ACADEMIA DA FORÇA AÉREA

Política Europeia de Segurança no Ciberespaço

Rodrigo Eurico Fidalgo Pombo

Aspirante a Oficial Aluno/Piloto Aviador 138971-J

Dissertação para obtenção do Grau de Mestre em

Aeronáutica Militar, na Especialidade de Piloto Aviador

Júri

Presidente:

Orientador: Professora Doutora Sandra Maria Rodrigues Balão

Coorientador: Tenente-Coronel Luís Manuel Pinto de Almeida da Rocha

Vogal:

Sintra, maio de 2019

(página intencionalmente em branco)

ACADEMIA DA FORÇA AÉREA

Política Europeia de Segurança no Ciberespaço

Rodrigo Eurico Fidalgo Pombo

Aspirante a Oficial Aluno/Piloto Aviador 138971-J

Dissertação para obtenção do Grau de Mestre em

Aeronáutica Militar, na Especialidade de Piloto Aviador

Júri

Presidente:

Orientador: Professora Doutora Sandra Maria Rodrigues Balão

Coorientador: Tenente-Coronel Luís Manuel Pinto de Almeida da Rocha

Vogal:

Sintra, maio de 2019

(página intencionalmente em branco)

Este trabalho foi elaborado com finalidade essencialmente escolar, durante a frequência do Curso de Mestrado em Aeronáutica Militar na especialidade Piloto-Aviador cumulativamente com a atividade escolar normal. As opiniões do autor, expressas com total liberdade académica, reportam-se ao período em que foram escritas, mas podem não representar doutrina sustentada pela Academia da Força Aérea.

(página intencionalmente em branco)

Agradecimentos

Esta dissertação culmina o final de uma etapa e o início de outra. Foi-me concedido o privilégio de frequentar o curso de Ciências Militares Aeronáuticas, da Academia da Força Aérea e agradeço à Academia por todos os ensinamentos que me transmitiu e por me ter feito crescer como militar e como pessoa.

Agradeço a Sra. Professora Sandra Maria Rodrigues Balão por ter aceite desafio de orientar esta dissertação e pela sua paciência e profissionalismo que se revelou crucial para a elaboração dessa dissertação.

Ao Sr. Tenente-Coronel Luís Rocha, pela definição de prazos e objetivos e liberdade que concedeu na escolha do tema da presente dissertação.

Aos meus camaradas e amigos pela boa disposição que transmitiram e pelos momentos partilhados ao longo deste percurso.

Um agradecimento especial aos meus pais e ao meu irmão que me têm apoiado incondicionalmente ao longo da minha vida e me ajudaram muito com a sua motivação e boa disposição.

Agradeço por último à minha namorada e amiga por toda a paciência, carinho e tempo abdicado na elaboração desta dissertação.

(página intencionalmente em branco)

Resumo

Atualmente a Europa e o mundo estão cada vez mais dependentes da tecnologia, e o aumento do uso da *internet* por parte da população fez com que fossem criadas imensas oportunidades mas ao mesmo tempo apareceram as ciberameaças e ciberataques que vieram afetar não só a privacidade e segurança dos utilizadores mas também das infraestruturas dos próprios Estados. Devido ao aumento da frequência das ciberameaças e ciberataques, a UE teve que atuar e tomar medidas para assegurar a segurança dos seus cidadãos e desenvolver medidas e políticas de cibersegurança.

A emergência de ciberataques como o dos Balcãs em 1999 ou mais recentemente o da Estónia ou da Geórgia em 2007 e 2008 respetivamente, vieram demonstrar que a Europa não estava preparada a nível estratégico nem político no domínio do ciberespaço. Em consequência disso, primeiro a NATO e depois a UE vieram desenvolver políticas e estratégias de cibersegurança para conseguirem responder às ciberameaças. Em particular a UE veio realçar a importância dos Estados-Membros cooperarem com o setor privado para que seja possível superar o desafio do ciberespaço.

De facto, as Parcerias Público Privadas têm vindo a tornar-se cruciais para a evolução do ciberespaço quer seja na ajuda à proteção de infraestruturas críticas, quer no acesso por parte do setor público aos recursos do setor privado bem como na possibilidade de criar sinergias entre as diversas iniciativas do setor privado com o objetivo de desenvolver o mundo do ciberespaço.

Neste sentido de melhorar a segurança do ciberespaço, torna-se fundamental a criação de parcerias por parte dos Estados-Membros promovendo as medidas necessárias para a sua cibersegurança bem como das principais Organizações Internacionais, conseguindo assim superar as adversidades que o Homem criou ao desenvolver esta dependência tecnológica.

Palavras-chave: Parcerias Público Privadas; Ciberespaço; Ciberdefesa; Cibersegurança; Ciberameaças; Relações Internacionais.

(página intencionalmente em branco)

Abstract

Nowadays, Europe and the world are increasingly dependent on technology, and the increasing use of the internet by the population has created huge opportunities. At the same time cyber-threats and cyber-attacks have come to affect not only the privacy and security of the users but also the infrastructures of the states themselves. Due to the increased frequency of cyber-threats and cyber-attacks, the EU had to act and take steps to ensure the safety of its citizens and to develop cyber-security policies and measures.

The emergence of cyber-attacks such as the Balkans in 1999 or more recently, the attacks against Estonia and Georgia in 2007 and 2008 respectively showed that Europe wasn´t strategically prepared in the cyberspace area. As a result, first NATO and then the EU have developed cyber-security policies and strategies to respond to cyber threats. In particular the EU has emphasized the importance of Member States cooperating with the private sector in order to overcome the challenge of cyberspace.

In fact, Public and Private Partnerships have become crucial to the evolution of cyberspace, both in helping to protect critical infrastructures and the access by the public sector to private sector resources as well as the possibility of creating synergies between the various private sector initiatives with the aim of developing the world of cyberspace.

In this sense to improve the security of cyberspace, it is essential to create cooperations between Member States in order to promote the necessary measures for their cyber security, as well as the main international organizations. Thus, they will overcome the difficulties that Man has created in this technological dependency.

Key words: Public and Private Partnerships; Cyberspace; Cyber-defense; Cyber-security; Cyber-threats; International Relations

(página intencionalmente em branco)

Índice

Índice de Figuras

Índice de Tabelas

Lista de Acrónimos

CCD COE	Cooperative Cyberdefence Center for Excellence
CDMACyber	Defence Management Authority
CEDN	Conceito Estratégico da Defesa Nacional
CERT	Community Emergency Response Team
CIS	Communication Information System
cPPP	Contractual Public-Private Partnerships
CSC	Cyber Security Commission
CSDP	Common Security and Defence Policy
CSIRT	Computer Security Incident Response Team
CSP	Cyber Securtiy Platform
DDoS	Distributed Denial of Service
DIH	Direito Internacional Humanitário
DOD	Department of Defence
DoS	Denial of Service

EC3	European Cyber Crime
ECSO	European Cyber Security Organisation
EDA	European Defence Agency
ENISA	European Network and Information Security Agency
EP3R	European Public Private Partnership for Resilience
EUA	Estados Unidos da América
Ex NCS	National Cybersecurity Exercise
Europol	European Police Office
FOC	Full Operational Capability
GI	Guerra de Informação
GPG	Good Practice Guide
ICT	Information and Communications Technology
ISAC	Informations Sharing and Analysis Centers
J-CAT	Joint Cybercrime Actions Taskforce
KSO	Kuratorium Sicheres Österreich
NATO	North Atlantic Treaty Organization
NCAs	National Competent Authorities
NCIA	NATO Communications and Information Agency
NCIRC	NATO Computer Incident Response Capability
NGOs	Non-Governmental Organisations
NICP	NATO Industry Cyber Partnership
NIS	Network and Information Security
NSA	National Security Agency
ONU	Organização das Nações Unidas
OSC	Outsourcing cybersecurity services

OSCE	Organization for Security and Co-Operation in Europe
PCSD	Política Comum de Segurança e Defesa
PNCS	Portuguese National Cybersecurity Center
PPP	Parceria(s) público-privada(s)
RCB	Rządowe Centrum Bezpieczeństwa
RIA	Riigi Infosusteemi Amet
SIC	Sistemas de Informação e Comunicações
SPIN	Sistemas de Proteção da Infraestrutura Nacional
SRI	Sistema de Redes de Informação
TI	Tecnologias de Informação
TIC	Tecnologias de Informação e Comunicação
UE	União Europeia

Introdução

A segurança do ciberespaço constitui um dos mais relevantes desafios para a sociedade dos dias de hoje. O uso da *internet* tem crescido ano após ano e, dados do *International Strategy for Internet*, apontam para um aumento do número de utilizadores da internet de cerca de dois mil milhões, o que dificulta o seu controlo (ISC, 2011). Obama, num discurso proferido em 2009, afirmou: “This world (cyberspace) is a world that we depend on every single day... [it] has made us more interconnected than at any time in human history.” (Obama, 2009).

De facto, a informação deixou de ser um mero instrumento de apoio às diversas atividades das organizações para se tornar num objeto, em si mesmo. Passou a ser um ativo que, quando transformado em conhecimento é, consequentemente, convertido em capital intelectual. Neste sentido, referimo-nos, simultaneamente, a processos, pessoas e tecnologias (Dinis, 2005).

Ao nível dos noticiários, são constantes as referências à temática do ciberespaço. Nos jornais internacionais encontramos manchetes constantes: “*cybercrime is up, watch out for the latest phishing attack trying to steal our identity”, “update our antivirus to avoid infraction, patch the operating system to avoid a hacker taking control”, “new zero day attack against smartphones”, “Facebook privacy compromised, someone took down Twitter”* (Andress & Winterfeld, 2014, p.1).

O desenvolvimento global, social e económico traz consigo implicações, assim como dependências, onde e com evidência se insere a *internet*. No que diz respeito ao setor da economia, o ciberespaço verifica-se como elemento chave. É exemplo, a criação de empresas *online,* como foi o caso de Pete Chasmore (Fundador e CEO do Mashable) que se tornou milionário através dos seus comentários sobre tecnologia. Em pouco tempo, este *website* superou outros canais de peso, como o Techcrunch, tendo atualmente dois escritórios, nos Estados Unidos da América (EUA) e na Europa. O seu *website*

tem quarenta e dois milhões de visitantes por mês e mais de vinte e um milhões de seguidores nas redes sociais (Mashable, 2014).

Por outro lado, o aparecimento das redes sociais e o crescente uso da *internet* na área comercial proporcionaram uma maior partilha de informação. No entanto, esse uso excessivo da *internet* pode ser motivo para um aumento dos ciberataques ao expor em demasia a sociedade, cria também vulnerabilidades que podem levar ao acesso ilícito nos sistemas (correio eletrónico das pessoas bem como das organizações e informações reservadas das mesmas) e possível roubo de informações que podem comprometer empresas/organizações/pessoas (ISC, 2011).

Neste contexto, a realidade do século XXI é bastante diferente daquela do século XX. O grande desenvolvimento tecnológico trouxe consigo imensas oportunidades, mas também inúmeras ameaças para as quais a sociedade tem que estar preparada (Balão, 2010).

Muito embora conceito de ciberespaço tenha surgido no século XX mais precisamente em 1982, quando Gibson criou uma história, embora de ficção, com o nome de "*Burning Chorme*" (Gibson, 1984) Há, no entanto, quem tenha previsto a *internet* e a *World Wide Web* muitos anos antes da sua existência. Herbert Marshall McLuhan filósofo Canadiano em 1964 desafiou as definições convencionais, quando afirmou que "*Medium is the Message*". Com esta afirmação ele demonstra o poder dos meios de comunicação, na medida em que despertam e alteram pensamentos e sentidos. Na "*medium theory*" os media não são apenas um jornal ou a *internet*. Pelo contrário, são o ambiente simbólico de qualquer ato comunicativo (Twente´s University, 2019). McLuhan previu o *World Wide Web* 30 anos antes de existir. Pode-se afirmar que foi com ele que o mundo deu os primeiros passos no desconhecido mundo do ciberespaço (Lee & Chomsky, 2015).

Manuel Castells, professor universitário e especialista em Relações Internacionais, Sociologia e Tecnologia de Comunicação, tem explorado a relação entre espaços urbanos e movimentos sociais durante décadas, sendo

que nos últimos anos orientou a sua atenção para os movimentos sociais e como eles se mobilizam através da media social (Castells, 2012).

Castells referiu que a tecnologia era uma condição necessária, embora não suficiente, para o aparecimento de uma forma de organização social diferente daquela que existia que se baseava na difusão de redes com base na comunicação virtual (Castells, 2012).

Há três décadas, o professor Noam Chomsky, visto por alguns como o mais brilhante e corajoso intelectual vivo e por outros como um teórico da conspiração anti-EUA, escreveu uma poderosa crítica aos media num livro intitulado "*Manufacturing Consent*" (Lee & Chomsky, 2015) referindo a propósito da *internet* que a mesma fornece novas oportunidades. A biblioteca tradicional, espaço para pesquisas, pode ser simplesmente substituída pelo abrir do computador e consequente pesquisa no *google*. Nos motores de busca dos nossos computadores, como o caso do *google chrome*, *firefox*, entre outros, pode-se certamente encontrar informações com mais facilidade e também distribuir informações diferentes de muitas fontes (Lee & Chomsky, 2015).

O conceito de ciberespaço foi evoluindo de tal maneira que hoje em dia é conhecido como uma rede global que liga, entre si, principalmente, os sistemas de processamento dos computadores e as redes de telecomunicações (Fernandes, 2012).

Assim, a segurança dos sistemas de informação *on-line* apresenta-se como uma mais-valia para obtenção de condições de maior competitividade perante concorrentes e outros atores (Dinis, 2005).

Existem diversos casos que demonstram a importância da cibersegurança para a vida humana. A problemática em apreço parece ter tido início em 1999, durante a Guerra dos Balcãs e que exploraremos mais adiante nesta dissertação.

Assim, é neste contexto que equacionamos a problemática da cibersegurança. Como exemplo ilustrativo da sua relevância, consideremos os

Jogos Olímpicos de Atenas em 2004. A preocupação com a cibersegurança foi, à época, assumida não apenas pelas (e para as) nações anfitriãs das Olimpíadas e o Comité Olímpico Internacional mas também pela (e para) a sociedade internacional em geral. Envolvendo atletas de mais de 200 países e com uma cobertura mediática mundial, o evento constituía em si mesmo um potencial alvo para aqueles que procurassem causar qualquer tipo de impacto negativo por motivos políticos (ou outros) através de ataques cibernéticos, como por exemplo sabotar as transmissões televisivas, impossibilitar o acesso à informação sobre resultados, calendários e horários de provas, etc disponibilizadas por *websites*, entre outras formas de ciberataques. De forma a reduzir as ameaças, o planeamento da segurança é fundamental para que seja possível garantir a segurança da realização de eventos desta dimensão e natureza (Rand Corporation, [s.d]).

Para se ter uma perceção da evolução do mundo no campo da cibersegurança, foi realizado um estudo de forma a procurar avaliar o nível da ameaça cibernética a que os jogo Olímpicos e Paralímpicos de Tóquio em 2020 poderão estar sujeitos para que, com base nesses dados, possam ser levadas a cabo as ações adequadas e necessárias ao nível político, de forma a reduzir o grau de risco de exposição a eventuais ciberataques que possam ocorrer (Rand Corporation, [s.d]).

De facto, após 2004, vários foram os casos que fizeram despoletar a atenção da União Europeia (UE) relativamente às questões da segurança do ciberespaço, como foram os casos da Estónia em 2007 e da Geórgia em 2008. No seguimento destes, a UE viu-se confrontada com a necessidade de criar uma estratégia de segurança para o ciberespaço uma vez que, para além de se terem vindo a tornar cada vez mais frequentes, casos como os de 2007 e 2008 afetam não apenas uma organização individualmente considerada mas, também, o próprio Estado (NATO, 2010).

Na verdade, segundo Miller, muitas organizações internacionais não possuem nos seus sistemas os mecanismos necessários à sua proteção ou,

quando os têm, a não atualização dos mesmos coloca-as numa posição de fragilidade perante possíveis ataques (2000).

Acrescente-se que é extremamente difícil conseguir saber de que parte do mundo é proveniente cada ciberataque. Em consequência, também a reação ao ataque é complexa. Como poderá reagir a Europa a um potencial ataque em larga escala cuja origem é totalmente desconhecida? Que Política de segurança a União Europeia deve adotar face a uma ofensiva que obedeça a tal tipologia?

1.1 Motivação e Pertinência

No último Conceito Estratégico da Defesa Nacional (CEDN) (2013) é reconhecida grande importância ao ciberespaço, e a cibercriminalidade é considerada como uma das principais ameaças e riscos que se colocam às sociedades humanas, o que permite desde logo antever a relevância e a opção pelo desenvolvimento e aprofundamento da cibersegurança. Sobretudo, num tempo em que as atividades criminosas no ciberespaço dependem cada vez mais de mercados especializados e sofisticados que lidam livremente com as ferramentas do cibercrime (Rand Corporation, 2016).

Neste contexto, merece destacar que o FBI financia o desenvolvimento de muitos programas de *software* de cibersegurança e privacidade dentro de seu mandato de direitos humanos (Rand Corporation, 2015). No entanto, investigadores dizem que há vantagens e desvantagens associadas a qualquer investimento em tecnologia e inovação (ibidem).

Parecem não subsistir dúvidas de que os conflitos, nos dias de hoje, são totalmente distintos dos que usualmente se identificavam no passado, sobretudo porque se verifica existir um diferente *modus operandi*, a implementação de novas ideias, além da utilização de novos ambientes com o consequente recurso a diferentes técnicas e ferramentas. Atualmente, o ciberespaço é o ambiente a forma mais comum em que se “dá” o conflito,

executado na forma de ciberataques, pela dificuldade que existe em reconhecer de onde veio o ataque e quem o executou.

