ciberespaço, ou seja, o perfil dos atores com maior probabilidade de conduzirem ataques. Neste âmbito, de acordo com o IDN-CESEDEN (2013), as fontes de ameaça podem ser classificadas em: *Hackers*; *Hacktivistas;* pessoal interno às organizações; cibercriminosos; espiões industriais; terroristas; nações. Por sua vez, no que concerne às motivações para a condução dos ataques, verifica-se que, podem ser independentes da origem da ameaça e classificadas conforme se apresenta em seguida na Tabela 4.

Tabela 4 - Motivações e fontes de ameaças no ciberespaço (IDN-CESEDEN, 2013, pp. 23-24)

Motivações	Descrição	Fontes de Ameaça
Fama ou vingança	• A procura de fama está intrinsecamente ligada aos *hackers,* os quais procuram obter reconhecimento em diversas comunidades e fóruns. Para esse efeito e como *modus operandi* empenham-se em destronar as barreiras de segurança, sem causar danos significativos; • O pessoal interno de uma organização, também poderá ser movido pela fama, embora, por norma, as suas ações estejam mais relacionadas com o descontentamento e vingança.	• *Hackers;* • Pessoal interno de uma organização.
Benefícios Económicos	• Motivação mais frequente; • Consubstancia-se na prática de atos fraudulentos, no roubo de informações ou na realização de ataques (ou ainda na disponibilização de meios para esse fim) com vista à obtenção de benefícios económicos.	• Cibercriminosos; • Espiões Industriais; • Pessoal Interno.
Vantagens competitivas	• Motivação que pode suscitar a atuação de diferentes atores; • Poderá estar associada a roubo de segredos de um Estado; • Ou estar na génese na obtenção de informações sensíveis a organizações ou empresas que permitam dar uma vantagem competitiva a terceiros.	• Espiões Industriais; • Nações.
Motivações políticas,	• Estão na génese da condução de ações prejudiciais e de ataques contra organizações públicas e governos por parte de diferentes grupos ou organizações; • Também existem conflitos entre nações que têm origem em motivações desta natureza.	• Hacktivistas; • Terroristas.

[25] De acordo com o IDN-CESEDEN (2013, p. 22), as tipologias de ameaças à segurança das TIC, que podem afetar a confidencialidade, integridade e disponibilidade da informação manipulada ou da integridade e disponibilidade de um sistema de informação, pode ser agrupadas em: desastres naturais; ameaças de origem industrial; erros ou falhas não intencionais; ataques deliberados. Apesar do facto de ser bastante importante saber lidar com as ameaças provenientes das catástrofes naturais, de origem industrial, de erros ou falhas não intencionais, na presente investigação serão apenas analisados os ataques deliberados, dado ser este o objeto em estudo.

ideológica e religiosa[26]		
Destruição ou dano	• Motivação que se encontra intrinsecamente ligada aos terroristas, os quais procuram a execução de ataques com esse objetivo; • De igual modo, as nações que se encontram em conflito também poderão levar a cabo ataques que com este fim.	• Terroristas; • Nações.

Por conseguinte, com base na motivação e no perfil dos autores, as ameaças no ciberespaço podem, de acordo com o IDN-CESEDEN (2013), ser agrupadas em cinco categorias, nomeadamente: *hacktivismo;* cibercrime; ciberespionagem; ciberterrorismo; e ciberguerra. Não obstante esta catalogação, a realidade demonstra que cada uma destas categorias possui fronteiras bastante difusas podendo ocorrer sobreposição. Neste seguimento, apresenta-se graficamente na Figura 7, o espectro das ameaças existentes no ciberespaço, o qual resulta da disposição das cinco categorias mencionadas, tendo em consideração as motivações e as fontes de ameaças identificadas[27]. Em seguida abordar-se-á, sumariamente, cada uma destas categorias.

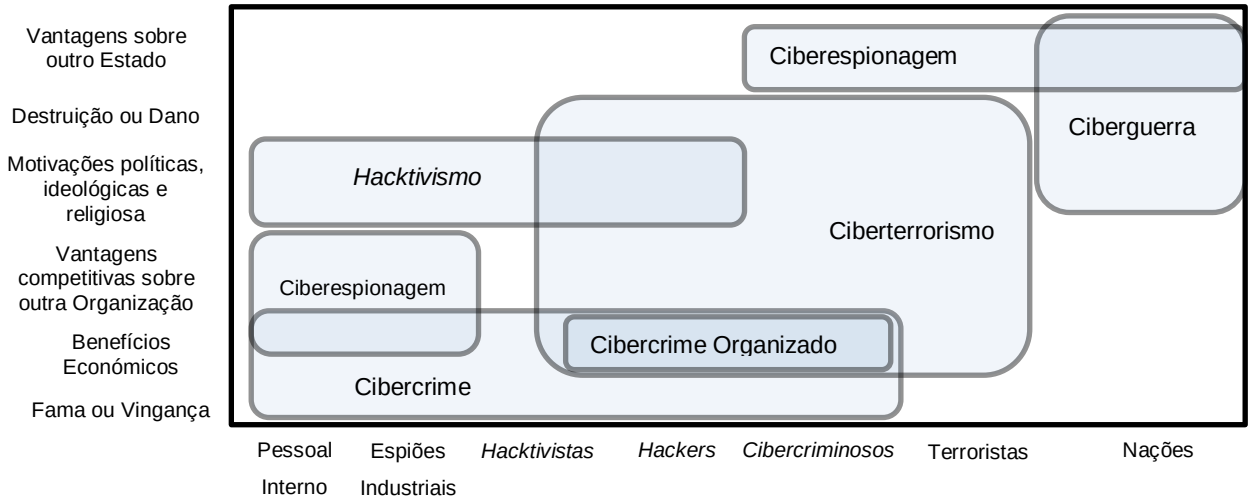

Figura 7 - Espectro das Ameaças ((Autor, 2020), adaptado de Santos (2011, p. 17))

2.3.1. *Hacktivismo*

No que concerne ao *hacktivismo* constata-se que este fenómeno se apresenta como uma ameaça face ao seu crescente impacto na sociedade. Sucintamente, por *hacktivismo* entende-se como a convergência entre o ativismo social e o *hacking*[28] tirando partido de uma possível cobertura mediática como forma de promoção de uma causa política (Denning, 2000). Assim, verifica-se que, conforme

[26] Embora o IDN-CESEDEN (2013), apenas identifique neste campo as motivações de ordem política, concorda-se com o apresentado por Santos (2011), ao acrescentar a estas, as motivações de ordem ideológica e religiosa.

[27] Especto de ameaças baseado no apresentado por Santos (2011), contemplando, por sua vez, as motivações e as fontes de ameaça identificadas nesta investigação. Além disso, e como principal diferença, é incluída no presente estudo a ameaça da ciberespionagem, corroborando-se com o defendido pelo IDN-CESEDEN (2013), também refletido na organização Portuguesa.

[28] Vd. conceito no Anexo A.

expõe Santos (2011, p. 27), o *hacktivismo* transporta para o ciberespaço as táticas do *hacktivismo* convencional, com o intuito de "chamar a atenção da opinião pública em geral, de um sector da sociedade ou da classe política, para a sua causa, tirando partido da cobertura mediática que a excentricidade e, por vezes, a espetacularidade que os seus métodos proporcionam".

O *hacktivismo* diferencia-se, quer do ativismo *on-line* que se caracteriza pela simples utilização das capacidades de comunicação da internet para a organização de uma agenda ou para a realização de ações de protesto, quer do ciberterrorismo, dado que a sua finalidade, ao contrário deste último, não pretende causar dano ou destruição, mas sim expressar uma ideia ou opinião.

Neste quadro, os casos de *hacktivismo* mais mediáticos foram conduzidos pelo grupo cognominado *Anonymous*[29], com destaque para os célebres ciberataques conduzidos nos finais de 2010[30] contra algumas grandes empresas, tais como a *Mastercard*, *PayPal* e *Amazon*, por terem atendido aos intentos do governo norte-americano, quer para bloquear as doações destinadas ao *Wikileaks*[31], no caso das duas primeiras, quer para impedir o acesso ao servidor que guardava o seu conteúdo, no caso da Amazon (Machado, 2015).

2.3.2. Cibercrime

Decorrente, em grande parte, da aplicação da capacidade técnica dos *hackers* na prática de crimes clássicos e de novos crimes proporcionados pelas novas tecnologias surge o fenómeno do cibercrime.

Neste quadro, a legislação portuguesa aglomera quatro tipos de atividade criminosa associada ao cibercrime, nomeadamente: **crimes com recurso a meios informáticos**[32]; **crimes relativos à proteção de dados pessoais ou da privacidade**[33]; **crimes informáticos em sentido estrito**[34], sendo o bem ou meio informático o elemento próprio do tipo de crime; **crimes relacionados com o conteúdo**[35]**.** Assim, nota-se que, conforme expõe o IDN-CESEDEN (2013), as principais motivações e as atividades que se inserem no âmbito do cibercrime se centram sobretudo na obtenção de benefícios económicos através da prática de ações ilícitas. Não obstante este ser o principal enfoque do

[29] Segundo Machado (2015), o A*nonymous* na sua essência trata-se de uma ideia e de um modo de ação partilhados por uma vasta, heterogénea e difusa rede de indivíduos e grupos. Além disso, não possui nenhum líder, recrutando e coordenando as suas ações em fóruns de conversação, tais como o *4chan* (um fórum de imagens onde os utilizadores conseguem permanecer anónimos*)* e em redes sociais. Em 2008, atingiram a fama ao conduzirem ataques contra a Igreja da Cientologia norte-americana, começando a realizar a partir de então, várias campanhas e ataques noutras áreas.

[30] Não obstante, já desde os meados de 1990, com a utilização generalizada das TIC, se tem observado a ocorrência de vários casos de *hacktivismo*. Neste âmbito, um claro exemplo deste tipo de ação, foi conduzido por vários grupos de hackers portugueses, na sequência dos massacres de Santa Cruz, em Timor Leste, a 12 de novembro de 1991. Esta ação de *hacktivismo* provocou o *web defacement* de diversos sites de internet indonésios, onde foi deixada a mensagem "Libertem Timor Leste" (Denning, 2000).

[31] *Wikileaks* é uma organização sem fins lucrativos, que visa partilhar informação, por vezes reservada e classificada. Esta organização defende a liberdade de expressão e de publicação dos *media*.

[32] Não alterando o tipo penal comum, correspondem a uma especificação ou qualificação deste, sendo exemplo a "devassa por meio de informática" (art.º 193º do Código Penal (CP)), o crime de burla informática e nas telecomunicações (art.º 221º do CP).

[33] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016.

[34] Neste grupo, inserem-se os crimes previstos na LC (Lei nº 109/2009, de 15 de setembro): falsidade informática (art.º 3); dano relativo a programas ou dados informáticos (art.º 4); sabotagem informática (art.º 5), acesso legítimo (art.º 6); interseção ilegítima (art.º 7); reprodução ilegítima de programa protegido (art.º 8).

[35] De onde se destacam a violação do direito de autor, a difusão de pornografia infantil (art.º 172º, nº 3, alínea d, do CP)) ou a discriminação racial ou religiosa (art. 240º, nº 1, alínea a, do CP)).

cibercrime, verifica-se que os crimes com recursos a meios informáticos podem ainda ser concretizados sobre a forma de ameaças, difamação, coação, usurpação, burla, pornografia de menores e extorsão (Cabreiro, 2016).

O cibercrime é um fenómeno transnacional que está a crescer e a desenvolver-se, quer em termos do número de ciberataques conduzidos, quer no que concerne ao seu impacto e sofisticação. Documentando este facto, a Tabela 5 apresenta uma relação de alguns dos mais mediáticos ataques de cibercrime ocorridos nos últimos 10 anos.

Tabela 5 - Relação de alguns ciberataques no âmbito do Cibercrime que ocorreram nos últimos 10 anos

Ano	Ciberataque	Descrição
2011	• Sony (Rede de PlayStation)	Ataque informático que "pirateou" as contas da PlayStation de 77 milhões de pessoas, tendo, ainda sido roubadas informações pessoais (nomes completos, e-mails, moradas, histórico de compras, números de contas bancárias, passwords, entre outros dados). Este ataque custou à Sony cerca 171 milhões de dólares, além de ter deixado a rede inoperacional durante cerca de um mês. Cfr. Soares (2018).
2013	• Yahoo	Ataque informático que tornou público os dados pessoais das contas de três mil milhões de utilizadores. Em concreto, foram expostos os nomes, os e-mails, as datas de nascimento, números de telemóveis e as próprias *passwords.* No decurso destes ataques, a Yahoo teve prejuízos avultados, até que em 2016 entrou em negociações com a Verizon para que esta a comprasse na totalidade Cfr. Soares (2018).
2016	• Candidatura de *Hillary Clinton*	No âmbito da candidatura de Hillary Clinton à presidência dos EUA, um ataque informático permitiu a apropriação de emails do partido democrata. Além disso, também foram divulgadas comunicações internas através do *site Wikileaks*. A CIA suspeita que este ciberataque foi obra de *hackers* ao serviço do governo russo, numa possível associação a membros da campanha de *Donald Trump*. Cfr. Soares (2018).
2017	• *WannaCry*	Estes ataques aproveitavam uma vulnerabilidade existente em versões antigas do sistema operativo *Windows*, nomeadamente num protocolo do *Windows Server* que permitia que os computadores comunicassem com outros computadores, impressoras e outros dispositivos conectados em rede. Através da existência desta vulnerabilidade, foi possível de forma remota, transmitir código malicioso do tipo *ransomware a* partir de um computador infecto para outros computadores conectados à mesma rede, bloqueando desta forma os computadores, encriptando toda a informação armazenada e exindo os atacantes um pagamento de 300 dólares em *bitcoins* para desbloquear o computador e a informação. Importa salientar, que a *Microsoft* disponibilizou um "*patch"* de segurança para corrigir esta vulnerabilidade, porém nem todos os utilizadores procederam à atualização do sistema (Simões, 2017). Segundo dados da empresa de segurança *Avast* foram infetados mais 230.000 computadores em todo o mundo, constituindo-se o W*annaCry* até aos dias de hoje, como o ataque do tipo *ramsomware* mais difundido no mundo. Cfr. *Avast* (2020).
2018	• *British Airways*	A companhia aérea britânica divulgou que os dados pessoais referentes a cerca de 380 mil clientes foram roubados por *hackers*. Cfr. Soares (2018).

2.3.3. Ciberespionagem

No que concerne às ameaças associadas à espionagem, constata-se que, estas não desapareceram com o términus da Guerra Fria. Ao invés, tornaram-se mais complexas e difusas devido ao aumento da concorrência económica entre as principais potências mundiais e do grande leque de ameaças que surgem à escala global. Nesta conjuntura, emergem com cada vez mais importância os riscos da exploração do ciberespaço por Estados e organizações, possuidores de grandes capacidades técnicas e de intentos, que colocam grandes desafios à segurança (SIS, 2020a).

Em consonância com o que se verifica na espionagem tradicional, infere-se que existem três tipos principais de ciberespionagem, nomeadamente: económica e industrial; política; militar (Kostadinov, 2013). Neste âmbito, a realidade demonstra que os casos em que a ciberespionagem não visa a obtenção de benefícios económicos no curto e médio prazo, através da venda da informação ou do aumento de competitividade, se encontra a ser conduzida a mando de um Estado. Esta circunstância é de acordo com Ribeiro (2019), especialmente, evidente nos casos de ataques perpetuados no tempo e com grande sofisticação tecnológica.

Tendo, ainda, em consideração os principais casos de ciberespionagem que têm sido tornados públicos nos últimos anos[36], nota-se que principalmente, três países têm vindo a ser mais acusados de ser incidentes nesta área, designadamente: os EUA, a Rússia e a China. Nos casos concretos da Rússia e da China, observa-se que estes dois países se têm dedicado, essencialmente, a atividades de recolha de informação na Europa e na América do Norte (CFR, 2020). Além disso, constata-se que na maioria dos casos estas atividades de ciberespionagem são realizadas por intermédio de agentes terceiros. Estes além de possuírem conhecimentos técnicos bastante avançados - permitindo uma eficiente e por diversas vezes indetetável recolha de informações – providenciam, nos casos das suas ações serem descobertas, um "manto protetor" para os verdadeiros orquestradores dos ataques. Em concreto, estes agentes inserem-se dentro do grupo de ameaças denominado de APT (IDN-CESEDEN, 2013).

Existem vários grupos de APT suspeitos de possuírem ligação aos serviços de informações Russos[37], sendo o APT 28 (também conhecido pelos cognomes *Fancy Bear, Pawn Storm Sofacy* e *Sednit Gang*) o mais mediático. Este grupo tem-se focado na condução de campanhas de desinformação, particularmente em países fronteiriços com a Rússia, e na obtenção de informação classificada e sensível de países membros da NATO. Para esse efeito, os principais alvos são os Ministérios de Soberania, tais como o Ministério dos Negócios Estrangeiros (MNE), Ministério da

[36] Um dos casos mais mediáticos e relevantes em que os EUA foram acusados de ciberespionagem, remonta a 2013, quando o antigo técnico da *Central Intelligence Agency* (CIA) e consultor da *National Security Agency* (NSA), *Edward Snowden*, divulgou vários detalhes sobre os programas de vigilância Global da NSA, entre eles, o mais conhecido, o programa "PRISM". Através deste programa, a NSA conseguia vigiar e monitorizar toda a atividade das telecomunicações a nível global, com a colaboração de várias empresas/organizações (*Microsoft, Google, Yahoo, Facebook, PalTalk, YouTube, Skype, AOL, Apple*, entre outras) que partilhavam os dados e conteúdos das comunicações de um determinado alvo ou suspeito. Em concreto, eram analisados os telefonemas, as atividades do cartão de crédito, mensagens nas redes sociais, sites da internet acedidos, mensagens de correio eletrónico, mensagens, chamadas *Skype,* fotografias, vídeos, IP, documentos transferidos, entre outros (The Washington Post, 2013).

[37] Neste âmbito, o *National Cyber Security Centre* (NCSC) do Reino Unido, apresenta uma relação de vários ciberataques ocorridos nos últimos anos, em que atribui claramente a responsabilidade pelo planeamento destes, aos Serviços de Informações Militares Russos (NCSC, 2018).

Administração Interna (MAI) e o Ministério da Defesa Nacional (MDN), e o seu modo de operação assenta, fundamentalmente, no comprometimento das contas de emails e na propagação de *malware* (NCSC, 2018). Neste âmbito, um caso concreto de ciberespionagem atribuído ao APT 28 e tornado público pelo Governo alemão, no final de fevereiro de 2018, consistiu no comprometimento de contas do MNE Alemão com a extração de informação. Após a análise dos dados, verificou-se que o ataque esteve em execução durante cerca de 8 meses até que as autoridades o conseguissem debelar.

De igual modo, a China é um Estado sistematicamente conectado à prossecução de atividades de ciberespionagem. Um dos grupos mais conhecidos com suspeitas de ligação à China é o APT 30. Este grupo tem traduzido a sua atividade na realização de espionagem industrial e/ou comercial, e na obtenção de informações que permitam ao Estado chinês estar preparado para um eventual futuro conflito (CFR, 2020).

2.3.4. Ciberterrorismo

O ciberespaço possui um conjunto características muito particulares que proporcionam também, aos grupos e/ou organizações terroristas grandes oportunidades para o desenvolvimento das suas atividades. Destas características, evidencia-se a elevada capacidade de processamento, o baixo custo de acesso, a facilidade de utilização e variedade de ferramentas, o carácter assimétrico, o anonimato e a capacidade para originar efeitos físicos.

Tendo por base estas características do Ciberespaço, Santos (2011) identifica e enuncia cinco vertentes em que a internet é utilizada como meio de suporte e promoção das atividades terroristas. Em primeiro lugar, a internet é amplamente utilizada para ocultar informação armazenada ou transmitida entre as organizações terroristas[38]. Em segundo lugar, constituindo-se a internet como uma gigantesca biblioteca de rápido e fácil acesso, constata-se que as organizações terroristas a utilizam como um meio privilegiado para obtenção de informação e planeamento de ataques. Em terceiro lugar, estas recorrem, também, à internet para concretizarem um dos seus principais objetivos: a propaganda. De facto, conforme evidencia Hoffman (2006), o terrorismo visa através da prática de violência atrair a atenção e transmitir uma determinada mensagem aproveitando a publicidade gerada. Em quarto lugar, observa-se que a internet é igualmente utilizada pelas organizações terroristas para promover e "impulsionar" a angariação de fundos essenciais ao suporte das suas atividades. Por fim, a internet é ainda utilizada como um meio de excelência para obtenção de apoiantes e recrutamento de ativos para a causa terrorista.

[38] Existem relatórios que evidenciam a utilização de técnicas de estenografia para a disseminação de informação na preparação dos atentados do 11 de Setembro de 2001 (Taylor E. et al, 2014). A esteganografia tem como finalidade esconder a presença de uma comunicação, através da introdução de uma mensagem secreta em documentos ou objetos inócuos e insuspeitos, tais como imagens digitais, vídeos e ficheiros de áudio. Deste modo, o ficheiro é transmitido através da internet para um destinatário que, com recurso à utilização de técnicas específicas (e por vezes a "chaves"), irá extrair a mensagem ocultada (J. Fridrich, 2001). De igual modo, a informação poderá ser escondida com recurso a técnicas de criptografia. A criptografia – "a arte de escrever em código", visa ocultar o significado da mensagem de modo a que apenas o seu recetor a consiga decifrar (Urgellés, 2016, p. 16). Releva-se nesta matéria, o caso em que o FBI, demorou cerca de um ano para decifrar os planos, que visavam a destruição de onze linhas aéreas norte-americanas, descobertos em casa de um terrorista condenado pelo ataque ao *World Trade Centre* em 1993 (Taylor E. et al, 2014).

2.3.5. Ciberguerra

"A ciberguerra está em curso e é permanente!" (Tribolet, 2020). Quem o afirma é o próprio presidente do Instituto de Engenharia de Sistemas e Computadores (INESC) do IST, José Tribolet, numa entrevista realizada no auge da crise entre os EUA e o Irão. Na realidade, na sequência da morte do General Iraniano *Qassem Soleimani*, por drones norte-americanos, em 27 de dezembro de 2019, o Irão prometeu retaliar este ataque sendo a hipótese de o fazer através de ciberataques a mais provável (Haynes, 2020). Porém, conforme se infere da afirmação do professor Tirbolet (2020), os ciberataques levados cabos por agentes estatais, não são uma novidade, já se realizam há muito tempo. Por exemplo, ainda no contexto da crise entre os EUA e o Irão, o governo norte-americano garantiu ter levado a cabo vários ciberataques contra as redes informáticas iranianas, utilizadas para controlar o sistema de lançamento de misseis, após a destruição de um *drone* norte-americano em junho de 2019 (Nakashima, 2019).

Em complemento às definições de ciberguerra, apresentadas no 1º Capítulo, importa tecer algumas considerações importantes. A primeira revela o facto de, na ciberguerra os alvos, corroborando com Tirbolet (2020), não são necessariamente militares, dado que os ciberataques podem ser dirigidos a infraestruturas vulneráveis da sociedade que suportam um adversário (i.e. IC e outras infraestruturas essenciais ao funcionamento do Estado). Uma segunda consideração resulta da análise dos mais relevantes e mediáticos ciberataques conduzidos em larga escala contra estados soberanos, tais como Estónia (2007), Geórgia (2008), Irão – *Stuxnet* (2010) e Ucrânia – *BlackEnergy* (2015), os quais, conforme afirma Fernandes (2012a, p. 60) "podem ser vistos como uma espécie de «guerras por procuração»". Com efeito, esta asserção de Fernandes (2012a) visa evidenciar o facto de, com frequência ocorrerem ciberataques contra estados nos quais a autoria é atribuída a agentes terceiros - tais como "cibercidadãos", *hacktivistas* ou "hackers patrióticos" - não sendo, responsabilizados, oficialmente, outros estados. Estes agentes, teoricamente, atuaram e atuam por sua livre iniciativa à margem e sem o consentimento dos estados onde residem e dos quais são cidadãos (Fernandes J. , 2012a). Nestas circunstâncias e após se analisarem os conflitos recentes enunciados emerge, ainda, uma terceira consideração que aponta no sentido de, mesmo nos casos da exploração mais hostil do ciberespaço, *per si* dificilmente se poderá considerar à luz do Direito Internacional vigente um ato de Guerra (Nunes, 2018).

Neste seguimento, abordar-se-ão em seguida, os principais casos da clara utilização do domínio operacional ciberespaço para a projeção de poder contra um Estado soberano evidenciando-se um aumento da sofisticação e da capacidade disruptiva dos ciberataques, causando efeitos, danos cinéticos e materiais cada vez maiores.

2.4. Os principais Ciberataques contra Estados

Em 2007, a Estónia foi alvo do primeiro grande ciberataque mediático e a comunidade internacional nunca mais olharia com a mesma leviandade para o impacto deste tipo de ataques. Pelo contrário, a partir deste momento, estes ataques passaram a ser entendidos como uma grande ameaça à segurança global com repercussões em todas as áreas de uma sociedade (Monteiro & Pinto, 2016). Entre abril e maio desse ano, a Estónia, alegadamente em consequência de uma situação de conflito

com a sua minoria russa[39], foi vítima de uma sequência de ciberataques, maioritariamente do tipo *Distributed Denial of Service*[40] (*DDoS*), aos servidores do Estado e de várias empresas provenientes de diversos países, conforme representado na Figura 8 (Traynor, 2007). Estes ataques prolongaram-se, por sensivelmente, dois meses provocando uma paralisação económica de consequências extremamente graves para o país.

Em agosto de 2008, durante a invasão russa na Geórgia, foram lançados diversos ciberataques para derrubar os sistemas bancários e os *sites* que noticiavam a invasão. Estes foram principalmente do tipo *Web Defacement*[41] e *DDoS,* tal como tinha ocorrido um ano antes na Estónia. Na origem dos ciberataques esteve o conflito armado, que opôs a Rússia à Geórgia, devido ao território da Ossétia do Sul[42] e reconhecido como parte integrante da Geórgia. Este território declarou independência no início da década de 1990 e pretendia unir-se à Ossétia do Norte, uma república autónoma, da Federação Russa. Os ciberataques foram levados a cabo por *hackers* russos com os quais o governo russo nunca admitiu qualquer envolvimento (CNN, 2019)[43].

Figura 8 – Representação da distribuição geográfica da origem dos ataques DDoS à Estónia 2007
(Ribeiro, 2019)

Em 2010, a sofisticação dos ciberataques alcançou um novo nível com a sabotagem das centrifugadoras de enriquecimento de urânio, do complexo de *Natanz*, utilizadas no programa nuclear do Irão. Estes ataques foram levados a cabo através do *malware Stuxnet*[44] desenvolvido,

[39] Vários autores referem que os ciberataques surgiram na sequência da decisão do governo da Estónia de mover, do centro da cidade para um cemitério na periferia da capital, Tallin, uma estátua de bronze de um soldado soviético da Segunda Guerra Mundial, a 27 de abril de 2007. Esta ação desencadeou vários protestos, tanto na Rússia como na Estónia, que foi ocupada pela União Soviética durante uma grande parte da Guerra Fria e, onde vive uma minoria russa. Segundo as autoridades Estónias, os ciberataques teriam sido ordenados pela Rússia, em retaliação pela remoção da estátua. Contudo, apesar de ter mostrado descontentamento e ter classificado a ação como "desumana", o governo russo negou qualquer envolvimento nos ataques (Traynor, 2007)

[40] Vd. conceito Anexo A.

[41] Vd. conceito Anexo A.

[42] Região separatista da Geórgia. Situa-se na zona montanhosa do Cáucaso que faz fronteira com a Ossétia do Norte.

[43] Os ciberataques duraram até ao final do mês de agosto, e a 26 de agosto de 2008, o presidente russo Dmitri Medvedev, anunciou que a Rússia reconhecia a independência da região separatista da Ossétia do Sul (CNN, 2019).

[44] O *Stuxnet* é considerado por diversos autores como a primeira *ciberarma* tornada pública, capaz de destruir máquinas, tendo este ataque em concreto, retardado, significativamente, o programa de enriquecimento de urânio Iraniano, ao danificar cerca de mil centrifugadoras (Natário & Nunes, 2014).

especificamente, para um ataque aos sistemas *Supervisory Control and Data Acquisition* (SCADA)[45] das IC. No plano técnico, a grande novidade do *Stuxnet,* em relação aos vírus até então conhecidos, assentou na capacidade de injeção de código nos Sistemas de Controlo Industrial (SCI) no caso concreto da empresa alemã *Siemens* (Figura 9). Os dados divulgados revelam que o *Stuxnet* foi deteriorando as centrifugadoras, durante aproximadamente um ano, até ser detetado pelas autoridades iranianas. Tendo em conta a sofisticação do S*tuxnet* e os recursos necessários para sua concretização, somente ao alcance de alguns Estados[46], fontes sugerem o alegado envolvimento dos EUA e Israel na origem destes ciberataques (Falliere, Murchu, & Chien, 2011).

Em 2014, no decurso das operações militares que conduziram à anexação da Crimeia pela Rússia, foram executados vários e persistentes ataques do tipo DDoS a serviços governamentais ucranianos. Estes ataques atingiram proporções, nunca antes observadas, tendo sido registados valores de tráfego 32 vezes superiores aos ataques aos sistemas da Geórgia em 2008 (Baezner, 2018).

No ano seguinte, a 23 de dezembro de 2015, a Urânica foi novamente alvo de ciberataques, desta feita, através de um vírus denominado por "*BlackEnergy*"[47], que afetou os sistemas de uma central elétrica ucraniana deixando sem aquecimento milhares de pessoas em pleno inverno. Na prática, estes ataques neutralizaram os SCI da central elétrica sem a possibilidade de restauração remota dos sistemas. Desde modo, para a mitigação e recuperação deste ataque, foi necessário proceder à operação manual dos sistemas da central elétrica por forma a repor o fornecimento de energia à população. O governo ucraniano acusou a Rússia de ser a responsável pelo ataque (Baezner, 2018).

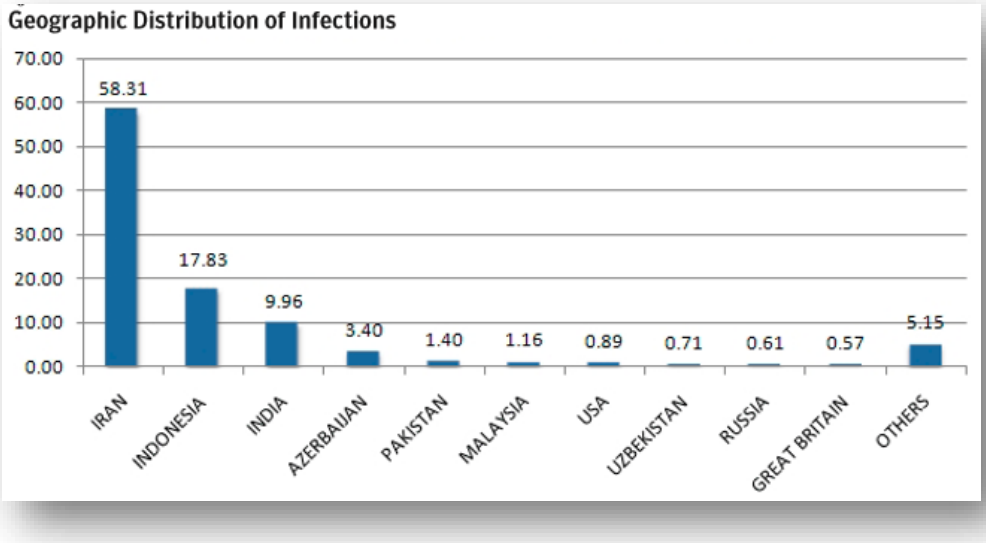

Figura 9 - Incidência geográfica dos ataques com o *malware Stuxnet* aos SCI *Siemens Step 7* entre julho e setembro de 2010 (Falliere et al. 2011, p. 6).

[45] São o maior subgrupo dos Sistemas de Controlo Industrial (SCI). Encontram-se presentes em quase todos os setores industriais, sendo por norma, o tipo de sistema utilizado na gestão dos processos das IC (ENISA, 2011).

[46] Tese também defendida por Fidler (2011), o qual considera o *Stuxnet* como um acto deliberado, contínuo e ofensivo, levado a cabo por meios e métodos inovadores à data, com a finalidade de destruir total ou parcialmente, concretizado, sem sombra de dúvidas, por um ou vários Estados, contra um Estado opositor.

[47] De acordo com os especialistas da *Endpoint Security*, estes ciberataques utilizaram o *Malware* tipo "cavalo de troia" denominado por *BlackEnergy*, para introduzir um componente designado por "*KillDisk*" nos computadores alvo, com o objetivo de eliminar os ficheiros de sistema e sabotar os SCI utilizados, neste caso, para controlo da produção de energia da central (Cherepanov & Lipovsky, 2016).

Como conclusão, e em resultado destes ciberataques, sublinha-se o exposto pelo IDN-CESEDEN (2013, p. 8), ao afirmar que cada "estado terá de garantir não só a utilização segura do ciberespaço aos seus cidadãos como a salvaguarda da própria soberania". Perante este facto, abordar-se-ão em seguida os conceitos de soberania e fronteira e procurar-se-á verificar em que medida o ciberespaço coloca em causa estes conceitos milenares.

2.5. Ciberespaço e os conceitos de Soberania e Fronteira

Em função da complexidade e da dimensão dos conceitos de Soberania e Fronteira tenciona-se, apenas, expor os conceitos e verificar em que medida o ciberespaço os desafia.

2.5.1. Conceito de Estado e Soberania

O conceito de soberania encontra-se intrinsecamente ligado ao conceito de Estado, pelo que importa elucidar, primeiramente, em que consiste este último conceito. É neste contexto que Jorge Miranda afirma que "a moderna ideia Estado tem o seu expoente na ideia de soberania" (Miranda, 2003, p. 43)[48].

Segundo Marcello Caetano, o conceito de Estado[49] define "um povo, fixado num território de que é senhor, e que institui, por autoridade própria, órgãos que elaborem as leis necessárias à vida coletiva e imponham a respetiva execução" (Caetano, 1973, p. 16). De igual modo, Marcelo Rebelo de Sousa afirma que o Estado é "um povo fixado num determinado território que institui por autoridade própria, dentro desse território, um poder político relativamente autónomo" (Sousa, 1978, p. 108). Deste modo, verifica-se que em ambas as definições, estão presentes os seguintes três elementos: povo, território e poder político.

A afirmação do Estado Moderno dotado de soberania materializou-se no seio das relações internacionais a partir da "Paz de Vestefália" em 1648 (Holsti, 1991)". Com efeito, a denominada "Paz de Vestefália", também apelidada como os Tratados de Munster e Osnabruck, além de formalizar o términus da Guerra dos Trinta Anos[50] marcou a transição histórica da sociedade medieval, dominada pelo poder da Igreja, para uma sociedade assente no ideal do Estado Moderno vinculado à noção de soberania e à centralização do poder político. É nesta senda que Kalevi Holsti sublinha que com a "Paz de Vestefália" "o sistema de Estados substituiu o sistema hierárquico sob a autoridade do Papa e dos Habsburgos" (Holsti, 1991, p. 26)".

[48] Apesar de, conforme elucida António José Fernandes, nem todos os Estados serem soberanos, uma vez que "para que um Estado seja soberano, o poder de querer e o poder de comandar não podem estar subordinados a nenhum outro" (Fernandes A. J., 1995, p. 92).

[49] Neste âmbito, importa referir que os conceitos de Estado e Nação são indissociáveis na medida em que conforme refere António Santos (2005, p. 14) "o Estado afirma-se assim como uma instituição política legitimada pela Nação, detentora da soberania que é recusada aos monarcas, os quais, desde a remota Antiguidade Oriental procuram justificá-la, identificando-a com a expressão da vontade dos deuses, que presidem aos destinos dos mortais".

[50] Um dos conflitos mais devastadores ocorridos na Europa decorreu, entre 1618 e 1648, sobretudo na Alemanha envolvendo grande parte dos países da Europa Ocidental. Na origem do conflito estiveram razões de cariz religioso ao abrigo do contexto da reforma Protestante. Porém, à medida que o conflito se foi desenrolando emergiu outras razões de disputa alicerçadas em rivalidades comerciais, lutas pelo poder e procura da hegemonia europeia, sobretudo entre o Império Sueco e a França contra a Monarquia dos Habsburgos (Infopédia, 2020).

Quanto ao conceito de Soberania, propriamente dito, este surgiu no séc. XVI principalmente com Bodin o qual refere que *"*soberania integra as características do poder absoluto com uma unidade que se sobrepõe à complexa rede de suseranias e de homenagens, de laços hierárquicos pessoais, ao parcelamento da autoridade, à confusão entre poderes públicos e privados existentes no feudalismo" (Santos A. R., 2005, p. 59). Por sua vez, Adriano Moreira (1997, p. 292) refere que "o conceito de soberania é o elemento organizador, ao mesmo tempo ideológico e estrutural. Trata-se do poder absoluto perpétuo de uma República".

Porém, o conceito de soberania sofreu uma evolução incontornável, fruto de diversos fatores, sendo os mais significativos a globalização e transferência de competências dos Estados para Uniões Económicas e Políticas, como é o caso da União Europeia (UE). Assim, como refere António Alves Pereira (2003):

> "não há, definitivamente, que falar em soberania absoluta, uma vez que este é um conceito desenvolvido à época do fastígio do eurocentrismo (…) sendo uma categoria político-jurídica de natureza eminentemente histórica, portanto, variável no tempo e no espaço, a soberania passa, nos dias atuais, por uma completa transformação" (Pereira, 2003, p. 20).

Não obstante, a panóplia de novas definições de soberania emergentes, as quais tentam retratar a nova ordem internacional, toma-se em consideração a definição exposta pelo IDN (2013, p. 2), referindo que "soberania significa independência e liberdade nacional, garantia da integridade do território, defesa do regime constitucional e salvaguarda coletiva de pessoas e bens … justifica a existência do Estado".

2.5.2. Conceito de Fronteira

Segundo o dicionário da língua portuguesa (2020), por fronteira entende-se como: a linha que delimita territorialmente um Estado, fixando a sua extensão; a linha que separa dois países, regiões, territórios, estrema; zona adjacente a essa linha.

Assim, verifica-se que, conforme refere Ribeiro (2001), a variedade de palavras que procuram elucidar o significado de fronteira evidencia a sua polissemia. Com efeito, o mesmo autor (2001) refere que, o aparecimento do termo ocorreu em meados do no século XIII a partir da palavra de origem *la front* – que designava o limite temporário e flutuante que separava dois exércitos numa batalha. Posteriormente, na era moderna, o conceito foi associado à noção de soberania, tendo o advento da linha fronteiriça acompanhado o desenvolvimento da conceção moderna de espaço, contribuindo inclusive para o aperfeiçoamento da cartografia e das estratégias militares.

Com o projeto colonial, a fronteira do Estado foi exportada para além da Europa e impôs-se ao planeta (Albaret-Schulz, 2004). Com a globalização diversos teóricos debruçaram-se sobre a temática das fronteiras nacionais tendo, conforme expõe Ribeiro (2001), surgido novas abordagens ao conceito para além da definição estritamente física. É também neste sentido, que Adriano Moreira (2011) afirma que na ordem atual, as fronteiras são de natureza múltipla e não apenas geográficas.

Não obstante, concretamente quanto à fronteira geográfica, conforme menciona Marchueta (2002), é um dos elementos que contribuem para que um Estado soberano seja distinto dos demais,

por circunscrever, num determinado território um povo, a sua cultura e o alcance dos órgãos de governação. Deste modo, verifica-se que a fronteira tradicional se constitui como um dos alicerces da soberania e da inserção diferenciada do Estado na ordem política internacional.

Acresce que com o advento da globalização e do desenvolvimento tecnológico, a fronteira geográfica tem vindo a perder relevância estratégica, mantendo-se esta como o último reduto a defender a todo o custo (Santos L. , 2001). É neste sentido que Adriano Moreia (2011) afirma que o sangue derramado durante o estabelecimento das fronteiras constitui um dos fundamentos do seu valor supremo.

2.5.3. Ciberespaço uma nova dimensão sem fronteiras

A internet assume-se como "uma dimensão de comunicação livre", constituindo-se como "um símbolo de liberdade e de capacidade para dominar o tempo e o espaço" pela sua acessibilidade, universalidade e por conduzir o processo de globalização (Wolton, 1999, p. 92). Por conseguinte, facilmente se infere que o ciberespaço desafia em larga medida o conceito de fronteira geográfica exposto anteriormente. Adicionalmente, o ciberespaço é também considerado um *global common* onde se defende uma utilização responsável, partilhada e livre, e sobre o qual nenhuma nação deverá reivindicar soberania[51].

Contudo, alguns estados com ideologia mais securitária demonstram uma tendência para a colocação de limites no mundo virtual. Neste sentido, emergem vários críticos que defendem esta limitação, dos quais se destacam Demchak e Dombrowski (2011, p. 40), afirmando que a edificação de "uma ciberfronteira nacional é tecnologicamente possível, psicologicamente confortável, sendo também sistematicamente e politicamente gerível". Este facto é, claramente, observado na China através da denominada "Grande *Firewall*[52] da China[53]" e mais recentemente na Rússia, com a implementação da *Runet*[54]*, i.e.,* uma rede nacional russa alternativa à internet global. Estes dois casos denotam claramente que se está perante o início de um processo de criação de fronteiras no ciberespaço.

Não obstante, esta corrente mais securitária de controlo do ciberespaço estar a ganhar cada vez mais defensores, Portugal, conforme defendeu o Ministro da Defesa Nacional, João Gomes Cravinho (2019), entende o ciberespaço como um bem comum da humanidade no qual as regras de uso

[51] Uma das correntes de pensamento que mais veemente defende as regras do uso partilhado e livre do ciberespaço, denomina-se por "Utopia Libertário-Anárquica do Ciberespaço", em alusão ao livro de Nozick (1977) originalmente publicado em 1974**.** Esta designação é frequentemente utilizada para descrever a "anarquia" dos primeiros tempos da internet, onde se defendia que os governos se deveriam abster de criar quaisquer legislações reguladoras deste "novo mundo". Ao invés, seriam os próprios utilizadores que se deveriam regular, pois teriam possibilidades de o fazer com mais justiça do que se fossem geridas pelos governos (Fernandes J. , 2012).

[52] Vd. conceito Anexo A.

[53] A grande *firewall* da China, também denominada por Escudo Dourado, é um sistema de vigilância e censura, implementado internamente naquele país, para controlar a utilização da internet pelos seus cidadãos, tendo sido assim apelidado em alusão à Grande Muralha da China (August, 2007). Este sistema tem como objetivo monitorizar, filtrar e/ou bloquear conteúdos considerados sensíveis pelas autoridades chinesas. Um curioso artigo sobre esta temática, sobre o qual se recomenda a sua leitura, foi escrito por Oliver August (2007), e publicado na revista *Wired*, o qual compara a Grande *Firewall* da China com a Grande Muralha.

[54] Em Dezembro de 2019, o Governo Russo anunciou que os testes realizados à internet nacional russa – a *Runet* - tinham sido bem-sucedidos. Com a implementação da *Runet,* a Rússia poderá, à semelhança da China e do Irão, controlar os "pontos" de encaminhamento por onde entram e são transmitidos os dados do país, permitindo quer, bloquear o tráfego que vem do exterior do país – p. ex. no caso de ser alvo de ciberataques -, quer, impedir o acesso dos seus cidadãos a conteúdos externos (Wakefield, 2019).

partilhado, livre e responsável devem ser respeitadas. Porém, como o mesmo sublinha, "o ciberespaço não pode ser um domínio em que há descontrolo total e uma ausência de regras (Cravinho, 2019, p. 8).

2.6. Síntese Conclusiva

Da análise realizada ao ambiente ciberespaço conclui-se que este se caracteriza, fundamentalmente, por: possuir um carácter muito dinâmico; ostentar um enorme potencial de crescimento; deter uma elevada capacidade de armazenamento e processamento de informação; potencializar a assimetria, originada pelo grande desequilíbrio entre os possíveis elevados danos e os reduzidos meios necessários para os concretizar; predominar o anonimato e a consequente dificuldade de imputação; a facilidade de um ator mistificar a sua presença; ser transversal e interdependente a todos os setores de uma sociedade; não possuir regulação adequada; ampliar a vulnerabilidade humana; ter um reduzido custo de acesso; os seus efeitos se repercutirem no mundo físico, pese embora, seja um espaço virtual; as infraestruturas encontram-se geograficamente dispersas, logo, submetidas a diferentes quadros legislativos e à intervenção de diversas entidades internacionais; existir uma indefinição dos limites das fronteiras no ciberespaço.

Perante a criticidade que o ciberespaço desempenha no garante da segurança e proteção dos Estados, verifica-se, ainda, que este ambiente se traduz num novo domínio para a condução de operações militares. Efetivamente observa-se que no ciberespaço são conduzidas operações militares cada vez mais importantes ao suporte e concretização das operações realizadas nos domínios físicos.

No que concerne à caracterização das ameaças presentes no ciberespaço, conclui-se que a correta identificação e catalogação do conjunto de ameaças existentes, capazes de conduzir ataques deliberados, é a chave para se poderem definir e implementar estratégias adequadas para a promoção e materialização da segurança do ciberespaço. Neste contexto, tendo por base a motivação e o perfil dos seus autores, as ameaças no ciberespaço podem ser agrupadas em cinco categorias principais, nomeadamente: *hacktivismo*; cibercrime; ciberespionagem; ciberterrorismo; e ciberguerra.

Numa outra dimensão, constata-se que o ciberespaço se particulariza por desafiar, em larga medida, os conceitos tradicionais de Soberania e de Fronteira. Perante isto, tomando os Estados consciência dos impactos que os ciberataques podem causar nas suas IC, e na sociedade em geral, tal como ficou evidente nos casos abordados da Estónia (2007), Geórgia (2008), Irão (2010), Ucrânia (2014) e Ucrânia (2015), denota-se que a utopia libertário-anárquica que dominou nos primórdios da internet está progressivamente a dar lugar a mecanismos de controlo e de afirmação da soberania dos Estados. Este aspeto encontra-se a ser materializado através da criação de "fronteiras" no ciberespaço, tal como evidenciam os casos da "Grande Firewall da China" e da *Runet*.

Por fim, perante o exposto ao longo deste capítulo e da análise resultante, considera-se que se obteve resposta à QD1 – "Como se caracteriza o atual ambiente ciberespaço?", na medida em que foram elencadas as principais características deste ambiente, expôs-se a razão pela qual é considerado um novo domínio das operações e caracterizou-se o espectro das ameaças existentes no ciberespaço.

3. Segurança no Ciberespaço

> "A segurança, (…), é uma responsabilidade coletiva onde todos os atores, sejam públicos ou, privados, devem cooperar para que, juntos, possamos estar mais preparados para as ameaças que conhecemos e que desconhecemos". Contra-Almirante Gameiro Marques, Diretor-geral do Gabinete Nacional de Segurança (Marques, 2019, pp. 7-8)

Os ciberataques de que a Estónia em 2007, a Geórgia em 2008, o Irão em 2010 (*Stuxnet*) e a Ucrânia em 2014 e 2015 foram alvos vieram despertar as autoridades nacionais e internacionais para uma nova realidade. Se há muito se debatia sobre a utilização da tecnologia nos conflitos tradicionais e nos ciberconflitos de cariz assimétrico, e sobre os impactos que estes teriam nas sociedades mais dependentes das TIC, estes ciberataques evidenciaram ser urgente edificar, desenvolver e empregar um conjunto de medidas com vista à proteção e defesa do ciberespaço limitando a sua exploração para fins maliciosos (Santos, Bravo, & Nunes, 2012).

3.1. Domínios e Áreas de Competência

Apesar de na atualidade se denotar a existência de uma opinião generalizada e transversal a muitos sectores da sociedade que defende a necessidade de se desenvolverem medidas adequadas para garantir a proteção e defesa do ciberespaço verifica-se que, na prática, estas são de difícil materialização e implementação. Tal assim se sucede, porque, para além das características muito particulares deste ambiente elencadas no capítulo anterior - que já de si, exigem a sua plena observância para a eficiente implementação de medidas - no ciberespaço as ameaças são também maioritariamente difusas. Acresce que estas se caracterizam por atuarem sobre a forma de anonimato, gerando incerteza na identificação dos autores, pela indefinição temporal da ameaça e pela imprevisibilidade dos efeitos consequentes à sua concretização. Estes fatores, conjugados com o cenário de ameaça assimétrica que paira atualmente na cena internacional, oferecem igualmente dificuldades acrescidas dado que, conforme enfatiza Santos (2011, p. 45), "resultam enormes dificuldades na gestão do risco, definição de políticas e prioritização de investimentos, sejam eles públicos ou privados".

Deste modo, os estados para enfrentarem os desafios e o conjunto de ameaças que existem no ciberespaço, do mesmo modo que o fazem para lidar com as ameaças transnacionais e assimétricas, deverão, conforme elucidam Santos *et al*. (2012, p. 2), desenvolver e implementar um conjunto de "domínios de atuação"[55] nos quais devem focar as suas políticas e estratégias tendo em vista a salvaguarda dos interesses nacionais. Neste seguimento, Santos (2018) identificou os seguintes domínios de atuação: proteção simples; prossecução criminal; guerra e defesa do Estado; diplomacia.

Após analisar-se, detalhadamente, cada um destes planos propostos e descritos, inicialmente por Santos *et al.*, (2012) e complementados por Santos (2018), considera-se, numa primeira análise,

[55] Também designados por Santos (2018), de "planos de atuação". O conceito de "domínios de atuação" em que se baseia a presente investigação, encontra-se exposto no Anexo A, tendo estes sido elencados por Santos *et al.* (2012), tendo por base a sistematização realizada por Pedahzur (2009) relativamente ao contra-terrorismo, atendendo às semelhanças e às diferenças entre o fenómeno de terrorismo e os ciberataques.

ser mais adequado enquadrar-se cada um destes planos no âmbito da ENSC 2019-2023. Assim, na presente investigação, os principais domínios que contribuem para a segurança do ciberespaço nacional serão designados da seguinte forma: o da proteção simples como o domínio da cibersegurança; o da prossecução criminal como o domínio do combate ao cibercrime; o da guerra e da defesa do Estado como o da ciberdefesa; ao da diplomacia será adicionado o prefixo *ciber*, denominando-se de ciberdiplomacia, acrescentando-se a este a área da cooperação nacional e internacional. Por outro lado, e em linha com o exposto na ENSC 2019-2023, considera-se que as informações contribuem de forma decisiva para a segurança no ciberespaço, pelo que este domínio será também incluído nesta análise. Face ao exposto, em seguida descrever-se-á, sumariamente, cada um dos domínios que contribuem para a segurança no ciberespaço nacional, conforme apresentados na Figura 10, elucidando-se as respetivas áreas de competência das principais entidades com responsabilidade em cada um deles.

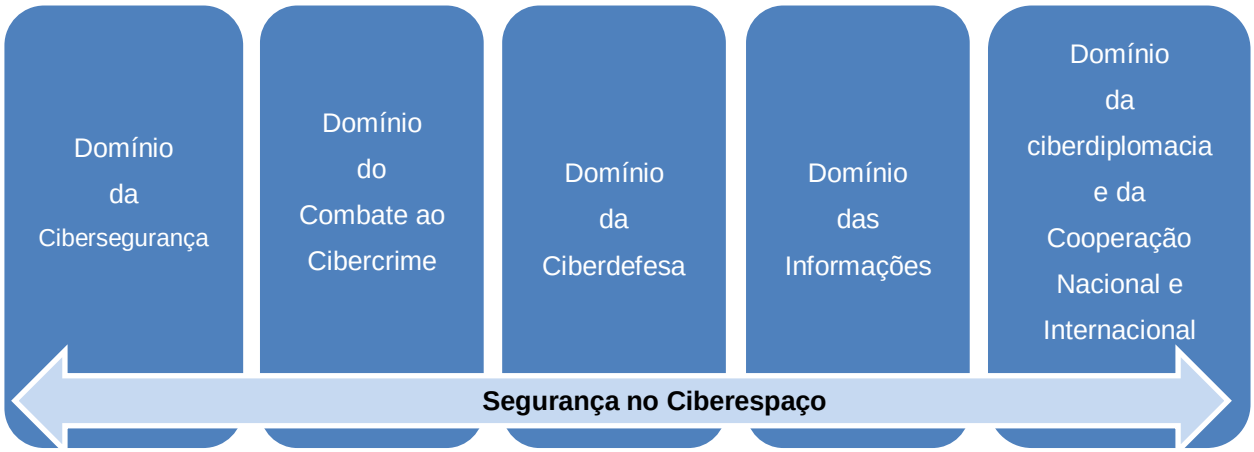

Figura 10 - Principais domínios que contribuem para a segurança do ciberespaço (Autor, 2020)

3.1.1. Domínio da Cibersegurança

Em traços gerais, o domínio da cibersegurança engloba os recursos técnicos, processuais e humanos que visam garantir, numa primeira instância, a Segurança da Informação (SI), dado que esta é, efetivamente, a primeira barreira de proteção das infraestruturas, dos serviços e da informação no ciberespaço. Assim, um ciberataque é interpretado como uma sequência de ações destinadas a produzir um efeito não autorizado ou uma perturbação não desejada na confidencialidade[56], na integridade[57] ou na disponibilidade[58] da informação ou num serviço.

Para além disso, em virtude de o ciberespaço, por um lado ser um domínio utilizado, quer por estados, quer por organizações transnacionais para a asserção do seu poder geoestratégico, e por outro as fronteiras de atuação entre as principais entidades com responsabilidade na segurança do ciberespaço serem bastante difusas, poder-se-á, de acordo com Marques (2020), afirmar que a cibersegurança possui quatro dimensões, designadamente: defesa; "segurança interna"; económica; cidadania. Em maior detalhe, a dimensão de defesa centra-se no exercício da soberania e da proteção

[56] Vd. conceito Anexo A.
[57] Vd. conceito Anexo A.
[58] Vd. conceito Anexo A.

dos interesses de um Estado no ciberespaço, nomeadamente por intermédio do planeamento e execução de *Computer Network Operations* (CNO)[59]. Por sua vez, a dimensão da "segurança interna" releva o contributo da cibersegurança para o combate ao cibercrime, para a proteção das IC e dos prestadores de serviços essenciais. A dimensão de mercado foca a cibersegurança enquanto "agente" acelerador e facilitador da economia digital. Por último, a dimensão de cidadania que atenta à preservação dos direitos, liberdades e garantias dos cidadãos neste ambiente. A Figura 11 sintetiza esquematicamente as 4 dimensões da cibersegurança enunciadas.

Figura 11 – As dimensões da cibersegurança (Marques, 2020, p. 17)

Por outro lado, verifica-se que a diferentes níveis contribuem para a cibersegurança os Estados, os fabricantes de produtos de *software*, *hardware* e de processos, os técnicos que administram as redes e os sistemas, as instituições reguladoras sectoriais, as escolas, as C*omputer Security Incident Response Team* (CSIRT) e ainda o utilizador final da tecnologia (no que se denomina de "ciber-higiene"[60]) (Santos L. , 2018).

No que concerne à indústria das TIC constata-se que esta desempenha um papel relevante na cibersegurança, dado que é, desde logo, responsável pela existência de algumas das vulnerabilidades nos produtos e aplicações que desenvolve as quais são objeto de exploração para a realização de ciberataques[61]. Neste quadro, evidencia-se a imperatividade dos produtos e aplicações concebidos pela indústria das TIC possuírem, como norma, o *security by design*[62] e quem os adquira exija que tal assim seja (Marques, 2017).

Por outro lado, a indústria das TIC em conjunto com as academias e universidades contribuem, consideravelmente, para a pesquisa e desenvolvimento de soluções de segurança. Não obstante, para a eficiente utilização destas soluções é essencial que os administradores de redes e sistemas das

[59] As CNO ou Operações no Ciberespaço incluem no seu âmbito a condução de ações de natureza defensiva, de exploração das capacidades dos possíveis adversários ou, inclusive, de resposta de cariz ofensivo (IDN-CESEDEN, 2013). De acordo com a doutrina do Departamento de Defesa dos EUA, as CNO compõem-se das seguintes capacidades: *Computer Network Defense (CND); Computer Network Exploitation (CNE); Computer Network Attack (CNA).* Os respetivos conceitos encontram-se apresentados no Anexo A.

[60] Palavra que deriva do termo anglo-saxónico *Cyber Hygiene* e que visa retratar os cuidados básicos de segurança que os Estados, as organizações e os cidadãos deverão ter no ciberespaço. Vd. conceito Anexo A.

[61] Um exemplo claro deste facto foi o caso dos ataques do tipo *ransomware* conduzidos, em larga escala em todo o mundo a partir de maio de 2017, através do vírus designado de *Wannacry*, conforme descrito, em maior detalhe, no subcapítulo 2.3.2 da presente investigação.

[62] Vd. conceito no Anexo A.

organizações possuam sólidos conhecimentos e bons recursos técnicos ao seu dispor, condição que, apenas será possível através de um robusto investimento público e privado em tecnologia e formação (Santos *et al.*, 2012).

Para que esta grande variedade de entidades e agentes possam *per si* tomar as medidas mais adequadas para a proteção no ciberespaço é necessário, ainda, promover a adoção de normas e de boas práticas comuns fomentando-se a utilização de uma taxonomia e um referencial de controlo de segurança uniforme[63]. Por fim, com o propósito de incrementar e sustentar a capacidade de resposta aos ciberincidentes foram criadas as *Computer Emergency Response Team* (CERT) ou CSIRT[64], com as funções essenciais de alerta e de reação aos incidentes. Em virtude dos ciberincidentes não se cingirem às fronteiras físicas de uma organização ou de um país e os seus efeitos se repercutirem a uma escala global é absolutamente fundamental, para o desempenho de uma CSIRT, fomentar e robustecer a cooperação nacional e internacional[65] (Santos L. , 2018).

Em Portugal, o CNCS[66] é a Autoridade Nacional de Cibersegurança e tem como missão:

> "contribuir para que o país use o ciberespaço de uma forma livre, confiável e segura, através da promoção da melhoria contínua da cibersegurança nacional e da cooperação internacional, em articulação com todas as autoridades competentes, bem como da implementação das medidas e instrumentos necessários à antecipação, à deteção, reação e recuperação de situações que, face à iminência ou ocorrência de incidentes ou ciberataques, ponham em causa o funcionamento das infraestruturas críticas e os interesses nacionais" (GOV-PT, 2014, p. 2712).

Integrada no CNCS opera a equipa nacional de resposta a ciberincidentes denominada por CERT.PT[67]. Esta equipa tem como função coordenar a resposta a incidentes envolvendo entidades do Estado, operadores de IC nacionais, operadores de serviços essenciais e prestadores de serviços digitais. Num quadro mais amplo e transversal existe, ainda, a Rede Nacional de CSIRT[68] que integra, atualmente, mais de quarenta e cinco membros - a maioria do sector privado. Neste contexto,

---

[63] Neste universo, salienta-se a publicação denominada Quadro Nacional de Referência para a Cibersegurança (QNRCS), desenvolvida pelo Centro Nacional de Cibersegurança (CNCS) que tem como finalidade disponibilizar as bases para que qualquer organização possa cumprir os requisitos mínimos de segurança das redes e sistemas de informação, reduzindo assim o risco proveniente das ciberameaças (CNCS, 2019).

[64] Conforme elucida o IDN-CESEDEN (2013), CERT é, provavelmente, o termo mais utilizado internacionalmente para designar uma Equipa com Capacidade de Resposta a Incidentes Informáticos, tendo sido, inclusive, a primeira marca registrada para retratar este tipo de equipas no final da década de oitenta. Porém, este termo foi protegido pela Universidade *Carnegie Mellon* nos EUA, razão pela qual, quando se implementou este modelo na Europa, foi dada a designação de CSIRT.

[65] Neste quadro, a nível Europeu, a Diretiva *Network and Information Security* (NIS), Diretiva (UE) n.º 2016/1148, do Parlamento Europeu e do Conselho (PEC), veio reforçar o papel das CSIRT através da promoção da harmonização de capacidades, da colaboração transfronteiriça e da supervisão de setores críticos, com o objetivo último, de edificar-se uma rede Europeia de reação a ciberincidentes (PEC, 2016).

[66] Criado em outubro de 2014 na sequência da publicação do DL n.º 69/2014 de maio (2ª alteração à Lei orgânica do GNS – DL n.º 3/2012, de 16 de janeiro), funciona no âmbito do Gabinete Nacional de Segurança (GNS) e está na dependência orgânica do Primeiro-Ministro (PM) através do Ministério da Presidência e da Modernização Administrativa.

[67] O CERT.PT é membro da Rede Nacional de CSIRT e representante nacional na Rede Europeia de CSIRT, instituída pela Diretiva NIS (Diretiva (UE) n.º 2016/1148).

[68] Âmbito, objetivos e constituição dos membros da rede disponível para consulta em: https://www.redecsirt.pt/ [07-03-2020].

efetivamente, conforme enfatiza Marques (2019, p. 8), “a densidade desta rede é um contributo assinalável para a resiliência do sistema nacional como um todo”.

3.1.2. Domínio do Combate ao Cibercrime

Em primeiro lugar, importa referir que, no domínio do combate ao cibercrime ou da prossecução criminal os ciberataques representam atos ilícitos à luz da legislação nacional e internacional, sendo passíveis de ação penal. Assim este plano de atuação, em consonância com o sistema judicial, tem como principal objetivo a dissuasão da prática de crimes e no limite a condenação do autor de um crime (Santos L. , 2018). Este aspeto é, efetivamente, conforme sublinha Batista (2016), o principal elemento diferenciador do domínio da cibersegurança para o domínio do combate ao cibercrime, dado que, enquanto na cibersegurança se procura almejar, numa primeira análise, a prevenção, no combate ao cibercrime - investigação criminal – o foco assenta na reação a um crime (conforme apresentado na Figura 12). Neste contexto, Batista (2016, p. 4) acrescenta ainda que o momento da passagem da prevenção para a investigação criminal ocorre com “a notícia do crime”.

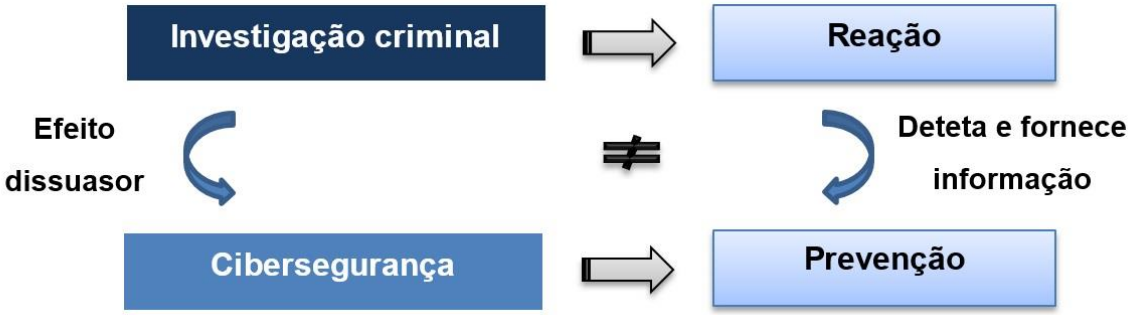

Figura 12 – Diferença entre os domínios do combate ao Cibercrime e da Cibersegurança. Esquema adaptado de Batista (2016, p. 3)

Neste quadro, perante a existência de crimes no ciberespaço, quer contra pessoas (p. ex. pornografia de menores, crimes contra a honra, proteção de dados pessoais e privacidade), quer contra interesses patrimoniais (p. ex. violação de direitos de autor e direitos conexos e a Burla Informática e nas Telecomunicações) ou ainda contra dados e informação (falsidade informática, dano relativo a programa ou outros dados Informáticos, sabotagem informática, acesso ilegítimo, interceção ilegítima e reprodução ilegítima de programa protegido), verifica-se que o enfoque do combate ao cibercrime é a investigação criminal, procurando determinar a autoria dos ciberataques e, em última instância, a condenação dos autores.

Não obstante, o domínio do combate ao cibercrime, conforme esclarece Bravo (2020), também desempenha um papel muito importante na prevenção criminal, por proceder à “recolha de informações, incluindo criminais, atuando no sentido de desmotivar para a prática de crimes através de exploração de vetores ligados com a vontade, capacidade e oportunidade de ação criminosa”.

Neste contexto, constata-se que apesar de o enfoque dos domínios da cibersegurança e do combate ao cibercrime serem diferentes no que concerne à finalidade, ambos visam contribuir para

segurança do ciberespaço sendo imperativo a existência de uma estreita colaboração entre estes domínios. A Figura 13 expõe, a nível nacional, a forte dependência existente.

Figura 13 – Esquematização da cooperação nacional e da forte dependência entre os domínios da cibersegurança e do combate ao cibercrime. Adaptado de Cabreiro (2019, p. 17).