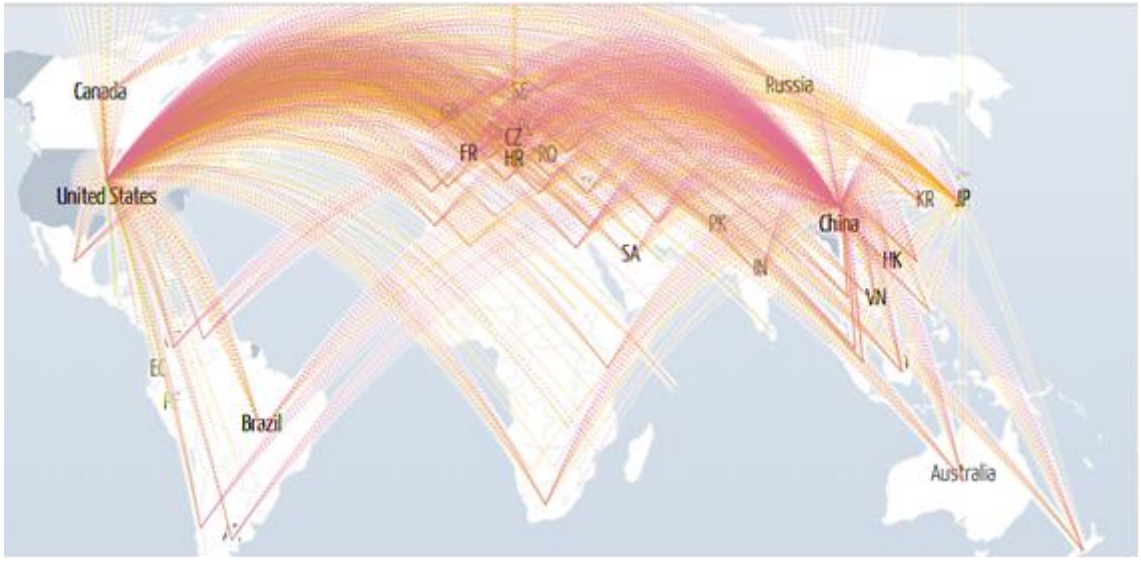

Figura 1- Ataque DDoS a acontecer no mundo a 22 de Março de 2018 (pelas 19h00 horas)

Fonte: (Digital Attack Map, 2019)

A figura 1 representa os ataques Distributed Denial-of-Service (DDoS) que estavam a acontecer em direto no dia 22 de Junho de 2018. O *website* "www.digitalattackmap.com" permite, a qualquer pessoa, verificar não só os ataques que estão a acontecer em tempo real como também ataques ocorridos 3 anos antes da presente data de acesso. Embora se verifique uma grande quantidade de ataques todos os dias, estima-se que o *website* só mostre cerca de 0.1% dos ataques que, efetivamente, têm lugar (Digital Atatack Map, 2019), sendo que este tipo de ataques é hoje extremamente comum, verificando-se a uma escala global.

O Departamento de Defesa dos Estados Unidos da América estima que em 10 anos (2000 para 2010) o número de utilizadores da *internet* aumentou mais de quatrocentos pontos percentuais, passando de 360 milhões para 2 mil milhões de pessoas (Fernandes, 2017) sendo, esta evolução uma das razões apontadas para o crescimento do investimento em cibersegurança.

Mais recentemente, veja-se o caso das eleições presidenciais dos EUA de 2016 no âmbito das quais, alegadamente, *hackers* russos terão pirateado contas de correio eletrónico de membros do partido democrata e em específico de Hillary Clinton e do seu diretor de campanha John Podesta para, posteriormente, disponibilizarem essas informações à *Wikileaks* com o objetivo de beneficiar a campanha de Donald Trump (Raínho, 2016). De acordo com US *intelligence Community*, *hackers* russos terão em diversas ocasiões, antes das eleições desse ano, tentado aceder às redes de algumas das principais instituições dos EUA, incluindo a Casa Branca e o Departamento de Estado (Harding, 2016).

Não era apenas nos EUA que os problemas com o ciberespaço existiam, em 2014 num livro "Crise, Estado e Segurança" a Professora Doutora Sandra Balão sustentou num artigo a importância de se criar um Estratégia Nacional de Segurança e Informações, no âmbito do ciberespaço (Balão, 2014)

Em face dos desafios suscitados por este novo tipo de cenário, e face às ameaças que se colocam à União Europeia, torna-se fundamental repensar e elaborar políticas e estratégias para a Cibersegurança e Ciberdefesa Europeias. Assim, é em 2016, no âmbito da *European Union Global Strategy*, reforçada a ideia de que é necessário haver esforços no sentido da UE assegurar autonomia estratégica apesar de cooperar com a *North Atlantic Treaty Organization* (NATO) (Silva, 2019).

Em 2010 num artigo publicado na Proelium a professora Sandra Balão abordou as necessidades e os contributos que eram necessários adequar através de uma Estratégias de Informação devido ao aumento da importância do ciberespaço nos sistemas de informação e comunicação (Balão, 2010).

Os atores das Relações Internacionais, onde se incluem as grandes potências como os Estados Unidos e também os Estados de menores dimensões como é o caso de Portugal, estão a desenvolver políticas e estratégias para aumentarem os seus recursos de informação para assegurar a segurança e proteção das suas infraestruturas relativas à mesma e, assim,

possibilitar que o ciberespaço seja um local de livre acesso e seguro para todos seus utilizadores (Nunes, 2018).

É fundamental reter que a *internet* é a base na qual assentam os sistemas de comunicação de instituições e organizações de grande importância como é o caso dos Governos, da NATO, das Forças Armadas, da União Europeia (Nunes, 2018).

A proteção do ciberespaço não é só da resposabilidade do setor público (Estado), mas também dos seus componentes que na maioria são privados. Esta responsabilidade pela segurança do ciberespaço é do utilizador, dos operadores de sistemas e redes e dos fabricantes desses sistemas. Terá que haver um investimento público e privado tanto em recursos humanos como tecnológicos para que se possa mitigar os ciberataques através do desenvolvimento de mecanismos de segurança. Após serem desevolvimendos esses mecansimos é necessário uma ficalização períodica. Para tal a Comissão Europeia, através da ENISA para certificar-se que há uma controlo no setor da comunicação apostou fortemente na independência dos próprios Estados Membros através da criação de CERTs (*Community Emergency Response Team*) (Balão, 2010).

Em 2016, aquando da cimeira de Varsóvia a NATO reconheceu formalmente o ciberespaço como um novo domínio operacional e desde 2014 a aplicabilidade do Direito Internacional no ciberespaço (Nunes, 2018). Reconhece, ainda, que possa ser considerado um ataque armado e, como cita o artigo 51º da Carta das Nações Unidas: “Nada na presente Carta prejudicará o direito inerente de legítima defesa individual ou coletiva, no caso de ocorrer um ataque armado contra um membro das Nações Unidas, até que o Conselho de Segurança tenha tomado as medidas necessárias para a manutenção da paz e da segurança internacionais. As medidas tomadas pelos membros no exercício desse direito de legítima defesa serão comunicadas imediatamente ao Conselho de Segurança e não deverão, de modo algum, atingir a autoridade e a responsabilidade que a presente Carta atribui ao Conselho para levar a efeito, em qualquer momento, a ação que julgar necessária à manutenção ou ao restabelecimento da paz e da segurança internacionais.” (Carta das Nações

Unidas, 1945, p.11) Logo, se o Estado for membro da NATO, poderá ser invocado o Artigo 5º do Tratado de Washington segundo o qual um ataque contra um membro da NATO é um ataque a todos os outros Estados (Nunes, 2018).

A nível pessoal este tema suscitou-me bastante interesse, não só por ser um tema atual, que me obriga a uma constante atualização ao longo da dissertação e a investigar as atuais ameaças e riscos dentro da temática das Relações Internacionais. Esta temática assume, igualmente, particular relevância para a instituição que represento pois está articulada com a defesa nacional que é uma das missões e objetivos da Força Aérea Portuguesa em geral bem como da instituição militar de ensino superior que represento que é a Academia da Força Aérea, em particular. Enfrentar este desafio também é suscetível de contribuir para a minha preparação para o futuro enquanto cidadão do estado Português e futuro Oficial da Força Aérea Portuguesa.

1.2 Contextualização

As novas tecnologias da informação e da comunicação (NTIC) afetam a vida quotidiana das pessoas em diversos aspetos: uma pessoa hoje em dia usa o telemóvel e *internet* quando quer ter conhecimento de algo e qualquer pessoa está conectada ao mundo em qualquer sítio do mundo se tiver na sua posse um aparelho eletrónico. A importância da *internet* tem vindo a aumentar pouco a pouco como, por exemplo, nas compras *online* que têm aumentando de forma drástica, na utilização das redes sociais, entre outras. A UE teve a necessidade a elaborar Políticas neste âmbito e domínio que vão desde a regulação de setores inteiros, tais como o comércio eletrónico, até a tentativa de proteger a vida privada dos indivíduos. Ano após ano a utilização da *internet* e do mundo cibernético tem aumentado exponencialmente para números nunca antes pensados e a preocupação a UE sobre este tema é cada vez maior.

Números do Eurostat de 2017 mostravam que, em 2007, mais de metade (55%) dos agregados familiares na UE tinham acesso ao mundo do

ciberespaço (*internet*). Estes números continuaram a aumentar e em 2014 quatro quintos da população já acedia à *internet*. Em 2017, a percentagem de agregados familiares da UE com acesso à *internet* aumentou para 87%, crescendo cerca de 32 pontos percentuais quando comparado com os dados referentes a 2007. Ainda há dois anos atrás, 98% da população na Holanda tinha acesso à *internet* a partir de casa enquanto a Dinamarca, Luxemburgo, Suécia, Finlândia, Reino Unido e Alemanha também apresentavam valores segundo os quais 9 em cada 10 pessoas tinham acesso à *internet*. A taxa mais baixa de acesso à *internet* entre os Estados-Membros da UE foi observada na Bulgária (67%). No entanto, este país - juntamente com a República Checa, Itália, Chipre, Grécia, Portugal e Espanha - registou uma rápida expansão no número de pessoas com acesso à *internet*, com aumentos na faixa de 16-18 pontos percentuais entre 2012 e 2017. Neste sentido, também não é surpreendente que tenham sido registados aumentos relativamente pequenos em vários Estados-Membros, onde o acesso dos agregados à *internet* já estava próximo da saturação em 2012, como é o caso dos Países Baixos, do Luxemburgo e da Dinamarca, assim como da Islândia e da Noruega (Eurostat, 2018).

Hoje em dia já não é só o telemóvel e computador que estão ligados à *internet*, também já existem *smart watches*, televisões e até mesmo eletrodomésticos que podem ser ligados à distância através da *internet* (Barrinha & Carrapiço, 2016).

Já no que se refere à realidade dos EUA, em matéria de cibersegurança, a *internet* é fundamentalmente um instrumento positivo para a sociedade, que permitiu uma troca de ideias sem precedentes e uma expansão massiva na economia, algo que se precisava de olhar para preservar e ampliar os seus benefícios. Por isso, assume-se como objetivo fundamental uma *internet* aberta, interoperável, segura e confiável. No entanto, apesar de todos os benefícios atrás mencionados, é necessário saber lidar com os problemas que podem resultar da existência e utilização de uma rede aberta e interoperável de disseminação e obtenção de informação. Devido aos inúmeros ciberataques que ocorrem diariamente e sabendo dos grandes ataques cibernéticos

registados em 1999 durante a guerra dos Balcãs, o caso da Estónia em 2007 e da Geórgia em 2008, os EUA, a NATO e, posteriormente, a UE e os seus membros viram-se obrigados a dar relevo e importância ao ciberespaço e definir objetivos concretos. Assim sendo, os objetivos da cibersegurança assentam, sobretudo, em medidas de carácter preventivo, de modo a reduzir o potencial disruptivo de eventuais ações de terceiros que possam pôr em causa o desejável aumento e extensão do valor da *internet* (Council on Foreign Relations, 2019), sendo neste contexto assumida a necessidade de definição de políticas e estratégias de cibersegurança.

1.3 Âmbito

O presente trabalho constitui o culminar de uma etapa na Academia da Força Aérea no Mestrado em Ciências Aeronáuticas Militares na especialidade Piloto Aviador. É neste contexto e âmbito que é elaborada a presente dissertação, que se insere na área de Relações Internacionais.

É incontornável referir que este trabalho se rege pelos valores da Instituição Militar e que, por essa razão, os princípios a eles associados são subjacentes a esta dissertação.

De forma a realizar este trabalho da forma mais séria e cuidada possível foi necessário procurar obter o conhecimento possível - em função do tempo disponível, dos objectivos e objeto de estudo definidos - sobre diversas questões no domínio das Relações Internacionais e não apenas, e mais especificamente, sobre o Ciberespaço. Só deste modo se entendeu ser possível elaborar o enquadramento necessário para a melhor compreensão da problemática e das questões a tratar ao longo da dissertação.

Por tudo isto, considerámos fundamental “começar pelo princípio”, procurando saber o que são as Relações Internacionais. Assim, e socorrendo-nos de um dos mais conhecidos autores e especialistas portugueses nesta matéria - o professor Adriano Moreira -, quando falamos de Relações Internacionais referimo-nos “[a]o conjunto de relações entre entidades que não

reconhecem um poder político superior, ainda que sejam estatais, somando-se as relações diretas entre entidades formalmente dependentes de poderes políticos autónomos" (Moreira, 2014, p.24). Por esta citação do Professor Adriano Moreira consegue-se afirmar que as Relações Internacionais são as relações que os Estados, indivíduos e Organizações Internacionais estabelecem entre sim.

As Relações Internacionais encontram-se enraizadas na nossa vida e lidamos diariamente com esta temática sem que nos apercebamos. Assim, por exemplo, quando assistimos a uma conferência sobre o terrorismo em que o conferencista é um elemento da NATO com vasto conhecimento na área, estamos no domínio das Relações Internacionais. Pelo facto de convivermos diariamente com esta temática, para se estudá-la esta área científica existe a necessidade de nos apoiarmos em várias disciplinas (Moreira, 2014).

Deste modo, devido ao caráter especial desta área do Saber, verifica-se a necessidade de se considerar os contributos do Direito Internacional, da Economia, da Ciência Política, da Geopolítica e da Estratégia, ou da História, de entre outras – e deste modo tornamos o nosso estudo multidisciplinar, ao mesmo tempo que potenciamos a sua eficácia e eventual assertividade (Dougherty & Pfaltzgraft Jr., 2003). Por exemplo, o estudo do espaço geográfico, a Geografia, auxilia o processo de formação dos internacionalistas, pois o espaço geográfico é um elemento sempre presente na análise dos especialistas em Relações Internacionais (Aron, 2002). O direito internacional por sua vez é a ciência que regula essa mesma área.

Considerando o "*status quo*" atual no que diz respeito às ameaças de ciberataques, os líderes da NATO viram-se obrigados a renovar as suas políticas e a tomar ações imediatas a fim de proteger os sistemas de informação da aliança (Abrial, 2011).

A relevância desta problemática é percetível, por exemplo, no facto de a guerra de informação (GI) surgir hoje inserida no âmbito do espectro dos conflitos Dinis, 2005).

Hoje em dia essa GI está ligada à utilização do ciberespaço, e diz respeito a questões do âmbito internacional numa sociedade que se carateriza pela globalização cibernética, e pela informação que afeta o cidadão nas suas ações e interações, quer a nível profissional quer a nível individual ou familiar. Para satisfazer as necessidades que parecem predominar nas sociedades do tempo moderno, sobretudo as de modelo ocidental, espera-se que a informação seja de fácil e rápida acessibilidade e disponibilidade. No entanto, as condições necessárias para o cumprimento de tais expectativas ficam, em determinadas circunstâncias, prejudicadas pelas necessárias e adequadas medidas de segurança e proteção a implementar em função dos riscos e ameaças subjacentes ao espaço virtual a que temos vindo a referir-nos e sobre a qual incide a nossa investigação. Por este motivo, maiores níveis de segurança implicam mais restrições no acesso à informação (Dinis, 2005).

Com o aumento da utilização das Novas Tecnologias de Informação e Comunicação (NTIC) em setores como a educação, economia, política entre outros e consequente automatização, inclusivamente aumento das TIC em setores que são reconhecidos pela Comissão Europeia como setores críticos, como por exemplo os transportes, a energia ou a água é necessário tomar medidas de proteção desses sistemas criando estratégias e políticas, evitando que a cibercriminalidade os afete (Escravana, Lima, & Ribeiro, 2012). Se a cibercriminalidade é considerada uma ameaça aos setores acima referidos, logo é uma matéria a que é necessário dar importância e, por consequência, verifica-se a aposta na definição de políticas de segurança do e para o ciberespaço.

Devido à atenção e respeito que o ciberespaço merece por parte dos cidadãos e dos Estados, e visto que há uma crescente evolução dos ciberataques (como podemos observar no website *Digital Attack Map* que permite qualquer pessoa observar os ataques que ocorrem em tempo real) tal como o seu atual reconhecimento como uma ameaça global, justifica-se o seu estudo e a sua análise no quadro da Política Europeia de Segurança do Ciberespaço discutindo, nomeadamente, a sua evolução ao longo dos

tempos. Uma Política Europeia de Segurança assume uma particular relevância, tanto na estrita perspectiva das Relações Internacionais, como no âmbito mais amplo dos atuais desafios que a comunidade internacional enfrenta em pleno século XXI (Escravana, Lima, & Ribeiro, 2012).

"O Conceito Estratégico de Defesa Nacional define os aspetos fundamentais da estratégia global a adotar pelo Estado para a consecução dos objetivos da política de segurança e defesa nacional." (MDN, 2013, p.6). Neste sentido, o CEDN realça que no domínio da cibercriminalidade, impõe-se uma avaliação das vulnerabilidades dos sistemas de informação, sistemas de proteção, infraestruturas e serviços vitais neles apoiados. Assim, identifica como prioridades: Garantir a proteção das infraestruturas críticas de informações através da criação de um Sistema de Proteção da Infraestrutura Nacional (SPIN); definir uma Estratégia Nacional de Cibersegurança (que, entretanto, já existe); montar a estrutura responsável por garantir a cibersegurança, nomeadamente através dos órgãos técnicos necessários; sensibilizar os operadores públicos e privados para a natureza crítica da segurança informática e aumentar a capacidade de ciberdefesa nacional (MDN, 2013).

Posto isto, e considerando que o mesmo CEDN define a cibercriminalidade como uma das principais ameaças e riscos, tanto numa esfera de segurança nacional como global (como anteriormente foi referido), a importância que o Estado Português tem vindo a dar ao mundo do ciberespaço é uma realidade inquestionável (MDN, 2013).

A *internet*, embora não represente todo o domínio do ciberespaço, é a principal rede de acesso ao mesmo. Como tal, é na análise do acesso e uso da *internet*, que se pode formar uma ideia de geografia de poder no que diz respeito ao ciberespaço (Martins, 2012).

O acesso à *internet* está, assim, diretamente relacionado não só com os meios financeiros de que cada indivíduo dispõe, mas também pela sua localização geográfica. Os Estados subdesenvolvidos, como é o caso de

alguns países africanos ainda tem um acesso à internet muito limitado e não está acessível a todos os cidadãos.

Se analisarmos o uso da *internet* no mundo conseguimos obter uma perspetiva da geografia do ciberespaço, nomeadamente através do número de utilizadores de *internet* por Continente, por exemplo. E, para uma análise mais detalhada com base neste tipo de dados, pode ser feita uma comparação entre países, ou mesmo dentro de um país, entre várias regiões ou localidades.