Porém, constata-se que a "Ciber Investigação" enfrenta vários e complexos desafios, que dificultam extensivamente a prossecução criminal, tais como: o predomínio do anonimato[69]; a complexa, diversificada e sofisticada rede de tecnologia que integra a infraestrutura do ciberespaço, traduzindo-se em diferentes dispositivos (computadores portáteis, computadores, *smartphone*s, *tablets*), sistemas operativos (*Windows, Android, Linux, Blackberry*) e tecnologias de acesso (2/3/4/5G); recurso à criptografia nas comunicações; automatização, mobilidade e velocidade; e ainda o crescente armazenamento de dados em *cloud*[70] e a sua localização.

Em relação à competência legal para a prevenção e investigação criminal do cibercrime encontra-se atribuída à Polícia Judiciária (PJ) sendo, ainda, participantes muito ativos e importantes neste domínio os órgãos de polícia criminal, o Ministério Público e os Magistrados Judiciais. Em concreto, no seio da Polícia Judiciária foi criada em 2016, e encontra-se em funcionamento uma

[69] O que dificulta a identificação da origem e a autoria dos ciberataques e, consequentemente, a atribuição de responsabilidades. Para isso, contribui, significativamente, a existência de várias aplicações e ferramentas ao dispor de todos, que contribuem para a anonimização, tais como: redes (*deep web)*; navegadores (*The Onion Routing* – TOR); mercados virtuais (*Silk Road*); moedas virtuais (*bitcoin*) (Cabreiro, 2016). A juntar a estes, poder-se-á ainda elencar outros aspetos que contribuem para a anonimização no ciberespaço, tais como, a existência de Falsas Identidades, a presença de "*Avatares*" e ainda a utilização de recursos alheios (*botnets)* (Cabreiro, 2019).

[70] Palavra anglo-saxónica que em português significa nuvem. Conforme defende Tribolet (2020), uma das medidas mais eficazes de proteção da informação no ciberespaço é proceder-se ao seu armazenamento em várias *clouds*, complementando-se com *backups offline*. Porém, como reverso da medalha, facilmente se infere que este facto irá dificultar a investigação criminal, sobretudo se os dados referentes à prática de um crime estiverem também armazenados em várias *clouds*, com os servidores físicos dispersos por vários locais do mundo.

unidade operacional especializada, denominada de Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica (UNC3T)[71], que tem como finalidade:

> "alcançar a necessária resposta estrutural, preventiva e repressiva ao fenómeno do cibercrime e do ciberterrorismo , e que é inspirada no modelo adotado pelo EC3 (*European Cybercrime Center*) da EUROPOL, cujos pontos focais são o abuso sexual de crianças através da Internet, a fraude com os cartões e outros meios de pagamento eletrónico e virtuais, a criminalidade informática pura (os crimes previstos na Lei n.º 109/2009, de 15 de setembro) e a criminalidade praticada com recurso a meios informáticos"[72]. (GOV-PT, 2016, p. 4215)

3.1.3. Domínio da Ciberdefesa

A ciberdefesa constitui um novo domínio das operações da defesa e um contributo essencial para a segurança do ciberespaço nacional. Em sentido lato, a ciberdefesa engloba as atividades de prevenção, monitorização e reação a ameaças que coloquem em risco a soberania nacional. Por conseguinte, compete às Forças Armadas assegurar a missão da ciberdefesa (MDN, 2020).

No rescaldo dos ciberataques de elevada magnitude conduzidos contra a Estónia (2007), Geórgia (2008) e Irão – *Stuxnet* (2010), o ciberespaço passou a assumir um papel de crescente relevância para o exercício da soberania e defesa dos interesses dos Estados. No plano nacional, em 2013, foram aprovados e promulgados importantes diplomas nesta matéria, nomeadamente o Conceito Estratégico de Defesa Nacional (CEDN)[73], a Reforma "Defesa 2020" e a Orientação Política para a Ciberdefesa (OPC)[74]. Como corolário da materialização destas linhas orientadoras para a Ciberdefesa nacional foi criado, no início de 2015, através da Lei Orgânica do Estado-Maior-General das Forças Armadas (EMGFA), o Centro de Ciberdefesa (CCD)[75], integrado na estrutura orgânica da Direção de Comunicações e Sistemas de Informação (DIRCSI) (MDN, 2014).

---

[71] Esta unidade operacional foi criada na estrutura orgânica da Polícia Judiciária em Novembro de 2016 na sequência da publicação do DL n.º 81/2016, de 28 de novembro. A UNC3T substituiu a Unidade Nacional da Investigação da Criminalidade Informática (UNICI) da PJ, criada em 2015 através da Lei 103/2015, de 24 de agosto. A UNC3T é inspirada no modelo adotado pelo EC3 da *European Union Agency for Law Enforcement Cooperation* (EUROPOL).

[72] Em maior detalhe, compete à UNC3T a prevenção, deteção e investigação dos seguintes crimes: informáticos em sentido estrito, previstos na LC (Lei 109/2009); praticados com recurso ou por meios informáticos, tais como: os previstos no regime legal da proteção de dados pessoais, no Código dos Direitos de Autor e Direitos Conexos, incluindo a interferência e o desbloqueio de formas de proteção tecnológica de bens e de serviços; contra a liberdade e autodeterminação sexual, sempre que praticados por meio ou através de sistema informático; devassa por meio da informática; burla informática e nas comunicações; interferência e manipulação ilegítima de meios de pagamento eletrónicos e virtuais; espionagem, quando cometido na forma de um qualquer programa informático concebido para executar ações nocivas que constituam uma ameaça avançada e permanente; ciberterrorismo, em articulação com a UNCT (Polícia Judiciária, 2017).

[73] O CEDN foi aprovado pela RCM n.º 19/2013, de 5 de abril, e define as prioridades do Estado em matéria de defesa, de acordo com o interesse nacional (PCM, 2013).

[74] Promulgada através do despacho n.º 13692/MDN teve como finalidade definir os objetivos e estabelecer as linhas orientadoras com vista à edificação da capacidade de ciberdefesa nacional. Em concreto, foram estabelecidos os seguintes objetivos: 1) garantir a proteção, a resiliência e a segurança das redes de CSI e CSI da Defesa Nacional contra ciberataques; (2) assegurar a liberdade de ação do país no ciberespaço e, quando necessário e determinado, a exploração proactiva do ciberespaço para impedir ou dificultar o seu uso hostil contra o interesse nacional; (3) contribuir de forma cooperativa para a cibersegurança nacional (MDN, 2013, p. 31978).

[75] Embora apenas tenha alcançado a *Initial Operational Capability* (IOC) em junho de 2016.

O CCD encontra-se na dependência do CEMGFA e no âmbito da defesa nacional "constitui o órgão responsável pela condução de operações no ciberespaço e pela resposta a incidentes informáticos e ciberataques, com responsabilidades de coordenação, operacionais e técnicas" (MDN, 2013, p. 31978). Acresce que, conforme estipulado no DR nº 13/2015, visando a prossecução da interoperabilidade, a eficiência de recursos e a tomada de ações integradas, compete, ainda, ao CCD garantir a coordenação, o trabalho colaborativo e integrado com os núcleos *Computer Incident Response Centre* (CIRC) do EMGFA e dos três ramos das Forças Armadas. De igual modo, com base numa estratégia de resposta cooperante, deverá partilhar informação com o CNCS[76], para o qual existe inclusive um Memorando de Entendimento[77], e com os demais CIRC nacionais e internacionais[78] conforme representado na Figura 14 (MDN, 2015).

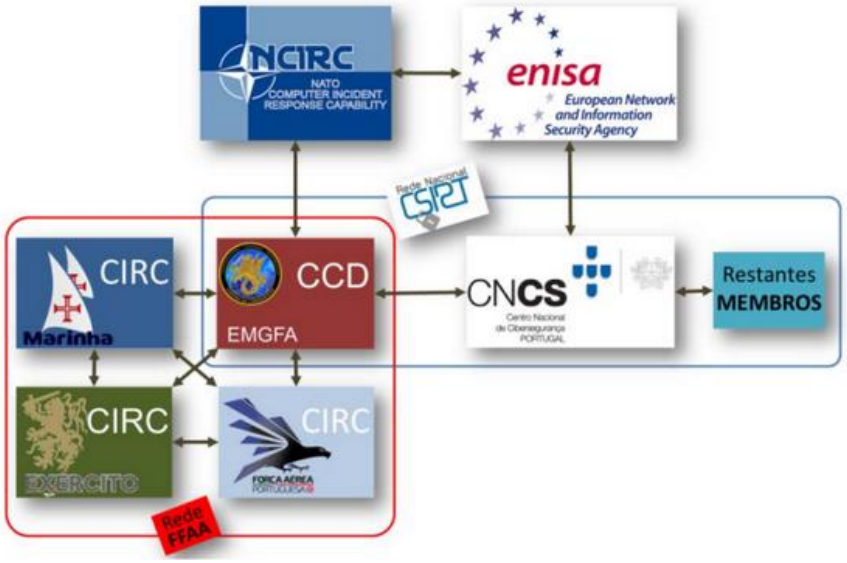

Figura 14 - Esquema ilustrativo da partilha de informação entre o CCD e os CIRC do EMGFA, Ramos e outras organizações nacionais e internacionais (MDN, 2020)

Concomitantemente, para além da consequente edificação e implantação do CCD, por forma a materializar os objetivos constantes na OPC e assim implementar a almejada capacidade militar para conduzir todo o espetro de operações no ciberespaço (defensivas, de exploração e ofensivas), de acordo com Jesus (2019), foram definidas seis grandes áreas de empenhamento da ciberdefesa, a saber: proteção e defesa; operações defensivas; informações, vigilância e reconhecimento; operações de resposta; operações de apoio; operações ofensivas. A primeira e a segunda área desenvolvem-se num plano interno de proteção das redes e sistemas, enquanto as últimas quatros integram o que se poderá designar pelo domínio de operações militares atuando no exterior através de ações de vigilância

[76] Não obstante, o facto do DR nº 13/2015, apenas fazer diretamente referência ao CNCS, atualmente a nível nacional, constituem-se como entidades muito relevantes e com responsabilidade na segurança do ciberespaço, a UNC3T – criada em 2016 – e o Serviço de Informações de Segurança, como se abordará adiante.

[77] Assinado em 2017, visa promover e facilitar a partilha de informação e a cooperação entre o CCD e o CNCS.

[78] Um claro exemplo de um CIRC internacional que o CCD colabora e partilha informação é o *NCIRC* da NATO, conforme representado na Figura 14.

e recolha de informação, apoio a operações, bem como na criação de efeitos. A Figura 15 apresenta as seis grandes áreas de atuação da ciberdefesa nacional.

A primeira área de atuação da ciberdefesa centra-se na Proteção e Defesa através do estabelecimento de uma arquitetura de rede, sistemas e aplicações, na definição e implementação de medidas de defesa e de resiliência.

Figura 15 – Representação das seis grandes áreas de atuação da Ciberdefesa Nacional (Jesus, 2019, p. 4)

As Operações Defensivas constituem a segunda área de atuação da ciberdefesa e concretizam-se através de uma monitorização em tempo real do ciberespaço com vista à deteção, análise e resposta a incidentes com especial relevância para os que possam vir a afetar a soberania nacional. Na prática, estas ações desenvolvem-se, também, num quadro de atuação interna, mas em permanente colaboração com as restantes entidades do Estado, Forças e Serviços de Segurança com responsabilidade nesta área. Na verdade, é o que se poderá designar de cibersegurança sectorial da Defesa Nacional.

Passando das operações defensivas para a condução de operações de exploração do ciberespaço surge uma terceira área de atuação da ciberdefesa que se centra na recolha e análise de Informações, Vigilância e Reconhecimento de potenciais ameaças no ciberespaço. Esta linha de ação visa contribuir para um "aviso antecipado" onde os serviços de informações assentam o seu esforço De facto, é absolutamente vital para a defesa das infraestruturas de informação e para a condução de operações no ciberespaço monitorizar a evolução das ciberameaças e percecionar as suas intenções.

Em complemento da área de atuação anterior, emerge uma quarta, que se focaliza na condução de Operações de Resposta com vista à limitação ou mitigação de ataques de adversários. É para esta área, que a asserção de Santos *et al.* (2018, p. 36) aponta, ao afirmarem que "uma capacidade operacional de ciberdefesa deverá envolver também o conhecimento e os recursos necessários para prever, influenciar ou bloquear as ações que potenciais adversários venham a desenvolver no ciberespaço, antes, durante e após as operações militares". A acrescentar que a área de atuação das

Informações, Vigilância e Reconhecimento em complemento com as Operações de Defensivas constituem aquilo a que se designa de CSC (Jesus, 2019).

Num contexto de integração do ambiente ciberespaço com os outros domínios na condução de operações militares, cada vez mais a componente cibernética desempenha um papel preponderante no sucesso das missões. Assim, as Operações de Apoio constituem uma área de atuação da ciberdefesa muito relevante. Estas operações visam, essencialmente, assegurar a proteção e segurança das Comunicações e Sistemas de Informação (CSI) empregues no Comando e Controlo (C2) das missões militares ou, atuar como um elemento facilitador de uma operação em curso.

Por último, numa situação de conflito a ciberdefesa deverá possuir capacidade para conduzir Operações Ofensivas no ciberespaço, por forma a alcançar uma vantagem operacional sobre os adversários. Efetivamente, estas três últimas grandes áreas da ciberdefesa são um elemento diferenciador das Forças Armadas.

3.1.4. Domínio das Informações

Os serviços de informações são, pela sua natureza, instrumentos essenciais na identificação e avaliação de ameaças e oportunidades em ambientes caraterizados pela volatilidade, incerteza, complexidade e ambiguidade (VUCA[79]), tais como aqueles que se vivenciam nos dias de hoje. Com efeito, as informações são um ativo estratégico do Estado, fundamentais no suporte da decisão política, sobretudo nos assuntos de segurança e defesa (PCM, 2013). Neste contexto, a segurança do ciberespaço não é, e nem pode ser, exceção, assumindo o domínio das informações um papel primordial na importante vertente da previsão das ameaças, na prevenção e na gestão do risco.

No regime jurídico nacional[80], aos serviços de informações compete assegurar a produção de informações decisivas para a preservação da segurança interna e externa, assim como, para a salvaguarda da independência e dos interesses nacionais. Quanto à estrutura orgânica, o quadro institucional português contempla a existência de dois serviços de informações: um serviço externo, o Serviço de Informações Estratégicas de Defesa (SIED) e um serviço interno, o Serviço de Informações de Segurança (SIS), ambos integrados no Sistema de Informações da República Portuguesa (SIRP) (AR, 2007). A par destes existe o Centro de Informações e Segurança Militares (CISMIL) que tem a missão específica da produção de informações necessárias para a cumprimento das missões das Forças Armadas, e que visem garantir a segurança militar, estando sob a dependência hierárquica do CEMGFA (MDN, 2015).

Adicionalmente, no seguimento da reforma orgânica de 2004[81], os dois serviços de informações integrantes do SIRP passaram a estar na dependência direta do PM, tendo sido criado o cargo de

[79] Acrónimo Anglo-saxónico utilizado para caracterizar ambientes dominados pela Volatilidade (*Volatile*), Incerteza (*Uncertain*), Complexidade (*Complex*) e Ambiguidade (*Ambiguous*).

[80] Composto pela Lei n.º 4/2004, de 6 de novembro (que alterou a Lei de Quadro do SIRP, n.º 30/84, de 5 de Setembro) e pela Lei n.º 9/2007, de 19 de Fevereiro, que estabelece a orgânica do Secretário-Geral (SG) do SIRP.

[81] Conforme esclarece Pereira (2012), a distinção estanque entre a segurança interna e segurança externa que se encontrava plasmada na Lei-Quadro n.º 30/84, foi perdendo fundamento com o surgimento das ameaças assimétricas, difusas e desterritorializadas, afigurando-se como premente que fosse alterado o modo de funcionamento do SIRP, o que veio a ocorrer com entrada em vigor da Lei n.º 4/2004, de 6 de Novembro.

Secretário-Geral do SIRP com o objetivo de dirigir e coordenar superiormente as atividades dos serviços de informações[82].

Neste quadro, o SIED tem por missão específica a "produção de informações que contribuam para a salvaguarda da independência nacional, dos interesses nacionais e da segurança externa do Estado Português" (AR, 2004, p. 6604). Enquadram-se na sua esfera de ação as dimensões euro-atlântica, lusófona e global da segurança portuguesa onde o SIED possui uma responsabilidade específica de produzir informações que concorram para a salvaguarda da independência nacional e dos interesses nacionais, assim como, para a segurança externa do Estado Português (SIRP, 2015). Por sua vez, compete ao SIS a "produção de informações que contribuam para a salvaguarda da segurança interna e a prevenção da sabotagem, do terrorismo, da espionagem e a prática de atos que, pela sua natureza, possam alterar ou destruir o Estado de direito constitucionalmente estabelecido" (AR, 2004, p. 6604). Por conseguinte, o SIS sem competências policiais ou de investigação criminal[83], atua no domínio, eminentemente, preventivo (SIRP, 2015). A Figura 16 representa, resumidamente, as principais dimensões da missão dos serviços de informações nacionais.

Figura 16 - Principais dimensões da missão dos serviços de informações nacionais (SIRP, 2015, p. 7)**.**

No que concerne à segurança do ciberespaço nacional, impõe-se aos Serviços de Informações portugueses que, para além das ameaças procedentes do terrorismo, da espionagem e da criminalidade organizada que sempre estiveram no seu domínio de atuação, adaptem as suas missões e prioridades para as novas realidades, onde as ciberameaças, traduzidas em ações de *hacktivismo*, cibercrime, ciberespionagem e ciberterrorismo são, cada vez mais, uma constante (SIRP, 2015).

[82] Este modelo orgânico, segundo Cruz (2019b, p. 7) segue ainda a "dicotomia clássica, mantendo a autonomia dos serviços, um interno e outro externo, mas que responde também à necessidade de atualização requerida pela cada vez maior porosidade das fronteiras em matéria de segurança, por força da transnacionalidade das novas ameaças".

[83] Neste âmbito, o legislador foi bastante claro na separação dos campos de atuação das informações de segurança das de investigação criminal, cirando e disponibilizando para as duas áreas, instrumentos distintos: Sistema de Informações / Sistema de Investigação Criminal e o Sistema de Segurança Interna (SIS, Contraespionagem, 2020a).

Neste quadro, conforme esclarece o SIS (2020b), “uma das principais tarefas das informações de segurança reside na deteção antecipada das intenções dos agentes concorrências ou de ameaça”. Em maior detalhe, releva-se que o trabalho de informações, atinente à aquisição de conhecimento profundo, sobre estruturas adversas aos interesses nacionais permite não só identificar os potenciais agentes de ameaça como perceber os seus intentos, as suas capacidades, as suas características de atuação e a pegada ou assinatura digital. Para além disso, numa vertente mais operacional, através da cibercontraespionagem ofensiva, das vulnerabilidades e falhas operacionais potencialmente exploráveis dos agentes de ameaça, será possível contrariar os seus intentos maliciosos sobre o ciberespaço de interesse nacional.

Por fim, compete ao SIS a produção de informações de segurança interna[84] necessárias para prevenir e antecipar as ameaças – que pela sua natureza, podem alterar ou destruir o Estado de direito constitucionalmente estabelecido - ou na impossibilidade contribuir para a proteção e mitigação dos seus impactos.

3.1.5. Domínio da Ciberdiplomacia e da Cooperação

As características do ciberespaço, conjugadas com o modelo de funcionamento de acesso aberto e global, dificultam a capacidade dos Estados em garantir de forma isolada a segurança do seu ciberespaço e a proteção dos seus cidadãos neste ambiente. Por isso, torna-se essencial, que os Estados atuem, quer no domínio diplomático, quer no plano da cooperação para que em colaboração com aliados e parceiros, nacionais e internacionais, possam em conjunto diminuir a insegurança no ciberespaço. Este mesmo desiderato da cooperação representa, inclusive, um dos seis eixos de intervenção da ENSC 2019 -2023, supracitados no subcapítulo 1.3.6, e representados na Figura 17 (GOV-PT, 2019).

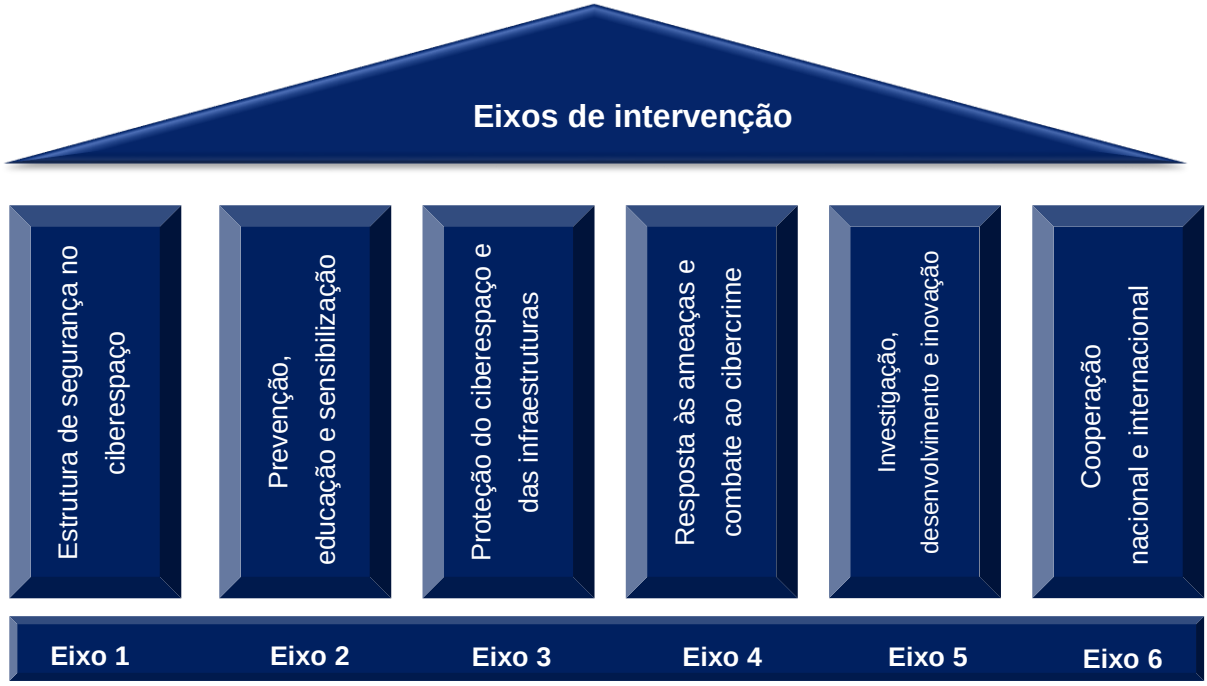

Figura 17 – Representação dos 6 Eixos de intervenção da ENSC 2019-2023 (Autor, 2020)

[84] Conforme Art.º 3º da Lei n.º 9/2007, de 19 de fevereiro.

3.1.5.1. Ciberdiplomacia

No plano internacional é essencial que um Estado atue, bilateral e multilateralmente, de forma a fortalecer a sólida rede de alianças existentes, exercer influência e promover a implementação de políticas tendo em vista a prossecução dos interesses nacionais. Com efeito, este é o desígnio do domínio da diplomacia.

No universo do ciberespaço, a nível nacional, a ENSC 2019-2023 classifica este âmbito de atuação internacional de ciberdiplomacia que se traduz na "disciplina da ação externa do Estado que visa promover, nomeadamente, a aplicação do direito internacional vigente ao ciberespaço a fim de garantir a respetiva estabilidade, a governação transparente e partilhada da sua utilização universal e a criação eficiente de capacidades normativas" - designadamente no seio da Comunidade dos Países de Língua Portuguesa (CPLP)[85] (GOV-PT, 2019, p. 2892). Neste âmbito, ressalva-se a criação do cargo de embaixador para a ciberdiplomacia[86], facto revelador da importância, que o país atribui a este domínio. Por fim, importa, ainda, referir que o desenvolvimento de um quadro internacional da ciberdiplomacia materializado na identificação de iniciativas prioritárias e na contribuição para a regulação e universalização do ciberespaço, configuram duas linhas de ação, que se encontram, igualmente, definidas no Eixo 6 da ENSC 2019-2023[87].

3.1.5.2. Cooperação Internacional

Neste quadro, das alianças e dos compromissos internacionais, os Estados têm de articular as suas políticas e estratégias nacionais procurando o fortalecimento e defesa dos interesses comuns e a salvaguarda dos valores coletivos.

Foi neste contexto que, os membros da NATO assumiram o compromisso designado de *Cyber Defence Pledge*, para o desenvolvimento das suas capacidades nacionais e coordenação de uma resposta conjunta para fazer face às ameaças no ciberespaço (NATO, 2016b). Paralelamente, Portugal integra e contribui, ativamente, em dois projetos na área da ciberdefesa, nomeadamente: o projeto S*mart Defence Multinational Cyber Defence Education & Training* (MN CD E&T) e o *Malware Informational Sharing Plataform* (MISP). Sucintamente, em relação ao *Smart Defence* MN CD E&T Portugal liderou este projeto entre 2014 e 2019, o qual teve como finalidade criar uma plataforma de coordenação da educação e do treino em Ciberdefesa e promover novas iniciativas nesta área, de

[85] A ENCS 2019-2023 atribui especial relevo à capacitação dos países da CPLP através da formalização e operacionalização de parcerias estratégicas, alicerçadas no desenvolvimento de confiança mútua, contribuindo ativamente para moldar o ecossistema e incrementar a resiliência da rede que todos os cooperantes utilizam (GOV-PT, 2019). Além dos países da CPLP, verifica-se que, Portugal tem vindo a desenvolver, nos últimos anos, esforços de cooperação com países ibero-americanos e da iniciativa 5+5, com o intuito de, a partir de afinidades culturais, linguísticas e mesmo organizativas se potenciar o desenvolvimento de iniciativas colaborativas ao nível da formação, do treino operacional, na análise de informações, na investigação e no incremento de capacidades (Santos L. et al., 2018).

[86] Embaixador Luís Barreira de Sousa, o qual exerce o cargo desde 2016.

[87] Além destas 2 linhas de ação, o Eixo 6 identifica mais 5 linhas de ação, num total de 7, com vista ao incremento da cooperação e colaboração, nomeadamente: aprofundar a participação nacional nos órgãos, organismos e agências internacionais relevantes; participar nos exercícios; integrar organismos de cibersegurança e ciberdefesa; aprofundar a cooperação com entidades nacionais com responsabilidade de segurança do ciberespaço; incrementar a articulação entre o CNCS e a ANACOM e com as entidades que compõem o Sistema de Certificação Eletrónica do Estado (GOV-PT, 2019).

modo a coadjuvar as nações aliadas no preenchimento das lacunas identificadas (MDN, 2020). O segundo projeto em que Portugal participa é o MISP*,* que se constitui como uma plataforma de excelência para partilha de informação, sendo esta plataforma abordada, em maior detalhe, mais à frente nesta investigação. Ainda na área da educação e do treino, Portugal acolhe, como *host nation*, desde 2019, a NATO *Communications, Information* (NCI) *Academy,* em Oeiras, cuja missão se centra na formação dos militares da NATO nesta área conferindo grande visibilidade ao país na comunidade internacional.

No âmbito da UE, numa ótica de eficiência e otimização de recursos, foi definido o conceito de *pooling & sharing*, por forma a agregar as várias iniciativas em curso a nível interno nos Estados-membros, implementando uma cooperação multilateral sinérgica e evitando assim duplicações desnecessárias, preservando os interesses da UE (Santos L. et al., 2018). No panorama da formação e do treino na área da ciberdefesa na UE, releva-se o papel de destaque que, Portugal tem vindo a desempenhar nos esforços cooperativos ao assumir em conjunto com a França a liderança do projeto *Cyber Defence Discipline do EU Military Training Group* (EUMTG), que visa identificar e estabelecer os requisitos de treino na área da ciberdefesa na UE. Ainda nesta área, importa destacar que em setembro de 2015, foi atribuída ao nosso País a responsabilidade pela gestão da *Cyber Defence Training and Exercise Coordination Platform* (CD TEXP) (MDN, 2020) .

No plano do combate ao cibercrime, destaca-se a cooperação entre a UNC3T e a *European Cybercrime Centre* (EC3), agência criada em 2013, no seio da EUROPOL com o objetivo de fortalecer a resposta da aplicação da lei da criminalidade informática na UE, e a nível internacional, com a *International Criminal Police Organisation* (INTERPOL). Neste plano, sublinha-se que, a própria conceção e desenvolvimento da UNC3T foi inspirada no modelo adotado pelo EC3 dotando-a de um núcleo de competências, semelhantes, às existentes naquela agência europeia (Cabreiro, 2016).

Por fim, também no domínio das informações, a cooperação internacional assume-se como um fator determinante para a segurança nacional no seu todo e em particular para a proteção do ciberespaço. Na realidade, conforme revela Cruz (2019a), os serviços de informações portugueses contribuem, diariamente, para a segurança interna da Europa[88], por meio da recolha e partilha de informações ou através da participação ativa em operações conjuntas. Em sentido inverso, recebem, diariamente, a colaboração e apoio no combate às ameaças de segurança interna por parte dos 27 Estados da União Europeia, a que se juntam a Suíça e a Noruega. A este respeito, tendo por base a cooperação a nível Europeu, Cruz (2019a, p. 13) realça que "trabalhando em rede contribuímos para uma Europa mais segura, para um Portugal mais seguro e para a segurança dos portugueses".

3.1.5.3. Cooperação nacional

Naturalmente, também, no plano interno é vital incrementar a coordenação e cooperação entre as diversas entidades nacionais com responsabilidades na segurança do ciberespaço a fim de obter uma capacidade de alerta e resposta às ameaças mais capaz, competente e robusta. Este é um aspeto

[88] Por exemplo, no âmbito do *Counter Terrorism Group* (CTG), o SIS e os serviços de segurança, contribuem e colaboram ao nível documental e com recursos humanos ao *Intelligence and Situation Centre* (INTCEN), mantendo uma comunicação construtiva com a EUROPOL e com o EU *Counter Terrorism Coordinator* (EU CTC) e com outras instituições da UE (Cruz, 2019a).

fundamental, o qual será abordado no subcapítulo seguinte - articulação entre os domínios – pois o conjunto dos domínios de atuação, enunciados e analisados, representa a capacidade nacional de segurança do ciberespaço.

Para terminar, importa salientar que neste contexto é ainda essencial que os cidadãos, as empresas, a administração pública, o sector privado, a indústria, a academia e os governos assumam, ativamente, cada uma das suas responsabilidades no exercício de uma cidadania digital segura. Para esse efeito, deverão atuar de forma sinérgica e com unidade de esforço, por forma a implementarem soluções que não só promovam uma maior racionalização dos recursos, mas que garantam a obtenção de repostas integradas e mais eficientes para a segurança do ciberespaço nacional (Santos L. et al., 2018).

3.2. Articulação entre os domínios de atuação

O conjunto dos domínios de atuação enunciados e os principais atores intervenientes, em cada um deles, representam a capacidade nacional de segurança do ciberespaço. Efetivamente, conforme sublinham Santos *et al.* (2018, p. 41), "a proteção do ciberespaço, constituindo uma tarefa extremamente exigente, não conseguirá ser garantida de forma isolada por qualquer instituição ou Estado". Deste modo, é essencial promover a complementaridade entre os vários domínios de atuação, dado que num mesmo cenário de conflito poderá ser necessário, mediante a gravidade, atuar, simultaneamente nos vários planos descritos, cada qual com o seu âmbito de atuação com os seus recursos, procedimentos e redes transnacionais de cooperação inseridos num quadro legal específico. É neste âmbito que Santos (2018, p. 27) realça que o "conjunto de planos de "contra-ciberconflitualidade" devem complementar-se e atuar simbioticamente para a eficácia do sistema".

3.2.1. Articulação entre os principais atores na segurança do ciberespaço: G4

Na prática esta necessidade premente de articulação entre os principais atores, com responsabilidade na segurança do ciberespaço, existe porque as fronteiras de atuação no ciberespaço são bastante difusas. Se com clareza se compreende que compete às Forças Armadas a responsabilidade nas ações de ciberdefesa e ao Ministério da Justiça, através da UNC3T e das Forças de Segurança, atuar nas ações de cibercrime ou *hacktivismo,* inúmeros casos haverá, com impacto na segurança do ciberespaço, em que surgirão dúvidas sobre qual o domínio de atuação. De um modo concreto, corroborando com Moniz (2018), perante um hipotético ataque a uma IC nacional poder-se-á ficar na incerteza se se trata de um ataque conduzido contra a organização, afetando o serviço aos seus clientes (domínio da cibersegurança), se este foi motivado por interesses económicos (domínio do cibercrime), ou ainda, se foi concebido com a finalidade de colocar em causa a soberania de um país (domínio da ciberdefesa). É, também, nesta sequência que Cravinho (2019, p. 6) afirma que no ciberespaço as "fronteiras entre o domínio interno e externo, entre o civil e militar e entre o público e o privado, esbatem-se de forma espetacular e talvez sem precedentes".