Tabela 1 - Estatísticas da população e do seu uso de *internet*

WORLD INTERNET USAGE AND POPULATION STATISTICS MARCH, 2019 - New Update						
World Regions	Population (2019 Est.)	Population % of World	Internet Users 25 Mar 2019	Penetration Rate (% Pop.)	Growth 2000-2019	Internet Users %
Africa	1,320,038,716	17.0 %	474,120,563	35.9 %	10,402 %	10.9 %
Asia	4,241,972,790	54.7 %	2,190,981,318	51.7 %	1,817 %	50.4 %
Europe	866,433,007	11.2 %	718,172,106	82.9 %	583 %	16.5 %
Latin America / Caribbean	658,345,826	8.5 %	438,248,446	66.6 %	2,325 %	10.1 %
Middle East	258,356,867	3.3 %	170,039,990	65.8 %	5,076 %	3.9 %
North America	366,496,802	4.7 %	326,561,853	89.1 %	202 %	7.5 %
Oceania / Australia	41,839,201	0.5 %	28,437,577	68.0 %	273 %	0.7 %
WORLD TOTAL	7,753,483,209	100.0 %	4,346,561,853	56.1 %	1,104 %	100.0 %

Fonte: (*Internet* World Stats, 2019)

Como podemos observar na Tabela 1 o continente com maior número de utilizadores é a Ásia com mais de dois mil cento e noventa milhões de utilizadores mas não é dos países com maior percentagem de uso de *internet*. A região com uma maior densidade de utilizadores de *internet* é a América do norte com oitenta e nove por cento e logo a seguir está a Europa com oitenta e três por cento, e a Ásia com apenas cinquenta e um por cento. Curioso também será analisar que a região onde se verificou um maior crescimento do número de utilizadores no século XXI foi África, com um aumento de dez por cento.

A UE dedica de facto mais atenção à cibersegurança em relação a continentes como a África e Ásia, equipando devidamente a mesma e ajudando os Estados-Membros a protegerem-se a si próprios contra ciberameaças, procurando assegurar e manter simultaneamente, um ciberespaço aberto, livre e seguro. Os Estados-Membros concordaram, na Estratégia da União Europeia para a cibersegurança em 2013, que a UE deveria continuar a reforçar a sua cooperação em todos os domínios identificados como prioritários (apoiar a *governance* global e as Nações Unidas) (EU, 2016).

Para que isso seja possível é necessário um aumento das capacidades tecnológicas destinadas a atenuar ameaças, a par com o aumento da

resistência das infraestruturas, redes e serviços críticos, bem como uma diminuição da cibercriminalidade. Isto significa promover sistemas de tecnologias da informação e da comunicação (TIC) inovadores que garantam a disponibilidade e a integridade dos dados, ao mesmo tempo que se garante a segurança dentro do espaço digital europeu através de políticas adequadas sobre o local de armazenagem dos dados e a certificação dos produtos e serviços digitais. Para tal, é necessário integrar de forma horizontal as questões de cibersegurança em todos os domínios de intervenção, reforçando os elementos da mesma nas missões e operações da Política Comum de Segurança e Defesa (PCSD), e continuar a desenvolver plataformas de cooperação. A UE apoiará a cibercooperação política, operacional e técnica entre Estados-Membros, designadamente no domínio da análise e gestão das consequências, e promoverá avaliações partilhadas entre estruturas da UE e instituições competentes dos Estados-Membros. Além disso, está igualmente previsto reforçar a cooperação em matéria de cibersegurança com parceiros essenciais como os EUA e a NATO. Por outro lado, a resposta da UE assentará igualmente em sólidas parcerias público-privadas. A cooperação e a partilha de informações entre Estados-Membros, instituições, o setor privado e a sociedade civil podem promover uma cultura de cibersegurança comum e aumentar a preparação contra eventuais ciberperturbações e ciberatentados (EU, 2016).

1.4 Objeto de Estudo

Por tudo o que foi referido até agora, é necessário definir e delinear o objeto de estudo para assim garantir-se o seu correto estudo e investigações. Em primeiro lugar, é necessário ter uma base sólida dos assuntos das Relações Internacionais e em específico sobre o Ciberespaço para assim se reduzir e mitigar as hipóteses de ambiguidades e imprecisões para que este trabalho de investigação possa assumir-se como detentor de um caracter científico (Quivy & Campenhout, 2008).

A definição dos objetivos nesta dissertação é bastante importante pelo que é necessário definir limites sobre a análise a realizar, reduzindo assim as ambiguidades no estudo (Quivy & Campenhout, 2008).

Além disso, é necessário ter presente que existem, desde logo, três tipos de limitações a ter em atenção para a elaboração das dissertações: limitação social, limitação temporal e também limitação geográfica (Quivy & Campenhout, 2008).

Começando pela limitação geográfica, não parecem restar dúvidas de que, de facto é complexo e difícil delimitarmos o objeto de estudo "ciberespaço", uma vez que o mesmo não possui uma grandeza física pelo que é necessário fazer-se uma análise geográfica para melhor entendimento. O ciberespaço tem como principal rede de acesso a *internet*. (Nunes, 2015). Quanto mais o ciberespaço cresce e mais pessoas tem acesso a ele, mais ele se torna universal (Lévy, 1999).

Em matéria de limitação social, vamos centrar a nossa análise nas estratégias e políticas "supranacionais" da UE e da NATO e nas mudanças políticas e estratégicas que têm mudado ao longo destes anos (Nunes, 2015). O protagonista é o Estado e será feita uma investigação no plano estratégico nacional e supranacional (UE). (Balão, 2014)

Por último, relativamente à limitação temporal, é fundamental ter a consciência de que estamos na era da tecnologia em que o ciberespaço tem estado a evoluir de forma dramática pelo que esta evolução pode ser, igualmente, um meio "facilitador" para aumentar os ataques e criar a instabilidade nos Estados e em específico na UE (Nunes, 2015). Foi definido a análise do período temporal entre os anos 80 do século passado e o presente por se considerar que é onde houve um maior crescimento do ciberespaço.

Em face destes factos, consideramos particularmente relevante equacionar no âmbito da nossa análise, o papel das parcerias público privadas como eventual "fórmula" capaz de minimizar as ameaças e riscos (Nunes, 2015).

1.5 Panorâmica

Como panorâmica do trabalho e consoante os objetivos que enunciei anteriormente, esta dissertação está dividida em quatro partes principais iniciando-se com uma Introdução/Enquadramento Ontológico onde se encontra a Revisão de Literatura no âmbito da/do qual será igualmente apresentada; o Enquadramento Teórico, seguida da Nota Metodológica, três Capítulos centrais e uma Análise Crítica. Após estas partes principais temos a Conclusão, a Bibliografia e Anexos.

Na Introdução contextualizamos a dissertação. Inicialmente é apresentada a motivação e pertinência do tema escolhido e a sua importância para a instituição militar e como último ponto a panorâmica geral do trabalho. Posteriormente referimos o seu âmbito e o objeto de estudo, demonstrando-se a relevância e atualidade do mesmo no quadro dos desafios que se colocam às Relações Internacionais no tempo presente. O objetivo da dissertação é perceber se as parcerias público privadas podem aumentar o nível de cibersegurança da UE. De seguida apresentamos os resultados da Revisão de Literatura onde abordamos a Guerra de Informação e também nos permite apresentar a operacionalização dos conceitos-chave para que se possa esclarecer, por exemplo, a diferença entre ciberataque, ciberterrorismo ciberguerra e cibercrime. Ainda nesta parte, são exploradas algumas teorias da Relações Internacionais de modo a que possamos justificar as nossas opções em matéria de perspetivas de análise de que nos socorremos no tratamento do objeto de estudo.

Na segunda parte da dissertação incluímos o enquadramento teórico destinado a esclarecer qual o “Estado de Arte” em matéria de temática e objeto de investigação da nossa dissertação, e que sustentará as nossas incursões no respetivo domínio, assim como a nossa análise e conclusão.

Posteriormente ao enquadramento teórico definem-se as opções metodológicas do trabalho a desenvolver segundo os objetivos que apresentamos na primeira parte (introdução). Começamos pela formulação da pergunta de partida e de seguida apresentamos as respetivas hipóteses de

trabalho, a que se segue o esclarecimento quanto ao método adotado (e justificação), técnicas e ferramentas de análise, fontes, Bibliotecas e Centros de documentação visitados no âmbito da instigação, dificuldades e limitações do estudo.

Posteriormente, surge a terceira parte constituída por três capítulos sendo que estes constituem o foco central da presente dissertação, pelo que será nestes três capítulos que se procura apresentar toda a informação reunida ao longo do trabalho de investigação de modo a que seja possível responder às hipóteses de trabalho que formulámos e com isso alcançar os objetivos definidos na introdução.

No primeiro capítulo, de maior amplitude em matéria de quadro analítico a considerar, procura-se analisar as políticas e estratégias da UE e NATO para o ciberespaço, e respetiva articulação. Procuraremos, também, concluir qual das duas Organizações primeiro reconheceu o ciberespaço como uma ameaça, quais as medidas que foram sendo adotadas e quais os acontecimentos que suscitaram em cada um dos casos um "novo" olhar sobre esta realidade. Com esta análise comparativa procuraremos discutir a existência (ou não) de uma relação "top-down" entre estas organizações em matéria de definição de Políticas e estratégias no âmbito do ciberespaço.

No segundo capítulo apresentamos um breve apontamento histórico-evolutivo e comparativo das políticas e estratégias da UE no ciberespaço onde se procurará identificar e discutir as principais mudanças no domínio da estratégia de segurança no ciberespaço de 2013 quando, pela primeira vez, a ciberameaça foi identificada pela UE como fator fundamental que pode por em causa a segurança europeia, arma política, económica e militar, passando por outros documentos mais recentes até aos dias de hoje. Por último, apresentar a estratégia que está atualmente em vigor na União Europeia e qual é o seu objetivo bem como abordar as organizações pertencentes à UE cuja missão está diretamente relacionada com o cumprimento dessa estratégia.

No terceiro capítulo discute-se a importância das parcerias público-privadas (PPPs) no âmbito do ciberespaço, assumindo-se que este parece ser

o rumo a tomar neste âmbito para que se possa assistir a uma diminuição significativa dos ciberataques e do cibercrime que é decorrente dos anteriores. Neste contexto, procuramos identificar os diferentes tipos de PPPs que existem atualmente e como é que a Europa reagiu à sua inclusão no domínio da Estratégia de Cibersegurança.

Finalmente, chegamos à análise crítica onde discutimos alguns dos principais factos apurados ao longo da nossa investigação com o objetivo de "preparar o caminho" para as conclusões e considerações finais do trabalho de investigação, demostrando os desafios que as PPPs enfrentam bem como algumas recomendações futuras para melhorem a sua efetividade.

Por fim, as conclusões a que for possível chegar nesta dissertação poderão não ter um caráter totalmente inovador, apesar de academicamente válidas, e procurarão constituir um contributo para o avanço do conhecimento científico no âmbito da segurança do e no ciberespaço. Aqui procuramos, também, dar respostas à pergunta de partida inicialmente proposta e demonstrar a validade e pertinência das hipóteses de trabalho formuladas.

1.6 Revisão da Literatura

Este ponto do trabalho tem como objetivo identificar, no âmbito da temática em que se situa o objeto de investigação e a problemática em análise, os principais contributos científicos e académicos existentes e publicados em artigos científicos, obras de referência, Teses de Doutoramento e de Mestrado. Após analisarmos os contributos científicos e académicos já existentes ficará mais fácil a compreensão da temática ao longo da dissertação.

Hoje em dia a arte de fazer a guerra tem mudado. Aquilo a que chamos vulgarmente “Guerra” passou por três gerações muito diferentes uma das outras e atualmente está-se a iniciar uma nova geração.

A Primeira Geração de Guerra foi desenvolvida no século XVII onde existiam pequenos exércitos profissionais que procuraram, através do treino, maximizar o poder de fogo (Lewicki & Bunker, 1996).

Na geração seguinte começou a haver mudança do típico soldado no campo de batalha e começou a existir a artilharia pesada, e o fogo indireto tomou conta desses mesmos campos de batalha (Lewicki & Bunker, 1996).

A Terceira Geração de Guerra baseava-se fundamentalmente em conceções tecnológicas como o surgimento da eletricidade e rádio. Um exemplo deste tipo de Guerra pode ser ilustrado através das táticas alemãs, desenvolvidas na Grande Guerra (Lewicki & Bunker, 1996).

A “Guerra de última Geração” é, também, designada como Guerra de Quarta Geração, possuindo algumas caraterísticas semelhantes às que caracterizavam a fase anterior, como a iniciativa e a descentralização. Mas inclui novidades como a digitalização, a ciberguerra, e a robotização, além de ter deixado de opor apenas forças militares especializadas, e por norma os civis tendem a ser as vítimas (Curtis, 2005).

O conceito de Quarta Geração com que hoje em dia nos deparamos surgiu no século passado, em meados dos anos 80 (Lind, 2004). Após longos anos ser abordado este tipo de guerra, voltou à discussão com os ataques

terroristas, nomeadamente do 11 de Setembro de 2001, voltou a ser abordada como sendo uma guerra cada vez menos entre Estados (como foi o caso das Primeira e Segunda Guerras Mundiais) mas, sim uma guerra de organizações terroristas como, por exemplo, a Al-Qaeda e DAESH. Este tipo de guerra é o culminar das gerações passadas (Lind, 2004).

Todos os estudos de guerras que estão presentes nesta dissertação têm as caraterísticas de uma Guerra de Quarta Geração.

Tem sido cada vez dado mais importância ao mundo do ciberespaço e diversos autores têm vindo a estudar de forma intensa esta temática em diversos domínios quer num cenário internacional ou nacional.

Ainda no século passado, Kitchin publicou um livro que remete as sucessivas mudanças sociais verificadas àquela data e também a importância deste mundo digital na economia dos países. Kitchin debateu também de forma exaustiva o facto das novas tecnologias estarem a mudar a vida do Ser Humano (Kitchin, 1998).

Em 2002 Leonard Shyles estuda o ciberespaço em três componentes: tecnologia, mercado financeiro e política. Nesse estudo chega a conclusão que o ciberespaço tem mudado a vida social das pessoas (Shyles, 2002).

Mais recentemente, em 2013, Healey escreveu um livro acerca dos conflitos que se foram registando ao longo da história no domínio do ciberespaço e concluiu que o ciberespaço é usado para atingir-se a superioridade entre nações (Healey, 2013).

Para se compreender melhor a superioridade do ciberespaço, Bryant estudou e analisou diversos conflitos que aconteceu no passado e escreveu uma obra intitulada "*International Conflict and Cyberspace Superiority: Theory and practice*?" onde demonstra, no domínio dos conflitos internacionais, a importância do ciberespaço nas operações militares (Bryant, 2016).

A ENISA tem vindo a trabalhar em formas de combater os conflitos que advém do ciberespaço na UE e uma das formas seria através de parcerias público privadas que ajudariam os Estados-Membros na criação de estratégias e políticas bem como na sua implementação (ENISA, 2017).

1.6.1 Conceptualização operacional

A conceptualização operacional tem como objetivo mitigar algumas dúvidas que possam existir sobre os conceitos-chave desta dissertação e deste modo poder clarificar os mesmos bem como a respetiva articulação, ao mesmo tempo que proporciona um melhor entendimento sobre os objetivos e os fins da investigação.

Guerra de Informação

A Guerra de Informação é um conceito recente que tem evoluído ao longo do Século XXI e é um conceito fundamental para as organizações que pretendem defender de forma eficaz o setor privado e público (Molander, Riddile, & Wilson, 1996).

A Guerra de Informação apesar do seu conceito ser abrangente está muitas vezes relacionada com a segurança da informação (Dinis, 2009).

Stein refere que a definição de Guerra de Informação tem vindo a ser bastante debatida, mas está longe de ser possível chegar a uma definição única e precisa, porque para além de ser um conceito recente tem sofrido abordagens bastante diferentes por partes de diversos autores (Stein, 1995). A Guerra de Informação é, assim e ainda, um termo bastante genérico que se baseia no princípio do uso da informação de forma a ganhar vantagem, de diversas forma, sobre o inimigo (Koop, 2009).

A Guerra de Informação não abrange apenas o mundo virtual. Ela está também inserida no espaço físico onde se desenrolam as ações ofensivas e defensivas para os intervenientes das mesmas alcançarem os objetivos propostos (Hewitt, 2009).

O grande objetivo da Guerra de Informação é tentar influenciar quem está no poder. Assim, no âmbito militar, os principais alvos são aqueles que têm nas “mãos” a decisão sobre o emprego dos meios e das capacidades definidos no respetivo plano estratégico (Stein, 1995).

Hoje em dia vivemos numa “Era” rodeada de tecnologia e informação onde as TIC têm um papel fundamental no que toca ao conflito e em última instância à guerra (Waltz, 1998), sendo que um dos grandes responsáveis por esta “Era” em que vivemos é a globalização (Held & McGrew, 2001).

A Guerra de Informação tem diversos elementos como demonstra a figura seguinte

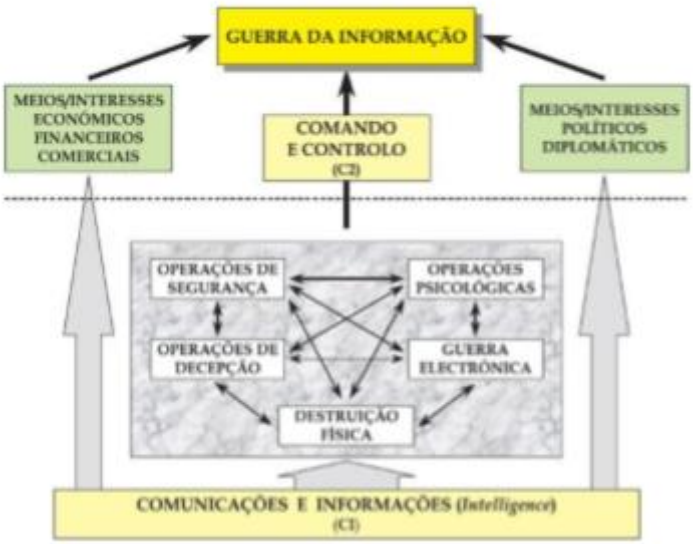

Figura 2 - Como se atinge a Guerra de Informação

Fonte: (Dinis 2009)

Este tipo de Guerra pode ocorrer em qualquer altura, independentemente das características do momento (quer esteja em tempo de guerra ou não) que o país atravessa. A nação que sofre um ataque desta natureza por vezes nem se apercebe que está a ser alvo dessa investida hostil.

Ciberataque

Ciberataque é um ataque de computador para computador que compromete a confidencialidade, integridade ou disponibilidade de uma informação do computador que sofre esse ataque (Carvalho & Silva, 2003).

Não existe um pré-aviso de um ciberataque. O mundo atual não tem meios nem capacidade para ser defender contra um ciberataque devido ao seu efeito surpresa e esse facto faz aumentar a eficácia das armas cibernéticas (Rustici, 2011).

Robert Wendell Lucky referiu que, independentemente do valor dos dados que uma pessoa tenha no seu computador ou dispositivo eletrónico, não existe nenhuma maneira de fornecer a esses dados uma segurança total contra um *hacker* experiente em ciberataques. Resumindo, os ciberataques não são apenas impossíveis de bloquear, mas também são usualmente difíceis de detetar e é possível nem saber que se está a ser alvo de um ciberataque (Lucky, 1996).

Uma ciberameaça ou um ciberataque é um ato mal-intencionado que visa danificar ou roubar dados ou, ainda, interromper a vida digital em geral. Os ciberataques incluem ameaças como vírus de computador, violações de dados e ataques de *Denial of Dervice* (DoS) (Taylor, 2018).