Neste sentido, verifica-se que, no plano tático e operacional, a prevenção e reação aos ciberataques é conduzida, concorrentemente, nos domínios de atuação supracitados. Na realidade, a

grande maioria dos ciberincidentes cingem-se à intervenção no domínio da cibersegurança, visando a continuidade do "negócio" e a defesa da cidadania no mundo digital, e no combate ao cibercrime por forma a conduzir-se uma investigação criminal procurando a identificação e condenação dos autores. Além destes, nos casos de se estar perante ações de espionagem ou de terrorismo terão de ser envolvidos na resposta os serviços de informações nacionais (Moniz, 2018). Por fim, poderão, ainda, ocorrer situações, mais complexas, com possíveis impactos no espaço físico desencadeando ocorrências de crise ou de emergência onde, também, o domínio da ciberdefesa e da ciberdiplomacia poderão ter de intervir (Santos L. , 2018).

Esta premente necessidade de articulação tem, segundo Santos *et al.* (2012), conduzido à edificação de estruturas nacionais com o fim de fazer face às ciberameaças em planos de atuação diferentes, mas concorrentes, visando a paz social e a salvaguarda da segurança nacional. Neste universo destaca-se o grupo de carácter operacional informal, designado de G4, constituído pelo CNSC, pelo CCD, pela UNC3T e pela unidade de cibersegurança que opera no âmbito do SIS (Figura 18). De acordo com Marques (2019, p. 8) "estas quatro entidades formam o núcleo operacional que coopera permanentemente em Portugal para a promoção da segurança no ciberespaço de interesse nacional".

Figura 18 – Constituição do G4 - núcleo operacional de cooperação permanente para a promoção da segurança do ciberespaço de interesse nacional (Jesus, 2019, p. 5)

Concretamente, o G4 tem como principal objetivo promover a cooperação e a partilha de informação entre as entidades que o integram de modo a que possam ser dadas respostas, mais eficazes e céleres, aos ciberataques que afetem o ciberespaço nacional (Assunção, 2020).

Para o SIS (2020b), o G4 desempenha um papel muito importante, na promoção da segurança do ciberespaço de interesse nacional, dado que permite "a cobertura da totalidade das áreas de relevo para a segurança do ciberespaço de interesse nacional, pela intervenção de cada entidade integrante o grupo nas suas matérias específicas de atuação".

Na mesma senda Bravo (2020) salienta a premência do G4 para a harmonização de metodologias de ação, o suporte a canais próprios e plataformas adequadas de partilha de informação, indícios e de assinaturas do crime.

De igual modo, destacando a importância do G4, Santos (2020) esclarece e sublinha que este grupo permite, às quatro entidades que o integram, "articular as suas operações para não comprometer os objetivos individuais de cada uma [e] partilhar conhecimento detalhado sobre as ocorrências mais relevantes para produzir um melhor quadro situacional e melhorar a ação individual".

Neste enquadramento, releva-se como um exemplo notório da atuação coordenada do G4 o mediático combate às ciberameaças que surgiram durante a pandemia associada à propagação do vírus SARS-COV-2 onde diversos atores hostis do ciberespaço procuraram, de forma encoberta por este contexto de crise, conduzir as suas campanhas de ciberataques. A Figura 19 dá exemplo de um comunicado conjunto emitido pelas entidades que constituem o G4, que visava alertar a população, sobre a tipologia dos ciberataques em curso e encobertos pelo tema do Covid-19 (G4, 2020).

Figura 19 - Extrato do comunicado conjunto emitido pelo G4 relativo ao Alerta COVID-19 e as ciberameaças (G4, 2020)

3.3. Síntese conclusiva

Perante o exposto ao longo deste capítulo, conclui-se em primeira análise que, para enfrentar os desafios e o conjunto de ameaças existentes no ciberespaço, os Estados e a sociedade deverão, do mesmo modo que o fazem perante uma ameaça assimétrica ou transnacional, desenvolver e implementar um conjunto de "planos de atuação" assentes nos seguintes domínios: cibersegurança; combate ao cibercrime; ciberdefesa; informações; ciberdiplomacia e cooperação nacional e internacional.

O domínio da cibersegurança centra-se na implementação de um conjunto de medidas e ações que visam a prevenção, monitorização, deteção e reação por forma a manter o estado de segurança desejado numa lógica de mercado e continuidade de negócio, de proteção da cidadania e de colaboração com a Segurança Interna e Defesa.

Por sua vez, o domínio do combate ao cibercrime tem como principal objetivo a dissuasão da prática de crimes e no limite a condenação do autor de um crime, dado que um ciberataque é considerado um ato ilícito à luz da legislação em vigor.

A ciberdefesa engloba as atividades de prevenção, monitorização e reação a ameaças que coloquem em risco a soberania nacional, bem como o apoio às operações militares no ciberespaço.

Ao domínio das informações compete assegurar a produção de informações decisivas que possibilitem a deteção antecipada das intenções dos agentes de ameaça. Para isso, a área das informações compreende todo trabalho desenvolvido com vista à obtenção de um conhecimento, profundo, sobre os potenciais agentes de ameaça, nomeadamente: os seus intentos; as suas capacidades; as suas características de atuação; e a sua pegada ou assinatura digital.

No domínio da ciberdiplomacia e da cooperação, a sua ação traduz-se em agir, bilateral e multilateralmente, de forma a fortalecer a sólida rede de alianças existentes, exercer influência e promover a implementação de políticas. Deste modo, os estados em colaboração com aliados e parceiros, nacionais e internacionais, poderão em conjunto diminuir a insegurança no ciberespaço.

O conjunto dos domínios de atuação enunciados e os principais atores intervenientes em cada um deles representam, em grande medida, a capacidade nacional de segurança do ciberespaço. Com o intuito de promover a cooperação e a partilha de informação entre as principais entidades operacionais, que contribuem para a segurança do ciberespaço nacional, foi criado o grupo de carácter operacional informal, designado de G4, constituído pelo CNSC, pelo CCD, pela UNC3T e pelo SIS.

Face ao exposto, entende-se que se obteve resposta à QD2 – “Quais são os principais domínios e entidades nacionais que contribuem para a segurança no ciberespaço e como se articulam?”, uma vez que foram identificados e caracterizados os principais domínios e entidades nacionais que contribuem para a segurança no ciberespaço e exposto como se articulam.

4. Informações no Ciberespaço

> "Se conheces o inimigo e te conheces a ti próprio, não tens que temer o desenlace de cem batalhas. Se te conheces a ti próprio mas não conheces o inimigo, por cada vitória ganha sofrerás uma derrota. Se não conheces o inimigo nem a ti próprio, sucumbirás em todas as batalhas". Sun Tzu em "A Arte Guerra" (cit. por Giles (2015, p. 84))

A revolução tecnológica, iniciada na segunda metade do século XX, prossegue a grande ritmo consubstanciando-se, entre outros aspetos, num significativo aumento do tempo em que os cidadãos se encontram, diariamente, conectados à internet permitindo o acesso à informação em quantidade e diversidade como em nenhuma outra época. Esta realidade é fielmente traduzida pela expressão "*always on*". Porém, conforme salienta Cruz (2019a, p. 4) "mais informação não significa mais conhecimento e, paradoxalmente, o mundo onde todos estão ligados tornou-se o espaço privilegiado do anonimato". Neste, cada vez mais, prolifera a desinformação, a manipulação, as *fake news*[89] e a propaganda. Acresce que o fim de uma era predominantemente bipolar[90], conciliado com o crescimento da globalização e o advento no sistema internacional de agentes de ameaça de natureza diversa – estados, organizações criminosas ou terroristas e indivíduos motivados pela ideologia, poder ou lucro - desencadeou o surgimento de ameaças aos Estados, caracterizadas por serem complexas, persistentes, assimétricas, intensas, imprevistas e híbridas (Cruz, 2019b). Com efeito, como resultado desta investigação constata-se, claramente, que estas características não só se enquadram na esfera das ciberameaças como, também, as vieram potencializar.

Neste sentido, importa salientar a utilização do ciberespaço num contexto de ameaça híbrida[91] em particular evidência nos conflitos híbridos mais recentes – p. ex. da Geórgia e Ucrânia. A guerra híbrida, conforme expõem Santos *et al.* (2018, p. 33), encontrou no ciberespaço "um instrumento de ação de elevado potencial em função do custo reduzido, rapidez de atuação, sensação de anonimato e leque crescente de possíveis alvos com potencial impacto no domínio cibernético". Em concreto, identificam-se duas perspetivas de utilização do ciberespaço num contexto de ameaça híbrida, designadamente: ambiente privilegiado para a realização de ações de propaganda, manipulação, distorção da informação e recrutamento; um domínio para a condução de operações militares.

Neste seguimento, atendendo por um lado às novas e complexas ameaças que despontam à segurança dos Estados, e por outro à vigência de uma conflitualidade de baixa intensidade, mas de natureza constante, transversal e híbrida, as informações surgem como uma componente fundamental para a obtenção de um CSC com vista à prevenção e dissuasão. Assim, face à capacidade cada vez

[89] São, comumente, entendidas como notícias falsas que se traduzem na disseminação intencional de desinformação, quer através dos meios de comunicação tradicionais, quer por via das redes sociais. Para uma consulta mais pormenorizado do conceito, Vd. Anexo A.

[90] A bipolaridade da ordem mundial chegou ao fim com o desmembramento do Pacto de Varsóvia, a 31 de março de 1991, consagrando os EUA como a potência hegemónica (Ferreira, 2019).

[91] De acordo com a NATO (2019c), as ameaças híbridas combinam o emprego de meios convencionais, não-convencionais e assimétricos que através do emprego de várias táticas, com postura aberta ou encoberta, conduzem operações de desinformação, ciberataques, pressão económica, operações de guerrilha, atividades criminosas e terroristas. Segundo Fernandes (2016) um dos principais objetivos dos conflitos híbridos consiste em destabilizar um governo contrário e as suas instituições como forma de gerar caos e vazio de poder.

mais disruptiva dos ciberataques, provocando efeitos cada vez mais destrutivos e cinéticos, reconhece-se que também no ciberespaço as informações são essenciais para a antecipação, prevenção e mitigação dos ataques.

Face ao exposto, abordar-se-á, em seguida, o que se entende por informações. Para alcançar este objetivo é necessário, segundo Lowenthal (2006), efetuar-se uma análise holística das informações, a qual deve ter em consideração três elementos essenciais, nomeadamente: o processo, o produto e a organização[92]. As informações enquanto processo compreendem os meios pelos quais certa informação é requerida, compilada, analisada e disseminada. As informações enquanto produto são entendidas como o resultado do processo, i.e., o conhecimento produzido. Por fim, as informações enquanto organização retratam a orgânica e o funcionamento dos serviços de informações.

4.1. Informações Vs. Informação

Em primeiro lugar, importa evidenciar que embora, as informações sejam desenvolvidas a partir da informação, são conceitos muito distintos. Aliás, conforme reitera Cruz (2019b, p. 2) "o termo é usado no plural, para desligar estas "informações" do conceito geral de "informação", termo polissémico que vai do acervo de conhecimentos sobre um assunto até à atividade dos meios de comunicação social". Esta distinção é, efetivamente, um aspeto muito importante dado que em Portugal se observa que, com frequência, os termos "informação" e "informações" são utilizados com o mesmo sentido da linguagem embora sejam conceitos diferentes.

Por forma a evitar erros de interpretação entre os termos "informação" e "informações", a terminologia Anglo-Saxónica recorre às palavras "*information*" e "*intelligence*". Neste âmbito, de acordo com o glossário da NATO (2019b, pp. 67-68), a informação consiste nos "dados não processados que podem ser utilizados na produção de informações" porquanto que, informações são "o produto resultante da recolha direta e do processamento de dados sobre o ambiente, e as capacidades e intenções dos atores, por forma a identificar as ameaças e proporcionar oportunidades a serem exploradas pelos decisores". Assim, conclui-se que, informação decorre da recolha e processamento do formato dos dados avulsos de qualquer tipo (p. ex. acontecimentos, rumores, factos, opiniões, estudos, notícias), enquanto as informações refletem o conhecimento obtido da integração, análise e avaliação prospetiva da informação com a finalidade de apoiar a decisão, encontrando-se num patamar superior, conforme representado na Figura 20.

Neste enquadramento, corroborando com Rêgo (2018, p. 108), poder-se-á inferir que a "lógica subjacente à tradução do termo em Portugal[93] assentou no facto de "*intelligence*" resultar da agregação de vários elementos de "*information*", passando então a ser usada a expressão "informações", por se tratar de um agregado de múltiplas "*information*".

[92] De acordo com Menezes (2012), Sherman Kent foi, em 1949, o pioneiro do modelo de análise do conceito de informações estratificado nos três elementos essenciais: processo, produto e organização. Posteriormente, Lowenthal (2006) seguindo o mesmo racional apresentado por Kent complementou a abordagem expondo uma melhor compreensão e adaptação à realidade.

[93] Na realidade, denota-se que, esta tradução tem originado, por vezes alguns equívocos de entendimento sobre os conceitos de informação e informações. Por esse motivo, países como a Espanha e o Brasil optaram por utilizar, respetivamente, os termos "*inteligenzia*" e "*inteligência*" de forma a reduzir e evitar erros de interpretação.

Figura 20 – Pirâmide das Informações – relação entre Dados, Informação e Informações (Rêgo, 2018, p. 108)

Ao integrar ambos os conceitos, verifica-se que a informação é, na sua essência, dados que serão objeto de organização, análise e avaliação, através de metodologias e técnicas específicas dos Serviços de Informações, sendo obtido um produto final estruturado a que se designa por informações (SIRP, 2020).

Neste contexto, após se ter definido informações e clarificada a diferença existente, entre este conceito e o de informação, serão analisados em seguida cada um dos elementos fundamentais das informações, nomeadamente: o processo, o produto e a organização.

4.2. Informações enquanto processo

As informações como processo referem-se à sequência de atividades pela qual determinados tipos de informação são requeridos, agregados, analisados, convertidos em conhecimento e disseminados com o objetivo de apoiar a tomada de decisão. Neste âmbito, Carvalho (2009) realça que a atividade de informações possui uma dinâmica própria, que se encontra refletida no conjunto de fases, que constituem aquilo que, tecnicamente, se denomina por "Ciclo de Informações". Em seguida, analisar-se-á em maior pormenor este ciclo que é, igualmente, designado por "Ciclo de Produção de Informações" (CPI).

4.2.1. O Ciclo de Produção de Informações

Na realidade o CPI, conforme refere Menezes (2012), procura representar um processo cíclico constituído por um conjunto de etapas, repetidas e interdependentes, que têm como finalidade acrescentar valor aos *inputs* iniciais por forma a obter um produto transformado, refinado e adequado às necessidades dos decisores. Complementarmente, verifica-se que estes *inputs* iniciais são, na prática, informação concretizando-se o CPI na "sequência de atividades através das quais a informação

é obtida, analisada, convertida em Informações, e disponibilizada aos utilizadores" (NATO, 2016, p. 41).

Contudo o CPI, conforme enfatiza Menezes (2012), não é consensual no que concerne às etapas que o compõe, particularmente, em relação ao papel dos decisores no ciclo. Não obstante, na presente investigação tomar-se-á como referência o modelo padrão da NATO, uma vez que, corroborando com Santos (2012), este não colide com as diferentes visões existentes e consubstancia um maior grau de sistematização. Assim, segundo o AJP-2 (NATO, 2016), o CPI é constituído por quatro fases[94], a saber: orientação; pesquisa; processamento; disseminação. Na Figura 21 encontram-se representadas as 4 etapas do CPI da NATO. Embora estas etapas, figurativamente, transpareçam uma certa simplicidade são na verdade um processo complexo colocado em prática através da execução de múltiplas tarefas realizadas a diferentes ritmos e que podem não ser obrigatoriamente sequenciais.

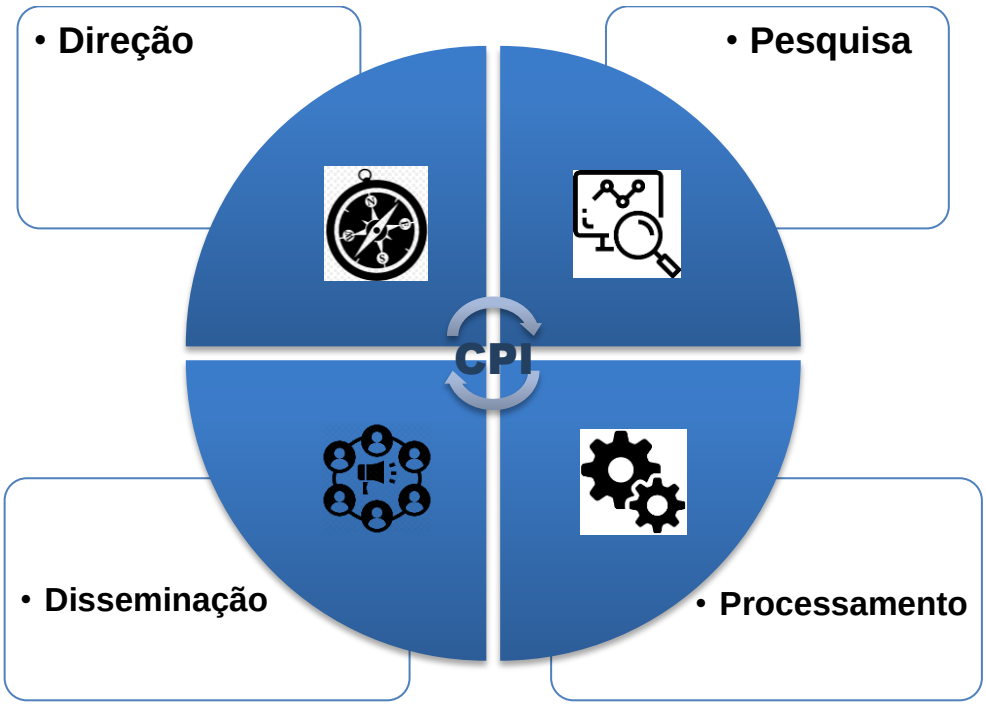

Figura 21 - Ciclo de Produção das Informações adaptado a partir do AJP – 2 (A) (NATO, 2016, p. 4_2)

A primeira fase do CPI é a direção[95] da pesquisa a qual consiste na definição dos requisitos de informação, no planeamento do esforço de pesquisa e no envio de diretrizes e pedidos para os órgãos de pesquisa. A segunda fase corresponde à pesquisa[96] traduzida na exploração das diversas fontes e ao envio da informação adquirida para o respetivo órgão de processamento competente para a produção de informações. A terceira fase denomina-se por processamento[97], na qual a informação

[94] Existem alguns autores, tais como Hughes-Wilson (1999) e Waltz (2003), que possuem um diferente entendimento quanto às fases que compõem o Ciclo de Informações, defendendo que este processo é constituído pelas seguintes etapas: direção e planeamento; pesquisa; processamento; análise e interpretação; disseminação.

[95] Tradução pelo autor a partir do termo *Direction*.

[96] Tradução pelo autor a partir do termo *Collection.*

[97] Tradução pelo autor a partir do termo *Processing.*

obtida será agregada, analisada e convertida em informações. Em concreto, esta fase subdivide-se em cinco etapas, nomeadamente: o registo; a avaliação; a análise; a integração e a interpretação. A disseminação[98] é a última fase deste ciclo e consiste em disponibilizar, em tempo oportuno e de modo apropriado, as informações obtidas aos respetivos decisores. Para este efeito, importa que, por um lado os meios utilizados na disseminação cumpram com os requisitos de segurança estabelecidos e, por outro as informações obtidas correspondam às necessidades dos decisores. Além disso, é ainda crucial neste processo a existência e utilização de um mecanismo de feedback por forma a otimizar e adequar as informações produzidas, de acordo, com as necessidades dos decisores (NATO, 2016).

4.2.2. Disciplinas das informações

Abordando mais ao pormenor a fase da pesquisa do CPI, importa realçar que, a recolha da informação pode ser realizada com recurso a diferentes fontes que se classificam e denominam por disciplinas das informações. Neste universo, de acordo com a NATO (2016), são utilizadas seis fontes principais de recolha de informação, nomeadamente: *Acoustic Intelligence* (ACINT); *Human Intelligence* (HUMINT); *Imagery Intelligence* (IMINT); *Measurement and Signatures Intelligence* (MASINT); *Signals Intelligence* (SIGINT); *Open-Source Intelligence* (OSINT)[99].

A ACINT concretiza-se através da recolha e análise de emissões sonoras. Neste universo, inserem-se como exemplos de fontes de ACINT os hidrofones, os sonares, os telefones submarinos e os sistemas integrados de vigilância submarina. Na realidade, face ao objeto de análise desta disciplina ser o som a ACINT cinge-se, sobretudo, ao movimento e consequentemente nas informações que provêm da sua deteção.

Por seu turno, a pesquisa de informação através de HUMINT realiza-se, tal como o próprio nome indica, por intermédio de fontes humanas. Segundo expõe Menezes (2012) o HUMINT é método mais antigo de recolha de informação, podendo ser efetuado de forma aberta – através de pessoal diplomático, postos consulares, contactos oficiais com governos estrangeiros, reportes de nacionais estrangeiros e cidadãos nacionais que viagem pelo estrangeiro – quer de forma encoberta – por meio da obtenção de fotografias, documentos e outro material.

[98] Tradução pelo autor a partir do termo *Dissemination.*

[99] De acordo com o AJP-2 (A), estas são as 6 disciplinas das informações que a NATO classifica como principais. Não obstante, denota-se que, atualmente existe uma tendência para alguns países e especialistas classificarem a *Geospatial Intelligence* (GEOINT) como uma disciplina das informações. Porém, a NATO (2016) refere-se ao GEOINT como sendo um produto especializado das informações, tendo-se seguido esta doutrina nesta investigação. Não obstante, observa-se que no Reino Unido, de acordo com o JDP-2-00 (MOD, 2011), a GEOINT é de facto considerada como uma disciplina das informações. Em maior detalhe, a GEOINT consiste na recolha de dados, por intermédio da exploração e análise de imagens e mapas, obtidos pela integração da IMINT com a informação geoespacial, por forma a estabelecer padrões ou extrair informação complementar. A GEOINT evoluiu a partir da IMINT fomentada pelo desenvolvimento dos Sistemas de Informações Geográficos (SIG) que permitiram a integração das imagens recolhidas, por meio de sensores remotos, com os dados georreferenciados provenientes de outras ciências (p. ex. aeronáuticos, geográficos, hidrográficos, oceanográficos e meteorológicos. Acresce que, a informação geoespacial pode ser obtida através de satélites (militares, de agências governamentais e comerciais) de aeronaves de reconhecimento, de *drones* ou através de mapas e bases de dados que possuam as posições geográficas.

A IMINT traduz-se na recolha de imagens sobre pessoas, alvos ou infraestruturas designadas. Estas imagens são obtidas através de sensores colocados e/ou transportados por meios terrestres, navais, aéreos ou espaciais e requerem uma análise especializada antes de serem utilizadas[100].

Por seu turno, a MASINT caracteriza-se pela informação tecnológica e científica utilizada para analisar os dados captados por diversos sensores com o intuito de detetar, localizar e/ou identificar quaisquer características distintivas associadas à fonte e ao emissor. Para esse efeito, recorrem à análise e ao emprego de um conjunto alargado de disciplinas, tais como: a acústica, a radiofrequência; a ótica; a química; a biologia; radiologia; o nuclear; e a sísmica.

A SIGINT consiste na interceção e monitorização de emissões eletrónicas e de comunicações. Por conseguinte, esta disciplina pode ser dividida em duas subcategorias, nomeadamente: *Communications Intelligence* (COMINT) que visa a captação de comunicações efetuadas entre emissores e recetores de interesse; *Electronic Intelligence (ELINT)* que resulta da interceção de emissões eletromagnéticas que não sejam comunicações.

Por fim, a OSINT reside na recolha de informação e notícias em fontes abertas, publicamente, disponíveis[101]. Nos últimos anos, com a globalização da internet a OSINT tem vindo a ganhar relevância face aos inúmeros conteúdos disponíveis para consulta e à rapidez de obtenção. Acresce que, a OSINT poderá ser, particularmente, útil no garante de uma melhor compreensão do contexto social, cultural e ideológico em que determinadas ações, operações e/ou missões se desenvolvem evitando erros de avaliação iniciais e apoiando a tomada de decisão.

4.3. Informações enquanto Produto

As informações enquanto produto visam descrever o conhecimento que é obtido no decurso do processo de informações, ou seja, do CPI.

Neste contexto, Carvalho (2009, p. 7), afirma que o produto das informações providencia o "conhecimento específico necessário à tomada de decisões". Este conhecimento, segundo a NATO (2016), deverá ser disponibilizado em tempo, de forma apropriada e por meios adequados para os decisores.

O General Pedro Cardoso (2004, p. 150) enfatiza que as "informações para serem úteis devem ser adequadas, oportunas e bastante precisas. Devem ainda ser muito bem coordenadas e integradas, e rápida, oportuna e apropriadamente difundidas e consideradas pelos responsáveis pela tomada de decisão". Por sua vez, Lowenthal (2006) acrescenta que as informações produzidas para serem consideradas úteis deverão respeitar quatro características principais, designadamente: serem

[100] Por norma, a IMINT é utilizada para corroborar ou confirmar a informação obtida através de outras fontes. Não obstante, existem casos ou situações concretas em que as informações obtidas pela IMINT são, por si só, suficientes sem necessidade de complemento de outra disciplina. Exemplo deste facto são os casos em que o objetivo se centra em mapear ou estabelecer determinados padrões de comportamento.

[101] Neste universo, verifica-se que, existe uma grande variedade de recursos disponíveis para a recolha de informação, designadamente: os *media,* tais como jornais, televisão, rádio, revistas; os documentos oficiais e registos públicos, como relatórios, informação estatística, bases de dados, orçamentos, etc.; a produção científica, como as conferências, as publicações académicas, os artigos de especialistas e as investigações; os inumeráveis conteúdos existentes na internet (Lowenthal, 2006).

atempadas; à medida; facilmente compreensíveis; objetivas no conhecido e desconhecido[102]. Em concreto, a exigência de as informações serem atempadas enfatiza que terão de ser recebidas pelos decisores em tempo útil por forma a poderem ser tidas em consideração durante o processo de tomada de decisão. A característica "à medida" implica que as informações obtidas correspondam às necessidades estabelecidas pelo decisor[103]. A capacidade de serem facilmente compreensíveis visa relevar que as informações produzidas deverão ser transmitidas de uma forma clara, assertiva e por meios apropriados aos decisores, de modo a facilitar a sua compreensão. Por último, separar o conhecido do desconhecido sublinha a necessidade de durante a transmissão das informações aos decisores afirmar-se, de forma clara e assertiva, o que se sabe, o que não se sabe e qual é o grau de confiança das informações.

Além destas características Hughes-Wilson (1999) defende que o produto do processo das informações deverá ser o mais honesto e imparcial possível resistindo a qualquer tipo de influências de cariz político, ideológico, religioso ou moral. Enfatiza ainda que as informações não deverão apresentar ao decisor aquilo que este espera obter como forma de sustentar uma decisão previamente tomada. Ao invés, o produto deve ser inquestionavelmente honesto, imparcial e objetivo.

Em relação à forma como o produto é apresentado ao decisor, observa-se que, este poderá assumir diversos formatos sendo os mais comuns os relatórios, os memorandos, as bases de dados e os *briefings* (Shlsky & Schmitt, 2002).

4.4. Organização

As informações enquanto organização focam os serviços de informações, analisando a sua estrutura orgânica e o modelo de funcionamento, através do qual conduzem o processo atinente à produção de informações.

Atualmente, constata-se que os interesses dos Estados são cada vez mais afetados por atores e ameaças de contornos indefinidos que dificultam, em larga medida, o emprego dos elementos tradicionais de poder[104] (Menezes, 2012). Neste enquadramento, é vital que os estados possuam estruturas capazes de identificar, caracterizar e avaliar, de forma permanente e sistemática, as ameaças do presente e que prevejam os riscos do amanhã, *i.e.*, é essencial a existência de Serviços de Informações. De acordo com Cepik (2003, p. 85) os serviços de informações consistem em "organizações permanentes e atividades especializadas em coleta, análise e disseminação de informações sobre problemas e alvos relevantes para a política externa, a defesa nacional e a garantia da ordem pública de um país"[105]. Em concreto, a estes compete-lhes, de acordo com Cruz (2019a, p.

[102] Tradução pelo autor a partir dos termos "*timing*", "*tailored*", "*digestible*", "*clear regarding the know and the unknown*", respetivamente.

[103] Neste âmbito, Lowenthal (2006) considera que o conhecimento mais adequado às necessidades dos decisores será aquele a que estes atribuíram um maior grau de prioridade na sua obtenção.

[104] Nesta temática, Carvalho (2009) salienta que, nos dias de hoje, o poder militar *per si* já não é suficiente para fazer face aos múltiplos desafios colocados pelas novas ameaças de natureza complexa, persistente, assimétrica, imprevisível e híbrida. Além disso, para a maioria dos Estados também não é exequível e sustentável deter um poder militar, verdadeiramente, dissuasor.

[105] De acordo com o SIRP (2020), a missão dos Serviços de Informações, num Estado de Direito Democrático, assenta na "proteção dos interesses nacionais, da soberania nacional, da segurança e salvaguarda de Portugal e dos cidadãos portugueses, preservando as instituições de ameaças, tanto a nível interno como a nível externo".

5), “produzir conhecimento que reduza drasticamente a esfera de incerteza, gerando avaliações e cenários que garantam que a tomada de decisão de hoje acautela e mitiga os riscos potenciais do amanhã.”

No que concerne ao desenho orgânico, que serve de base à articulação e ao funcionamento dos Serviços de Informações, Warner (2009) defende que existem três fatores fundamentais a considerar, nomeadamente: a Grande Estratégia Nacional (GEN), o regime político e a tecnologia.

Em traços gerais, segundo Warner (2009), é através da GEN que um estado define os seus objetivos internacionais e identifica os estados ou organizações, contrárias ou adversárias, à prossecução daqueles[106]. Por conseguinte, conforme sublinha Menezes (2012), a GEN é a base para a determinação dos recursos que uma nação irá alocar para a atividade de informações.

O segundo fator que condiciona, em larga medida, a organização dos serviços de informações é o regime político[107]. Com efeito, conforme expõe Warner (2009), os regimes democráticos tendem a dar mais importância às informações externas que internas, dado que, ideologicamente, a base da democracia são os direitos, liberdades e garantias dos seus cidadãos. Pelo contrário, os regimes ditatoriais o enfoque assenta na manutenção do poder estabelecido, pelo que tendem a relevar mais as informações de natureza interna, a fim de controlar possíveis incitadores e beligerantes contra o regime.

O terceiro fator é a tecnologia[108] que ao determinar, copiosamente, quer os tipos e a quantidade dos meios empregues, quer os métodos utilizados na produção de informações condiciona as estruturas dos sistemas de informações.

Importa relevar, ainda, que os serviços de informações enquanto organização “são o resultado de processos específicos de criação de soluções para os desafios na área do interesse nacional” (Menezes, 2012, p. 20). Perante a circunstância de, no panorama atual, ser bastante complexo identificar as intenções e as movimentações dos novos agentes de ameaça observa-se uma mudança de paradigma do *need to know* (necessidade de conhecer) para o *need to share* (necessidade de partilhar), dado que a imprevisibilidade, complexidade e assimetria que caracterizam estas ameaças não se coaduna mais com uma estratégia de segredo, antes pelo contrário. Ora, esta mudança de paradigma, também, impõe aos serviços de informações a necessidade de possuírem estruturas

[106] Segundo Warner (2009), a delimitação da GEN deverá ter em linha de conta com sete fatores fundamentais, a saber: a postura, que poderá ser passiva, belicosa, ou ativa; a geopolítica que retrata as relações de poder na região em que se insere; os motivos, ou seja, os fins da política externa; os objetivos subsequentes aos motivos; a identificação dos aliados e dos parceiros; o panorama internacional em que se insere, que poderá ir desde a cooperação ao conflito; e a cultura estratégica.

[107] Neste âmbito, Warner (2009) defende que, existem cinco elementos importantes associados ao regime político que influenciam a organização, nomeadamente: a tipologia da soberania (p. ex. um Estado, uma Cidade-Estado, um Império, etc); a forma de governo, nomeadamente, a tirania, a aristocracia, ou representativa; a fiscalização, i.e., o modo pelo qual realizam a supervisão dos Sistemas de Informações; a própria estrutura ministerial e/ou departamental; e os desafios internos desencadeados por oposição, criminalidade e conflitos internos.