Um ciberataque é considerado, ainda, um ataque que é executado contra as pessoas (ou seja, os dispositivos digitais das mesmas) por meio do ciberespaço. O ciberespaço é por sua vez, um espaço virtual que não existe, tornou-se a metáfora para nos ajudar a entender o armamento digital que pretende prejudicar o mundo digital (Taylor, 2018).

O que é real, no entanto, é a intenção do *hacker* (pessoa que leva a cabo o ciberataque), bem como o impacto potencial. Embora muitos ciberataques sejam apenas incómodos, alguns são bastante perigosos, e podem até mesmo pôr vidas humanas em risco (Taylor, 2018).

Um ciberataque, para se ter noção da sua dimensão, pode causar prejuízos de biliões de euros e caso seja efetivado pode não deixar qualquer pista física. Por isso, espera-se que a criação de políticas de segurança neste âmbito possa contribuir para aumentar o nível de segurança das organizações na medida em que quanto maiores forem as vulnerabilidades dos sistemas informáticos das organizações, maiores riscos correrão as mesmas (Levy´s, 1994).

Havendo uma lacuna no sistema, se a mesma for explorada por alguém, a entidade suscetível de sofrer o ciberataque nunca estará segura e os ataques só serão devidamente inutilizados quando essa falha no sistema for reparada (Libicki, 2009).

Neste domínio podem identificar-se, quanto à sua natureza, quatro tipologias de ataques:

- Ataque ativo – suscetível de alterar um sistema afetando a sua operação normal (ITU, 2012).
- Ataque passivo – não tem como objetivo destruir, nem inutilizar informação, apenas retirar a mesma do sistema (ITU, 2012). Como exemplo podemos considerar o caso do *hacker* Rui Pinto quando efetuou um ciberataque às instalações do *Football Leaks* retirando de lá informação mas sem a destruir (Roseiro, 2018).
- Ataques do interior – como o próprio nome indica são ataques feitos por alguém com acesso direto e legítimo à informação-alvo, dificultando a perceção de que esse mesmo ataque está a ocorrer (ITU, 2012).
- Ataques do exterior – levados a cabo por pessoas sem acesso autorizado ao sistema, normalmente é *hackers*, terroristas, entre outros (ITU, 2012).

Existem, também, diversos tipos de ciberataques e de alterações de sistemas informáticos:

- ✓ *Backdoor* – Os "*Backdoor´s*" aparecem quando o utilizador compra um sistema que no seu interior tem um mecanismo para no futuro poder dele retirar a informação sem que seja detetado pelos sistemas de segurança (Haeni, 1997).
- ✓ Cavalo de Tróia – Um tipo de vírus com caraterísticas muito específicas, que se baseia num código que "entra" num programa e deixa o utilizador (*hacker*) que leva a cabo o ciberataque com possibilidade de programar o "cavalo de tróia" para,

posteriormente, analisar as debilidades ao nível da segurança do sistema, enviando para si próprio essas informações sem o danificar nem deixar vestígios de que tal informação foi retirada (Haeni, 1997).

- ✓ *Denial of Service* (DoS) – Quando ocorre este incidente o seu utilizador fica privado dos seus Sistemas de Informação e Comunicações (SIC) (RFA 390-6, 2011);
- ✓ *Distributed Denial of Service* (DDoS) – Incidente em que vários sistemas se juntam para levar a cabo um cibertataque causando um DoS como, por exemplo, fazer *spam*, enviando inúmeras mensagens para um determinado correio eletrónico dos Sistemas de Informação e Comunicações o que pode fazer com que esse sistema, devido a dificuldade de processamento, se desligue (RFA 390-6, 2011);
- ✓ *Spam* – É uma técnica usada para sobrecarregar um sistema, por exemplo, uma caixa de correio eletrónico através do envio de inúmeras mensagens para um destinatário que pode provocar um incidente (DoS) em que o utilizador ou a organização fica privado dos uso dos seus SIC (RFA 390-6, 2011);
- ✓ *Web Defacement* – Cibertaque bastante comum, que consiste em alterar a *webpage* para que o utilizador não tenha a capacidade de perceber a informação porque a mesma se encontra modificada, o que leva a falsas conclusões por parte do utilizador da mesma (Haeni, 1997);
- ✓ *Worms* – Programa com capacidades especiais, que através das redes se consegue replicar de computador em computador, sendo que a grande diferença dos *worms* para os vírus é que não destroem a informação – causam apenas falhas de comunicação (Haeni, 1997);
- ✓ Vírus – São normalmente associados a computadores ou telemóveis, sendo usados como instrumento de Guerra de

> Informação. O vírus é inserido num programa e quando esse programa é iniciado espalha-se aos restantes programas e pode fazer com que o aparelho eletrónico se desligue ou fique com defeitos no sistema (Haeni, 1997).

Quando falamos de ataques neste capítulo do ciberespaço ocorrem-nos de imediato os acontecimentos do século passado na Guerra dos Balcãs no Kosovo, os de 2007 na Estónia ou da Geórgia em 2008.

Em 1999, no fim da Guerra dos Balcãs, no Kosovo, encontrava-se em conflito a antiga Jugoslávia, a NATO, as forças sérvias e ainda a Albânia. Nessa guerra houve um ataque por parte da Rússia, que através de hackers, afetando os sistemas da NATO através de DDoS modificando as suas páginas de *internet* (AC, 2012).

Mais recentemente, em 2007, a houve um ataque à Estónia. *Hackers,* alegadamente russos, fizeram inúmeros ciberataques às redes cibernéticas àquele pequeno país do norte da Europa que impossibilitaram o seu bom funcionamento (Libicki, 2009). Tal como aconteceu oito anos antes no Kosovo, através de DDoS, atacaram os *websites*. Sendo a Estónia um país em que a maioria das suas transações comerciais são feitas através do ciberespaço consegue-se perceber o impacto que este ciberataque que terá causado. Devido ao grande *spam* que foi efetuado nesse ciberataque, a incapacidade de processamento dos sistemas atacados foi de tal maneira grande que os websites dos governos e até de bancos ficaram impossibilitados de efetuar transferências ou compras online - estima-se que 98% das transferências bancárias à data eram feitas *online*. Devido a estes ciberataques muitos serviços ficaram indisponíveis por mais de duas semanas (NATO, 2008).

Cibercrime

O cibercrime é uma das palavras mais utilizadas pelos indivíduos na sociedade contemporânea. Para entender o seu verdadeiro significado, é

preciso assimilar e entender o correspondente significado do termo “Cyber” e “Crime”. O termo “Cyber” é um prefixo usado para descrever um ambiente de virtual. Cibercrimes são definidos como: ofensas que são cometidas contra indivíduos ou grupos de indivíduos com motivos criminais para intencionalmente prejudicar a reputação da vítima ou causar danos físicos ou mentais prejudicando a vítima direta ou indiretamente, e utilizando redes de telecomunicações como a *internet* (salas de chat, e-mails, telemóveis) (Hassan, Lass, & Makinde, 2012).

O cibercrime pode, simplesmente, ser explicado como tratando-se de um tipo de crime levado a cabo com o auxílio/recurso a um sistema informático, constituindo um problema mundial que custa milhões aos países. Por exemplo, na Nigéria, os cibercrimes são executados por pessoas de todas as idades, de jovens a velhos, mas na sua maioria por jovens, muitos deles ainda menores de idade (Hassan, Lass, & Makinde, 2012).

Existem, também, vários tipos de cibercrimes, sendo um dos mais conhecidos o ciberterrorismo, sobre o qual nos debruçamos a seguir.

Ciberterrorismo

Um ciberterrorista pode ser descrito como alguém que lança um ciberataque a um governo ou organização com o objetivo ou propósito de distorcer e/ou aceder a informação armazenada num computador e/ou nas suas redes e, deste modo, intimidar os atores-alvo desses ataques.

Parker (1983) definiu ciberterrorismo como um ato terrorista cometido através do uso do ciberespaço ou outros recursos de computador. Significa que qualquer ato destinado a instalar medo ou aceder e distorcer quaisquer informações em organizações ou órgãos governamentais usando computadores e a internet é geralmente referido como ciberterrorismo. Outra forma de ciberterrorismo é a ciberextorsão – um conjunto de ações como roubo de dados de *websites*, e-mails e sistemas de computadores, levadas a cabo por um *hacker*. Os *hackers* estão cada vez mais a atacar *websites* e redes

corporativas, prejudicando a sua capacidade para operar (Hassan, Lass, & Makinde, 2012).

O ciberterrorismo é um termo que surge a partir da conjugação entre os objetivos do terrorismo e a utilização do ciberespaço para a sua concretização, pelo que pressupõe, normalmente, o recurso a computadores associado ao uso ilegal e ou indevido das tecnologias de informação (Mark, 1997).

Ciberdefesa

Ciberdefesa é também um conceito difícil de explicar. Ciber, abreviatura de ciberespaço, refere-se à infraestrutura da rede (computadores, *hubs*, *switches* e *firewalls*) e aos ativos de informação (dados críticos dos quais uma organização depende para cumprir sua missão). Defesa, por sua vez, é o ato de tornar algo seguro de modo a que, por exemplo, não seja danificado em caso de ataque. Portanto, a ciberdefesa refere-se a um processo ativo de proteção do ciberespaço, definido ao nível da política nacional, levado a cabo de forma confiável, com o objetivo de tornar um sistema seguro face a eventuais ataques e recorrendo, sobretudo, aos meios militares disponíveis.

Em Portugal, existe um sistema de Proteção da Infraestrutura Nacional (SPIN) que define as linhas de ação prioritárias de modo a garantir a proteção das infraestruturas de informação crítica e, desse modo, assegurar o sucesso no combate à cibercriminalidade (MDN, 2013).

A ciberdefesa, de um modo simplificado, consiste então na capacidade de um país, por exemplo através de ações militares, proteger contra inimigos que executam ciberataques, os seus sistemas de informação e as respetivas infraestruturas críticas. A ciberdefesa envolve o rastreio, deteção e interceção de ataques destrutivos. É considerado ciberdefesa o recurso a sistemas e metodologias cujo objetivo é evitar ou minimizar os efeitos de um ciberataque. Por exemplo, nos nossos computadores usamos um antivírus de forma a minimizar esses ataques, e por isso a utilização de um antivírus é considerado o nível mais básico de ciberdefesa (Coleman, 2008). Por outras palavras, os sistemas existentes e as atividades prosseguidas por cada Estado, no âmbito

da sua esfera nacional, com recurso a meios de natureza militar com o objetivo de garantir a segurança da sua informação e das infraestruturas críticas refere-se à esfera de segurança do ciberespaço que é usualmente denominada ciberdefesa (Hayes, 2012).

Cibersegurança

A cibersegurança refere-se à proteção e defesa dos interesses gerais da população no âmbito do ciberespaço, sendo relevante destacar que neste domínio um qualquer erro, de qualquer indivíduo, é suscetível de comprometer a segurança de todas as pessoas e instituições que a ele estão ligados, quer a nível pessoal quer a nível profissional (US DHS, 2016).

Ela abarca toda a área que envolve as Tecnologias de Informação, nomeadamente sistemas e atividades que são fundamentais para a segurança, tanto da informação como da infraestrutura física do ciberespaço (Hayes, 2012).

Quando se fala em medidas de cibersegurança referimo-nos a todas as que são adotadas na esfera política, jurídica, económica e, também, da educação para a sensibilização da população relativamente aos perigos do ciberespaço para que as mesmas tomem medidas preventivas e assumam comportamentos cautelosos, de modo a contribuir para que o ciberespaço possa ser um local mais seguro, tanto para as interações sociais como económicas ou outras, que naquele âmbito tenham lugar (GH, 2013).

Ciberdefesa versus cibersegurança

A ciberdefesa e a cibersegurança podem parecer conceitos bastante semelhantes porque se encontram relacionados em alguns aspetos, mas existem algumas diferenças que importa assinalar.

A cibersegurança entra no domínio do ciberespaço internacional, nacional e governamental (assumindo relevância numa perspetiva multinível, portanto), enquanto a ciberdefesa foca, exclusivamente, aspetos relativos ao

ciberespaço de domínio militar, mas não se envolve diretamente em aspetos da esfera internacional ou externa ao Estado. Apesar disto, as ciberameaças e ciberataques provenientes do ambiente externo às fronteiras do Estado nacional poderão, ainda assim, necessitar de intervenção tanto da ciberdefesa como da cibersegurança, pelo que o treino e exercício por parte dos países da UE são iguais para ambas(Hayes, 2012). A cibersegurança, sendo um aspeto mais macro, necessita e recorre às capacidades da ciberdefesa. As ferramentas usadas para a proteção da informação, quer no que se refere aos sistemas, quer às infraestruturas, podem ser utilizadas em ambas (Hayes, 2012).

Ciberguerra

A definição de ciberguerra é, à semelhança das anteriores, igualmente complexa. O *Department of Defence* (DoD) dos EUA define ciberespaço como o espaço em que a informação digitalizada é comunicada através de redes de computadores. Quando se ouve falar deste termo associa-se à cibersegurança, redes de computadores operacionais, guerra eletrónica, entre outros (Andress & Winterfeld, 2014). Obviamente, pode-se perceber intuitivamente que a ciberguerra é uma guerra no ciberespaço. No entanto, é necessário ter em conta que a conceção atual do ciberespaço está a mudar a um ritmo elevado (Carvalho & Silva, 2003).

Hoje em dia não existe apenas a guerra tradicional e apareceu esta "nova" guerra, a ciberguerra, porque o termo "guerra" tomou outros significados e passou a poder-se praticar através do ciberespaço (Carvalho & Silva, 2003).

São os *hackers* que têm o principal protagonismo nos ciberataques e esses ataques se evolverem unidades organizadas segundo um Estado, usando meios eletrónicos, como por exemplo computadores, damos o nome de ciberguerra. O grande objetivo da ciberguerra é conseguir derrotar o nosso inimigo comprometendo a viabilidade e confidencialidade dos seus Sistemas de Informações e Comunicações (SIC). O número de notícias sobre ataques a

organizações de cada vez maior dimensão e complexidade parece apresentar-se como uma tendência crescente (Billo & Chang, 2004).

A ciberguerra carateriza-se por uma operação militar onde se tentando retirar ou danificar a informação do inimigo. Algumas das caraterísticas das ciberguerras são as seguintes (Parks & Duggan, 2001):

- A ciberguerra tem um efeito significativo na vida real, pois tem a capacidade de destruir sistemas de armas;
- É necessária uma constante vigilância e um grande nível de segurança porque, mesmo no ciberespaço, as informações ali armazenadas podem ser detetadas através da ciberguerra pelo que é crucial recorrer aos melhores e mais avançados/eficientes métodos suscetíveis de garantir o maior nível de eficácia em matéria de segurança;
- O ciberespaço é repleto de situações inesperadas: ao contrário do mundo físico cujas condições permitem um nível de previsibilidade razoavelmente elevado, no ciberespaço não sabemos quando é que, por exemplo, o nosso *software* pode falhar;
- Qualquer utilizador do ciberespaço pode planear e executar um ciberataque e por sua vez iniciar uma ciberguerra, ou seja, milhares de milhões de pessoas têm esse poder;
- Os instrumentos utilizados na ciberguerra tanto podem ser usados de forma ofensiva como defensiva;
- Na ciberguerra, a partir do momento em que dominamos o espaço virtual do adversário, podemos controlar o inimigo;
- Na segunda guerra mundial quando as bombas atómicas foram lançadas, foi necessário sobrevoar o Japão para se proceder ao e concretizar o ataque. No ciberespaço os limites físicos não se aplicam, logo podemos iniciar uma ciberguerra do lado oposto do mundo executando um ciberataque eficaz.

A ciberguerra divide-se, por sua vez, em vários tipos, como ciberguerra ofensiva, a defensiva, a estratégica, a de preempção e *intelligence.*

A ciberguerra ofensiva, como o próprio nome indica, está destinada à produção de armas cibernéticas para executar ciberataques. A designação 'armas cibernéticas' constitui mais um conceito recente e refere-se a ferramentas que conseguem destruir, inutilizar ou apenas alterar sistemas e redes de computadores, para além de terem a capacidade de criar danos nos dispositivos eletrónicos. A construção destas armas, por sua vez, tem dois objetivos claros: criar instrumentos que servem para efetuar testes de segurança dos sistemas (já existem organizações que constroem armas cibernéticas com o propósito de as testar contra as suas próprias redes e sistemas de computadores) e/ou como armas para ataques efetivos (Coleman, 2008).

A ciberguerra defensiva refere-se à capacidade de um Estado, através de políticas e estratégias no âmbito do ciberespaço, conseguir proteger e salvaguardar quer as informações quer as suas infraestruturas críticas dos inimigos por exemplo, através de ações militares. Essa capacidade de defesa consiste num sistema que tem que incluir a capacidade de deteção de um ciberataque, um mecanismo para o seu rastreamento assim como a capacidade de intersectar os ciberataques contra as infraestruturas da nação. Perante a ciberameaça tem que existir a capacidade de uma nação minimizar, através dos meios disponíveis, os efeitos colaterais das mesmas (Coleman, 2008).

A ciberguerra de preempção está associada às medidas que um Estado define para reduzir o nível da ciberameaça e, em certos casos, impedir que o ciberataque tenha lugar. A Nação delineia medidas preventivas antes sequer de ocorrer um ataque, porque o grande objetivo é preservar o ciberespaço nacional por antecipação (Coleman, 2008).

A ciberguerra de *intelligence* pressupõe o recurso a mecanismos que permitam a infiltração no ciberespaço do inimigo com o objetivo de recolher informação e dados sobre possíveis ciberataques planeados para que os

mesmos possam ser objeto de análise tendo em vista a posterior definição e implementação de medidas proactivas que permitam impedir ou minimizar os efeitos dos possíveis ciberataques. No entanto, as redes e sistemas de computadores dão poucas garantias contra esta nova capacidade, denominada de *cyberintelligence* (Coleman, 2008).

A estratégia de ciberguerra é independente de cada Estado. Cada um define a sua própria estratégia, ou seja, o Estado tem que definir quais são as medidas que melhor se adequam para responder às ciberameaças com que, eventualmente, possa vir a ser confrontado para, dessa forma, conseguir controlar e proteger as redes e sistemas de computadores na sua Nação. Um dos aspetos mais importantes na estratégia de ciberguerra é estar sempre a par das novas ciberarmas e acompanhar a evolução deste mundo de forma exímia. Outro fator crucial ao qual é necessário que o Estado esteja atento é à banalização das armas que executam os ciberataques, pois quanto mais fácil for o acesso às mesmas mais os pequenos grupos irão fazer uso delas. Aliado a estes factos, e somando o uso cada vez maior da *internet* por parte da população mundial, faz cada vez mais sentido considerar que a criação de uma ciberdefesa cada vez mais avançada para combater a capacidade ofensiva dos inimigos tende a apresentar-se como fundamental para o sucesso dos Estados (Coleman, 2008).

Como já foi referido anteriormente, uma das grandes vantagens das ciberarmas que executam os ciberataques é o facto de poderem ser usadas através de uma plataforma que se encontra disponível praticamente em qualquer lugar do mundo. Para se conseguir titular o ataque, as equipas de investigação que se dedicam aos ciberataques, procuram identificar não apenas a partir de que plataforma física foi lançado o ataque mas, sobretudo, quem o executou. Essas equipas de investigação procuram aquilo que é usualmente denominado ‘ADN Digital’. Como os ataques deixam sempre alguns rastos, através dos mesmos pode ser possível identificar-se novas estratégias, técnicas e ferramentas que, ao serem descobertas, são cruciais para o desenvolvimento de medidas de pré-ataque (Coleman, 2008).

Ciberameaças

As ciberameaças como o próprio nome indica constituem uma ameaça, ainda não concretizada, à segurança de um Estado e pode ter várias caraterísticas e formas:

- Ameaças acidentais – Não têm qualquer propósito de danificar ou desligar um sistema e resultam, apenas, de falhas do mesmo (ITU, 2012);
- Ameaças intencionais – Quando se observa, através da monotorização das redes e sistemas de computadores, a existência de ameaças intencionais que possibilitam a efetiva concretização de um ciberataque (ITU, 2012).

Quando somos confrontados com ameaças intencionais podemos identificar dois tipos de ameaças em relação à sua natureza:

- Ameaças ativas – Verifica-se a tentativa de adulteração dos dados ou até mesmo a tentativa de danificar a plataforma, ou seja, há uma intenção de alterar o estado natural do sistema (ITU, 2012);
- Ameaças passivas – Este tipo de ameaças ocorrem quando, intencionalmente, se vai ao sistema do inimigo roubar informação de caráter privado sem danificar a plataforma inimiga. Quando se consegue obter essa informação esta ameaça passa a ser considerada um ciberataque (ITU, 2012).

Quando se trata de ciberameaças há que equacionar, também, os respetivos atores e fontes. Assim, os atores das ciberameaças são todos aqueles que efetivamente levam a cabo um ciberataque procurando destruir sistemas ou recolher informações dos inimigos. Já as fontes de ameaças são aquelas organizações que tentam e desejam realizar ciberataques como é o caso dos *hackers*, organizações extremistas, jornalistas de investigação,

grupos de crime organizados, serviços de inteligência estrangeiros, entre outros (ITU, 2012).

Política de segurança

A política de segurança dos Estados-Membros da União Europeia é definida tendo em conta os interesses do próprio Estado, interesses esses que dependem da sua posição e poder perante as outras nações. Consoante as suas limitações são definidos os objetivos necessários a garantir uma atuação eficaz contra qualquer ataque que tente retirar informação ou danificar os seus sistemas (Waltz, 1998).

Waltz apresenta três elementos fundamentais a ter em consideração e salvaguardar para, no âmbito da Guerra de Informação, qualquer Estado garantir um elevado nível de segurança no domínio do ciberespaço (Waltz, 1998):

- Interesse Nacional – Todas as infraestruturas nacionais, quer sejam militares ou civis, e que têm informações privadas que possam ser suscetíveis de sofrerem um ciberataque;
- Vulnerabilidades – À medida que o tempo passa, se o Estado não acompanhar a evolução das ciberarmas, a ciberdefesa deixa de ter efetividade e a Nação fica vulnerável aos ataques que, no domínio do ciberespaço, não necessitam de ser praticados dentro das suas fronteiras;
- Objetivo da Segurança – É fundamental o Estado, consoante o tipo de informações que tem em seu poder, definir níveis de segurança para as mesmas e classificá-las consoante a sua importância.

Estratégia de segurança

A estratégia de segurança nacional é transversal a qualquer país e é a forma como o Estado cumpre e assegura os seus objetivos, delineados na sua Política de Segurança. Ela envolve a articulação da economia e da política do Estado em conjunto com as suas Forças Armadas, que desempenham um papel fundamental na concretização de muitos dos objetivos do Estado, desde logo porque qualquer que seja a estratégia que o Estado defina, ela tem que ser compatível com as possibilidades das suas Forças Armadas e tem que ter as seguintes caraterísticas (Waltz, 1998):

- Analisar quais são as infraestruturas críticas, ou seja, aquelas que são mais suscetíveis de sofrer um ataque;
- Conforme a política de segurança nacional propor objetivos estratégicos e definir quais os sistemas que têm uma maior importância;
- Caso não seja possível defender um eventual ataque ter um plano secundário;
- Esses planos secundários devem ser equacionados consoante os seus custos/benefícios e perigos;
- A estratégia do Estado tem que ter em conta os seus riscos e possíveis consequências que daí advêm;
- A estratégia do Estado tem que ter em conta as organizações que estão envolvidas no projeto, bem como as missões e objetivos das mesmas;
- É necessário um constante acompanhamento da estratégia de forma a avaliá-la para que seja sempre o mais atual (e adequada) possível.

Segundo Waltz (1998) existem diferentes componentes de um plano estratégico:

- Determinar claramente as missões. Sabendo que existem missões de dois tipos (militares e não militares) é fundamental definir as fronteiras entre ambas;

- Analisar os contratos bilaterais que o Estado tem com outros países e, desse modo, analisar bem todos as políticas de segurança em que ele se insere - quer sejam elas de caráter nacional ou internacional;
- Definir a “meta” do Estado com exatidão, delineando claramente os objetivos;
- Todas as organizações que estiverem envolvidas no plano estratégico têm que saber com exatidão os seus direitos e deveres;
- Tem que existir um plano que analise a performance da estratégia adotada.

O mesmo autor (Waltz, 1998) também identifica elementos que devem ser incluídos no plano estratégico como por exemplo:

- ✓ Perigos que enfrenta a Nação;
- ✓ Qual a força da Guerra de Informação naquele país;
- ✓ Estratégias das suas organizações;
- ✓ Estratégias operacionais;
- ✓ Estratégias no âmbito das TIC;
- ✓ Processo de prevenção através de um plano que avalie os riscos.

Enquadramento Teórico

Nas dissertações de RI, o objeto de estudo é associado a uma teoria das Relações Internacionais. Independente da área de interesse que escolhemos para realizar a dissertação, quer seja o liberalismo, o regionalismo, segurança, identidade ou política externa, a teoria ajuda-nos a explicar o mundo das Relações Internacionais (Dunne, Kurki, & Smith, 2010).

Para o Professor Adriano Moreira, a melhor definição de Relações Internacionais é “o conjunto de relações entre entidades que não reconhecem um poder político superior, ainda que não sejam estaduais, somando-se as relações diretas entre entidades formalmente dependentes de poderes políticos autónomos” (Moreira, 2014, p.54). Este conceito operacional desenvolvido por Adriano Moreira considera também as organizações internacionais que ajudam na cooperação entre Estados bem como outros agentes de RI,

O estudo das RI é evendenciado no estudo das causas de guerra bem como nas condições para a paz. Esse estudo é era particulamente importantes no século passado, com o acontecimentos das duas guerras mundiais, porém, hoje em dia, existe outras questões, como: “Qual o papel que as instituições internacionais podem desempenhar na alteração de preferências de poderosos atores internacionais?; Como é que as relações globais de poder podem ser identificadas?; Onde e com quem é que o pode reside na política mundial?; Quais são os limites e as possibilidades de progresso na resolução de problemas mundiais urgentes, desde a pobreza e a crise financeira, até ao terrorismo e às alterações climáticas?” (Dunne, Kurki, & Smith, 2010).

No período pós-Guerra Fria testemunhou a realização de que os critérios para alcançar o poder efetivo eram algo além de armas sofisticadas e grandes projeções militares, que requeriam uma fundação segura através de eficiência económica e avanço tecnológico. Isto levou a um debate interessante entre realistas e liberais, cada um a defender os seus argumentos como mais válidos e relevantes para as tendências globais predominantes (Rana, 2015).

Quando analisamos as relações internacionais têm que ser com sutentação em alguma teoria, sendo que a escolha dessa teoria reside se

estamos cientes das suposições que trazemos para o estudo. (Dunne, Kurki, Smith, 2010) .

Destacando o aumento da importância das Organizações Internacionais, a teoria da Interdependência Complexa, desenvolvida por Robert O. Keohane e Joseph S. Nye (1977), antecipou o que é hoje conhecido como globalização. Keohane and Nye destacaram a economia como a área que mais alterações teve com as Relações Internacionais e o mundi tornou-se mais interdependente especialmente nessa área. Esta teoria não rejeitou o realismo mas levantou a preocupação que por vezes, as suposições e explicações dos realistas não eram suficientes e tornou-se uma componente fundamental da perspetiva neoliberal (Rana, 2015) .

Em primeiro lugar, o neoliberalismo é uma variante da teoria liberal das RI que se foca no papel das instituições internacionais têm na obtenção de resultados coletivos, e por este motivo é muitas vezes denominada "institucionalismo neoliberal". Os neoliberais alegamque as praticamente todas as instituições internacionais benefeciam a cooperação internacional e reconhecem que, a cooperação pode ser difícil de alcançar em condições anárquicas (Dunne, Kurki & Smith, 2010) .

No mundo contemporâneo globalizado, a Interdependência Complexa é definida como: "Um conceito transnacionalista económico que assume que os Estados não são os únicos atores importantes, as questões do bem-estar social partilham o palco central com as questões de segurança na agenda global, e a cooperação é tão dominante quanto o conflito na política internacional" (Genest, 1996, p. 140) .

Neste sistema de interdependência, os Estados cooperam porque é do interesse comum e o resultado direto dessa cooperação é a prosperidade e a estabilidade do sistema internacional. Os transnacionalistas/neoliberais acreditam que "os Estados não são motivados apenas pelo interesse nacional em termos de poder" (Genest, 1996, p. 133) . Teoria bem diferente do realismo, os neoliberais argumentam que é que a política internacional não pode ser dividida, na chamada "alta" e "baixa" política. Embora a alta política de

segurança nacional e poder militar ainda permaneça importante e relevante, estes argumentam que as questões económicas, sociais e ambientais, considerada baixa política, são altas prioridades na agenda internacional. Ao contrário dos neorealistas, que acreditavam no papel menor das instituições internacionais limitadas por interesses maiores dos Estados na segurança nacional e militar, a interdependência complexa considera que o potencial papel que as instituições internacionais têm na negociação política aumenta exponencialmente (Rana, 2015, p. 291) .

Embora se note um aumento na cooperação quer a nível económico quer da interdependencia tecnológica, a probabilidade de conflitos militares não é nula. (Rana, 2015, p. 291) . “As políticas de interdependência económica e ecológica envolvem competição mesmo quando grandes benefícios líquidos são esperados através da cooperação” (Nye & Keohane, 1977, p. 10) .

Robert O. Keohane e Joseph S. Nye (1977) caraterizaram a Interdependência Complexa em três caraterísticas basilares . Em primeiro lugar, os diversos canais que ligam as sociedades, quer sejam as transações interestatais, transgovernamentais e transnacionais. Keohane e Nye referem também a inexistência de uma hierarquia entre os problemas. Existem vários problemas que não estão organizados numa hierarquia clara em que, “a segurança militar não domina consistentemente a agenda” (Nye & Keohane, 1977, p. 25). Apesar da segurança ser o foco mais importante dos Estados, e ao contrário do que os realistas pensam, as agendas das relações exteriores são bastantes diversas. Dependendo do momento qualquer área temática/científica pode estar no topo dessa agenda.

A força militar pode ser “irrelevante na resolução de desentendimentos sobre questões económicas entre membros de uma aliança, embora seja, simultaneamente, muito importante para as relações públicas e militares da aliança contra um bloco rival”. O objetivo da força militar, enquanto instrumento que ajuda minimizar os conflitos, diminui drasticamente quando o mundo se tornou mais globalizado. Apesar do seu papel como ferramenta de negociação continua a ser vital logo não se pode ignorar a sua importância (Rana, 2015, p. 292) .

Quando se trata de alta e baixa política, na alta política os países desenvolvidos têm uma vantagem e quando se trata de baixa política, mais uma vez esses países beneficiam aqueles que estão integrados na economia mundial capitalista. A força militar não é o instumento normalmente usado, mas continua a ser o escolhido por países menos dependentes para seu proveito. A força militar, apesar de tudo, continua a ser uma ferramenta decisiva. Emobra haja uma constante mudança da natureza das relações internacionais, e o mundo se ter globalizado a uma grande escala a força ainda permanece um instrumento vital, mesmo no mundo interdependente. Logo aseguir ao surgimento de regimes e instituições internacionais, as capacidades militares normamente conhecidas (tradicionais) foram compensadas com a importância do bem-estar e do comércio em questões de política externa (Rana, 2015, p. 296).

As Organizações Internacionais e os próprios movimentos transnacionais transcendem as fronteiras nacionais. Os próprios países desenvolvidos que, enquanto mundo industrializado, não querem entrar em guerra para não porem em causa o desenvolvimento (Rana, 2015, p. 296).

Na Interdependência Complexa, as organizações ajudam os Estados a trabalharem entre si ou com outras outras organizações, até mesmo com o setor privado estimulando a sua cooperação e auxiliando em ferramentas e conhecimento. Envolve os elementos liberais de eliminar barreiras para o comércio internacional, atrair o investimento/financiamento estrangeiro e enfatizar o papel das organizações internacionais, em detrimento dos Estados. Nesta perspetiva e sendo o foco a atuação das organizações internacionais como a UE e da NATO na criação e desenvolvimento de uma política de segurança no ciberespaço, parece-nos que a Interdependência Complexa é a teoria que mais se enquadra com a presente dissertação.

Nota Metodológica

A metodologia, como o próprio nome indica, é constituída por um conjunto de métodos pelos quais se rege um trabalho de investigação de natureza científica. Metodologia é uma palavra derivada do termo método, que vem do Latim *methodus*, que significa caminho ou via para a realização de algo. No âmbito de um trabalho de natureza científica e académica, método poderá ser definido como o percurso que se tem que percorrer para chegar ao conhecimento científico considerado válido. Envolve, no âmbito desta dissertação, pesquisa bibliográfica ou documental com o objetivo de atingir um resultado final desejado que depois será apresentado. Existem vários modelos teóricos sobre a metodologia por isso é necessário fazer um planeamento cuidadoso conforme as regras e normas específicas do autor do modelo pelo qual se vier a optar (Quivy e Champeanhout 2008).

Quivy e Champeanhout, abordam os problemas de métodos muitas vezes existentes na elaboração do trabalho. São focados três problemas, a chamada "gula livresca ou estatística" que consiste em ler um número desenfreado de livros e documentos esperando retirar daí o objetivo do trabalho. O segundo problema é designado "A passagem de hipóteses", ou seja: é necessário fazer-se a dissertação por fases e realizar cuidadosamente as primeiras etapas, só depois pensar em passar às seguintes. Passar diretamente às hipóteses pode ser uma precipitação e primeiro é necessário saber mesmo aquilo que se procura. Por último, os mesmos autores referem a ambição excessiva e a mais completa confusão, que são duas caraterísticas que prevalecem neste tipo de trabalhos e que exprimir-se de forma luxuosa e incompreensível não será um bom método (Quivy e Champeanhout 2008).

Segundo Gaston Bachelard, o processo científico tem somente três fases. Uma primeira fase em que "conquistamos" o preconceito, onde se deixa de ter uma opinião desfavorável sobre um determinado tema. É nesta fase que se "rasgam" as falsas evidências e esta fase, portanto, será primeiro ato constituído do processo científico. Seguidamente, o autor é "construído" pela razão. É nesta fase que vêm à tona as proposições elucidativas do objeto a

estudar pelo autor, assim como a previsão sobre qual o caminho da pesquisa a definir para se atingir os objetivos. Por último, “verificado” nos factos pois uma proposição só tem direito ao estatuto científico se for verificada pelos factos com sustentação em autores credíveis sobre esses mesmos conceitos (Lakatos & Marconi, 1994).

Neste contexto, torna-se fundamental esclarecer os métodos que se vai adotar bem como as técnicas, meios utilizados e os seus procedimentos para atingir os objetivos propostos da investigação (Lakatos & Marconi, 1994).

Muitos investigadores da área dos modelos de investigação científica diferenciam métodos de método, pois afirmam que estão em patamares diferentes. Sendo assim, o método é qualificado por ter uma abordagem mais alargada e uma abstração superior, quer dos fenómenos de natureza quer da sociedade (Lakatos & Marconi, 1994).

Existem diversos métodos para realizar investigação de modo a aferir a veracidade das hipóteses. Um dos métodos que temos de ter em conta é o método hipotético-dedutivo, proposto pelo filósofo Karl Popper. Para Popper a veracidade das hipóteses é baseada no confronto da conclusão com os factos, o que pode conduzir a dois tipos de situações: a conclusão é incompatível com os factos apurados, logo a premissa será refutável; ou a conclusão é compatível com os factos e nesse caso a premissa é verdadeira (Silveira, 1989).

Existem também outros métodos que são mencionados pelos autores Lakatos e Marconi, que são o dedutivo, o dialético e o indutivo. Além destes são identificados, também, o método de análise documental e o comparativo. No âmbito da nossa dissertação e considerando a investigação que desenvolvemos, o método que mais se adequa é o hipotético-dedutivo. Por seu intermédio, e depois de termos definido as hipóteses com base numa falha reconhecida testamos em seguida a veracidade das mesmas para buscar alcançar conclusões que nos permitam (contribuir para) colmatar a lacuna identificada (Lakatos & Marconi, 1994) e, nesse caso, confirmar as premissas de partida que originariamente formulámos.

Neste trabalho de investigação, a metodologia adotada é suportada no modelo de Raymond Quivy e Luc Van Campenhoudt. De forma genérica, este modelo divide-se, como foi dito anteriormente, em três grandes atos (Rutura, Construção e Verificação) que, por sua vez, se subdividem em sete etapas (Quivy e Champeanhout 2008).

Na fase de Rutura, segundo este modelo, temos três etapas que se iniciam pela pergunta de partida, onde se procura formular uma pergunta bastante clara, precisa e fundamentalmente de forma a não criar confusões. Outras caraterísticas fundamentais da pergunta de partida são a exequibilidade da mesma e a pertinência, sendo fundamental assumir desde logo que nunca uma pergunta de partida poderá ter o objetivo de julgar. A segunda etapa é a exploração que, neste caso, consiste na leitura de documentos para mitigar as dúvidas sobre a pergunta de partida, assumindo como objetivo estruturante explorar mais sobre a temática que nos propusemos investigar para conceber uma problemática de investigação, um objeto de estudo. A última etapa desta fase é a problemática, que tem como foco responder à pergunta “Como vou abordar este fenómeno?”. Esta última etapa já começa a entrar na fase seguinte, a fase da Construção (Quivy e Champeanhout 2008).

A fase da Construção tem como meta a elaboração do modelo de análise, focando-se no porquê das hipóteses e qual o caminho das mesmas de modo a que forneçam um fio condutor à investigação. As hipóteses devem ser expressas sob uma forma observável, e manifestadas como uma antecipação de correlação de conceções/conceitos (Quivy e Champeanhout 2008).

A última fase, a Verificação, abrange as três últimas etapas que são: a observação - devendo responder a três perguntas (observar o quê?; em quem?; como?) - a análise de informação e, por fim, as conclusões, onde se faz uma retrospetiva do trabalho desenvolvido e considerações sobre o mesmo (Quivy e Champeanhout 2008).