[108] A este respeito, Warner (2009) identifica cinco elementos que condicionam o emprego e utilização da tecnologia para a obtenção de informações, designadamente: a informação, i.e. o modo como esta é recolhida, arquivada, disseminada e protegida; os tipos e características dos “alvos”; os recursos disponíveis; o modelo sociocultural em que a sociedade se organiza; e o predomínio ou não de uma corrente securitária e/ou militar, dado que, estas irão determinar os tipos, as capacidades e a relevância relativa aos meios de pesquisa e disseminação das informações produzidas.

orgânicas mais ágeis e flexíveis por forma a se adaptarem, de um modo eficiente, à evolução do meio em que operam[109].

4.5. Conhecimento Situacional no Ciberespaço (CSC)

Nos dias de hoje, face à conjuntura atual verifica-se que, inequivocamente, a "capacidade para avaliar a dinâmica das ameaças e perceber as possibilidades e intenções potenciais atacantes constitui uma precondição para a proteção das infraestruturas de informação e para a condução de operações no ciberespaço" (MDN, 2013, p. 31978). Em concreto esta relevante capacidade denomina-se por CSC[110], sendo inclusive, aludida como o "Santo Graal" do ciberespaço (Ali, 2016).

Segundo a NATO (2020) o CSC resulta da combinação em, praticamente, tempo real do panorama situacional no ciberespaço *(Recognized Cyberspace Picture* (RCP)) com a análise e a gestão das informações. A montante, importa salientar que o conceito de conhecimento situacional nos últimos anos aplicado, também, ao ciberespaço foi primeiramente notabilizado pelo célebre piloto alemão, da Primeira Guerra Mundial, Oswald Boelcke[111]. Em concreto, Boelcke demonstrou a importância de nas disputas (estratégicas, operacionais e táticas) ser crucial obter um conhecimento sobre o inimigo e/ou contrário antes que este consiga ganhar um conhecimento similar (Jesus, 2019b).

4.5.1. Ciclo de *Boyd* e o Conhecimento Situacional no Ciberespaço

Transversalmente ao domínio de condução de operações em que se opere, evidencia-se que o conhecimento situacional é um dos fatores que contribuiu, decisivamente, para a eficiência dos processos de tomada de decisão.

Neste âmbito, um dos modelos de tomada de decisão mais conhecidos e amplamente utilizados denomina-se por OODA *Loop*, acrónimo para Observar, Orientar, Decidir e Agir[112]. Este ciclo de tomada de decisão foi proposto pelo Coronel da Força Aérea dos EUA John Boyd[113], tendo sido formalizado com base na sua experiência, enquanto piloto na Guerra da Coreia e mais tarde como instrutor. Em concreto o OODA Loop tem como finalidade apoiar e simplificar o processo de tomada de decisão através da implementação de um ciclo lógico constituído pelas quatro etapas, citadas e apresentadas, na Figura 22.

[109] A título de exemplo, tome-se em consideração a afirmação do antigo SG do SIRP, Júlio Pereia, ao referir que o tratamento das ciberameaças "impôs novas áreas de especialização profissional e novos desafios técnicos e metodológicos" (SIRP, 2015, p. 3).

[110] Tradução do autor da designação anglo-saxónica Cyber *Situation Awareness.*

[111] O piloto alemão Oswald Boelcke (1891 - 1916) evidenciou-se durante a Primeira Guerra Mundial, ao formalizar várias estratégias e táticas sobre o combate aéreo. É inclusive, considerado por muitos investigadores como o "pai" da Força Aérea Alemã (2019b).

[112] Tradução do acrónimo OODA, que constituído pelas seguintes fases: O – *Observe*; O – *Orient*; D – *Decide*; A – *Act.*

[113] *John Boyd (1927 – 1997)* foi um piloto da Força Aérea dos EUA, que combateu na Guerra da Coreia (1950-1953), desempenhando posteriormente funções de instrutor de voo. Após passar à reserva, foi consultor do Pentágono, onde desenvolveu investigação sobre a história, a teoria e as táticas da guerra. Como resultado destas investigações, formulou o Ciclo OODA, ou Ciclo de *Boyd*, assim, também, denominado em sua homenagem, o qual representa, no fundo, o resultado de uma vida de análise e estudo.

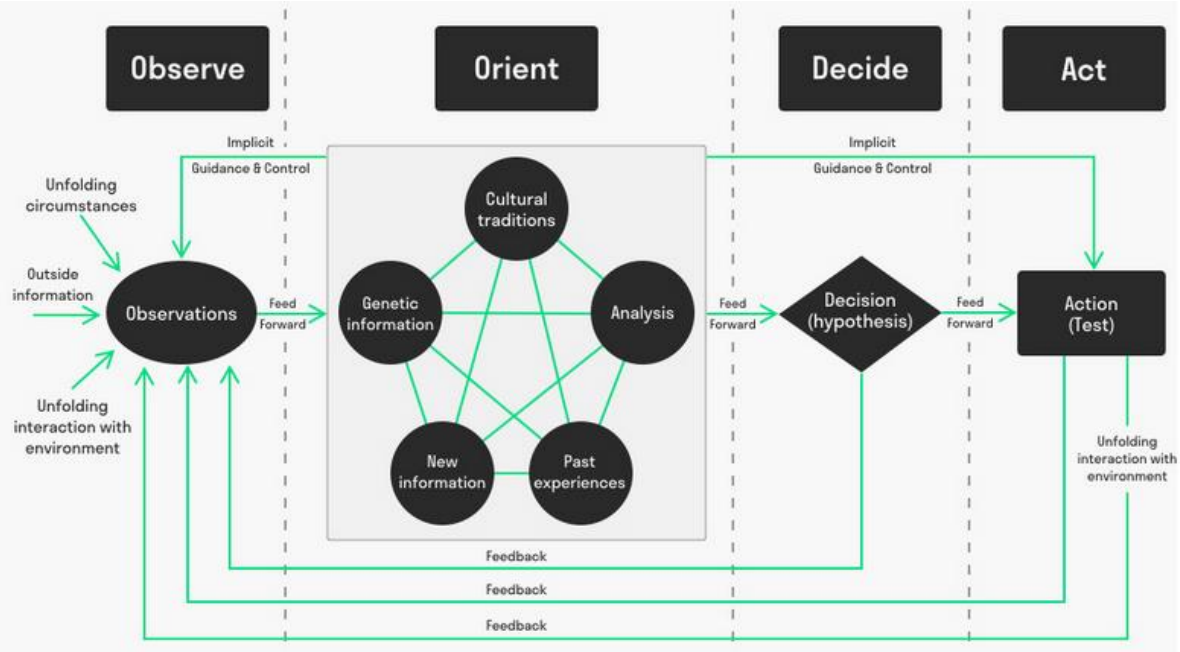

Figura 22 – Modelo OODA *Loop* (Ciclo de Boyd) (Mulder, 2017)

Em traços gerais a observação, corresponde à primeira fase do *OODA Loop*, consubstancia-se na recolha de informação no ambiente externo e na identificação das circunstâncias em curso. Esta fase deverá ser realizada de forma permanente sendo a fonte primária, de colheita de informação, para apoio do processo de decisão. Considerando o ambiente ciberespaço a observação corresponde à tomada de consciência e perceção por parte dos estados, organizações e cidadãos do que está a ocorrer e a evoluir no ciberespaço de interesse. No fundo, a fase de observação é concretizada através de uma constante e atenta vigilância do ciberespaço.

A segunda etapa, do *OODA Loop,* é a orientação que tem como objetivo a assimilação e compreensão da realidade através do processamento da informação captada durante a observação. A orientação é bastante condicionada pelas características, intrínsecas e particulares, de cada indivíduo e da organização, dado que poderá ser influenciada por diversos fatores, tais como a herança genética, a cultura, contexto sociocultural e experiência acumulada (Jesus, 2019b). A orientação no ambiente digital realiza-se por intermédio de ferramentas e métodos de análise, bem como da correlação e agregação da informação disponibilizada pelas diversas fontes existentes no ciberespaço de interesse. Após isso, as informações obtidas serão, desejavelmente, partilhadas entre as organizações de uma determinada *Community of Interest* (COI) com vista à tomada de decisão. Por conseguinte, conforme evidencia Jesus (2019b), as fases da observação e da orientação formam o conhecimento situacional.

A terceira fase do ciclo é a decisão que se fundamenta na seleção de uma linha de ação concebida durante a fase da orientação. No ciberespaço, como em qualquer outro domínio da condução de operações, a decisão dever-se-á apoiar no conhecimento situacional resultante das fases anteriores.

A quarta etapa do *OODA Loop* corresponde à ação que é, no fundo, a colocação em prática da linha de ação selecionada na fase da decisão.

Após ser executada a ação o ciclo inicia-se, novamente, com a observação de modo a confirmar se os resultados obtidos correspondem ao efeito final desejado. Caso corresponda, o ciclo manter-se-

á na observação até existir alguma alteração significativa. Pelo contrário, caso não tenha sido alcançado o efeito desejado, o decisor deverá continuar com a implementação do *OODA Loop*, passando às fases subsequentes e assim continuadamente.

Por fim, considera-se que a implementação do *OODA Loop* é fundamental para que se obtenha uma eficiente tomada de decisão em qualquer um dos domínios da condução de operações. Conforme evidenciado o ciberespaço não é exceção. Pelo contrário, num ambiente que se caracteriza pela velocidade, intangibilidade, anonimato e assimetria é essencial recorrer a ferramentas e a processos que possibilitem a obtenção de um célere e completo conhecimento situacional, por forma a apoiar a tomada de decisão, com vista à antecipação, defesa e mitigação dos ciberataques.

Por isso, em seguida, analisar-se-ão, os principais aspetos a considerar para a obtenção de um integral CSC.

4.5.2. Principais aspetos a considerar para a obtenção do Conhecimento Situacional no Ciberespaço

Segundo o Chefe da *Task-Force Cyber* no *Supreme Headquarters Allied Powers Europe (SHAPE),* Coronel *Rizwan Ali* (2016), para se alcançar um amplo e robusto CSC é necessário tomar em linha de conta com três aspetos principais, a saber: as ameaças; a rede; e a missão. A Figura 23 representa esquematicamente a relação de dependência destes três fatores para a obtenção de um robusto CSC.

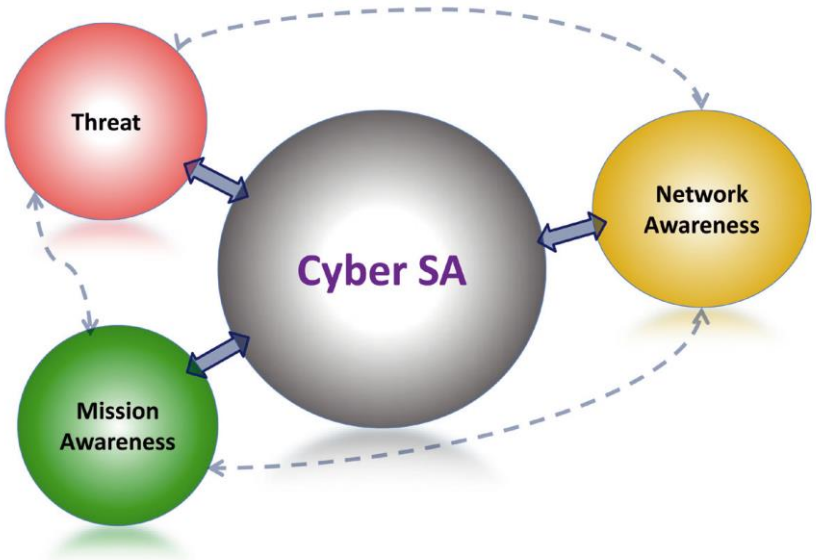

Figura 23 – Os fatores essenciais para a obtenção de um Conhecimento Situacional no Ciberespaço (Ali, 2016, p. 73)

Em relação às ameaças, tema bastante aprofundado no 2º Capítulo da presente investigação, Ali (2016) classifica-as, sumariamente, em provenientes de Atores Estatais e de Atores não Estatais (Figura 24). As ameaças com origem em Atores Estatais podem ser levadas a cabo por nações ou por intermediários a mando destas. Por sua vez, no conjunto das ameaças procedentes de Atores não Estatais destacam-se os cibercriminosos, os *hacktivistas*, os espiões industriais, os *hackers* e os terroristas.

Figure 2: The Threat Component

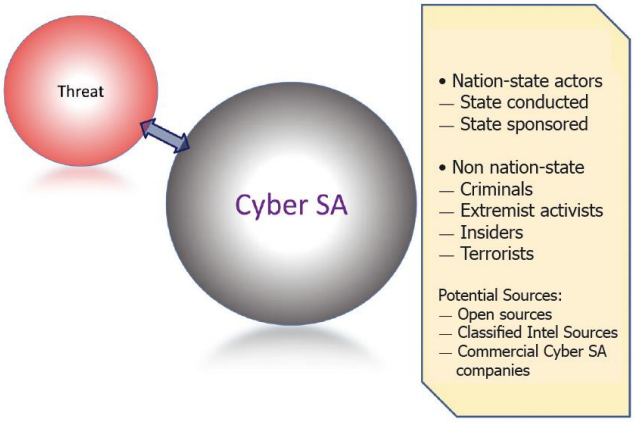

Figura 24 - As Ameaças enquanto componente essencial para o CSC (Ali, 2016, p. 74)

Um segundo aspeto essencial para o CSC é a perceção integral do estado de situação da infraestrutura da rede (Figura 25). Para esse efeito, é necessário realizar, simultaneamente, uma monitorização contínua do estado da cibersegurança e da integridade geral da rede e, ainda, uma constante correlação dos diversos incidentes que vão surgindo, por forma a determinar a existência de tendências ou de ameaças persistentes pairando sobre a rede. Para além do conhecimento do estado de situação da segurança interna da rede é, também, importante observar e monitorizar as principais mudanças e os incidentes que ocorrem na infraestrutura da rede global. Desta forma, será possível acompanhar os seus impactos, retirar possíveis ilações e ensinamentos úteis para a prevenção de futuros incidentes[114].

Figure 3: Network Component

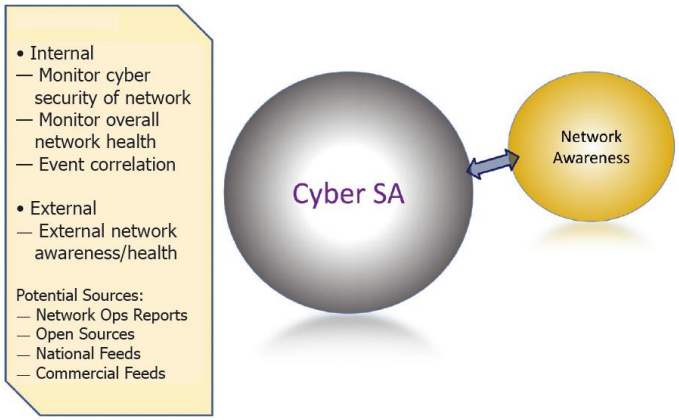

Figura 25 - O conhecimento da rede enquanto componente essencial para o CSC (Ali, 2016, p. 74)

Um terceiro aspeto relevante para o CSC centra-se na monitorização do ciberespaço durante a condução de operações e, consequentemente, no cumprimento de missões. Na perspetiva de Ali (2016) a perceção da evolução da situação no ciberespaço é crucial, quer durante a fase do

[114] Um exemplo, paradigmático deste facto ocorreu, segundo Ali (2016), com a descontinuidade a nível global do Windows XP. Com efeito, e apesar de, a nível interno a NATO e os seus Estados-membros terem acompanhado a evolução e o impacto que esta mudança teve nas suas redes, demonstrou-se ser bastante importante e avisado seguir as implicações originadas à escala global.

planeamento das missões (por forma a identificarem-se ameaças, potenciais problemas, e possíveis respostas de proteção pré-planeadas), quer durante a fase do cumprimento das missões pois a segurança do ciberespaço é um aspeto vital para o sucesso das mesmas. A Figura 26 enfatiza a importância da monitorização da missão, para a obtenção de um robusto CSC no teatro, onde esta se desenrola.

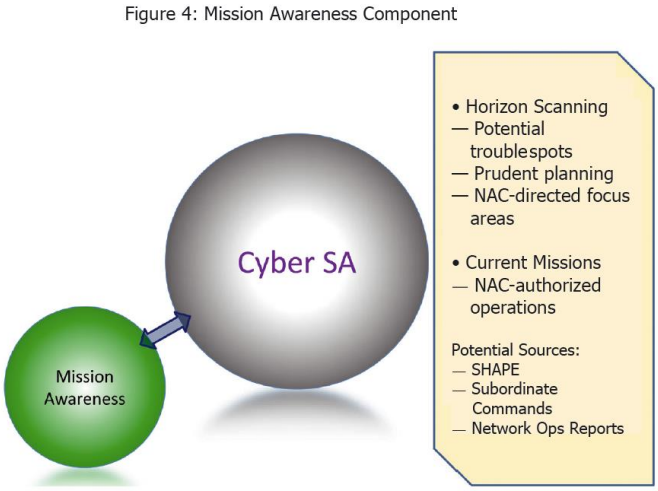

Figura 26 - A monitorização da missão enquanto componente essencial para o CSC (Ali, 2016, p. 75)

Por fim, por forma a construir e obter-se um amplo e mais completo possível CSC, torna-se necessário agregar e analisar, em simultâneo, estes três componentes essenciais elencados. Este processo deverá, conforme evidencia Ali (2016), ser realizado por uma equipa especializada e com *Know-how* apropriado capaz de apresentar as informações produzidas de uma forma adequada, eficiente e fidedigna aos principais decisores.

4.6. Partilha de informação no ciberespaço: O Caso do MISP

A incerteza contínua que paira sob a segurança no ciberespaço, resultante das várias ameaças de natureza difusa, de limites indefinidos e em constante evolução, exige a existência de uma capacidade que permita detetar e identificar, em tempo útil, os indicadores que possam estar relacionados com ataques potenciais e em curso. A esta capacidade, conforme evidenciado, denomina-se de CSC.

Para a construção de um robusto CSC é essencial existir, ainda, entre as principais autoridades, entidades e organizações, nacionais e internacionais, que contribuem para a segurança do ciberespaço uma partilha de informação, conhecimento e informações, eficiente e atempada, que possibilite realizar uma avaliação precoce da ameaça. Visando a prossecução deste objetivo, afigura-se como crucial possuir um sistema que permita realizar a partilha de forma automatizada, sistematizada e eficaz destes indicadores de ameaça.

Com efeito, foi para acorrer a esta necessidade que foi edificada, desenvolvida e implementada a plataforma *MISP*, a qual se abordará, no próximo subcapítulo. Por fim, antes disso, importa apenas

salientar que a escolha da análise desta plataforma, em detrimento de outras ferramentas[115], deveu-se aos seguintes fatores: é uma plataforma *open-source*, com muita informação disponível para consulta; é uma plataforma em funcionamento ou já em processo de implementação em todas as entidades do G4; facilidade de acesso e exploração da plataforma por parte do autor e dos peritos que contribuíram para a presente investigação.

4.6.1. A origem do MISP e o conceito *Smart Defence* da NATO

Em 2012, a NATO, no seguimento da Cimeira de Chicago, lançou a iniciativa *Smart Defence* (SD) que tem como finalidade estimular e apoiar os Estados-membros a adquirirem, desenvolverem e manterem capacidades militares. Para esse efeito a NATO através do conceito SD procura promover sinergias e a integração das capacidades dos países aliados e parceiros, com base num racional *pooling & sharing*, por forma a minimizar a duplicação de recursos e melhorar a coordenação de esforços entre a Aliança e as nações aliadas (NATO, 2015).

Assente neste racional a NATO, no âmbito da ciberdefesa, promoveu o desenvolvimento de três projetos de SD, nomeadamente: o *Multinational Cyber Defence Capability Development* (MN CD2); o MN CD E&T; o MISP.

Sucintamente, o projeto MN CD2 foi criado em 2013[116] e tem como objetivo edificar e desenvolver, ao nível genético, as capacidades de ciberdefesa das nações aliadas com vista à prevenção, deteção, defesa e recuperação de ciberataques.

Por sua vez, o projeto MN CD E&T foi liderado por Portugal[117], terminou em 2019[118] e teve como resultado a criação de um currículo *cyber*, a ser ministrado na NCI *Academy* em Oeiras, e a elaboração de um conjunto de recomendações para colmatar as lacunas detetadas nas áreas da educação e do treino (Academia Militar, 2019).

Finalmente o projeto MISP, de gênese *open source*, foi concebido por *Christophe Vandeplas*[119], em junho de 2011, inicialmente denominado de *Cyber Defence Signatures* (CyDefSIG). Em meados de agosto de 2011 o Ministério da Defesa Belga, observando os benefícios e as capacidades do projeto, decidiu patrocinar e colaborar na sua edificação. De igual modo, a NATO, em 2012, após ter tomado conhecimento das potencialidades do CyDefSIG decidiu, também, apoiar o seu desenvolvimento. Mais

[115] Em virtude da limitação da dimensão da presente investigação, o autor, teve naturalmente de fazer escolhas sobre os conteúdos a abordar e neste caso, sobre a plataforma a estudar. Na secção 4.7.4 será discutida a relevância do *MISP,* enquanto plataforma de partilha de informação, expostas, em maior detalhe, as razões da sua escolha como objeto de estudo e identificadas mais-valias e aspetos a melhorar.

[116] Formalmente, o MN CD2 foi criado a 14 de março de 2013 pelas cinco nações fundadoras, a saber: o Canadá; a Dinamarca; a Holanda; a Noruega; e a Roménia (NCIA, 2020).

[117] Em resultado do grande *know-how* adquirido com a liderança do projeto MN CD E&T, Portugal decidiu lançar uma extensão nacional deste projeto, denominando por *Cyber Academia and Innovation Hub* (CAIH). Em concreto, o CAIH é um projeto na área da ciberdefesa e da cibersegurança que tem como "missão estimular a Educação, Treino, Investigação, Inovação e o Desenvolvimento da Indústria no domínio *ciber*, para alimentar o ecossistema nacional e internacional com o conhecimento e competências necessárias à nova geração de profissionais, e para apoiar o desenvolvimento de capacidades" (MDN, 2020).

[118] O projeto MN CD E&T foi dado como formalmente concluído, em 16 de maio de 2019, durante a realização da 5ª Conferência Internacional dos Projetos *Smart Defence* de Ciberdefesa da NATO, que teve lugar na Academia Militar, culminando com a entrega do Relatório Final à NATO e com o desenvolvimento de uma plataforma web que permite a coordenação das atividades de formação na Aliança (Academia Militar, 2019).

[119] A origem do projeto remonta a junho de 2011, quando o investigador Christophe Vandeplas teve a iniciativa de idealizar e criar uma plataforma que partilhava os Indicadores de Compromisso de forma automática, ao invés de, utilizar para o efeito, o e-mail ou relatórios (MISP, 2020a).

tarde, em 2013, a NATO, perante a virtualidade e os avanços alcançados, instituiu formalmente o CyDefSIG como um projeto SD (SD 1.35), com o desígnio da partilha de informação como meio vital para "derrotar" os ciberataques, renomeando-o de *MISP* (MISP, 2020a).

O projeto MISP foi liderado pela Bélgica e tem como finalidade promover a partilha de informações sobre características técnicas de *malware* e de indicadores de potenciais ameaças, através de uma plataforma comum, a uma comunidade de utilizadores, procurando garantir a segurança no ciberespaço através da detenção antecipada de ciberataques. Além disso, o MISP estimula, em larga medida, a interoperabilidade entre as nações aliadas, sendo que na atualidade a rede de utilizadores vai muito para além da Aliança e dos Estados Membros (NATO, 2013). Com efeito, desde a sua génese até aos dias de hoje, muitos outros países, organizações e parceiros têm vindo a adotar e a contribuir para o desenvolvimento desta plataforma, tais como o CERT da UE, o CIRC do Luxemburgo, entre muitos outros[120]. A Figura 27 exemplifica os vários grupos de partilha de informação instituídos a partir do *NATO Computer Incident Response Capability* (NCIRC).

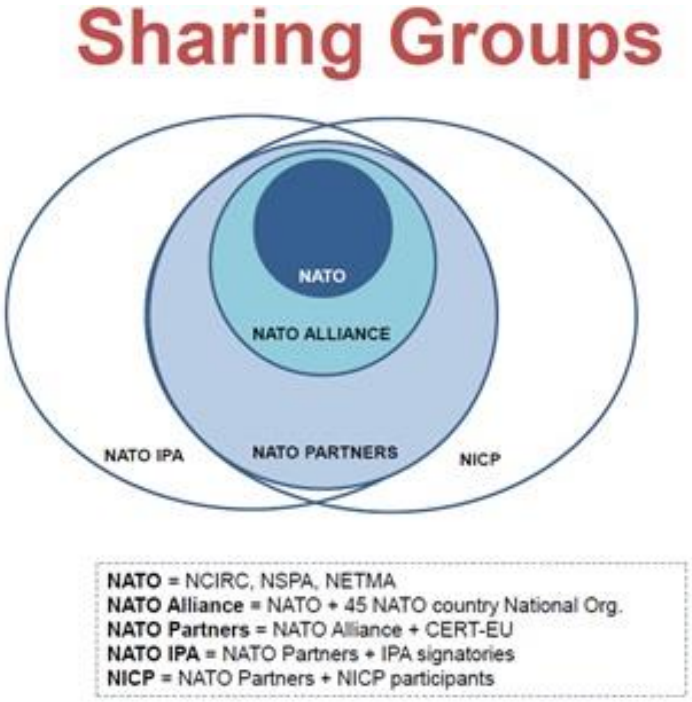

Figura 27 – Representação da rede de partilha MISP a partir do NCIRC (Schrooyen, 2017, p. 13)

4.6.2. Conceito, objetivos e tipos de utilizadores do MISP

O *software* MISP – *Open Source Threat Intelligence and Sharing Platform* – visa facilitar a partilha, armazenamento e correlação de informações sobre ameaças, Indicadores de Compromisso (IoC)[121] referentes a *malware* e a ataques, fraudes financeiras ou qualquer outro tipo de informações

[120] Com a expansão do projeto MISP, o MISP não cobre apenas os indicadores de *malware*, mas também informações sobre fraudes ou vulnerabilidades. O MISP é agora um projeto comunitário, com um número bastante elevado de participantes, os quais poderão ser consultados na página oficial do projeto (www.misp-project.org).

[121] São artefactos e/ou traços relevantes observados numa rede ou num sistema de informação conectados a uma intrusão ou a uma técnica utilizada por um invasor de uma rede ou sistema de informação (CIRCL, 2019). Os IoC são um subgrupo dos indicadores de ameaças, conforme Mapa Conceitos Anexo A.

importantes de cibersegurança e proteção, dentro de uma comunidade de membros confiáveis. A partilha de informação através do MISP operacionaliza-se tendo por base uma plataforma segura e de fácil utilização, assente num modelo de partilha distribuído[122], através da troca de informação de ordem técnica e não técnica relacionada com m*alware,* que poderá ser partilhada dentro de uma comunidade privada, semiprivada ou aberta (MISP Community, 2019) .

Assim, poder-se-á referir que o MISP, de uma forma simplificada e não exaustiva, resulta da combinação e articulação entre três pilares essenciais, nomeadamente: a infraestrutura técnica (plataforma); a informação que é partilhada; a comunidade de utilizadores que o integram. Com efeito, como resultado da conjugação eficiente entre estes três componentes, emerge uma relação de confiança importante, quer para o sucesso e utilidade do próprio MISP, quer para a segurança e proteção do ciberespaço (Schrooyen, 2017). A Figura 28 representa esquematicamente a relação entre os três pilares, supracitados, destacando-se na base do sistema a confiança.

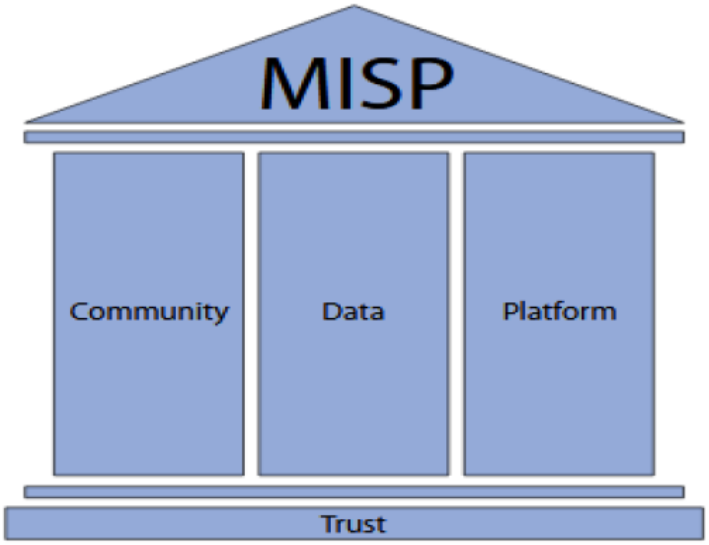

Figura 28 – Representação dos três componentes essenciais para o funcionamento do MISP, evidenciando-se a confiança como a base do sistema (Schrooyen, 2017, p. 4**)**

De facto, conforme realça Schrooyen (2017, p. 3), a finalidade do MISP poderá ser, justamente, sintetizada pela expressão "*share to win*", onde todos os utilizadores se beneficiam, mutuamente, do conhecimento sobre *malware* e indicadores[123] de ameaça. Neste sentido, infere-se que, um dos objetivos do MISP visa ajudar a melhorar as contramedidas utilizadas para a defesa de ataques direcionados e apoiar a definição de medidas preventivas e de deteção (CIRCL, 2020a) . Na Tabela 6, identificam-se, complementarmente, mais alguns objetivos do MISP.

[122] No qual os membros podem contribuir com informação ou serem apenas consumidores, não existindo, a obrigatoriedade de os membros partilharem informação, embora, naturalmente, assim seja desejável para o sucesso da própria plataforma e da proteção e segurança do ciberespaço de interesse no geral.

[123] De acordo com o Glossário MISP do CIRCL (2019), indicadores de ameaça, ou simplesmente indicadores são um padrão que pode ser utilizado para detetar atividades suspeitas ou maliciosas no ciberespaço. Conforme referido anteriormente, os IoC são um subgrupo dos indicadores.

Tabela 6 – Objetivos gerais do MISP, adaptado de (CIRCL, 2020a)

Objetivos do MISP – *Open-Source Treat Intelligence and Sharing Platform*
Partilhar atributos de *malware* e IoCs com parceiros e grupos de confiança.
A partir da troca de informações, entre parceiros e grupos de confiança, reduzir a duplicação de esforços atinentes à implementação de soluções para a proteção e mitigação de ataques.
Facilitar o armazenamento de informações técnicas e não técnicas sobre *malware* e ataques detetados.
Criar automaticamente relações entre o *malware* e os seus atributos.
Armazenar dados em formatos estruturados, por forma a permitir a utilização automática da base de dados para alimentar os sistemas de deteção ou as ferramentas de análise forense.
Definir regras para o *Network Intrusion Detection System* (NIDS) que poderão ser importadas para sistemas do tipo *Intrusion Detection System* (IDS), como p. ex., endereços de IP, nomes de domínio, *hashes* de arquivos maliciosos, padrões de memória, entre outros.
Melhorar a deteção de *malware* para promover a troca de informações entre as organizações (por exemplo, evitando trabalhos duplicados).
Edificar um ecossistema de confiança, assente em informações fiáveis de parceiros confiáveis.
Armazenar localmente todos os dados e informações das diversas instâncias, garantindo a disponibilidade, integridade e confidencialidade na consulta.

4.6.3. Aspetos gerais sobre o funcionamento do MISP

Nesta secção serão analisadas, em traços gerais, alguns dos principais aspetos da arquitetura de funcionamento do MISP e suas principais funcionalidades[124]. Com efeito, com esta análise, pretende-se demonstrar a importância que o MISP em concreto e as plataformas de partilha de informações, em geral, podem desempenhar na salvaguarda da segurança das redes e dos sistemas de informação dos Estados, organizações e cidadãos e, por conseguinte, na segurança do ciberespaço.

4.6.3.1. Partilha e sincronização automática de atributos

A principal funcionalidade do MISP é, conforme já enfatizado, a partilha de informação onde todos os membros participantes podem ser consumidores e/ou contribuidores. Neste âmbito, em virtude de o MISP permitir o funcionamento integrado de diferentes servidores, também, denominados por *MISP Instances*, tem capacidade para sincronizar os eventos[125] e os atributos[126] de forma automática entre os diversos servidores MISP, conforme representado na Figura 29.

[124] Importa esclarecer que, as funcionalidades do MISP expostas na presente investigação não são exaustivas, tendo-se selecionado aquelas que se considerou como mais importantes para a descrição do funcionamento e demonstração da utilidade da plataforma. Por conseguinte, para uma maior consulta das funcionalidades do MISP, recomenda-se a consulta da página oficial do projeto (misp-project) (MISP, 2020b).

[125] Segundo o Glossário MISP do CIRCL (2019), são "encapsulamentos" de informações contextualmente relacionadas sobre um determinado acontecimento numa rede ou sistema de informação, representadas como um atributo e objeto.

[126] De acordo com o CIRCL (2020b), os atributos podem ser qualquer tipo de dados que ajudem a prever a intenção de um pacote de eventos, retirados a partir de indicadores, vulnerabilidade detetadas ou qualquer outra informação relevante extraída. Na prática, os atributos podem ser indicadores de rede (p. ex. endereços de IP), indicadores do sistema (p. ex. uma sequência na memória) ou até, inclusive, detalhes de uma conta bancária. Por conseguinte, um atributo é descrito por um tipo de informação, p. ex. MD5, URL (CIRCL, 2019).

Para esse efeito, o sistema utiliza funcionalidades de filtragem avançada por forma a respeitar as políticas de partilha das várias instâncias, incluindo, mecanismos de distribuição ao nível dos atributos (MISP, 2020b).

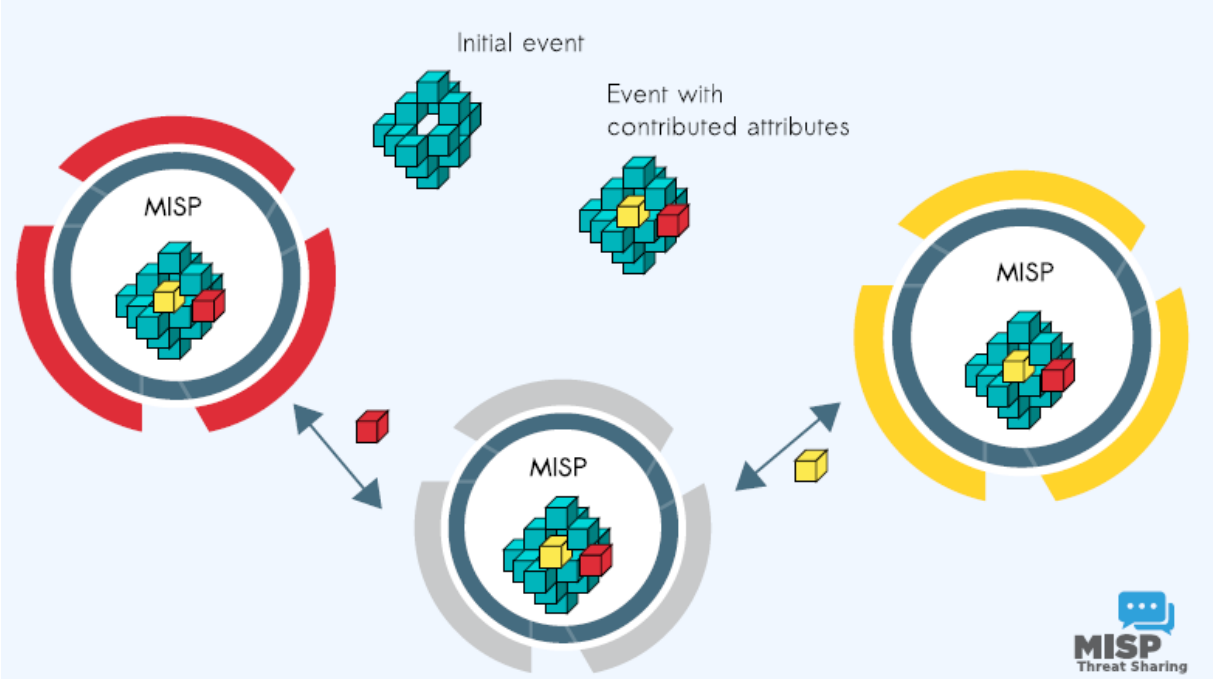

Figura 29 – Representação geral da partilha de informação entre os vários servidores MISP (CIRCL, 2020, p. 13)

4.6.3.2. Base de dados de IoC e atributos

No centro da arquitetura do MISP encontra-se a base de dados de armazenamento de IoC e de indicadores de ameaça, gerada e alimentada através da partilha de informação pelos membros que integram a comunidade, que permite guardar uma elevada quantidade de dados técnicos e não técnicos, sobre amostras de *malware,* incidentes e informações referentes a ameaças. Estes dados são armazenados num formato estruturado permitindo a utilização automática da base de dados. Assim, o MISP facilita, desde logo, a partilha de informação entre os vários técnicos, organizações e entidades parceiras na segurança do ciberespaço.

Complementarmente, o MISP, a fim de otimizar a partilha e sincronização automática de informação, utiliza *Application Programming Interface* (API)[127], por forma a incrementar a comunicação "maquina para máquina" [128]. Em traços gerais, API são um conjunto de métodos de comunicação pré-definidos entre os diversos componentes de *software* existentes (CIRCL, 2019). Por conseguinte, o MISP com recurso a API permite a geração de regras do tipo IDS[129]/*Intrusion Prevention Systems* (IPS)

[127] Para comunicar com o MISP a API padrão denomina-se por PyMISP (CIRCL, 2019).
[128] Segundo o CIRCL (2019), uma boa API potencializa o desenvolvimento de um programa de computador, fornecendo todos os blocos de construção, que são reunidos pelo programador. Por norma, as API caracterizam-se por serem bastante versáteis, podendo ser utilizadas como apoio a sistemas web, sistemas operacionais, sistemas de bases de dados, *hardware* ou mesmo bibliotecas de *software*.
[129] Vd. conceito de IDS no Anexo A.

(p. ex. Snort /Suricata/Bro (Zeek)[130] e de dados no formato compatíveis para *Security Information and Event Management* (SIEM)[131] (p.ex. CEF), *Structured Threat Information Expression* (STIX)[132], *Open IoC*, ou simplesmente texto, permitindo a sua exportação de forma automática para os sistemas de deteção de intrusos possibilitando uma deteção, mais eficiente e célere, de futuras intrusões (MISP, 2020b). A Figura 30 ilustra a base de dados no centro da arquitetura do MISP relevando-se a sua importância para a eficácia do funcionamento da plataforma.

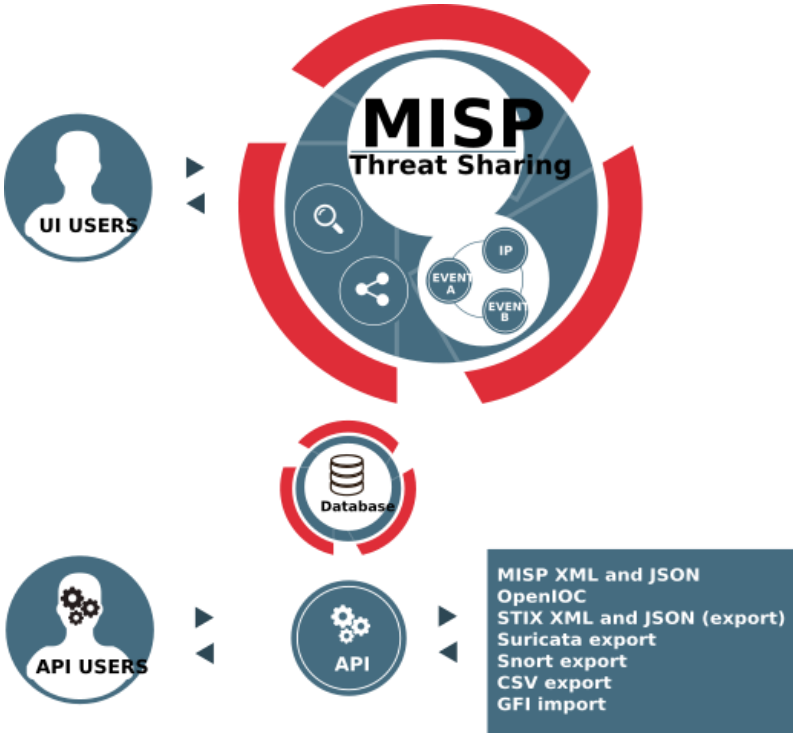

Figura 30 – Importância da base de dados na arquitetura de funcionamento do MISP (MISP, 2020b)

4.6.3.3. MISP *Instances*

Como já referido anteriormente, o MISP permite o funcionamento integrado e simultâneo de várias comunidades de utilizadores. Sucintamente, as comunidades são grupos de utilizadores que partilham um conjunto de objetivos e de valores comuns (CIRCL, 2020b).

Uma das grandes preocupações que emerge aos potenciais utilizadores do MISP, aquando da avaliação da adoção ou não desta plataforma, é a possibilidade de se conseguir limitar a partilha de informações, consideradas sensíveis, para uma comunidade específica. Neste enquadramento, surgiu a necessidade de se criar e operacionalizarem várias instâncias no MISP, que na prática, são

[130] Correspondem a sistemas *Open Source* de IDS. Para mais informações sobre estes sistemas de deteção de intrusos, as suas vantagens e potencialidades, recomenda-se a consulta do artigo publicado por Langston (2020).

[131] Em traços gerais, um SIEM é um *software* que permite correlacionar os eventos gerados por diversas aplicações de segurança informática transformando-os em informação facilmente percetível e de fácil utilização pelos utilizadores do sistema. Para mais informações sobre a origem, funcionamento, tipos, vantagens e potencialidades dos SIEM recomenda-se a consulta do artigo publicado na Exabeam (2020).

[132] O MISP permite exportar dados no formato STIX (XML e JSON), bem como importar e exportar no formato STIX 2.0 (MISP, 2020b).

servidores que poderão ser utilizados por várias organizações[133]. Na Figura 31 encontra-se representada uma visão geral das principais instâncias MISP a nível global.

Nas instâncias MISP, a informação é armazenada, primeiramente, na base de dados desse servidor podendo ser partilhada com outras instâncias, através de ações de sincronização, consoante as configurações de distribuição selecionadas (MISP Community, 2019). A título de esclarecimento desta funcionalidade, atenda-se à Figura 32, na qual uma Organização (denominada de OrgB), embora esteja a ser servida por duas instâncias do MISP diferentes (servidor A e B), encontra-se a sincronizar a informação de ambos os servidores.

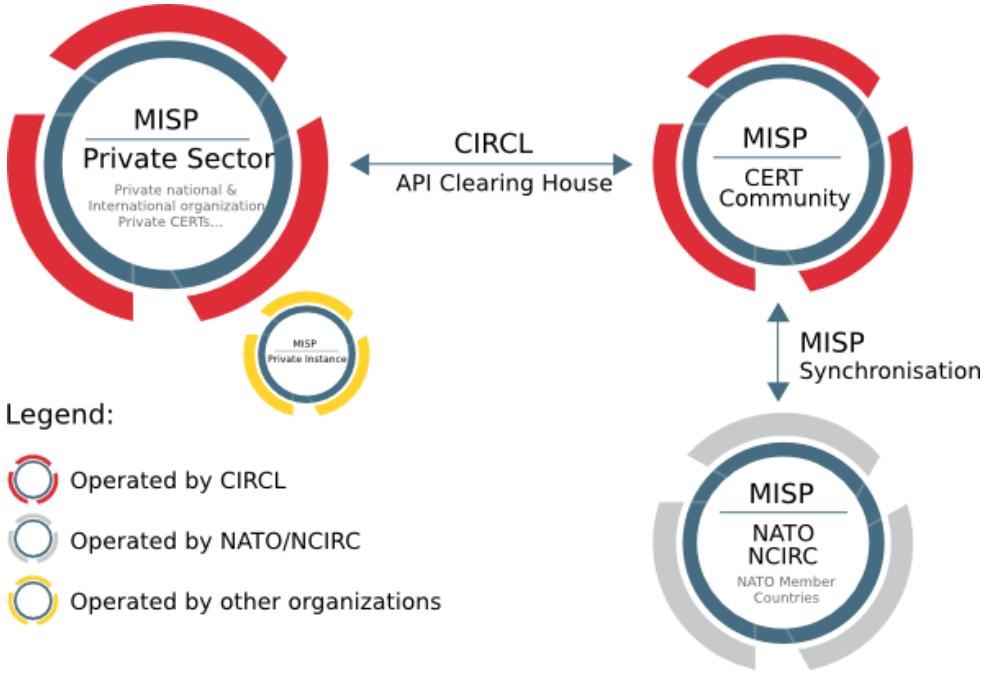

Figura 31 – Representação das principais instâncias MISP (CIRCL, 2020a)

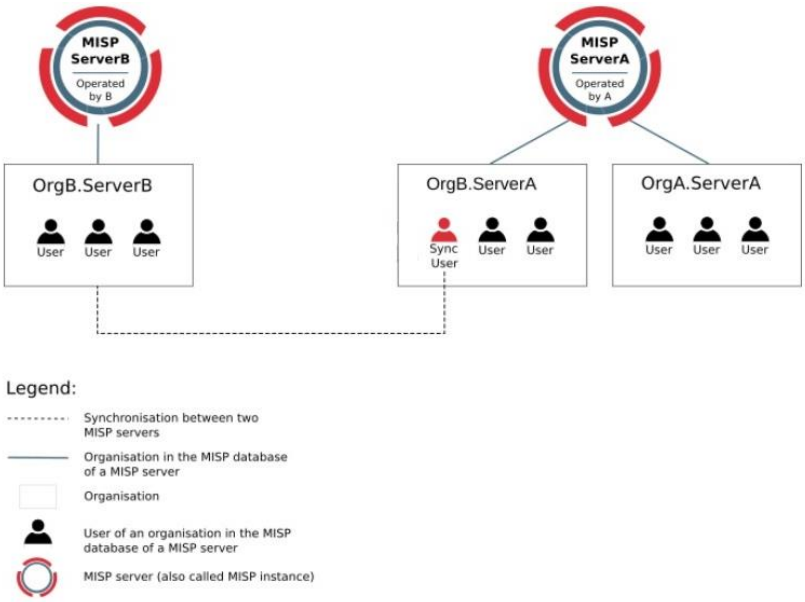

Figura 32 – Sincronização da informação MISP de uma organização servida por instâncias MISP distintas. Adaptado de MISP Community (2019, p. 331)

[133] Por exemplo, no caso da ciberdefesa, existe uma única instância para o CCD que é, igualmente, utilizada pelos CIRC da Marinha, Exército e da Força Aérea.

A configuração da distribuição da informação nas instâncias permite, desde logo, selecionar os utilizadores que serão capazes de ver um determinado evento introduzido. Além disso, permite definir que utilizadores terão permissões para aceder ao evento dentro da própria instância e controlar a sincronização do evento com outras instâncias.

Neste quadro e em concreto o MISP permite a um utilizador selecionar cinco modos de configuração de distribuição de eventos e seus respetivos atributos, a saber: "*your organisation only",* sendo a informação do evento partilhada apenas na própria organização[134]; "*this community only"*, partilhando-se a informação em todas as organizações dentro da mesma instância e nas organizações de servidores diretamente conectados[135]; *connected communities*, sendo a informação do evento partilhada em todas as organizações dentro da própria instância e que se encontram em servidores que se encontram em segundo grau de ligação[136]; *all communities,* partilhando-se a informação do evento em todas as comunidades de utilizadores; *sharing group*s[137], adequados para a partilha de informação em grupos específicos, podendo incluir organizações locais, da própria instância, bem como organizações externas de instâncias conectadas, direta ou indiretamente.

4.6.4. Rede Nacional

A nível nacional a importância do MISP, conforme refere Assunção (2020) , tem vindo a crescer progressivamente, embora a sua implementação nas organizações ainda seja generalizada. No que concerne às entidades que integram o G4, Assunção (2020), acrescenta que "tanto o CNCS como o CCD já se encontram interligados desde 2016, tendo sido integrado nesta plataforma mais recentemente o SIS e encontra-se em desenvolvimento a integração da UNC3T da PJ". Neste âmbito, a Figura 33 apresenta um esquema da rede nacional MISP entre o CNCS e o CCD expondo as principais organizações providas de informação por estas entidades.

No que concerne à UNC3T, Bravo (2020) reconhece a importância do MISP, corroborando que "está para ser operacionalizada na minha Organização".

Na mesma senda, o SIS (2020b) sublinha que o MISP se tem constituído como uma ferramenta muito útil, dado que "se revela um instrumento de partilha alimentado por entidades de várias geografias e tipologias".

Não obstante, todas as vantagens e utilidades que se reconhece a uma utilização e operacionalização efetiva do MISP, a nível nacional, sublinha-se o exposto por Assunção (2020), ao afirmar que "os benefícios deste tipo de plataforma dependem em grande parte da qualidade da informação partilhada, pelo que para que possa vir a ter um papel relevante há que garantir a partilha de informação em tempo e acionável nos sistemas de proteção de fronteira".

---

[134] No caso do exemplo supracitado da ciberdefesa a partilha de informação seria apenas dentro do CCD.

[135] No exemplo em análise, com este modo de distribuição, a informação do evento ficaria disponível para consulta no CCD, no CIRC dos ramos, no CNSC e no NCIRC.

[136] Ou em outra linguagem mais técnica, em servidores que se encontrem até 2 *"hops*" de distância.

[137] A partilha nos grupos pode ser realizada ao nível do evento ou dos atributos, sendo, usualmente, utilizada, p. ex., para a partilha de indicadores financeiros em grupos financeiros ou de indicadores de segurança da informação numa comunidade CSIRT.

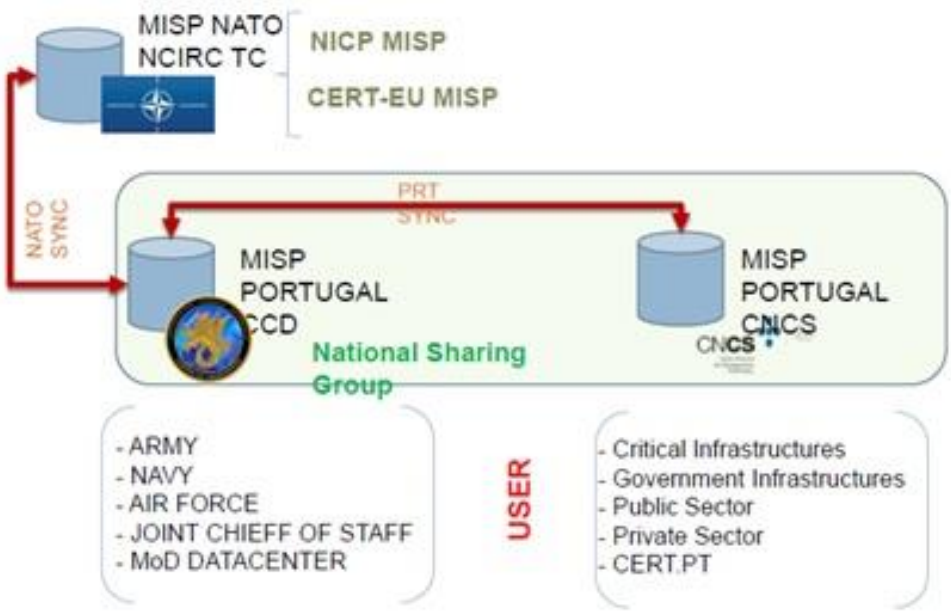

Figura 33 – Representação da rede nacional MISP entre o CNCS e o CCD (Schrooyen, 2017, p. 15)

4.7. Discussão da investigação. A importância das informações e a premência da sua partilha no ciberespaço

4.7.1. Contributo das informações para a construção do CSC e a sua importância na segurança do ciberespaço

No decurso da presente investigação, verifica-se que, perante o ambiente de completa incerteza em que o ciberespaço se encontra envolto e face às novas e complexas ameaças, que despontam à segurança dos Estados, as informações se constituem como um ativo, cada vez mais, essencial e preponderante para a obtenção de um integral CSC capaz de contribuir, significativamente, para a segurança no ciberespaço.

Na verdade, releva-se o facto de todos os peritos participantes na presente investigação, unanimemente, reconhecerem a importância da obtenção de um CSC global, atual e preciso para a prevenção e antecipação de ciberataques.

Nesta senda, Silva (2020), concretiza que "o acompanhamento e monitorização do que acontece no ciberespaço, permite de certo modo compreender tendências e identificar indícios que poderão levar a ciberataques". Porém, o mesmo autor alerta que, para a consecução de um conhecimento situacional mais ajustado e capaz, perante a imprevisibilidade dos ciberataques e a elevada capacidade e *know-how* de quem os executa, é fundamental promover a educação de quadros e o investimento em equipamento e infraestruturas especializadas.

Por sua vez, Assunção (2020), em linha com a posição de Ali (2016), defende que o CSC "assenta em vários pilares e diferentes vertentes". Numa primeira análise deverá focar o conhecimento das ameaças, nomeadamente, no que concerne às suas capacidades, modos de operação e estruturas de suporte. Uma segunda vertente cingir-se-á à deteção das vulnerabilidades internas, aquilo ao que Ali (2016) designou de conhecimento da própria rede. Importa referir que a visão de Assunção (2020)

e de Ali (2016), sobre os principais aspetos a considerar para a obtenção de um robusto CSC, diferem apenas no facto de este último, seguindo uma perspetiva mais operacional, relevar o conhecimento do ambiente onde decorre a missão.

Em relação à importância do CSC corrobora-se, integralmente, com Assunção (2020) ao afirmar que aquele "permite-nos conhecer quais os pontos de maior probabilidade de serem sujeitos a ciberataques, e desta forma atuar na sua defesa preventiva".

Quanto aos critérios que o CSC se devera reger, Rodrigues (2020) destaca a abrangência e a precisão, dado que conforme sublinha "ele é a peça fundamental para um rápido processo de tomada de decisão, num ambiente que está sempre em mutação, e cujos agentes de ameaça se encontram em permanente evolução".

Por fim, como evidência clara da importância das informações para a construção do CSC e a relevância deste, para a prevenção e antecipação de ciberataques, destaca-se a afirmação do SIS (2020b) expondo que "toda a atuação e responsabilidade do Serviço de Informações de Segurança enquanto elemento basilar da segurança do ciberespaço de interesse nacional reside nesse pressuposto".

4.7.2. Principais aspetos em que as informações podem contribuir para a segurança no ciberespaço

Por outro lado, conceitua-se que, a importância e a utilidade das informações não se encerra apenas na contribuição para o CSC mas vai muito para além disso. Na realidade as informações enquanto produto resultante da análise e processamento de informação, sobre as ameaças que atuam no ciberespaço, após uma pesquisa direcionada permitem, por um lado mitigar a incerteza e por outro, proporcionar o apoio oportuno e esclarecido que coadjuve no processo de tomada de decisão com vista à antecipação, defesa e mitigação de ciberataques.

Esta asserção é, de resto, corroborada por todos os especialistas que contribuíram para a presente investigação apresentando-se na Tabela 7, como corolário, uma relação dos principais aspetos em que as informações podem contribuir, significativamente, para a segurança no ciberespaço.

Tabela 7 – Quadro resumo dos principais aspetos identificados na investigação em que as informações poderão contribuir para a segurança no ciberespaço

Especialista	Contributos das informações para a segurança no ciberespaço
SIS (2020b)	• Contribuir para a obtenção de uma imagem clara das pegadas digitais dos agentes maliciosos; • Identificação atempada de infraestruturas de ataques; • Fundamentar programas de sensibilização específicos, a entidades públicas e privadas, partilhando o conhecimento especializado sobre os agentes da ameaça e seus modos de atuação, para que estas robusteçam a sua vertente comportamental de segurança em ambiente digital.
Santos (2020)	• Contextualizar a informação técnica que o conjunto de entidades operacionais reúne e trata;

	• Alimentar e atualizar o quadro de ameaças global e especial e contribuir para a análise de risco; • Produzir informação técnica que alimente o Quadro situacional.
Bravo (2020)	• Desvendar perigos e tendências; • Sensibilizar os decisores para esses perigos; • Contrariá-los de forma ativa (contrainformação, desinformação, gestão de crise e ações técnicas 'CNO'.
Assunção (2020)	• Prevenção: ao obter informação sobre os *modus operandi* e perfis dos atores adversários, bem como, das suas estruturas no ciberespaço, garante-se um significativo incremento da capacidade de defesa dos ataques; • Mitigação: No âmbito da mitigação, recuperação e reposição de sistemas de informação após um ciberataque, as informações também terão um papel contributivo bastante importante, permitindo que no decorrer da análise se possam seguir caminhos para a chegada às conclusões pretendidas mais céleres e diretos; • Imputação: no que se refere à componente técnica da imputação de um ciberataque a um determinado ator, as informações podem dar também o seu contributo, através do conhecimento do *modus operandi*, perfil e infraestrutura de ataque desse ator.
Rodrigues (2020)	• Garante de uma adequada tomada de decisão; • Disponibilização do premente aviso antecipado para as unidades cibernéticas que garantem a defesa de perímetro de uma organização.
Silva (2020)	• As Informações em sentido lato, e a Contrainformação em sentido estrito assumem preponderância enquanto elemento mitigador de ameaças; • Através da integração e relacionamento com outras disciplinas das Informações (e.g. HUMINT) poderá ser desenvolvido um produto mais completo e ajustado no que respeita ao real conhecimento situacional.

4.7.3. A premência da partilha de informação e de informações no ciberespaço

Num mundo globalizado e altamente interligado como o de hoje, constata-se que é bastante difícil, praticamente inexequível, que um estado e uma organização consigam assegurar de forma isolada a segurança do seu ciberespaço de interesse. Por isso, considera-se que de nada valerá guardar informações sobre ameaças, suas intenções, ações e ataques em curso, para si só, pois mais tarde ou mais cedo, de forma direta ou indireta, sofrer-se-á as consequências das ações dos agentes de ameaça. Por este motivo, entende-se ser premente e vital para a segurança no ciberespaço, a partilha de informação e de informações relativas a *malware*, indicadores de ameaças, IoC, orquestração, condução de ciberataques, entre outros elementos importantes neste domínio.

É nesta linha de pensamento que Rodrigues (2020) assegura que "atento às características do ciberespaço, a única forma de assegurarmos a segurança das organizações é através de uma permanente partilha de informação". O mesmo perito esclarece que, neste ambiente em constante mutação, é impossível que uma organização consiga garantir a sua segurança de forma isolada, uma vez que os códigos do *software* maliciosos e os vetores de ataque inicial encontram-se permanentemente a ser melhorados e aperfeiçoados. Por este motivo, conclui que "uma equipa que está preparada para um determinado código malicioso, passado duas semanas deixará de o estar, pelo que é crucial existir uma permanente troca de informação".

Com o mesmo entendimento, Assunção (2020), acrescenta que “a rapidez com que um ciberataque se pode propagar pelo ciberespaço é determinada pela [celeridade] com que se consegue partilhar informação válida sobre o mesmo, e atuar com essa informação na defesa dos sistemas”. Neste âmbito, o mesmo especialista foca o incidente do *WannaCry*, como um exemplo caro desta asserção, expondo que estes ataques despontaram no leste europeu, alastrando-se muito rapidamente a todo o continente, tendo sido somente possível mitigar os seus efeitos através da partilha célere e eficiente de informação entre as várias comunidades de segurança.

De igual modo, Silva (2020) enfatiza a importância da criação e o desenvolvimento de comunidades de interesse tendo como fim “estimular e otimizar os meios e capacidades díspares a complementarem e resultar num esforço mais eficiente para fazer face a eventuais ciberataques”. Nesta senda, Santos (2020) evidencia que é essencial a partilha de informação entre as várias entidades com responsabilidade operacional no ciberespaço.

Também, no âmbito do combate ao cibercrime a premência e urgência da partilha de informação e de informações é notada, afirmando Bravo (2020) que este desiderato “é muito importante, por nos permitir aferir a motivação e afetar a vontade e a capacidade de ação criminosa”.

Por último, o SIS (2020b) refere, igualmente, que a informação deverá estar necessariamente disponível a quem dela necessita. Não obstante, alerta, também, para a imperatividade de serem tomadas as devidas medidas de segurança da informação e a observância do principio do *need to know*, “sob pena de, em virtude de os agentes de ameaça mais sofisticados monitorizarem em contínuo o conhecimento publicamente disponível sobre eles, procederem a alterações de monta em termos de técnicas, táticas e procedimentos que dificultem a deteção das suas ações hostis” SIS (2020b).

4.7.4. Plataforma para a partilha de informação no ciberespaço: o caso do MISP

Reconhecendo-se, no seio das comunidades de segurança das redes e dos sistemas de informação a nível global, a importância da partilha de informação e informações para a segurança do ciberespaço surgiram, nos últimos anos, várias plataformas de partilha de Observáveis, de TTPs, de indicadores de ameaça e compromisso.

Como se expôs, anteriormente, o *MISP* é um exemplo claro, de uma dessas plataformas de partilha de IoC associados a ciberataques, desenvolvida sobre a égide da *NATO,* no âmbito de um projeto SD (SD 1.35), mas que rapidamente, face às vantagens e potencialidades apresentadas, se estendeu a outras comunidades de segurança um pouco por todo o mundo. Atualmente constitui-se como uma plataforma *open-source* que visa incrementar a partilha, o armazenamento e a correlação de informações sobre ameaças afirmando-se, conforme sublinha Santos (2020), como “uma plataforma de partilha de IoCs bem-sucedida”.

Neste quadro, Rodrigues (2020) salienta a importância e a mais-valia que o MISP acrescenta para a segurança no ciberespaço, referindo que “sendo umas das características do ciberespaço a velocidade na geração de efeitos, uma forma de combater essa velocidade é a partilha de informação de forma célere e através de canais credíveis”. Assim, quando uma determinada organização tem informação sobre um IoC quanto mais rápido este for disseminado, entre as entidades com responsabilidade de atuação na segurança do ciberespaço, menores serão os efeitos.

Da mesma forma, Bravo (2020) acentua a mais-valia do MISP para a antecipação e prevenção de ciberataques, pela capacidade de "permitir aferir intensidade e concentração temporal de incidentes em curso e bem assim usar IOCs e FTTPs na sua disrupção". Acrescenta ainda que esta plataforma encontra-se em fase de operacionalização na PJ.

Por seu turno, o SIS (2020b) destaca que, na perspetiva das informações, o MISP constitui-se ainda como um importante repositório de "indicadores sobres os quais um trabalho de análise aprofundado poderá permitir a deteção antecipada de novas técnicas, táticas e procedimentos de atuação de agentes de ameaça, bem como de ajuda clara, pela mesma análise de atribuições mais fidedignas das diversas pegadas digitais de cada agente de ameaça".

Não obstante, conforme alerta Assunção (2020), em virtude de o MISP ser uma plataforma *open-source*, em desenvolvimento por uma comunidade sem fins lucrativos, constata-se que esta nem sempre acompanha, por esta circunstância, as reais necessidades das organizações. Neste âmbito, Assunção (2020) identifica, desde logo, a necessidade de a informação partilhada poder ser "rapidamente incorporada nos sistemas de defesa das organizações, situação que atualmente se encontra em desenvolvimento por forma a atingir graus de confiança mais aceitáveis, para que se possam criar automatismos sem prejudicar a usabilidade dos sistemas de informação da organização".

De igual modo, Santos (2020), reconhece que "o MISP pode ser uma boa ferramenta para repositório e comunicação de IoC de forma rápida a quem deles precisa". Porém, o mesmo especialista identifica algumas limitações da plataforma, nomeadamente: a tipologia de informação partilhada; o facto de ainda não estar compatibilizada com os principais modelos de *threat intelligence;* não comportar uma visão de gestão de ciclo de vida dos IoC.

Concomitantemente, reconhece-se o exposto por Santos (2020) ao mencionar que, para além do MISP "existem outras ferramentas mais eficazes para a partilha de Observáveis ou de TTPs". Não obstante, entende-se que o *MISP,* além de ser uma boa ferramenta para a partilha de IoC e informação associados a ciberataques, apresenta a grande mais-valia de ser uma plataforma *open-source* gratuita e de se encontrar amplamente difundida por uma grande franja da comunidade de peritos em Portugal. Em linha com esta asserção surge Rodrigues (2020) expondo que, atualmente, o CCD possui várias instâncias de MISP com parceiros externos, entre os quais a NATO, o Brasil e o CNCS. Acrescenta que toda a informação trocada após validação interna no CCD, "é partilhada pelos CIRC´s dos Ramos das FFAA, deste modo cria-se uma defesa ativa que permite mitigar muitos ataques logo na sua génese. Todo este procedimento está bem oleado e a partilha de informação é bastante célere entre canais técnicos" (Rodrigues, 2020).