3.1 Formulação da pergunta de partida

Um trabalho científico assenta em algo que se procura, o que implica dúvidas, desvios e indecisões. O investigador tem, por isso, que escolher uma

pergunta de partida clara e coerente para que seja possível verificar-se a existência de um fio condutor lógico e coerente que confira sentido e decorrência causal do início ao fim do trabalho.

Assim, formulou-se no contexto desta investigação a seguinte **pergunta de partida:**

Qual a importância do papel dos privados na Política Europeia de Segurança do Ciberespaço?

Após a formulação da pergunta de partida e de modo a dar-lhe resposta é necessário formular hipóteses, que constituem argumentos em que nos baseamos para definir os objetivos com maior rigor. No final da investigação procurar-se-á verificar se essas mesmas hipóteses de trabalho são verificáveis ou refutáveis.

3.2 Hipóteses de Trabalho

Segundo Quivy e Campenhout, as hipóteses de trabalho têm que apontar o caminho da investigação para posteriormente se poder comparar os dados obtidos com essas mesmas hipóteses. Para tal, é necessário formular várias hipóteses de trabalho pois muito dificilmente somente uma hipótese de trabalho dará resposta à pergunta de partida (Quivy e Champeanhout 2008).

A hipótese é uma proposição que tem que ser verificada através dos resultados da investigação para, no final da dissertação, poder concluir se é verificável ou refutável, sendo que se considera que uma hipótese só deve ser refutável se tiver um caráter genérico.

As hipóteses de trabalho têm um caráter fundamental, no entanto tentam apenas fornecer uma explicação para a problemática que se estuda e não passam de meras proposições. Por outras palavras, as hipóteses têm como objetivo testar o modelo de análise utilizado.

É possível observar que a formulação das hipóteses de trabalho se enquadra na quarta etapa (a construção do modelo de análise) do modelo de investigação científica adotado.

De acordo que o objeto de estudo utilizado e tendo em conta a pergunta de partida referenciada anteriormente foram, no âmbito da investigação que desenvolvemos, formuladas as seguintes hipóteses de trabalho (HP):

HP.1: As Parcerias Público-Privadas têm demonstrado ser determinantes na criação de infraestruturas críticas de cibersegurança na EU

HP.2: As Parceria Público-Privadas contribuem para potenciar a Cibersegurança na UE.

HP.3: Parcerias público-privadas têm mais força sendo lideradas instituições privadas.

HP.4: A Participação de PMEs aumenta significativamente a cibersegurança na UE.

Políticas e Estratégias para o Ciberespaço: UE vs. NATO

Hoje em dia, falar de cibersegurança é comum, mas no início da década de ‘90 do século XX o conceito de segurança ainda não se encontrava associado ao ciberespaço. Quando algo corria mal neste domínio apontava-se de imediato para problemas informáticos de natureza técnica.

No final do século XX, durante a guerra do Balcãs (1999), a NATO foi atacada ao nível dos seus *websites* por um grupo de *hackers* “pró” Sérvia (AC, 2012). O *website* onde eram atualizadas as notícias e informações referentes à guerra do Kosovo ficou inoperativo durante alguns dias devido a esses mesmos ataques do tipo DDoS. *Hackers* não-sérvios conseguiram com sucesso o acesso público ao principal servidor da *World Wide Web* no qual se baseava todo o serviço de Diplomacia Pública da NATO no Kosovo, mantendo-o praticamente inoperativo por vários dias. O ataque foi lançado contra o servidor *Web* da sede da NATO em Bruxelas, na Bélgica, e incluiu um ataque por correio eletrónico a partir da Jugoslávia que entupiu o servidor de correio eletrónico da NATO com 2.000 mensagens por dia (Verton, 1999). Um ataque *DDoS* (ou ataque de negação de serviço), como atrás operacionalizamos, visa tornar um servidor ou uma infraestrutura indisponível. Em face destes ataques, como voltou a suceder em 11 de Setembro de 2001, a NATO começou a ter uma visão diferente das ameaças não-convencionais, pelo que as mesmas começaram a ser tratadas como prioridade estratégica tornando-se deste modo uma das principais preocupações das organizações internacionais e das potências mundiais (Barrinha & Carrapiço, 2016). Podemos considerar que, nesse sentido, o ponto de viragem nesta matéria ter-se-á verificado durante a cimeira de Praga em 2002 (NATO Parliamentary Assembly, [s.d])

Nesse contexto, foi reconhecido que era necessário fortalecer as capacidades da NATO para se defender contra ataques cibernéticos e para

esse fim é criado o *NATO Computer Incident Response Capability* com o objetivo de responder de imediato a qualquer ataque cibernético contra a organização (UNIDIR, 2013).

No que se refere à UE, até esta data ainda não se tinha abordado o assunto da cibersegurança. O primeiro documento que é publicado por esta organização foi designado *A Secure Europe in a Better World* e surge apenas em 2003, embora neste documento não haja ainda um claro reconhecimento do ciberespaço nem da cibersegurança como uma prioridade estratégica (EU, 2003). A União Europeia veio, apenas bastante mais tarde, a adotar uma estratégia de segurança europeia (*A Secure Europe in a Better World*), que analisou o aspeto externo de segurança da Europa (EU, 2010). Podemos, neste sentido, concluir que a NATO foi a organização que deu os primeiros passos no reconhecimento da importância dos assuntos do ciberespaço (EU, 2003).

Em 2007 têm lugar os ataques à Estónia e, logo a seguir, em 2008, a guerra entre a Rússia e a Geórgia obriga a NATO a tomar medidas severas. Em Janeiro de 2008, na *Nato Bucharest Summit*, assiste-se à criação de uma política de segurança para o ciberespaço.

A guerra cibernética de que a Estónia foi alvo em 2007 constitui um evento que ainda hoje influencia. Em abril aquele ano, uma discussão por causa de uma estátua provocou o primeiro ciberataque conhecido em todo o país e que mostrou quão facilmente um Estado hostil pode explorar potenciais tensões dentro de outra sociedade (McGuinness, 2017). De facto, em 26 de abril de 2007, Tallinn entrou em conflito durante duas noites durante as quais se verificaram motins de que resultaram 156 feridos, um morto e 1.000 pessoas detidas. A partir de 27 de abril, a Estónia também foi atingida por grandes ataques cibernéticos que, em alguns casos, duraram semanas. Os serviços *online* dos bancos, meios de comunicação e órgãos governamentais da Estónia foram derrubados por níveis sem precedentes de tráfego na *internet*. Ondas massivas de *spam* foram enviadas por *botnets* e enormes quantidades de solicitações automatizadas *online* sobrecarregaram os servidores. O resultado para os cidadãos da Estónia foi, segundo McGuinness (2017):

- As máquinas automáticas de disponibilização de dinheiro e os serviços bancários *online* estiveram esporadicamente fora de serviço;
- Os funcionários do governo e dos demais partidos políticos não conseguiam comunicar por correio eletrónico;
- Os jornais e os restantes meios de comunicação de repente descobriram que não podiam difundir notícias pela falta de capacidade dos *websites*.

Os *websites* que sofreram danos graças a esses ataques virtuais eram websites importantes para o funcionamento do país como do governo, bancos, partidos políticos e esses ataques causaram um prejuízo a rondar as dezenas de milhões de euros (Tisdall, 2010).

No entanto, todo este *statu quo* também ajudou a transformar a Estónia num de segurança cibernética, tal como se verifica nos dias de hoje (McGuinness centro, 2017).

Face a isto, e para continuar comprometida em fortalecer os principais sistemas de informação da Aliança contra ataques cibernéticos, na *NATO Bucharest Summit* (2008) foi assumida a necessidade de definir uma Política sobre Defesa Cibernética, tendo sido igualmente identificadas e enunciadas as medidas a desenvolver, assim como as estruturas e autoridades fundamentais para a sua concretização. A Política de Defesa Cibernética enfatiza a necessidade de que a NATO e as nações protejam os principais sistemas de informação nacionais de acordo com as suas responsabilidades, que compartilhem as melhores práticas e forneçam meios para garantir a capacidade necessária para ajudar as nações aliadas, mediante solicitação, a combater um ataque cibernético. À época, esperava-se que pudesse ser possível continuar o desenvolvimento das capacidades de defesa cibernética da NATO e fortalecer as ligações entre a mesma e as autoridades nacionais dos vários Estados Membros (NATO, 2008).

Após esta cimeira, ocorreu meses depois, em Agosto de 2008, um ataque cibernético contra a Geórgia. A coincidência foi, de facto, “sugestiva”: a

invasão da Geórgia em 2008, devido ao conflito militar russo-georgiano na Ossétia do Sul, é precedida por operações no ciberespaço, tendo este ataque sido associado a operações militares, algo que no ano anterior não tinha acontecido na Estónia (Guedes, 2009). Mais curioso ainda é que nesse mesmo ano e após o término do conflito instalado na Geórgia, a UE teve a necessidade de reavaliar o documento que tinha publicado em 2003 e a que anteriormente nos referimos, onde não eram abordados aspetos do ciberespaço, e após essa reavaliação é incluída em 2008 a cibersegurança como uma das ameaças e riscos globais que os Estados têm que ter em conta (Balão, 2014). Nessa mesma reavaliação conclui-se que as economias modernas são fortemente dependentes das infraestruturas críticas, incluindo transporte, comunicação e fontes de alimentação, mas também da *internet*. A UE já tinha emitido uma estratégia para a Sociedade da Informação, adotada em 2006, que tratava de crimes baseados na *internet*, ou seja cibercrimes. No entanto, os ataques contra sistemas de Tecnologias de Informação (TI) privados ou governamentais nos Estados-Membros da UE deram às TIC uma 'nova' dimensão: a de potencial arma económica, política e militar, que exigia uma abordagem mais abrangente da UE, maior sensibilização e reforço da cooperação internacional (EU, 2008).

Nesse mesmo ano de 2008, a NATO criou também a *Cyber Defence Management Authority* (CDMA) para coordenar a ciberdefesa e assim dar uma resposta efetiva a um possível problema que pudesse ocorrer nesse domínio. Para isso, um Estado membro que sofresse um ciberataque pedia auxílio e a CDMA iria estar capacitada para ajudar esse Estado membro, através da coordenação da ciberdefesa, revisão das capacidades de ciberdefesa e criação de uma conduta apropriada sobre risco de segurança transversal a toda a Aliança. Acreditaram também o *Cooperative Cyber Defence Centre for Excellence* (CCD COE), com o principal objetivo de melhorar a interoperabilidade da NATO e reforçar a sensibilização, aos Estados-Membros, dos perigos do ciberespaço (NATO Parliamentary Assembly, [s.d])

Em 2009 inclui-se, pela primeira vez, a ciberdefesa em exercícios NATO, e no ano seguinte, na Cimeira de Lisboa, a NATO identificou diversas falhas a

nível da ciberdefesa incluindo desenvolvimentos ao nível das *NATO Computer Incident Response Capability* (NCIRC) sendo que, nesse mesmo ano de 2009, realizou-se o *Cyber Coalition* onde participaram todas as nações que faziam parte da Aliança (NATO, 2010a). As ameaças cibernéticas estavam a aumentar a uma escala 'frenética' e a evoluir em sofisticação, razão pela qual para garantir o acesso permanente e restrito da NATO ao ciberespaço e à integridade dos seus sistemas críticos, foi necessário ter em conta a dimensão cibernética dos conflitos modernos na doutrina da própria organização. Para tal era fundamental que a NATO melhorasse as suas capacidades para detetar, avaliar, prevenir, defender e recuperar os seus sistemas em caso de ataque cibernético contra sistemas de importância crítica para a Aliança. Nessa mesma cimeira de Lisboa de 2010 ficou definido que a NATO iria empenhar-se, em particular no que se referia à aceleração da capacidade de resposta a incidentes informáticos da NCIRC, até à total operacionalidade (*Full Operational Capability*) apontada à época para 2012, bem como a disponibilização - a todos os membros da NATO – de proteção cibernética centralizada para melhorarem a sua ciberdefesa (NATO, 2010). Em 2012 verificou-se o cumprimento do prazo inicialmente estipulado pelo que a *NATO Compututer Incident Response Capability* estava na sua *Full Opeational Capability*, estando associada a um contrato cujo custo rondou os 50 milhões de euros, e que previa um serviço cuja gestão garantia o fornecimento de informações a cerca de cinquenta *websites* da NATO em vinte oito países do mundo (NATO, 2012a).

Os processos de planeamento de defesa da NATO foram, neste contexto, orientados para promover o desenvolvimento das capacidades de defesa cibernética dos Aliados, para ajudar Aliados individuais mediante pedido e para otimizar a partilha de informação, colaboração e interoperabilidade. Para abordar os riscos de segurança que emanam do ciberespaço, os Aliados trabalharam em estreita colaboração com outros atores, como a Organização das Nações Unidas (ONU) e a UE, conforme acordado. Foi igualmente solicitado ao Conselho Europeu que desenvolvesse, baseando-se nomeadamente nas estruturas internacionais existentes e com base numa

revisão da política criada em 2008 após o conflito da Geórgia, uma política de defesa cibernética em profundidade até Junho de 2011 e que se preparasse um plano de ação para a sua implementação (NATO, 2010).

Ainda em 2010, a Comissão Europeia ficou alerta para o aumento significativo dos ciberataques registados no âmbito da UE, tendo o Conselho complementado a estratégia europeia de segurança de 2003 - que abordava essencialmente aspetos de cibersegurança externa -, e passando, nesse sentido, a adotar uma estratégia interna de segurança, a *Internal Security Strategy* onde passou a estar contemplado o cibercrime. Esta última forma de criminalidade representa uma técnica global, que envolve cooperação transfronteiriça e anónima, que ameaça os sistemas de informação da UE e, por isso, coloca muitos desafios adicionais a quem aplica a lei (NATO, 2012b).

Assim, e de acordo com o compromisso previamente assumido, a NATO apresentou em junho de 2011 uma nova revisão da política de ciberdefesa e os ministros da defesa aprovaram a segunda Política da NATO sobre ciberdefesa e que definiu, por sua vez, uma visão para esforços coordenados em toda a Aliança no contexto do ambiente de ameaça tecnológica em rápida evolução, bem como um plano de ação associado para a sua implementação (NATO, 2018).

Nesse sentido, em abril de 2012, a ciberdefesa foi introduzida no Processo de Planeamento da Defesa da NATO. Os requisitos relevantes neste domínio passaram então a ser identificados e priorizados por meio do referido processo de planeamento de defesa. Na Cimeira de Chicago, em maio de 2012, os líderes da Aliança reafirmaram o seu compromisso no sentido de melhorar as ciberdefesas da Aliança, colocando todas as redes da NATO sob proteção centralizada e implementando uma série de atualizações para o NCIRC (NATO, 2018). Nessa Cimeira, concluiu-se que os ciberataques continuaram a aumentar significativamente em número e evoluíram em sofisticação e complexidade. A NATO reafirmou, por isso, os compromissos de ciberdefesa assumidos inicialmente na Cimeira de Lisboa em 2010. Depois de Lisboa, foram adotados uma Política e Plano de Ação de Ciberdefesa, que estavam a ser implementados àquela data (NATO, 2012). Com base nas

capacidades NATO existentes e os elementos críticos da *Full Operational Capability* (FOC) da NCIRC, incluindo a proteção da maioria dos sites e utilizadores, era expectável que os mesmos estariam implementados até ao final de 2012. A NATO comprometeu-se, à época, a fornecer recursos e concluir as reformas necessárias para colocar todos os seus organismos sob proteção cibernética centralizada, para garantir que as capacidades reforçadas de defesa cibernética pudessem proteger o investimento coletivo na e da organização. Nesse sentido, ficou acordado integrar, ainda mais, as medidas de defesa cibernética nas estruturas e procedimentos da Aliança sendo que os Estados membros, como nações individuais, continuariam empenhados em identificar e fornecer capacidades nacionais de defesa cibernética que fortalecessem a colaboração e a interoperabilidade da Aliança, também através dos processos de planeamento de defesa da NATO. De facto, assistiu-se, nos anos seguinte, da parte daqueles, à busca pelo crescente desenvolvimento da capacidade de prevenir, detetar, defender e recuperar de ciberataques (NATO, 2012). Para abordar as ameaças à ciberdefesa e melhorar a segurança comum dos países da Aliança, a NATO comprometeu-se a colaborar com as nações parceiras, caso a caso, e com organizações internacionais, como por exemplo a UE, o Conselho da Europeu, a ONU e a OSCE, a fim de aumentar a cooperação concreta (NATO, 2012).

Em julho de 2012, como parte da reforma das agências da NATO, a *NATO Communications and Information Agency* (NCIA) foi estabelecida (NATO, 2018).

Em 2013, no âmbito da “Estratégia de Cibersegurança da União Europeia”, são definidas cinco prioridades estratégicas para a UE (COMMISION, 2013):

- Alcançar a ciber resiliência;
- Diminuir drasticamente o cibercrime;
- Desenvolver políticas e capacidades de ciberdefesa relacionadas com a *Common Security and Defence Policy*.

Este documento refere, igualmente, que os Estados Membros deveriam concentrar os seus esforços em desenvolver ciber-capacidades de defesa (EUROPEAN COMMISION, 2013).

Em paralelo, ainda em 2013, o mandato da ENISA aumentou, o que assegurou a permanência desta agência e possibilidade de se continuar a desenvolver as questões sobre o ciberespaço. Em simultâneo houver a criação da plataforma público-privada NIS e foi associada à Estratégia Europeia nesta temática da segurança do ciberespaço. A NIS foi criada como um grande objetivo: aumentar a gestão de risco cibernético por parte de todas as organizações, quer sejam elas privadas ou públicas (Balão 2014).

Em fevereiro de 2014, os ministros da defesa dos aliados encarregaram a NATO de desenvolver uma nova e melhorada política de ciberdefesa relativa à defesa coletiva, assistência aos Aliados, governança simplificada, considerações legais e relações com a indústria (NATO, 2018).

Em abril de 2014, renomeou-se o Comité de Política de Defesa e Planeamento/Ciberdefesa como o Comité de Ciberdefesa. Em maio de 2014, a *Full Opeational Capability* NCIRC (NCIRC FOC) foi alcançada, proporcionando maior proteção às redes e utilizadores da NATO. Na Cimeira realizada no País de Gales, em setembro de 2014, os Aliados definiram uma nova política de ciberdefesa e aprovaram um plano de ação que, juntamente com a respetiva política, contribui para o cumprimento das principais tarefas da Aliança. A política e sua implementação passaram a estar, então, sob revisão rigorosa nos níveis políticos e técnicos da Aliança, sendo aprimoradas e atualizadas de acordo com a crescente ameaça cibernética. Na sequência da decisão tomada na Cimeira do País de Gales em 2014, a *NATO Industry Cyber Partnership* (NICP) foi apresentada na conferência da *NATO Information Assurance Symposium* realizada a 17 de setembro de 2017 em Mons, na Bélgica, onde 1.500 líderes da indústria e formuladores de políticas se reuniram para discutir a colaboração cibernética, uma vez que a NICP reconhece a importância de trabalhar com parceiros da indústria para permitir que a Aliança atinja os seus objetivos de política de ciberdefesa (NATO, 2018).

À medida que a Aliança olha para o futuro, é expectável que ameaças e ataques cibernéticos continuem a ser mais comuns, sofisticados e potencialmente prejudiciais. Para enfrentar esse desafio em evolução, criou-se nessa cimeira uma Política de Ciberdefesa Reforçada, com o objetivo de contribuir para o cumprimento das principais tarefas da Aliança. Essa política reafirma os princípios da indivisibilidade da segurança aliada e da prevenção, deteção, resiliência, recuperação e defesa. Recorda que a responsabilidade fundamental da ciberdefesa da NATO é defender as suas próprias redes e que a assistência aos Aliados deve ser abordada de acordo com o espírito de solidariedade, enfatizando a responsabilidade dos Aliados de desenvolver as capacidades relevantes para a proteção das redes nacionais. Relevante é, a nosso ver, destacar que a política da NATO também reconhece que o direito internacional, incluindo o direito internacional humanitário e a Carta da ONU, se aplica ao ciberespaço (NATO, 2014).

De facto, os ataques cibernéticos podem atingir um limiar que ameaça a prosperidade, segurança e estabilidade nacional e euro-atlântica. O seu impacto pode ser tão ou mais prejudicial para as sociedades modernas do que um ataque convencional. Afirma-se, portanto, que a defesa cibernética é parte da tarefa central da NATO em matéria de defesa coletiva. Caso a caso, iria ser tomada uma decisão pelo Conselho do Atlântico Norte sobre quando um ataque cibernético levaria à invocação do Artigo 5º. Neste sentido, a NATO, na cimeira de 2017, reiterou que se encontra ainda mais empenhada em desenvolver as capacidades nacionais de ciberdefesa e reforçar a cibersegurança das redes nacionais das quais a NATO depende para as suas tarefas principais, de modo a contribuir para tornar a Aliança resiliente e totalmente protegida(NATO, 2014). A estreita cooperação bilateral e multinacional desempenha um papel fundamental no aprimoramento das capacidades da ciberdefesa da Aliança. A NATO irá continuar a integrar a defesa cibernética nas operações da mesma e no planeamento operacional e de contingência, além de melhorar a partilha de informações e o conhecimento da situação entre os Aliados. Parcerias fortes, como a ONU e UE desempenham um papel fundamental na abordagem de ameaças e riscos

cibernéticos. Portanto, é necessária uma contínua evolução em questões cibernéticas com países parceiros relevantes, caso a caso, dependendo da sua posição, objetivos e poder perante as outras nações e com outras organizações internacionais, inclusive a UE, conforme acordado naquela Cimeira de 2017. Para além disso, é importante destacar que foi assumido, logo em 2014, o interesse na intensificação da cooperação com a indústria através da *NATO Industry Cyber Partnership* (NATO, 2014).

Assim, para que a NATO e os Aliados atinjam os objetivos da Política de Ciberdefesa Reforçada são cruciais as inovações tecnológicas e as parcerias com o setor privado (NATO, 2014). A NATO melhorou o nível das atividades de educação, treino e exercício de ciberdefesa, desenvolveu a capacidade de alcance cibernético, construindo, como primeiro passo, o *Estonian Cyber Range Capability Center*, tendo em consideração as capacidades e os requisitos da *NATO Communications and Information Systems School* e de outros organismos de formação e educação da NATO (NATO, 2014).

Passando em paralelo para a UE, à data, as prioridades definidas para o quadro político de ciberdefesa da UE eram, então, as seguintes (COMMISSION, 2013):

1. Apoiar o desenvolvimento das capacidades de ciberdefesa dos Estados Membros relacionadas com a *Common Security and Defence Policy* (CSDP);

2. Melhorar a proteção das redes de comunicação da CSDP, usadas por entidades da UE;

3. Promover a cooperação civil-militar através de ciberpolíticas mais abrangentes, relevantes para as agências e instituições da UE, e também do setor privado;

4. Melhorar as oportunidades de treino, educação e exercícios;

5. Fortalecer a cooperação com parceiros internacionais relevantes.

Nesse mesmo ano de 2014, na EU, é apresentado o *EU Cyber Defence Policy Framework*, com o objetivo de definir aspetos da estratégia de

cibersegurança da UE. O objetivo deste documento era fornecer um enquadramento ao Conselho Europeu sobre as conclusões da Comissão Europeia, bem como os aspetos da ciberdefesa da Estratégia de Segurança Cibernética da UE. O documento identifica áreas prioritárias para a ciberdefesa da CSDP e esclarece os papéis dos intervenientes europeus, respeitando plenamente as responsabilidades e competências respetivas dos intervenientes e dos Estados-Membros, bem como o quadro institucional da UE e a sua autonomia de tomada de decisão, sendo que o processo de implementação da estratégia de cibersegurança da UE foi acordado pelos *Friends of the Presidency Group on Cyber Issues* (EU, 2014).

Como temos verificado, até ao ano de 2014 a NATO foi quem iniciou e primeiro implementou políticas sobre a ciberdefesa, sendo que a UE parece atuar mais a um nível estratégico.

Na sequência de toda a evolução registada neste contexto, há que destacar a cooperação habitual entre peritos da UE e da NATO tendo, em fevereiro de 2016, sido elaborado um acordo técnico sobre Ciberdefesa entre a NATO (NCIRC) e a UE.

Ainda em 2014, as organizações que ofereceram maior apoio, ao nível da cibersegurança, à UE foram: a *European Network and Information Security Agency* (ENISA), a *European Police Office* (Europol), o *European Cyber Crime Center* (EC3), e a *European Defence Agency* (EDA).

Em 2016 é, então, elaborada uma nova estratégia global da UE onde se aborda a Ciberdefesa. No contexto desse documento, ficou previsto que a UE aumentaria a sua concentração na cibersegurança, equipando-se e ajudando os Estados-Membros a fazê-lo para, através do fornecimento de conhecimento e de ferramentas, se protegerem contra ameaças cibernéticas e ajudando a manter um ciberespaço aberto, livre e seguro (EU Council, 2016).

Nesse mesmo ano os ministros da defesa dos países pertencentes à NATO no dia 8 e 9 de julho na Cimeira Varsóvia deram um grande “passo” no mundo do ciberespaço, reconhecendo-o como um “teatro de guerra” na política de defesa da NATO (Euronews, 2016).

No âmbito dessa Estratégia Global da União Europeia (EGUE), as capacidades tecnológicas destinadas a mitigar as ameaças e a resiliência das infraestruturas críticas, redes, serviços e redução do cibercrime, passam a ter que estar à disponibilidade de todos os Estados Membros. Isso significa fomentar *as Information and Communications Technology* (ICT), que possam garantir a disponibilidade, a segurança e integridade dos dados, e que por sua vez possam garantir a segurança no espaço digital europeu através de políticas sobre a localização do armazenamento de dados e a certificação de produtos e serviços. Requer, igualmente, planear as questões cibernéticas associadas a todas as políticas, reforçando os elementos cibernéticos nas missões e operações da Política Comum de Segurança e Defesa (PCSD), a par com o desenvolvimento de plataformas de cooperação. A UE apoiará, nesse contexto, a cooperação cibernética, política, operacional e técnica entre os Estados-Membros, nomeadamente na análise e gestão das consequências, assim como na avaliação partilhada da(s) ameaça(s) e risco(s) entre as estruturas da UE e as instituições relevantes nos Estados-Membros. Procurará fazê-lo melhorando a cooperação no campo da Cibersegurança com parceiros como os EUA e a NATO. Do mesmo modo, a resposta da UE também será incorporada em fortes parcerias público-privadas (EU Council, 2016) – questão que abordaremos com detalhe no último capítulo desta dissertação.

De facto, é assumido no quadro da EGUE que a cooperação e partilha de informação entre Estados-Membros, instituições, sector privado e sociedade civil pode fomentar uma cultura comum de cibersegurança e aumentar a preparação para possíveis interrupções e ciberataques (Council, 2016).

Na mesma linha, na Cimeira de Bruxelas (2018), conclui-se que as ciberameaças à segurança da Aliança estão a tornar-se mais frequentes, complexas, destrutivas e coercivas. Em face de tal facto, assume-se que a NATO continuará a adaptar-se ao cenário de ciberameaças em evolução, que é afetado por atores estatais e não estatais, incluindo os patrocinados pelo Estado. Por isso, tem que ser capaz de funcionar tão eficazmente no ciberespaço como no ar, em terra e no mar para fortalecer e apoiar a postura geral de dissuasão e defesa da Aliança. Portanto, a NATO irá continuar a

implementar o ciberespaço como um domínio de operações, na linha do que foi assumido no quadro da Cimeira de Varsóvia. Na Cimeira de 2018 os líderes da Aliança acordaram entre si criar um novo *Cyberspace Operations Centre*. Esse centro fornecerá o designado *situational awareness* e será a partir dele que será assegurada a coordenação da atividade operacional da NATO no ciberespaço. Os aliados também concordaram que a NATO pode delinear no âmbito cibernacional, os recursos necessários para as suas missões e operações (NATO, 2018).

Reafirmando o mandato defensivo da NATO, os Aliados assumiram a sua determinação em empregar toda a gama de recursos, incluindo o ciber-recursos, para deter, defender-se de e combater todo o espectro de ciberameaças, incluindo aquelas resultantes de uma campanha híbrida. Conclui-se, ainda, que é necessário reforçar o *situational awareness* liderado pela *intelligence* para apoiar a tomada de decisões e a ação da NATO, pelo que é fundamental continuar a trabalhar em conjunto para desenvolver medidas que permitam imputar custos àqueles que prejudicam a Aliança (NATO, 2018).

Os Aliados fizeram um balanço dos seus progressos para melhorar a resistência nacional através do *Cyber Defense Pledge*, que é essencial para melhorar a resiliência cibernética e aumentar os custos de um ataque cibernético conduzido por forças opositoras. Reafirma, assim, o compromisso de agir de acordo com o Direito Internacional, incluindo a Carta da ONU, o Direito Internacional Humanitário e a legislação dos Direitos Humanos, conforme aplicável. Também apoia o trabalho para manter a paz e a segurança internacionais no ciberespaço e promover a estabilidade e reduzir o risco de conflito, reconhecendo que todos podem beneficiar de um ciberespaço baseado em normas, previsível e seguro. Nesse sentido, continuará a apostar no desenvolvimento de parcerias com a indústria e a Academia de todos os Aliados para acompanhar os avanços tecnológicos por meio da inovação (NATO, 2018).

Perspetiva Histórico-Evolutiva + comparativa das Políticas e Estratégias do Ciberespaço na UE

Este capítulo tem como finalidade analisar os documentos da UE em matéria de estratégias e políticas de cibersegurança e compará-los entre si para, desse modo, conseguirmos identificar alinha evolutiva desta questão no quadro da UE.

Assim, começaremos por considerar a *Proposta de Resolução do Parlamento Europeu* que tem incluída várias medidas de cibersegurança e ciberdefesa que terão que ser adotadas pela UE. Nesse contexto, os conceitos que anteriormente foram operacionalizados terão particular utilidade na medida em que contribuirão para a sua compreensão.

Depois, avançaremos para o aprofundamento da análise do documento intitulado *Estratégia de Cibersegurança da União Europeia* de 2013 de modo a poder comparar as prioridades estratégicas que aí são definidas até ao último contributo para a reforma da cibersegurança na Europa, e que data de 28 de março de 2019.

Já anteriormente foi possível constatar que a UE não se encontra sozinha no capítulo da cibersegurança, sendo que algumas organizações contribuem para um importante apoio institucional no que diz respeito a esta matéria. Neste sentido, consideraremos na nossa análise o contributo da *European Network and Information Agency* (ENISA), e da *European Union for Law Enforcement Cooperations* (anteriormente designada *European Police Office*) (Europol). A Europol tem incluídas, entre outras organizações, a *European Cyber Crime Centre* (EC3), e a *European Defence Agency* (EDA) (Pernik, 2014).

No final deste capítulo, procuraremos apresentar uma conclusão que evidencie os aspetos mais relevantes de cada um dos documentos analisados e, subsequentemente, o resultado de uma análise comparativa entre eles de modo a concluir sobre os principais contributos em matéria de cibersegurança.

5.1UE: Cibersegurança e Ciberdefesa. *Quid Juris*?

Neste subcapítulo, como referido anteriormente vamos analisar em detalhe a Resolução do Parlamento Europeu de 2012 em matéria de cibersegurança. Esta proposta tem incluídos vários pontos que refletem o tema do ciberespaço, bem como medidas que a UE deveria adotar em termos de coordenação, tanto com o setor público como com o privado, assim como com parcerias internacionais, com a NATO e com os Estados Unidos da América. Possui, ainda, referências a questões relativas ao ciberespaço na eu que surgem articuladas com a Agência Europeia de Defesa e com os vários Estados que pertencem à União Europeia (CAE, 2012).

Devido à vasta amplitude de informação contemplada por este documento, iremos focar-nos, apenas, nas questões de relevância central para esta dissertação, e que acima identificámos. Assim, ao longo desta proposta é demonstrado que as nações que pertencem à UE e a própria organização estão fundamentalmente dependentes da cibersegurança (segurança no ciberespaço) (CAE, 2012).

Atualmente os ciberataques têm aumentado a um ritmo nunca dantes pensado e muitos desses ataques por razões políticas (CAE, 2012).

Verificava-se, 2012, uma vulnerabilidade enorme por parte da UE no que tocava ao ciberespaço, à sua segurança e à sua defesa. Os Estados-Membros "acusavam", ainda, uma grande lacuna: a falta de comunicação e de entrosamento da informação era enorme o que fazia com que os aspetos da cibersegurança e ciberdefesa variassem de país para país. Focando-nos nos países da Aliança, muitos dos ciberataques não eram reportados o que dificultava a sua posterior análise e a melhoria no seu sistema de proteção - por outras palavras, não havia uma evolução constante. Também em alguns Estados-Membros registava-se a falta de ferramentas e infraestruturas para a sua própria proteção, estando os mesmos muito dependentes de outros países em tudo o que se referia a tecnologia de segurança. O cenário, tal como se apresentava, apontava para uma clara necessidade de uma intervenção por

parte da UE para reforço das capacidades dos seus Estados-Membros em termos individuais e, desse modo, reduzir a sua dependência face a terceiras partes (CAE, 2012). Assim, ficou definido nessa Proposta de Resolução do Parlamento Europeu de 2012 um plano conjunto entre a UE e os Estados Unidos da América, país que até à data se apresenta como o mais evoluído ao nível das questões da cibersegurança e da ciberdefesa, para tentar pôr fim a estas lacunas por parte dos Estados-Membros recorrendo a medidas como, por exemplo (CAE, 2012):

- Elaboração de um plano estratégico único e global na UE, com uma definição clara dos conceitos de cibersegurança e ciberdefesa;
- Diferenciar os diferentes níveis de ciberataques tanto na esfera política como na esfera militar em função das suas motivações e repercussões e com base nisso criar um documento onde isso fique bem esclarecido;
- Modificar a estratégia europeia de segurança, principalmente no capítulo do ciberespaço, atualizando-a para mais facilmente se reconhecer e descobrir meios para detetar os ciberataques e encontrar os seus autores.

Para responder a tais objectivos, a UE assumiu como fundamental implementar diversas outras medidas (CAE, 2012):

- Além da imprescindibilidade de uma avaliação aos ciberataques, as instituições da UE têm que ser submetidas [também] a uma contínua avaliação para se conseguir garantir uma resposta eficaz a eventuais ciberataques;
- É obrigatório criar um sistema onde se incluam as informações sobre alertas de novas ameaças, assim como as fragilidades das TIC de cada Estado-Membro;

- É fundamental a criação de planos de contingência e de gestão de risco dos sistemas. A criação de ações de sensibilização para todos aqueles que trabalham com sistemas de informação e exercícios sobre cibersegurança;
- Criação de uma equipa especializada que consiga atuar prontamente caso ocorra um ciberataque, de preferência com capacidade de operar em menos de um dia. O nome dessa equipa seria *Community Emergency Response Team* (CERT);
- Existe a necessidade de cada Nação criar, com a ajuda das Forças Armadas, as suas próprias unidades de cibersegurança e ciberdefesa para serem cada vez mais independentes, ao mesmo tempo que facilitam o entrosamento e a comunicação com os restantes Estados-Membros e a própria UE.

No âmbito da mesma Resolução, a UE decidiu apostar na cooperação com a NATO para melhorar o seu nível de cibersegurança (CAE, 2012):

- Ambas as organizações (para evitarem esforços extras e duplicação de ações, pela sua estreita relação e aumento dos problemas no âmbito do ciberespaço) irão complementar-se para assim conseguirem uma segurança do ciberespaço mais forte e uma ciberdefesa mais eficaz;
- Através de exercícios, irão promover a partilha de experiências entre as organizações para, também assim, poder contribuir para a diminuição da vulnerabilidade dos sistemas de informação;
- É necessário estreitar a relação entre ambas as organizações, em especial nos planos estratégicos, tecnológico, sensibilização através de ações de formação e infraestruturas em matéria de cibersegurança e ciberdefesa.

Em jeito de conclusão, esta Resolução do Parlamento Europeu sobre a ciberdefesa e cibersegurança demonstra a fragilidade que existia à época nestes domínios e que se percecionava ser necessário colmatar através da

aposta numa estratégia clara e objetiva. Ao analisarmos esta resolução apercebemo-nos inexistência de uniformidade entre os Estado-Membros em relação às estratégias a adotar nestas áreas, pelo que para ser possível potenciar os seus efeitos e resultados, desde logo se assumiu a importância de buscar harmonizá-las para que todos os Estados-Membros da UE pudessem estar em sintonia.

Em primeiro lugar, Concluiu-se que era necessário “compartimentar” os ciberataques, ou seja criar-se “níveis” de acordo com seu grau de destruição, tipo de informação que foi alvo do ataque bem como a organização afetada.

Esta Resolução prioritizava ainda, para ser possível ambicionar um aumento da segurança no ciberespaço, a criação de instituições militares bem como de mecanismos de ciberdefesa que pudessem funcionar com base em relações de cooperação suscetíveis de serem estabelecidas com a UE e com os seus organismos.

Como último ponto abordado nessa proposta, destacava-se a necessidade de a UE não atuar sozinha mas sim com a ajuda, principalmente, dos EUA e da NATO - tanto no que se referia a ações de formação como de sensibilização, visto que são organizações mais experientes no âmbito do ciberespaço, bem como na execução de planos de emergência, gestão de análise de risco e exercícios nesse mesmo domínio.

5.2O que mudou na estratégia da UE desde 2013 até hoje?

2013 foi o primeiro grande ano do ciberespaço na União Europeia porque corresponde ao primeiro momento temporal em que a Comissão Europeia comunicou ao Parlamento Europeu, ao Conselho, ao Comité Económico e ao Comité das Regiões uma “Estratégia da União Europeia para a cibersegurança” com o objetivo de ter uma ciberespaço aberto, seguro e protegido.