Por último, importa referir que a seleção do MISP para plataforma de estudo, em detrimento de outras, também, se deveu em parte, aos motivos acabados de elencar adicionando-se a facilidade, concebida ao autor, em aceder e explorar à ferramenta. Por sua vez, perante a necessidade de selecionar as matérias a investigar optou-se por apenas se estudar e detalhar o MISP, servindo esta plataforma, como um claro exemplo da importância da partilha de informação e da utilidade de ferramentas que o concretizem de forma rápida e autonomamente, para além de servir como repositório de informação técnica e não técnica relativa a ameaças.

4.8. Síntese Conclusiva

As informações, propriamente ditas, são na sua essência o conhecimento útil, atempado e rigoroso produzido através de um processo e de uma organização específica, com o objetivo de apoiar a tomada de decisão. As informações enquanto processo referem-se, essencialmente, ao CPI implementado por forma a converter a informação em conhecimento. Por sua vez, as informações como produto visam descrever o conhecimento que é produzido e disseminado no decurso do processo identificando, ainda, as principais características que aquelas devem obedecer para que sejam consideradas úteis, oportunas e precisas. As informações enquanto organização abordam os serviços de informações, analisando a sua estrutura orgânica e o seu modelo de funcionamento, através do qual conduzem o processo atinente à produção de informações.

Por sua vez, o CSC, para o qual as informações contribuem decisivamente para a sua construção e alimentação, traduz-se na capacidade de determinar a dinâmica das ameaças e percecionar as intenções, os movimentos e as possibilidades de potenciais atacantes. Para a edificação de um robusto e profícuo CSC afigura-se como fundamental implementarem-se processos que permitam apoiar e simplificar o processo de tomada de decisão. Neste quadro, o modelo *OODA Loop,* há muitos anos testado com sucesso e em utilização nos outros domínios da condução de operações, poderá e deverá ser, também, utilizado no ciberespaço como ferramenta essencial para a obtenção do CSC.

Simultaneamente, conclui-se que, para a obtenção de um integral CSC de interesse, os Estados e organizações deverão tomar em linha de conta com três aspetos principais, nomeadamente: as ameaças; o conhecimento da rede; e o conhecimento do contexto e ambiente onde se realiza a missão e/ou atividade.

Face ao exposto e perante a imprevisibilidade, a complexidade, o anonimato e a assimetria que caracterizam as ameaças de hoje, verifica-se na comunidade internacional e nas organizações, uma visível mudança de paradigma, do *need to know* para o *need to share*, dado que a cooperação e partilha de informações são, inequivocamente, fatores vitais para a segurança no ciberespaço.

Foi neste contexto que a NATO lançou o projeto MISP por forma a promover a cooperação e a partilha de informação entre as nações aliadas e no âmbito nacional, Portugal encontra-se a operacionalizá-la ao nível do G4. Em concreto, o MISP constitui-se como uma plataforma de excelência para a partilha, armazenamento e correlação de informações sobre ameaças, IoC ou qualquer outro tipo de informação importante de cibersegurança e proteção. Através do contributo dos especialistas, identificaram-se algumas limitações da plataforma. Porém, conclui-se que não existem sistemas perfeitos e que as potencialidades e os benefícios que o MISP, enquanto ferramenta *open-source* gratuita, confere no âmbito da partilha de informação e em última instância na antecipação e mitigação de ciberataques, supera os aspetos que ainda tem para melhorar.

Por fim, da análise das entrevistas e da discussão realizada, considera-se que se conseguiu responder à QD3 – "De que forma as informações poderão contribuir para a segurança no ciberespaço?", pois, para além de se ter realizado uma abordagem holística ao conceito de informações, foi evidenciada a sua importância para a segurança no ciberespaço, identificando-se contributos diretos, relevando-se a sua importância na construção de um robusto CSC e enfatizando-se a premência da sua partilha em tempo e de forma adequada.

5. Conclusões

Num mundo cada vez mais digital e interligado o ciberespaço é, sem sombra de dúvidas, um dos grandes assuntos da atualidade captando um crescente interesse dos vários atores da sociedade. Este novo bem global comum criado pelo homem, assume, atualmente, uma indiscutível relevância no modo de vida e no bem-estar das populações, conferindo extraordinárias oportunidades de desenvolvimento. Porém, acarreta também um conjunto variado de desafios à segurança dos cidadãos, das organizações e dos estados soberanos.

Desde logo, verifica-se que prolifera no ciberespaço a desinformação, a manipulação, as *fake news,* a propaganda e o anonimato. Na verdade, embora a humanidade viva na era da informação, constata-se que paradoxalmente, mais informação não significa mais conhecimento. A par disto, observa-se um aumento das ameaças neste domínio, com um fator de complexidade crescente, por parte de atores estatais e não estatais que desenvolvem as suas ações de forma, cada vez mais sofisticada e disruptiva. Neste âmbito, releva-se a perigosidade inerente ao grave impacto que as ações destes agentes de ameaça podem provocar nas IC de suporte ao normal funcionamento das sociedades. Por fim, denota-se que o fenómeno da guerra híbrida, em particular evidência nos últimos anos, encontrou no ciberespaço um instrumento de elevada capacidade para alcançar os seus fins.

Por conseguinte, é fundamental que os Estados e as organizações consigam enfrentar a constante incerteza que paira sobre o ciberespaço, consequente das múltiplas e complexas, ameaças que operam neste ambiente. Para este fim, as informações surgem como um ativo essencial e decisivo dado que permitem, por um lado mitigar a incerteza de ambientes caracterizados pela imprevisibilidade e complexidade e, por outro assegurar o apoio oportuno e esclarecido no processo de tomada de decisão.

Neste enquadramento, a presente investigação teve como objeto de estudo as "informações no ciberespaço" procurando evidenciar a importância que as informações e a sua partilha, entre os principais atores, desempenham na segurança do ciberespaço.

Neste quadro, o **OG** desta investigação consistiu em "**analisar o contributo e a importância que as informações podem desempenhar para a obtenção da segurança no ciberespaço**". Nesta senda, o estudo foi delineado tendo em vista a resposta à **QC** - "**como poderão as informações contribuir para a segurança no ciberespaço**" e consequentemente às três QD subsequentes.

A estratégia de investigação seguiu uma metodologia de raciocínio dedutivo com recurso a uma estratégia qualitativa. Para a recolha de dados realizou-se uma revisão da literatura e análise documental de âmbito legal, doutrinário e produzida por especialistas, bem como entrevistas estruturadas a especialistas em cibersegurança, ciberdefesa, combate ao cibercrime e informações. Durante a seleção dos entrevistados foram considerados os elementos que poderiam permitir ao investigador conceber uma perceção geral de diferentes realidades.

Por conseguinte, tendo presente o OG da investigação e a subsequente QC foram definidos, respetivamente, têS OE e três QD associadas. Neste âmbito, procurou-se, em primeiro lugar, "**caracterizar o ambiente ciberespaço**", propósito estabelecido como o **OE1** da investigação. Do estudo e análise realizada identificam-se algumas características que permitem dar resposta à **QD1 -** "**como se caracteriza o atual ambiente ciberespaço**", das quais se destacam as seguintes: possui

um carácter muito dinâmico; tem um enorme potencial de crescimento; apresenta uma elevada capacidade de armazenamento e processamento de informação; potencializa a assimetria, originada pelo grande desequilíbrio entre os possíveis elevados danos e os reduzidos meios necessários para os concretizar; predomina o anonimato e a consequente dificuldade de imputação; facilidade de um ator mistificar a sua presença; transversalidade e interdependência entre todos os setores de uma sociedade; não possui regulação adequada; capacidade de ampliação da vulnerabilidade humana; possui um reduzido custo de acesso; os efeitos repercutem-se no mundo físico; as infraestruturas encontram-se geograficamente dispersas, logo, submetidas a diferentes quadros legislativos e à intervenção de diversas entidades internacionais; indefinição dos limites das fronteiras no ciberespaço.

Em concreto, depreende-se que esta particularidade da indefinição dos limites das fronteiras no ciberespaço resulta do facto deste ambiente se assumir como uma dimensão de comunicação livre e praticamente isento de regulação jurídica desafiando, em larga medida, os conceitos tradicionais de Soberania e de Fronteira. Esta problemática e o modo como os Estados a poderão superar têm estado, frequentemente, na ordem do dia do debate. De facto, cada vez mais os Estados e as organizações têm consciência dos severos impactos que os ciberataques podem causar nas IC, sobre as quais assentam os serviços essenciais e na sociedade em geral. De resto, este aspeto ficou evidente nos casos apresentados da Estónia (2007), Geórgia (2008), Irão (2010), Ucrânia (2014) e Ucrânia (2015). Com efeito, estes ciberataques denotam e alertam, claramente, para a primordialidade de os Estados assegurarem não só a utilização livre e segura do seu ciberespaço aos seus cidadãos e organizações, como a preservação da sua própria soberania.

Para ocorrer a este desafio, entende-se que a caracterização das ameaças presentes no ciberespaço é um aspeto fundamental, pois permite definir e implementar estratégias adequadas, com vista à promoção e materialização da segurança do ciberespaço. Para isso, é essencial proceder-se à correta identificação e catalogação do conjunto de ameaças capazes de conduzir ataques deliberados. Neste contexto, tendo por base a motivação e o perfil dos seus autores, conceitua-se que as ameaças no ciberespaço podem ser agrupadas em cinco categorias principais, nomeadamente: hacktivismo; cibercrime; ciberespionagem; ciberterrorismo; e ciberguerra. Não obstante, a realidade demonstra que cada uma destas categorias possui limites difusos e pode ocorrer sobreposição.

Neste seguimento, após se ter caracterizado o ciberespaço, efetivamente, um novo espaço de conflitos e disputas, a investigação centrou-se em "**descrever os principais domínios e entidades que a nível nacional contribuem para a segurança no ciberespaço",** i.e., no **OE2.** Decorrente da investigação, foram **identificados e caracterizados os principais domínios e entidades nacionais, que contribuem para a segurança no ciberespaço, e exposto como se articulam,** respondendo-se deste modo à **QD2**.

Da análise efetuada, conclui-se que para enfrentar os desafios e o conjunto de ameaças que pairam sobre o ciberespaço, os Estados deverão, à semelhança do que fazem perante uma ameaça assimétrica ou transnacional, implementar e operacionalizar um conjunto de planos de atuação que neste ambiente específico deverão incidir sobre os seguintes domínios: cibersegurança; combate ao cibercrime; ciberdefesa; informações; e ciberdiplomacia e cooperação nacional e internacional.

O domínio da cibersegurança engloba a implementação de um conjunto de medidas e ações que tem como finalidade a prevenção, a monitorização, a deteção e a reação, com o intuito de manter o estado de segurança pretendido, numa lógica de mercado e continuidade de negócio, de proteção da cidadania e de colaboração com a Segurança Interna e Defesa.

Quanto ao domínio do combate ao cibercrime o foco principal centra-se na dissuasão da prática de crimes e, no limite, na condenação do autor de um crime.

A ciberdefesa engloba as atividades de prevenção, monitorização e reação a ameaças que coloquem em risco a soberania nacional, bem como o apoio às operações no ciberespaço.

Em relação, ao domínio das informações compete assegurar a produção de informações decisivas que possibilitem a deteção antecipada das intenções dos agentes de ameaça. Para isso, a área das informações compreende todo trabalho desenvolvido com vista à obtenção de um conhecimento, profundo, sobre os potenciais agentes de ameaça, nomeadamente: os seus intentos; capacidades; características de atuação; e pegada ou assinatura digital.

Por seu turno, no domínio da diplomacia e da cooperação procura-se agir, bilateral e multilateralmente, de modo a estreitar a rede de alianças existentes, exercer influência e promover a implementação de políticas que em colaboração com aliados e parceiros, nacionais e internacionais, visem diminuir a insegurança no ciberespaço.

No global, poder-se-á referir que estes domínios de atuação e os principais atores intervenientes em cada um deles constituem, em grande parte, a capacidade nacional de segurança do ciberespaço.

Para incrementar a cooperação, estimular a partilha de informação e promover a articulação de ações entre as principais entidades dos domínios da cibersegurança, combate ao cibercrime, ciberdefesa e informações, foi edificado o grupo de carácter operacional informal denominado de G4. Em concreto, integram este grupo, respetivamente, o CNSC, a UNC3T, o CCD e o SIS.

No que concerne ao **OE3** - "**com base na análise das informações identificar aspetos em que estas poderão contribuir para a segurança no ciberespaço"** foi formalizada a respetiva **QD3** - "**de que forma as informações poderão contribuir para a segurança no ciberespaço?"**.

Esta questão foi respondida, numa primeira instância, através da delimitação da diferença entre este conceito e o conceito de informação. Em resultado, conclui-se que as informações são o conhecimento útil, atempado e rigoroso produzido, por intermédio de um processo e tendo com suporte uma organização específica, com o objetivo de assegurar o apoio oportuno e elucidado no processo de tomada de decisão.

Adicionalmente, por forma a se obter uma visão holística sobre o que são as informações, dever-se-á dissecar cada um dos seus elementos fundamentais, nomeadamente: o processo, o produto e a organização. As informações enquanto processo retratam o CPI que é implementado por forma a converter a informação em conhecimento. Por sua vez, as informações como produto visam descrever o conhecimento que é produzido e disseminado no decurso do processo. Além disso, são ainda relevadas as principais características que as informações devem ostentar para que sejam consideradas úteis, oportunas e precisas. As informações enquanto organização referem-se, fundamentalmente, aos serviços de informações, à estrutura orgânica e ao modelo de funcionamento em vigor e através do qual é conduzido o CPI.

Para além das informações propriamente ditas, constata-se que, para a segurança do ciberespaço, como de em qualquer outro ambiente, é fundamental possuir uma capacidade que permita determinar a dinâmica das ameaças e percecionar as intenções, os movimentos e as possibilidades de potenciais atacantes. Esta capacidade no ciberespaço denomina-se de CSC verificando-se que as informações contribuem decisivamente para a sua construção e alimentação. Acresce que, para a obtenção de um robusto e integral CSC de interesse é necessário ter-se em consideração três aspetos fundamentais, nomeadamente: as ameaças; o conhecimento da rede; e o conhecimento do contexto e ambiente onde se realiza a missão e/ou atividade.

De igual modo, perante a imprevisibilidade, a complexidade, o anonimato e a assimetria que caracteriza as ameaças de hoje, observa-se na comunidade internacional, uma mudança do paradigma do *need to know* para o *need to share*, alicerçado na, cada vez maior, perceção de que a cooperação e a partilha de informações serem fatores chaves para a obtenção da segurança no ciberespaço.

Tomando consciência desta primordialidade e a fim de promover a cooperação e a partilha de informação entre as nações aliadas, a NATO lançou, em 2012, o projeto MISP. Fundamentalmente, o MISP constitui-se como uma plataforma de excelência para a partilha, armazenamento e correlação de informações sobre ameaças, IoC ou qualquer outro tipo de informação relevante de cibersegurança e de proteção. Não obstante, esta plataforma não se encontra isenta de limitações e oportunidades de melhoria, tal como ficou expresso, na opinião de alguns dos especialistas entrevistados. Contudo, tal como estes peritos também expuseram, as potencialidades e os benefícios que o MISP, enquanto ferramenta *open-source,* confere no âmbito da partilha de informação e IoC, e consequentemente, na antecipação e mitigação de ciberataques são tão relevantes que superam as limitações existentes. Também, por esta razão se verifica que a nível nacional o MISP se encontra em fase de implementação e operacionalização em todas as entidades pertencentes ao G4.

Face ao exposto, como resposta à **QC** desta investigação, "**como poderão as informações contribuir para a segurança no ciberespaço"**, destaca-se o seguinte:

- Possibilitam a obtenção de uma imagem clara das pegadas digitais dos agentes maliciosos;
- Viabilizam a identificação atempada de infraestruturas de ataques;
- Sustentam a formulação e preparação de programas de sensibilização específicos, a entidades públicas e privadas, partilhando o conhecimento especializado sobre os agentes da ameaça e seus modos de atuação, para que estas robusteçam a sua vertente comportamental de segurança em ambiente digital;
- Permitem reduzir a incerteza sobre ameaças e intenções hostis;
- Asseguram o apoio oportuno e clarificado no processo de tomada de decisão;
- Apoiam decisivamente na construção e alimentação do CSC;
- Disponibilização o premente aviso antecipado para as unidades cibernéticas que garantem a defesa de perímetro de uma organização;
- Possibilitam contextualizar a informação técnica que o conjunto de entidades operacionais reúne e processa;

- Alimentam e atualizam o quadro de ameaças global e especial e contribuir para a análise de risco;
- Concorrem para a prevenção (informação sobre *modus operandi*, perfis das ameaças e suas capacidades), mitigação (recuperação e reposição de sistemas de informação após um ciberataque) e imputação de ciberataques (através do conhecimento do *modus operandi*, perfil e infraestrutura de ataque desse ator);
- Assumem preponderância, em conjunto com a Contrainformação em particular, como elemento mitigador de ameaças;

No fundo, conferem uma vantagem estratégica sobre um contrário ou adversário.

Por conseguinte, após se ter, no geral evidenciado a relevância das informações para a segurança no ciberespaço, e no particular identificado contributos das informações para esse desiderato, considera-se que o **OG** da presente investigação foi alcançado e que os dados recolhidos permitiram dar resposta à **QC**.

Para além da análise da importância que as informações desempenham na segurança do ciberespaço, considera-se como um importante contributo para o conhecimento, o facto de se ter evidenciado a relevância e a premência que a partilha de informação e de informações, entre as principais entidades, na segurança no ciberespaço. Neste âmbito, enfatiza-se ainda a importância de se dotar os principais atores, com responsabilidade na segurança do ciberespaço e as organizações, que dependem do ciberespaço para o exercício da sua atividade, de plataformas de partilha de informação, tal como o MISP ou outras ferramentas de *Threat Intelligence*, por forma a conseguirem antecipar, prevenir e mitigar eventuais ciberataques.

Como contributos para o conhecimento destaca-se, ainda, a caracterização pormenorizada do ambiente ciberespaço efetuada tendo por base a doutrina do IDN-CESEDEN (2013) e as opiniões dos peritos entrevistados e que poderá servir de suporte a futuros estudos. De igual modo, releva-se a análise e caracterização dos principais domínios que contribuem para a segurança do ciberespaço, a nível nacional, tendo-se identificando o âmbito e finalidade, apresentada a principal legislação enquadrante e delimitadas as principais diferenças entre cada um eles.

Relativamente às limitações da investigação identifica-se, desde logo a impossibilidade de se terem entrevistado especialistas estrangeiros, nas áreas das informações e da segurança do ciberespaço, facto que teria conferido maior abrangência e diferentes perspetivas ao estudo.

Num quadro mais particular, reconhece-se como outra limitação do estudo a circunstância de se ter cingido a análise da segurança do ciberespaço aos domínios da cibersegurança, do combate ao cibercrime, da ciberdefesa, das informações e da ciberdiplomacia e cooperação. Com efeito, face à limitação da extensão da investigação não foi possível abordar, em maior detalhe, outros atores que, também, desempenham um importante papel na segurança do ciberespaço, tais como, p. ex. as organizações privadas, a indústria, as escolas e universidades.

Da mesma maneira, perante o limite imposto na extensão da investigação, identifica-se como outra limitação o facto de não ter sido possível estudar outras plataformas de partilha de informação,

de observáveis ou de *threat intelligence,* o que providenciaria dados concretos para poder realizar uma comparação fundamentada com a plataforma MISP.

Como proposta para futuras investigações, recomenda-se alargar a análise e o estudo da importância das informações e a sua partilha para a segurança do ciberespaço a organizações fora do G4 de modo a ser possível inferir as reais necessidades destas entidades, obter-se diferentes pontos de vista e alcançar uma maior abrangência possível.

6. Bibliografia

Academia Militar. (16 de 5 de 2019). *5ª Conferência Internacional dos Projetos Smart Defence de Ciberdefesa da NATO*. Fonte: Academia Militar: https://academiamilitar.pt/5-conferencia-internacional-dos-projetos-smart-defence-de-ciberdefesa-da-nato.html

Albaret-Schulz, C. A. (29 de 10 de 2004). *La frontière, un object spatial en mutation.* Fonte: EspacesTemps.net: http://www.espacestemps.net/document842.html

Ali, R. (7 de 2016). Cyber Situational Awareness for the NATO Alliance. *The Three Swords Magazine*(30), pp. 72-75. Acesso em 20 de 7 de 2020, disponível em https://www.jwc.nato.int/newsroom/The-Three-Swords-Magazine

APDSI. (06 de 2019). *Glossário da Sociedade da Informação*. Acesso em 01 de 10 de 2019, disponível em APDSI: http://apdsi.pt/glossario/

AR. (6 de 11 de 2004). Altera a Lei Quadro do Sistema de Informações da República Portuguesa. *Lei Orgânica n.º 4/2004*, 6598 - 6606. Lisboa: DR n.º 261/2004, Série I-A. Fonte: https://data.dre.pt/eli/leiorg/4/2004/11/06/p/dre/pt/html

AR. (19 de 2 de 2007). DR n.º 35/007. *Orgânica do SG do SIRP, do SIED e do SIS*, 1238 - 1252. Lisboa: DR n.º 35/2007, Série I.

AR. (2018). *Lei n.º 46/2018 - Regime jurídico da segurança do ciberespaço.* Lisboa: Diário da República n.º 155/2018, Série I de 2018-08-13 .

Assunção, F. (2 de 11 de 2020). A importância das informações para a segurança no ciberespaço. *Especialista Ciberdefesa - Centro de Ciberdefesa*. (A. Carvalho, Entrevistador)

August, O. (23 de 10 de 2007). *The Great Firewall: China's Misguided – and Futile – Attempt to Control What Happens Online.* Acesso em 05 de 01 de 2017, disponível em Wired Magazine: http://archive.wired.com/politics/security/magazine/15-11/ff_chinafirewall?currentPage=all

Baezner, M. (2018). *Cyber and Information warfare in the Ukrainian conflict.* ETH Zürich: Center for Security Studies (CSS).

Barrett, M., Bedford, D., Skinner, E., & Vergles, E. (2011). *Assured Access to the Global Commons.* Norfolk: Supreme Allied Command Transformation, NATO.

Batista, R. (27 de 9 de 2016). Legislação do Cibercrime. *Cursi Geral de Cibersegurança: uma perspectiva Whole-of-Society*. Lisboa: CNSC.

Belfiore, M. (2010). *The Department of Mad Scientists.* Nova Iorque: Harper Perennial.

Blockbit. (4 de 9 de 2018). *O que é security by design*. Fonte: Blockbit: https://www.blockbit.com/pt/blog/security-by-design/

Bravo, R. (26 de 10 de 2020). A importância das informações para a segurança no ciberespaço. *Especialista Combate ao Cibercrime - Polícia Judiciária*. (A. Carvalho, Entrevistador)

Breakspear, A. (2013). A New Definition of Intelligence, . *Journal Intelligence and National Security*, 678-693.

Cabreiro, C. (27 de 09 de 2016). Cibercrime e Cibercrime Organizado. *Curso Geral de Cibersegurança: uma perspectiva Whole-of-Society*. Lisboa: CNCS.

Cabreiro, C. (3 de 6 de 2019). Em defesa do ciberespaço. *2ª Conferência de Cibersegurança: "A Ciber-resiliência no setor financeiro"*. Lisboa: Banco de Portugal.

Caetano, M. (1973). *Manual de Ciência Política e Direito Constitucional.* Coimbra: Coimbra Editora.

Caldas, A., & Freire, V. (2013). *Cibersegurança: das preocupações à Ação.* Lisboa: IDN.

Cardoso, P. (2004). *As informações em Portugal.* Lisboa : Gradiva - Publicações, Lda^{a} & Instituto da Defesa Nacional.

Carvalho, J. (2009). Segurança Nacional e as Forças Armadas. Lisboa: Faculdade de Letras de Lisboa.

Cepik, M. (2003). *Espionagem e democracia.* Rio de Janeiro: FGV Editora.

CFR. (12 de 01 de 2020). *APT 30*. Fonte: Cyber Operations Home: https://www.cfr.org/interactive/cyber-operations/apt-30

CIRCL. (13 de 7 de 2019). *MISP Glossary.* Fonte: MISP Treat Sharing: https://www.circl.lu/doc/misp/GLOSSARY.html

CIRCL. (6 de 10 de 2020a). *MISP - Open Source Threat Intelligence Platform*. Fonte: Computer Incident Response Center Luxembourg: https://www.circl.lu/services/misp-malware-information-sharing-platform/

CIRCL. (14 de 09 de 2020b). *misp-training.* Fonte: misp-project: https://www.misp-project.org/misp-training/0-misp-introduction-to-information-sharing.pdf

Clark, D. (2010). *Characterizing cyberspace: past, present and future.* MIT. Acesso em 09 de 01 de 2017, disponível em https://projects.csail.mit.edu/ecir/wiki/images/7/77/Clark_Characterizing_cyberspace_1-2r.pdf

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

CNN. (01 de 4 de 2019). *2008 Georgia Russia Conflict Fast Facts*. Acesso em 03 de 11 de 2019, disponível em CNN Library: http://edition.cnn.com/2014/03/13/world/europe/2008-georgia-russia-conflict/

Cravinho, J. (2019 de 01 de 2019). Ciberdemocracia e cibersegurança. *Intervenção do Ministro da Defesa Nacional, João Gomes Cravinho, no âmbito do VI Seminário SIRP*, 1-19. Lisboa: Universidade Nova de Lisboa.

Cruz, A. (29 de 10 de 2019a). Ameaças à Segurança Interna: Estado da Arte. *Comunicação OSCOT e revista Segurança e Defesa*. Lisboa: SIS.

Cruz, A. (12 de 11 de 2019b). A missão do SIS na Prevenção das Ameaças ao Estado de Direito Democrático. *I Congresso Internacional Juscrim, sobre "prevenção, Policiamento e Segurança-Implicações nos Direitos Humanos".* Braga: SIS.

Denning, D. (01 de 06 de 2000). Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. *Networks and Newars: The Future of Terror, Crime, and Militancy*, 239-288. Acesso em 28 de 12 de 2019, disponível em https://nautilus.org/global-problem-solving/activism-hacktivism-and-cyberterrorism-the-internet-as-a-tool-for-influencing-foreign-policy-2/

Denning, D. (23 de 05 de 2000a). *Cyberterrorism.* Acesso em 12 de 01 de 2020, disponível em Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives: https://faculty.nps.edu/dedennin/publications/Testimony-Cyberterrorism2000.htm

Department of Defense, U. S. (2010). *Joint Terminology for Cyberspace Operations.* Washington, D.C.: Joint Chiefs of Staff.

Dicionário infopédia da Língua Portuguesa. (2020). *Infopedia*. Acesso em 2 de 8 de 2019, disponível em Porto: Porto Editora, 2003-2020: https://www.infopedia.pt/dicionarios/lingua-portuguesa/fronteira

ENISA. (2013). *Cybersecurity cooperation - Defending the digital frontline.* Heraklion: ENISA. Acesso em 30 de 12 de 2019, disponível em https://www.enisa.europa.eu/publications/cybersecurity-cooperation-defending-the-digital-frontline

Exabeam. (28 de 10 de 2020). *What is SIEM?* . Fonte: Exabeam: https://www.exabeam.com/siem-guide/what-is-siem/

Falliere, N., Murchu, O., & Chien, E. (2011). *W32.Stuxnet Dossier (Version 1.4).* Cupertino, Calif.: Technical report, Symantec.

Fernandes, J. (2012). Utopia, Liberdade e Soberania no Ciberespaço. Em IDN, *Cibersegurança* (pp. 11-31). Lisboa: IDN.

Fernandes, J. (03 de 2012a). A ciberguerra como nova dimensão dos conflitos do século xxi. *Relacções Internacionais (R:I)*, pp. 53-69.

G4. (17 de 3 de 2020). *Alerta COVID-19 e as ciberameaças.* Fonte: CNCS: https://www.cncs.gov.pt/recursos/boas-praticas/

GAO, U. S. (2010). *Hybrid Warfare .* Washington, DC: United States Government Accountability Office. Acesso em 20 de 5 de 2020, disponível em https://www.gao.gov/assets/100/97053.pdf

Giandomenico, G. (24 de 10 de 2019). *What is Spear-phishing? Defining and Differentiating Spear-phishing from Phishing*. Fonte: Digital Guardian: https://digitalguardian.com/blog/what-is-spear-phishing-defining-and-differentiating-spear-phishing-and-phishing

Giles, L. (2015). *A Arte da Guerra.* Lisboa: Sílabo.

GOV-PT. (9 de 5 de 2014). Decreto-lei n.º 69/2014. *2ª Alteração à Lei Orgânica do GNS - Estabelecendo os termos de funcionamento do CNCS*, 2712 - 2719. Lisboa. Acesso em 7 de 3 de 2020, disponível em https://data.dre.pt/eli/dec-lei/69/2014/05/09/p/dre/pt/html

GOV-PT. (28 de 11 de 2016). Decreto-Lei n.º 81/2016. Lisboa: Publicado no D.R. n.º 228 (Série I).

GOV-PT. (5 de 6 de 2019). Estratégia Nacional de Segurança do Ciberespaço 2019-2023. *Resolução do Conselho de Ministros n.º 92/2019*. Lisboa: DR. Acesso em 18 de 10 de 2019, disponível em https://data.dre.pt/eli/resolconsmin/92/2019/06/05/p/dre

Grabosky, P. (2004). The Global Dimension of Cybercrime. *Global Crime, 6(1)*, 146-157.

Guterres, A. (18 de 2 de 2018). Cerimónia de distinção com o doutoramento honoris causa pela ULisboa. *Alterações climáticas e cibersegurança são os temas do dia, diz novo doutor Guterres*. Lisboa, Universidade de Lisboa: Diário de Notícias. Fonte: dIÁRI: https://www.dn.pt/portugal/guterres-alerta-que-a-proxima-guerra-sera-precedida-de-um-ciberataque-9128969.html

Haynes, D. (04 de 01 de 2020). *Qassem Soleimani: What will revenge look like for Iran in wake of general's killing?* Acesso em 30 de 01 de 2020, disponível em Skynews:

https://news.sky.com/story/qassem-soleimani-what-will-revenge-look-like-for-iran-in-wake-of-generals-killing-11900263

Hoffman, B. (2006). *The Use of the Internet By Islamic Extremists.* Rand Corporation.

Holsti, K. (1991). *Peace and War: Armed Conflicts and International Order 1648-1989.* Cambridge: Cambridge University Press.

Hughes-Wilson, J. (1999). *Military Intelligence Blunders.* Londres: Carroll & Graf.

IDF. (05 de 05 de 2019). *Israel Defence Forces*. Acesso em 12 de 08 de 2019, disponível em Official IDF Twitter.

IDN. (2013). *A Defesa Nacional no Contexto da Reforma das Funções de Soberania do Estado.* Lisboa: IDN. Acesso em 14 de 01 de 2017, disponível em http://www.idn.gov.pt/index.php?mod=008&cod=13032013x2#sthash.Ni6K6Xak.dpbs

IDN-CESEDEN. (2013). *Estratégia da Informação e Segurança no Ciberespaço: Investigação conjunta IDN-CESEDEN* (Vol. IDN Cadernos nº 12). Lisboa: Instituto da Defesa Nacional.

Infopédia. (20 de 2 de 2020). *Guerra dos Trinta Anos (1618-1648)*. Fonte: Infopédia: https://www.infopedia.pt/$guerra-dos-trinta-anos-(1618-1648)

Jesus, H. (17 de 12 de 2019). Ciberdefesa - Capacidade Nacional. *Biefing Visita MDN Angola ao CCD*. Lisboa: CCD.

Jesus, H. (13 de 2 de 2019b). Situation Awareness. *Cyber Advisory Course - NATO Communications & Information System Services Agency*. Lisboa, Oeiras: Forças Armadas Portuguesas.

Kostadinov, D. (25 de 02 de 2013). *Cyber Exploitation.* Acesso em 31 de 12 de 2019, disponível em Infosec: https://resources.infosecinstitute.com/cyber-exploitation/

Langston, R. (22 de 5 de 2020). *Open Source IDS Tools: Comparing Suricata, Snort, Bro (Zeek), Linux*. Fonte: Cybersecurity.att: https://cybersecurity.att.com/blogs/security-essentials/open-source-intrusion-detection-tools-a-quick-overview

Lowenthal, M. (2006). *Intelligence. From Secrets to Policy.* Washington, DC: CQ Press.

Machado, M. (2015). Entre o controle e o ativismo hacker: a ação política dos Anonymous Brasil. *História, Ciências, Saúde-Manguinhos, 22*, pp. 1513-1549. Acesso em 8 de 2 de 2020, disponível em www.scielo.br/scielo.php?script=sci_arttext&pid=S0104-59702015001001531&lng=pt&tlng=pt

Maj. Gen. Barrett, M., Bedford, D., Skinner, E., & Vergles, E. (2011). *Assured Access to the Global Commons.* Norfolk: Supreme Allied Command Transformation, NATO.

Marchueta, M. (2002). *O Conceito de Fronteira na Época da Mundialização.* Lisboa: Cosmos.

Marques, A. (2017). The challenges of IOT &IIOT for the digital resilience of the Defense community. *National & NATO security: Challenges for Portuguese Industry.* Lisboa: Academia Militar.

Marques, A. (Abril - Junho de 2019). A segurança do ciberespaço em Portugal e no setor marítimo. *Cadernos Navais*, pp. 1-31.

Marques, A. (2020). Cibersegurança no Setor Marítimo. *CyberLaw*, 12-25.

MDN. (28 de 10 de 2013). DP n.º 13692/2013. *Orientação para a política de Ciberdefesa*, 31976 - 31979. Lisboa: DR n.º 208/2013, Série II de 2013-10-28 . Fonte: https://dre.pt/web/guest/pesquisa/-/search/3295679/details/maximized?jp=true

MDN. (29 de 12 de 2014). DL n.º 184/2014. *Lei Orgânica do Estado-Maior General das Forças Armadas*, 6382 - 6397. Lisboa: Diário da República n.º 250/2014, Série I de 2014-12-29. Fonte: https://data.dre.pt/eli/dec-lei/184/2014/12/29/p/dre/pt/html

MDN. (31 de 7 de 2015). DR n.º 13/2015. *Aprova a orgânica do Estado-Maior-General das Forças Armadas*, 5275 - 5295. Lisboa: Diário da República n.º 148/2015, Série I de 2015-07-31. Fonte: https://data.dre.pt/eli/decregul/13/2015/07/31/p/dre/pt/html

MDN. (24 de 3 de 2020). *Ciberdefesa*. Fonte: Defesa Nacional: https://www.defesa.gov.pt/pt/pdefesa/ciberdefesa

Menezes, A. (2012). *Sistemas de Informações Nacionais – Contributos para a perceção da eficiência.* Lisboa: ISCTE.

Miranda, J. (2003). *Manual de Direito Constitucional, Tomo I.* Coimbra: Coimbra Editora.

MISP. (7 de 9 de 2020a). *Who is behind the MISP project?* Fonte: MISP - Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing: https://www.misp-project.org/who/

MISP. (27 de 10 de 2020b). *Features of MISP, the open source threat sharing platform*. Fonte: misp-project: https://www.misp-project.org/features.html

MISP Community. (2019). *MISP - User Guide. A Treat Sharing Platform.* Luxembourg: CIRCL. Fonte: CIR.

MOD, U. (2011). *JDP 2-0 - Understanding and Intelligence Support to Joint Operations.* Shrivenham: Doctrine Editor.

Moniz, P. (2018). Impacto do Ciberespaço na Sociedade em Rede. Em IDN, *Contributos para uma Estratégia Nacional de Ciberdefesa* (pp. 18-24). Lisboa: IDN Cadernos.

Monteiro, S., & Pinto, S. (2016). Cibersegurança e ciberdefesa − Portugal e NATO. *Revista da Armada*, 4-5.

Moreira, A. (1997). *Teoria das Relações Internacionais* (2ª ed. ed.). Coimbra: Aldemina.

Moreira, A. (2011). *A Circunstância do Estado Exíguo* (3ª Ed. ed.). Loures: Diário de Bordo.

Mulder, P. (19 de 5 de 2017). *OODA Loop*. Fonte: Toolshero: https://www.toolshero.com/decision-making/ooda-loop/

Nakashima, E. (22 de Julho de 2019). *Trump approved cyber-strikes against Iran's missile systems.* Acesso em 8 de 8 de 2019, disponível em The Washington Pots: https://www.washingtonpost.com/world/national-security/with-trumps-approval-pentagon-launched-cyber-strikes-against-iran

Natário, R. (Outubro de 2013). O Combate ao Cibercrime: Anarquia e Ordem no Ciberespaço. *Revista Militar N.º 2541*, pp. 823-858.

NATO. (4 de 12 de 2013). *Sharing malware information to defeat cyber attacks* . Fonte: NATO: https://www.nato.int/cps/en/natolive/news_105485.htm

NATO. (2015). *Smart Defence*. Fonte: NATO Review: https://www.nato.int/docu/review/Topics/EN/Smart-Defence.htm

NATO. (2016). *AJP-2 - Allied Joint Doctrine for Intelligence, Counterintelligence And Security Doctrine* (Edition A Version 1 ed.). Brussels: NATO Standardization Office.

NATO. (8-9 de 07 de 2016). *Warsaw Summit Communiqué*. Acesso em 2019 de 08 de 2019, disponível em NATO: https://www.nato.int/cps/en/natohq/official_texts_133169.htm

NATO. (8 de 7 de 2016b). *Cyber Defence Pledge*. Acesso em 13 de 4 de 2020, disponível em NATO: https://www.nato.int/cps/en/natohq/official_texts_133177.htm

NATO. (12 de 04 de 2019). *NATOTerm*. Acesso em 18 de 10 de 2019, disponível em NATO STANDARDIZATION OFFICE: https://nso.nato.int/natoterm/Web.mvc

NATO. (2019b). *AAP-06 NATO Glossary of terms and definitions.* Brussels, Belgium: NATO Standardization Office.

NATO. (2020). *AJP-3.20 - Allied Joint Doctrine for Cyberspace Operations.* Brussels: Nato Standardization Office (NSO).

NCIA. (1 de 9 de 2020). *Multinational Cyber Defence Capability Development*. Fonte: NATO Communications and Information Agency: https://www.ncia.nato.int/what-we-do/cyber-security/multinational-cyber-defence-capability-development.html

NCSC. (3 de 10 de 2018). *Reckless campaign of cyber attacks by Russian military intelligence service exposed*. Acesso em 12 de 1 de 2020, disponível em National Cyber Security Centre: https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed

Nunes, P. (2018). Em I. d. Nacional, *Contributos para uma Estratégia Nacional de Ciberdefesa* (pp. 13-16). Lisboa: IDN - Cadernos.

PCM. (5 de 4 de 2013). RCM 19/2013. *Conceito Estratégico de Defesa Nacional*, 1981 - 1995. Lisboa: DR n.º 67/2013, Série I . Fonte: https://data.dre.pt/eli/resolconsmin/19/2013/04/05/p/dre/pt/html

PEC. (6 de 7 de 2016). Diretiva (UE) 2016/1148. Estrasburgo, Bélgica. Fonte: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016L1148

Pereira, A. (2003). A Soberania no Estado Contemporâneo. *Carta Mensal, 48*.

RASI. (2019). *Relatório Anual da Segurança Interna 2018.* Lisboa: Sistema de Segurança Interna.

RASI. (2020). *Relatório Anual da Segurança Interna 2019.* Lisboa: Sistema de Segurança Interna.

Ravindranath, M. (2014). Panetta: Cyberspace is “battlefield of the future”. *The Washington Post*, 12 março.

Rêgo, N. (maio de 2018). As informações na Nato - Contextualização de um Choque Doutrinário e Estrutural. *Revista de Ciências Militares, VI(1)*, 105-133. Acesso em 7 de 6 de 2020, disponível em https://www.ium.pt/cisdi/index.php/pt/publicacoes/revista-de-ciencias-militares

Ribeiro, A. (2001). A retórica dos limites. Notas sobre o conceito de fronteira. Em B. Santos, *Globalização: fatalidade ou utopia?* (pp. 463-488). Porto: Afrontamento.

Ribeiro, A. (15 de 04 de 2019). Prós e Contras: Quem Protege a Democracia? (F. Fernandes, Entrevistador)

Ribeiro, A. (5-6 de 2020). Informações Estratégicas. *Pós-graduação em Informações e Segurança*. Lisboa: ISCSP.

Rodrigues, N. (2 de 11 de 2020). A importância das informações para a segurança do ciberespaço. *Especialista Informações - Centro de Ciberdefesa*. (A. Carvalho, Entrevistador)

Romana, H. (Abril-Junho de 2008). Informações: Uma reflexão teórica". *Segurança e Defesa, Revista Trimestral de Grande Informação*, pp. 98-101.

Santos L. et al. (2018). Defesa do Ciberespaço. Em I. d. Nacional, *Contributos para uma Estratégia Nacional de Ciberdefesa* (pp. 33-46). Lisboa: IDN Cadernos.

Santos, A. R. (2005). *As Metamorfoses do Estado - Rumo à Mega-Confederação Europeia?* Coimbra: Almedina.

Santos, L. (2001). *Segurança e Defesa na Viragem do Milénio.* Mira: Publicações Europa-America.

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

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

Santos, L. (28 de 10 de 2020). A importânica das informações para a segurança no ciberespaço. *Especialista Cibersegurança - Centro Nacional de Cibersegurança*. (R. Carvalho, Entrevistador)

Santos, L., Bravo, R., & Nunes, V. (3 de 1 de 2012). Proteção do Ciberespaço: Visão Analítica. *FCCN - Fundação para a Computação Científica Nacional*. Fonte: http://hdl.handle.net/10400.26/3578

Santos, L., Lima, J., Garcia, F., Monteiro, F., Silva, N., Silva, J., & Piedade, J. (2019). *Orientações metodológicas para a elaboração de trabalhos de investigação* (2.ª ed., revista e atualizada ed.). Lisboa: Instituto Universitário Militar.

Santos, L., Nunes, P., Ralo, J., & Mendes, C. (2018). Defesa do Ciberespaço. Em I. d. Nacional, *Contributos para uma Estratégia Nacional de Ciberdefesa* (pp. 33-46). Lisboa: IDN Cadernos.

Santos, R. (2012). *A Partilha de Informações em Portugal: Contributo para o Aperfeiçoamento do Sistema.* Lisboa: 2012. Fonte: http://hdl.handle.net/10400.26/10033

Schmitt, M. N., & et al. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare.* Cambridge: Cambridge University Press.

Schrooyen, J. (27-28 de Abril de 2017). MISP usage in NATO. *3ª Conferência CD SDP da NATO*. Amadora, Lisboa: Academia Militar. Fonte: https://academiamilitar.pt/3rd-nato-cyber-defence-smart-defence-projects-conference.html

Shlsky, A., & Schmitt, G. (2002). *Silent warfare: understanding the world of intelligence.* Virginia: Potomac Books, Inc.

Silva, C. (15 de 11 de 2020). A importância das informações para a segurança no ciberespaço. *Especialista Informações - Centro de Informações e Segurança Militares*. (A. Carvalho, Entrevistador)

SIRP. (2015). *O Ano em Revista.* Lisboa: SIRP.

SIRP. (4 de 6 de 2020). *Quem somos*. Fonte: SIRP: https://www.sirp.pt/quem-somos/o-sirp

SIS. (7 de 4 de 2020a). *Contraespionagem*. Fonte: Serviço de Informações de Segurança: https://www.sis.pt

SIS. (12 de 12 de 2020b). A importância das informações para a segurança no ciberespaço. *Contributo institucional do Serviço de Informações de Segurança*. (A. Carvalho, Entrevistador)

Soares, V. (26 de 10 de 2018). *9 ataques informáticos que ficaram para a história*. Acesso em 12 de 2 de 2020, disponível em E-konomista: https://www.e-konomista.pt/ataques-informaticos-ficaram-para-historia/

Sousa, M. R. (1978). *Direito Constitucional, I - Introdução à Teoria da Constituição.* Braga: Livraria Cruz.

Tavares, P. (23 de 4 de 2018). *A Ciber Higiene no Ciberespaço*. Acesso em 28 de 2 de 2020, disponível em Segurança Informática: https://seguranca-informatica.pt/a-ciber-higiene-no-ciberespaco/#.XlkDC0pBrIU

The Guardian. (28 de 07 de 2014). *William Gibson: the man who saw tomorrow* . Fonte: The Guardian: https://www.theguardian.com/books/2014/jul/28/william-gibson-neuromancer-cyberpunk-books

The Harris Poll. (2020). *2019 CYBER SAFETY INSIGHTS REPORT. GLOBAL RESULTS.* NortonLifeLock. Fonte: https://www.nortonlifelock.com/content/dam/nortonlifelock/pdfs/reports/2019-nortonlifelock%20-cyber-safety-insights-report-global-results-en.pdf

Traynor, I. (17 de 05 de 2007). Russia accused of unleashing cyberwar to disable Estonia. *The Guardian*. Brussels. Acesso em 03 de 11 de 2019, disponível em https://www.theguardian.com/world/2007/may/17/topstories3.russia

Tribolet, J. (14 de 01 de 2020). A ciberguerra em curso entre os EUA e o Irão. (L. Medeiros, Entrevistador) Fonte: https://sicnoticias.pt/programas/futurohoje/2020-01-14-A-ciberguerra-em-curso-entre-os-EUA-e-o-Irao

U.S. Army. (2017). *FM 3-12: Cyberspace and electronic warfare operations.* Washington, DC: Department of the Army. Fonte: http://www.apd.army.mil

Unit, T. E. (2019). *Cause for concern? The Top 10 Risks to The Global Economy 2019.* London: The EIU.

USJCS. (2018). *JP 3-12 - Cyberspace Operations.* Joint Force Development. Acesso em 28 de 10 de 2019, disponível em https://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/3-0-Operations-Series/

Venâncio, P. (2011). *Lei do Cibercrime.* Lisboa: Coimbra Editora.

Viana, V. (2018). Prólogo. Em IDN, *Contributos para uma Estratégia Nacional de Ciberdefesa* (pp. 11-12). Lisboa: IDN Cadernos.

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

Warner, M. (2009). Building a Theory of Intelligence Systems. Em G. F. Treverton, *National Intelligence Systems* (pp. 11-37). Cambridge: Cambridge University Press.

We Are Social. (2020). Digital in 2020: Global Digital Overview. We Are Social and Hootsuite. Acesso em 24 de 05 de 2020, disponível em https://wearesocial.com/digital-2020

Wolton, D. (1999). *E depois da Internet?* Algés: Difel.

Anexo A – Corpo de Conceitos

Ameaça - Potencial causa de um incidente indesejado, que pode provocar danos a um sistema, indivíduo ou organização (ISO/IEC 27032).
Ameaça híbrida – Ameaça que combina o emprego de meios convencionais, não-convencionais e assimétricos, que através do emprego de várias táticas, com postura aberta ou encoberta, conduz operações de desinformação, ciberataques, pressão económica, operações de guerrilha, atividades criminosas e terroristas (NATO, 2019c).
Cibercrime – "Os factos correspondentes a crimes previstos na Lei do Cibercrime (LC)[138] e ainda a outros ilícitos penais praticados com recurso a meios tecnológicos, nos quais estes meios sejam essenciais à prática do crime em causa" (GOV-PT, 2019, p. 2890)
Ciberdiplomacia - "disciplina da ação externa do Estado que visa promover, nomeadamente, a aplicação do direito internacional vigente ao ciberespaço a fim de garantir a respetiva estabilidade, a governação transparente e partilhada da sua utilização universal e a criação eficiente de capacidades normativas" (GOV-PT, 2019, p. 2892).
Ciberespaço – "Ambiente complexo, de valores e interesses, materializado numa área de responsabilidade coletiva, que resulta da interação entre pessoas, redes e sistemas de informação" (GOV-PT, 2019, p. 2889).
Ciberguerra – "Luta ou conflito entre duas ou mais nações ou entre diferentes fações dentro de uma nação onde o ciberespaço é o campo de batalha" (IDN-CESEDEN, 2013, p. 23).
Ciber-higiene - Palavra que deriva do termo anglo-saxónico *Cyber Hygiene* e que visa retratar os cuidados básicos de segurança que os Estados, as organizações e os cidadãos deverão ter no ciberespaço. Este conceito tem como objetivo salientar a importância da aplicação de boas práticas de segurança, nas diversas vertentes da segurança da informação, por forma a proteger a informação, prevenir a ocorrência de ciberataques e em caso destes serem eficazes, minimizar os danos e as perdas decorrentes (Tavares, 2018).
Ciberespionagem – Fundamenta-se como sendo uma variante da espionagem tradicional, consistindo na obtenção de conhecimento e informações sensíveis ou classificadas sobre indivíduos, organizações, Estados e competidores e/ou inimigos, que possam conceder uma vantagem económica, política ou militar, obtidas com recurso à utilização de métodos de exploração ilegal da internet, redes, software ou computadores (ENISA, 2013).
Ciberterrorismo – Ataque ou tentativa de ataque a rede de comunicação, computadores e informação neles contida, com o objetivo de intimidar ou coagir um governo ou o seu pessoal para atingir fins políticos ou sociais. Adicionalmente, para ser considerado ciberterrorismo, o ataque deve resultar em violência contra pessoas ou propriedade, ou pelo menos causar dano suficiente para provocar medo. Ataques que resultem em morte ou dano físico, explosões, queda de aviões, contaminação de água ou perda económica grave são alguns exemplos. Ataques que apenas

[138] Lei do Cibercrime (lei nº 109/2009, de 15 de setembro)

provocam disrupção de serviços não essenciais ou são principalmente perdas financeiras irrelevantes não o são" (Denning, 2000a).
Conhecimento Situacional no Ciberespaço - resulta da combinação, em praticamente, tempo real, do panorama situacional no ciberespaço com a análise e a gestão das informações (NATO, 2020).
Confidencialidade - A propriedade de a informação não ser divulgada a pessoas ou entidades não autorizadas, ou segundo processos não autorizados (ISO/IEC 27000).
Criptografia – "A arte de escrever em código", visa ocultar o significado de uma mensagem de modo a que apenas o seu recetor a consiga decifrar (Urgellés, 2016, p. 16).
***Distributed Denial of Service* -** um ataque do tipo DDoS (em Português - Negação de Serviço Distribuída) tem origem em vários computadores e visam atacar um sistema ou uma rede de modo a impedir o acesso dos seus utilizadores. Por norma, este tipo de ataque provoca a perda de conexão à rede e aos serviços, devido a consumir a largura de banda da rede ou por sobrecarga dos sistemas alvo (APDSI, 2019).
Disponibilidade - Propriedade de estar acessível e de poder ser utilizada a pedido de uma entidade autorizada (ISO/IEC 27000).
Domínios ou planos de atuação - "conjunto dos meios técnicos e humanos (atores), bem como do enquadramento legal, envolvidos na prossecução de um conjunto de objetivos, os quais são em parte determinados por uma perspetiva relativamente ao fenómeno da ciberconflitualidade" (Santos, Bravo, & Nunes, 2012, p. 2).
Endereço *Internet Protocol* - Frequentemente designado pela expressão inglesa IP address, constitui um protocolo Internet (ou Internet Protocol) que controla a comunicação e troca de dados entre os computadores. Um dos mais importantes entre todos os protocolos presentes na Internet, tem por missão identificar as máquinas e redes e fazer o reencaminhamento (*routing*) correto das transmissões entre elas (*endereço IP* in Infopédia [em linha]. Porto: Porto Editora, 2003-2020. [consult. 2020-09-29 00:28:39]. Disponível na Internet: https://www.infopedia.pt/$endereco-ip)
Espionagem – "A espionagem consiste na obtenção de informação que, pelo seu valor e relevância para o interesse nacional, está protegida por medidas de segurança. O acesso ilícito a essa informação faz-se através de métodos clandestinos, recorrendo a meios técnicos cada vez mais sofisticados ou a agentes e fontes humanas que se encontram ao serviço dos interesses políticos, militares e económicos de um Estado estrangeiro" (SIS, 2020).
Estado – "povo, fixado num território de que é senhor, e que institui, por autoridade própria, órgãos que elaborem as leis necessárias à vida coletiva e imponham a respetiva execução" (Caetano, 1973, p. 16).
Estenografia – A esteganografia tem como finalidade esconder a presença de uma comunicação, através da introdução de uma mensagem secreta em documentos ou objetos inócuos e insuspeitos, tais como imagens digitais, vídeos e ficheiros de áudio. Deste modo, o ficheiro é transmitido através da internet para um destinatário que, com recurso à utilização de técnicas específicas (e por vezes a "chaves"), irá extrair a mensagem ocultada (J. Fridrich, 2001).

Evento no MISP – No quadro da taxionomia utilizada no MISP, eventos correspondem a "encapsulamentos" de informações contextualmente relacionadas sobre um determinado acontecimento numa rede ou sistema de informação, representadas como um atributo e objeto (CIRCL, MISP Glossary, 2019).
Fake news - são comumente entendidas como notícias falsas, as quais, se traduzem na disseminação intencional de desinformação, quer através dos meios de comunicação tradicionais, quer por via das redes sociais. Integram e enquadram-se no conceito de *fake news* as seguintes interpretações: falsidades deliberadas para atrair visitantes; notícia satírica que é projetada para ser humorística e abertamente falsa; reportagens tendenciosas que exageram certos fatos, em deturpando outros; a rejeição de relatos e opiniões por um indivíduo ou organização, porque eles apresentam um desafio à sua própria narrativa ou à da sua organização e/ou facão (Lilleker *et al.,* 2017).
Firewall – Em português barreira de proteção, a qual no âmbito das TIC designa um "sistema informático concebido para proteger uma rede de computadores do acesso externo de utilizadores não autorizados" (APDSI, 2019).
Fronteira – "linha que delimita territorialmente um Estado, fixando a sua extensão; linha que separa dois países, regiões, territórios, etc.; estrema; zona adjacente a essa linha; o que separa duas coisas distintas ou contrárias; figurado limite; termo" (Dicionário infopédia da Língua Portuguesa, 2020).
Grande Estratégia Nacional – Estratégia na qual um Estado define os seus objetivos internacionais e identifica os Estados ou organizações, contrárias ou adversárias, à prossecução daqueles (Warner, 2009),
Global Commons – São espaços ou domínios partilhados pelos diversos Estados da comunidade internacional, não sendo propriedade de nenhum Estado em específico (Maj. Gen. Barrett, Bedford, Skinner, & Vergles, 2011).
Hacker – "Pessoa com grandes conhecimentos de informática e programação, que se dedica a encontrar falhas em sistemas e redes computacionais". ("hacker", in Dicionário Priberam da Língua Portuguesa [em linha], 2008-2013, https://www.priberam.pt/dlpo/hacker [consultado em 17-07-2019]).
Hacking – Termo que se refere "a ações realizadas com recurso a ferramentas de *software* para exploração de vulnerabilidades em sistemas informáticos com o objetivo aumentar o nível de acesso ou controlo sobre os mesmos" (Santos, 2011, p. 27).
Hacktivismo – A convergência entre o ativismo social e o *hacking*, tirando partido da cobertura mediática usualmente garantida a este tipo de eventos como forma de promoção de uma causa política (Denning, 2000). O *hacktivismo tem* como finalidade "chamar a atenção da opinião pública em geral, de um sector da sociedade ou da classe política, para a sua causa, tirando partido da cobertura mediática que a excentricidade e, por vezes, a espetacularidade que os seus métodos proporcionam" (Santos, 2011, p. 27).
Indicadores de ameaça – No quadro da taxionomia utilizada no MISP, indicadores são um padrão que pode ser utilizado para detetar atividades suspeitas ou maliciosas no ciberespaço (CIRCL, MISP Glossary, 2019).

***Indicators of Compromise (IoC)* –** Indicadores de compromisso são artefactos e/ou traços relevantes observados numa rede ou num sistema de informação conectados a uma intrusão ou a uma técnica utilizada por um invasor de uma rede ou sistema de informação. Os IoC são um subgrupo dos indicadores de ameaças. (CIRCL, MISP Glossary, 2019).
Informação – são "dados não processados que podem ser utilizados na produção de informações" (NATO, 2019b, pp. 67-68).
Informações – Também chamadas de *"intelligence"*, são um produto que resulta de um processo designado de "ciclo de informações" que contempla, à vez, a recolha de dados/factos/informações através de meios humanos, documentais e tecnológicos, e a sua organização, análise e avaliação através de técnicas e metodologias próprias. As informações são um instrumento essencial de apoio à decisão política, contribuindo para a segurança, salvaguarda e defesa dos interesses nacionais (SIRP, 2020).
Infraestrutura Crítica – "A componente, sistema ou parte deste situado em território nacional, que é essencial para a manutenção de funções vitais para a sociedade, a saúde, a segurança e o bem-estar económico ou social, e cuja perturbação ou destruição teria um impacto significativo, dada a impossibilidade de continuar a assegurar essas funções" Lei 46/2018 (AR, 2018, p. 4032).
Integridade - A propriedade de salvaguardar o caráter exato e completo da informação e dos ativos. (ISO/IEC 27000).
***Intrusion Detection System* (IDS) -** Produto de *hardware* ou *software* que recolhe e analisa informação de várias áreas num computador ou rede de modo a identificar possíveis falhas de segurança, que incluem intrusões (ataques a partir do exterior da organização) e má utilização (ataques a partir do interior da organização) (NIST, 2013).
***Malware* -** Termo que deriva de "*malicious software*" (*software* maligno), o qual tem como objetivo perturbar, alterar ou destruir todos ou parte dos módulos responsáveis ao normal funcionamento de um sistema ou rede informática. No fundo, define uma variedade de formas de *software* hostil ou intruso, onde se incluem os vírus, os cavalos de troia, *spyware*, entre outros códigos (APDSI, 2019).
Pooling & Sharing – Conceito "agregar e partilhar" definido pela UE, tendo em vista o desenvolvimento de capacidades militares através da integração de diversas iniciativas emergentes dos Estados-membros sobre a forma de uma cooperação multilateral sinérgica, evitando desta forma duplicações desnecessárias e salvaguardando os interesses da EU (Santos, Nunes, Ralo, & Mendes, 2018, p. 44).
***Security by design* –** é um conceito de grande importância para a indústria de segurança da informação. Significa pensar em segurança desde o escopo de desenvolvimento de um novo software, prevendo toda possibilidade de riscos aos quais aquela aplicação pode estar sujeita (Blockbit, 2018) .
Segurança da Informação – "Proteção dos sistemas de informação contra o acesso ou a modificação não autorizados da informação, durante o seu armazenamento, processamento ou transmissão, e contra a negação de serviço a utilizadores autorizados ou o fornecimento de serviço a utilizadores não autorizados, incluindo as medidas necessárias para detetar, documentar e contrariar tais ameaças" (APDSI, 2019).

Segurança das redes e dos sistemas de informação – "A capacidade das redes e dos sistemas de informação para resistir, com um dado nível de confiança, a ações que comprometam a confidencialidade, integridade, disponibilidade, autenticidade e o não repúdio dos dados armazenados, transmitidos ou tratados, ou dos serviços conexos oferecidos por essas redes ou por esses sistemas de informação, ou acessíveis através dos mesmos". Lei 46/2018 (AR, 2018, p. 4032).
Spear-phishing – "é uma tentativa direcionada de roubar informações confidenciais, como dados de contas ou informações financeiras de uma vítima específica, geralmente por motivos criminosos. Este ataque é concretizado através da aquisição de dados pessoais da vítima". (Giandomenico, 2019)
Serviços de Informações – Consistem em "organizações permanentes e atividades especializadas em coleta, análise e disseminação de informações sobre problemas e alvos relevantes para a política externa, a defesa nacional e a garantia da ordem pública de um país" (Cepik, 2003, p. 85).
Soberania – "Significa independência e liberdade nacional, garantia da integridade do território, defesa do regime constitucional e salvaguarda coletiva de pessoas e bens … justifica a existência do Estado" (IDN, 2013, p. 2).
***Web Defacement* –** "Tipo de ataque cuja finalidade visa mudar a aparência dos *sites* alvo, alterar o conteúdo e desfigurar o site original" (APDSI, 2019).

Apêndice A – Carta de apresentação das entrevistas

Exmo. (a) Senhor (a)

No âmbito da realização da Dissertação para obtenção do Grau de Mestre em Segurança da Informação e Direito no Ciberespaço (SIDC), no Mestrado em SIDC lecionado no Instituto Superior Técnico da Universidade de Lisboa, em parceria com a Faculdade de Direito da Universidade de Lisboa e da Escola Naval, encontro-me a investigar sobre o tema "A importância das informações para a segurança no ciberespaço".

O objeto de estudo desta investigação são as "Informações no Ciberespaço", procurando evidenciar a importância que as informações e a sua partilha, entre os principais atores, desempenha na segurança do ciberespaço. Neste quadro, o objetivo geral da presente investigação consiste em analisar o contributo e a importância que as informações podem desempenhar para a obtenção da segurança no ciberespaço. Neste sentido, para efeitos de prossecução da investigação, considero pertinente e relevante auscultar peritos e especialistas de reconhecido mérito, quer na área específica das informações, quer na área da cibersegurança, da ciberdefesa e do combate ao cibercrime, dado que, estes últimos dependem, significativamente, das informações e da sua partilha, em tempo útil e de forma adequada, para garantirem a segurança no ciberespaço.

Nesse sentido, solicito que V. Exa. se digne a colaborar na realização do estudo, disponibilizando-se para responder a um conjunto de questões.

Desde já agradeço a disponibilidade manifestada, contribuindo com o seu conhecimento e experiência para a solidez deste tema, sublinhado que esta entrevista tem objetivos meramente académicos.

Antecipadamente grato pela disponibilidade,
Cordiais cumprimentos,
Lisboa, 22 de setembro de 2020
António Augusto Ramos Carvalho

Apêndice B – Exemplo do guião das entrevistas estruturadas

Secção 1: Caracterização do Ciberespaço

1. Na sua ótica quais são as principais características do ambiente ciberespaço (máximo 5)?

2. Das características que identificou, quais são as 3 que considera que impõem maiores desafios à segurança no ciberespaço? Justifique a sua opinião.

Secção 2: Segurança no Ciberespaço

3. Como especialista num dos principais domínios de atuação (cibersegurança, combate ao cibercrime, ciberdefesa e informações), refira, sucintamente, em que medida esse domínio, em que é perito, contribui para a segurança no ciberespaço.

4. Com o intuito de promover a cooperação e a partilha de informação entre as principais entidades que contribuem para a segurança do ciberespaço nacional, foi criado o grupo de carácter operacional informal, designado de G4.
   a. No seu ponto de vista, qual é o contributo que o G4 desempenha na promoção da segurança no ciberespaço de interesse nacional?
   b. Ainda no âmbito do G4, existe algum aspeto na área da cooperação, coordenação, partilha de informação ou outro, que considere que pudesse ou devesse ser incrementado para uma articulação ou resposta mais eficiente.

Secção 3: Informações no Ciberespaço

5. De que forma considera o Conhecimento Situacional no Ciberespaço importante para a prevenção e antecipação de ciberataques?

6. Em que medida considera que a partilha de informação e de informações no ciberespaço poderá ser importante para antecipar, prevenir e mitigar os ciberataques?

7. Por forma a promover a partilha de informação de forma mais célere e eficiente foi criado e desenvolvido o *Malware Information Sharing Plataform (*MISP).
   a. Na sua perspetiva, qual é a importância e a mais-valia que o MISP acrescenta na partilha de informação entre as entidades e organizações com responsabilidade na segurança do ciberespaço?
   b. A nível nacional como considera que o MISP desempenha um papel relevante na antecipação e prevenção de ciberataques?
   c. Existe algum aspeto que julgue que possa ou devesse ser melhorado na rede nacional?

8. Tendo em conta que não há sistemas perfeitos, e que há sempre campo para melhoria, existe alguma lacuna que considera que deverá ser corrigida na abordagem nacional à partilha de informação no ciberespaço?

9. Por fim, indique os 3 aspetos em que, na sua opinião, as informações podem contribuir, significativamente, para a segurança no ciberespaço?

Apêndice C – Matriz de peritos entrevistados e questões das entrevistas estruturadas

Apêndice Entrevista	Especialista	Função	Relação das questões efetuadas
26OUT20	Inspetor Chefe Rogério Bravo	Coordenador da Seção Central de Investigação Digital da PJ	Todas, da Q1 à Q9.
28OUT20	Engenheiro Lino Santos	Coordenador do CNCS	Todas, da Q1 à Q9.
2NOV20	Capitão-de-fragata EN-AEL Francisco Assunção	Chefe Secção de Tecnologias do CCD	Da Q1 à Q9, exceto a questão Q8.
2NOV20	Major Nuno Rodrigues	Chefe da Célula Conhecimento Situacional CCD	Da Q1 à Q9, exceto a questão Q8.
15NOV20	Major Carlos Silva	Especialista área de Informações do CISMIL	Questões Q1, Q3, Q5, Q6 e Q9
12DEZ20	Contributo institucional do Serviço de Informações de Segurança		Todas, da Q1 à Q9.