Nesse plano estratégico eram sublinhados diversos objetivos (EU, 2013):

- Reduzir a cibercriminalidade:
    - ✓ Através da adoção por parte da UE e dos Estados-Membros de uma legislação rigorosa e eficaz. A Convenção de Budapeste (Conselho Europeu, 2001) fornece, na forma de tratado internacional vinculativo, as diretivas para a adoção de uma legislação nacional;
    - ✓ Em 2013, a UE já tinha adotado uma Diretiva (EU, 2011) relativa à luta contra a exploração sexual das crianças em linha e a pornografia infantil relativa à cibercriminalidade e também estava, à data, prestes a chegar a acordo sobre uma diretiva relativa a ataques contra os sistemas de informação, especialmente através da utilização de «botnets».
- Desenvolver as políticas e as capacidades de ciberdefesa no quadro da Política Comum de Segurança e Defesa (PCSD) (EU, 2013):
    - ✓ Desenvolver o quadro político da UE em matéria de ciberdefesa para proteger as redes no quadro das missões e operações da PCSD;
    - ✓ Desenvolvimento das capacidades e das tecnologias da UE nessa matéria;
    - ✓ Coordenação entre os atores civis e militares na UE;
    - ✓ Assegurar o diálogo com os parceiros internacionais (NATO e outras organizações internacionais).
- Desenvolver os recursos industriais e tecnológicos para a cibersegurança (EU, 2013):
    - ✓ Promover um mercado único dos produtos de cibersegurança para aumentar a cooperação e a transparência sobre a segurança dos produtos TIC;

- ✓ Em 2013 criação de uma plataforma público-privada sobre soluções dos Sistemas de Redes de Informação (SRI) para incentivar à adoção de soluções TIC seguras;
- ✓ Propor, em 2014, recomendações para garantir a cibersegurança em toda a cadeia de valor das TIC;
- ✓ Utilizar o programa Horizonte 2020, para desenvolver ferramentas de combate ao cibercrime e ciberterrorismo, para abordar diversos aspetos da privacidade e da segurança nas TIC.

- Definir uma política internacional em matéria de ciberespaço para a União Europeia (EU, 2013):
  - ✓ Se os conflitos armados se estenderem ao ciberespaço poderá aplicar-se o Direito Internacional Humanitário (DIH) e, se for caso disso, a legislação sobre os direitos do homem;
  - ✓ A Convenção de Budapeste é um instrumento aberto à adoção pelos países terceiros;
  - ✓ A UE continuará a apoiar os países menos desenvolvidos para que possam alargar o acesso à *internet* por partes das populações, mas sempre em segurança.

Neste documento são, igualmente, expostas as funções e responsabilidades dos Estados-Membros, da UE e das restantes organizações a nível internacional no âmbito do ciberespaço (EU, 2013).

Pelo que foi referido acima e para que os Estados-Membros consigam cumprir com as suas funções e responsabilidades e otimizem a coordenação entre os seus ministérios é crucial o papel setor privado principalmente ao nível da cibersegurança. Os Estados-Membros têm que envolver o seu setor privado, várias entidades responsáveis pelos diferentes níveis de cibersegurança, para otimizar a coordenação entre os ministérios. É fundamental criar uma estratégia nacional de cibersegurança em todos os

Estados-Membros e definir as responsabilidades das suas várias entidades nacionais. O Conceito Estratégico da Defesa Nacional foi, em Portugal, atualizado nesse mesmo ano de 2013, incluindo já nas suas preocupações e objetivos a cibersegurança (MDN, 2013).

Ao nível da UE existem diversas organizações que são responsáveis pela cibersegurança: a ENISA no campo da Segurança das Redes de Informação (SRI), a Europol na parte da repressão e a AED nas questões associadas à defesa. Apesar de existirem diversas organizações, elas colaboram entre si e apoiam os Estados-Membros no desenvolvimento da cibersegurança (EU, 2013).

Ao nível internacional, a Comissão Europeia com o apoio os seus Estados-Membros, apoia os restantes países no domínio da cibersegurança. Neste âmbito, verifica-se, igualmente, a existência de um diálogo político com diversas organizações internacionais como o Conselho da Europa, as Nações Unidas, a NATO, entre outras (EU, 2013).

Como conclusão, a Estratégia da União Europeia para a cibersegurança publicada em 2013 definia as ações necessárias por parte da UE para tornar o mundo do ciberespaço aberto, seguro e protegido. Merece destacar que esta estratégia assumia como crucial para a sua concretização a existência de parecerias com diversas organizações bem como o apoio por parte do setor privado e da sociedade civil (EU, 2013).

A nova reforma de cibersegurança (Conselho Europeu, 2019), revista no dia 28 de março de 2019 destaca, tal como o documento de 2013, que é necessário combater os aumentos das ciberameaças e ciberataques e aproveitar este novo mundo digital e as oportunidades que o mesmo possa oferecer (Conselho Europeu, 2019)

Essa reforma pretende promover o desenvolvimento de medidas estabelecidas em relação à cibersegurança, nomeadamente em matéria relativa à segurança das redes e da informação (Conselho Europeu, 2019).

Esta proposta contém três novas propostas (Conselho Europeu, 2019):

- Criação de uma agência de cibersegurança da UE mais forte;
- Introdução de um sistema de certificação da cibersegurança ao nível da UE;
- Implementação, assim que possível, da diretiva SRI (European Parliament, 2016).

Criação de uma agência de cibersegurança da UE mais forte

A Comissão Europeia criou uma agência para a sua cibersegurança com base na já existente (ENISA) para ajudar os Estados-Membros a lidar de forma mais eficiente com os ciberataques (Conselho Europeu, 2019). No dia 4 de Abril de 2019 foi publicada uma notícia no *website* oficial da ENISA, "ENISA *supports Portuguese National Exercise on Elections*" que demonstra o auxílio que a Reforma de Cibersegurança recentemente publicada pretende conceder aos países pertencentes à UE. Através de um pedido oficial por parte do *Portuguese National Cybersecurity Center* (PNCS), a ENISA, de forma imediata, propôs-se ajudar Portugal no *Portugal's National Cybersecurity Exercise* (ExNCS) providenciando uma *Cyber Exercise Platform* que oferece funcionalidades de controlo do exercício, diferentes cenários do mesmo e permite a simulação realista de *websites* da comunicação social igual aos da vida real (ENISA, 2019).

Introdução de um sistema de certificação da cibersegurança ao nível da UE

A introdução deste sistema tem como objetivo reduzir a divisão/fragmentação do mercado e aumentar a confiança de quem a ele recorre garantindo, desta forma, que as empresas dos Estados-Membros conseguirão efetuar trocas comerciais de forma mais segura e agilizada (Conselho Europeu, 2019). Esse sistema de certificação será adotado por todos os Estados-Membros que, nesse contexto, terão que seguir as regras

que naquele âmbito vierem a ser definidas, cumprir os requerimentos tecnológicos e os procedimentos associados (European Commission, 2018).

Implementação, assim que possível, da diretiva SRI

O Conselho Europeu introduziu, em 2016 (European Parliament, 2016), normas sobre a cibersegurança que são retomadas e consideradas no âmbito desta reforma. A diretiva das SRI obriga os Estados a adotar certos níveis de segurança, a designar autoridades nacionais competentes em matéria de cibersegurança, bem como a delinear uma estratégia para lidar com as ciberameaças com o objetivo de melhorar a cooperação entre os Estados Membros (Conselho Europeu, 2019).

A última medida que a UE adotou foi no dia 20 de fevereiro de 2019, quando anunciou o aumento da transparência nos negócios realizados por meio de plataformas em linha. Estas novas regras passam pela exposição de motivos por parte das plataformas caso queiram suspender ou pôr termo à utilização de um serviço. Assim, as plataformas deverão divulgar a classificação dos utilizadores empresariais assim como individuais. No caso destes últimos, tal está previsto para os casos em que se verifique a existência de qualquer tipo de tratamento diferenciado, nomeadamente através da doação de bens e/ou serviços. As plataformas terão, ainda, de criar um sistema interno para resolver as reclamações que são efetuadas. Para uma real noção do quanto as plataformas em linha são cruciais, torna-se relevante ter presente que mais de um milhão de empresas da UE realizam as suas trocas comerciais através de plataformas em linha e 60% do consumo privado também é feito com recurso a este tipo de plataformas (Conselho Europeu, 2019).

5.3 Organizações pertencentes à UE

Para conseguir assegurar este plano estratégico, a UE conta com o apoio crucial da ENISA, da Europol, da EC3 e da EDA, como atrás já referimos.

A ENISA, embora tendo sido criada em 2004, tem vindo a desenvolver-se ano após ano, trabalhando com os Estados-Membros e também em parceria com o setor privado ao nível de ciberexercícios, de apoio à construção de estratégias de cibersegurança coesas e eficazes por parte dos Estados-Membros e também de aconselhamento no domínio da cibersegurança a organizações como a *Computer Security Incident Response Team* (CSIRT). A ENISA tem como missão entender o ciberespaço e dar resposta aos problemas relacionados com a sua segurança. Não existe qualquer tipo de capacidade operacional por parte da mesma pois para isso existem outras organizações como a Europol (Balão, 2014). O objetivo fundamental desta Agência é desenvolver políticas e estratégias no âmbito do ciberespaço da UE, bem como melhorar as capacidades tecnológicas para que se possa proteger os sistemas de informação de uma forma mais eficaz e que se identifique melhor as ciberameaças (ENISA, 2017).

O EC3 é uma agência mais recente que a ENISA pois só foi criada, através da Europol, em 2013 e com o objetivo não de criar políticas para resolver incidentes como sucede com a ENISA, mas de desenvolver leis no âmbito do cibercrime para que a UE consiga salvaguardar os seus Estados-Membros em geral e as respetivas empresas em particular, pois hoje em dia a maior percentagem de negócios são realizadas *online*. Neste sentido, a estratégia de atuação do EC3 é relativamente simples: possui duas equipas, uma das quais sensibiliza os Estados-Membros através de ações de formação e define medidas de prevenção, enquanto a outra está apenas dedicada ao desenvolvimento de políticas com o objetivo de que as mesmas venham a ser futuramente aplicadas com o objetivo de reduzir a cibercriminalidade. Para simplificar o seu trabalho, o EC3 divide, ao nível operacional, os cibercrimes em: crimes cometidos por criminosos - com o objetivos de enriquecer e obter grandes lucros, como é o caso da exploração sexual infantil que foi a primeira diretiva de sempre emitida pela UE no âmbito do ciberespaço, e em que existe vítimas afetadas a nível psicológico –, e crimes que tentam retirar informação crucial de um Estado ou organização através de ciberataques. Para este último tipo de crimes, a EC3 conta com uma divisão que lhes é inteiramente dedicada.

Em caso de crimes de maior dimensão, que afetem vários Estados a nível mundial, a Europol criou em 2014 a *Joint Cybercrime Actions Taskforce* (J-CAT). Este EC3, apesar de estar sob a alçada da Europol regendo-se pelas suas políticas pode também apoiar os Estados-Membros em investigações (Europol, 2017).

Por último, a EDA é uma agência que coopera com instituições militares de forma a criar mecanismos de ciberdefesa. Após um estudo desenvolvido em 2013 chegou-se à conclusão que a UE era muito frágil em matéria de ciberespaço e que tinha que criar ciber-capacidades para aumentar a sua ciberdefesa militar - que necessitava de desenvolvimento quer ao nível da UE quer ao nível dos Estados-Membros individualmente considerados. A EDA, no que toca à UE, pretende que a mesma cimente a relação com a NATO no que diz respeito à ciberdefesa, nomeadamente com a criação de equipas de *intelligence* para melhor assegurar a proteção dos seus SRI e uma resposta rápida a qualquer ciberataque. Nesse contexto, ao nível nacional, a EDA apoia os Estados Membros em ciberexercícios e em mecanismos de partilha de informação no âmbito da ciberdefesa (EDA, 2013).

Privados ou Parcerias Público-Privadas

Neste Capítulo abordaremos o papel das parcerias público-privadas (PPPs) no mundo do ciberespaço. Começaremos por definir o que é uma PPP e apresentar os resultados do primeiro estudo sobre a sua relevância no contexto do ciberespaço, que foi levado a cabo pela ENISA em 2011.

Depois, analisaremos a primeira parceria público-privada Pan-Europeia, a *European Public-Private Partnership for Resilience* (EP3R), nomeadamente no que se refere ao seu contributo para aprofundar a cibersegurança europeia.

Em seguida, falar-se-á do contrato que a Comissão Europeia assinou em 2016 com as *contractual public-private partnerships* (cPPP) e os melhoramentos no âmbito da cibersegurança que daí advieram, bem como o porquê da UE estabelecer PPPs e quais os seus objetivos.

Por último iremos analisar os quatro tipos de PPPs que existem, o seu papel na ajuda aos Estados-Membros bem como as suas diferenças.

6.1 As PPPs no domínio da Cibersegurança

Para além de todas as estratégias que a UE possa implementar para enfrentar os riscos e problemas da cibersegurança é necessário que se verifique, igualmente, a colaboração, cooperação e articulação entre organizações. Nesse sentido, assume-se que a melhor maneira de se evoluir no campo da cibersegurança não é só existir uma colaboração e partilha de informações entre as partes interessadas mas, também, a criação de parcerias público-privadas (ENISA, 2011).

Uma PPP constitui um acordo mútuo entre dois ou mais setores dos domínios público e privado que colaboram/cooperam numa determinada área, neste caso no mundo do ciberespaço em particular na sua cibersegurança (ENISA, 2011).

A estratégia de cibersegurança da UE dá importância à criação de PPP para o aumento da confiança por parte dos Estados Membros (ENISA, 2011).

Em 2011, a ENISA realizou um estudo sobre as PPPs, com o objetivo de reunir informações sobre as mesmas a partir das suas aprendizagens e experiências. Os resultados deste estudo da ENISA foram apresentados sob a forma de um relatório disponibilizado no seu *website*, constituindo este o primeiro relato desse estudo, e a partir do qual se definiu a fase inicial de um possível projeto de pesquisa para se estudar "modelos cooperativos para parcerias públicas privadas efetivas" (Dupré, Falessi, & Liveri, 2011).

O facto é que a *Critical Information Infrastructure Protection* (CIIP) é uma parte vital da segurança nacional. Grande parte das infraestruturas críticas dos Estados-Membros são, em simultâneo, reguladas pela indústria. Logo, a indústria e o governo têm que trabalhar em conjunto para garantirr a segurança e a resiliência dessas mesmas infrastruturas críticas. No referido relatório é apresentada uma lista de questões que as PPP equacionam e às quais tiveram que dar resposta, razão pela qual assume particular relevância a disponibilidade de conhecimento sobre as decisões tomadas e o *benchmarking* dali resultante. De facto, no relatório são incluídas 36 recomendações sobre como constituir PPPs com sucesso para a segurança dos Estados-Membros e das quais optamos por destacar a 11ª recomendação: "*National PPPs should look closely at the benefits of becoming members of an organization, which represents their wider geographic/economic interests in relation to CIIP and who could facilitate the creation of an interface with other parts of the world. For example in Europe this could be the European Public Private Partnership for Resilience (EP3R)*". (ENISA, 2011, p. 26).

6.2 O impacto da EP3R na União Europeia

A *European Public-Private Partnership for Resilience* (EP3R) foi criada em 2009 e foi a primeira tentativa a nível pan-europeu de utilizar uma PPP para abordar questões de segurança e resiliência nos sectores das telecomunicações. Em 2013 a EP3R acaba, após 4 anos de existência e 3

anos de operações (2010-2013). Em novembro de 2014 a ENISA lançou um relatório escirto por Lionel Dupré sobre o impacto da primeira parceria público-privada europeia para a resiliência dos Estados-Membros, bem como lições que deviam ser aprendidas antes de delinear futuras iniciativas do mesmo teor. Esse relatório aborda os benefícios das PPP, sendo referido que antes da sua existência se verificava existir uma lacuna na segurança e resiliência da referida indústria e que as PPPs poderiam ser uma solução para colmatar esses problemas (Dupré, 2014).

Os principais objetivos das PPPs com a indústria do setor das comunicações e das tecnologias de informação são (Dupré, 2014):

- Melhorar a definição dos objetivos entre as autoridades públicas e o setor privado;
- Maior confiança entre os participantes do lado público e privado;
- Abordagem partilhada para obter resultados comuns para um determinado esforço;
- Método eficaz para conseguir uma poupança de custos a curto, médio e longo prazo.

Nesse mesmo relatório apurou-se que a vantagem mais relevante de uma abordagem por parte de uma PPP é a oportunidade de trocar informações, conhecimentos, conhecimentos especializados, boas práticas e o *networking* (Dupré, 2014).

Em 2014 já havia vários exemplos da efetividade das PPPs no setor das telecomunicações e de tecnologia de informação a nível nacional. Alguns casos de sucesso foram (Dupré, 2014):

- A *Superfast Cornwall Project* no Reino Unido;
- A *Asturcorn10* em Espanha;
- A *Auvergne Region11* em França através de *outsourcing*.

6.3 A criação da cPPP e objetivos das PPPs

Em 2011, a ENISA já tinha elaborado um documento de boas práticas sobre os Modelos Cooperativos para uma PPP eficaz. Esse estudo também forneceu informações sobre com configurar e executrar um PPP. Passado seis anos a ENISA achou oportuno voltar ao tema das PPPs e analisar o seu estado na UE. O estudo identifica os principais modelos de colaboração, os desafios atuais que tanto os privados e o setor público enfrentam, o processo de criação e desenvolvimento das PPPs e fornece recomendações para o desenvolvimento das PPPs na Europa. Este estudo abrange todos os tipos de cooperação e colaboração entre entidades públicas e privadas no domínio da cibersegurança (ENISA, 2017).

A 5 de julho de 2016 a Comissão Europeia e a *European Cyber Security Organisation* (ECSO), como parte da estratégia de cibersegurança na eu, assinaram o *contractual Public-Private Partnerships* (cPPP). O objetivo da parceria era fomentar a cooperação entre o setor público e privado nas fases iniciais do processo de investigação e inovação, a fim de permitir que os cidadãos Europeus tivessem acesso a soluções europeias inovadoras e fiáveis (produtos, serviços e software TIC) garantindo, desde logo, que tais soluções têm em consideração direitos fundamentais do Homem, como o direito à privacidade (ECS, [s.d]).

Essa parceria visa também estimular o setor da cibersegurança, ajudando os setores onde é importante assegurar soluções de cibersegurança (por exemplo setores como energia, saúde, transporte, finanças) (ECS, [s.d]).

O cPPP assumiu, assim, um papel fundamental na estruturação e coordenação de recursos industriais de segurança digital na Europa. Incluiu uma vasta gama de intervenientes, desde pequenas e médias empresas inovadoras até produtores de componentes e equipamentos, operadores de infraestruturas críticas e institutos de investigação, reunidos sob a responsabilidade da ECSO. A UE investiu quase quatrocentos e cinquenta milhões de euros nesta parceria, ao abrigo do seu programa de investigação e inovação Horizonte 2020, que é o maior programa de investigação e inovação

da UE (com início em 2014 e conclusão em 2020). No entanto, esperava-se à data, que os intervenientes no mercado de cibersegurança investissem três vezes mais (ECS, [s.d]).

O principal objetivo do ECSO é apoiar todos os tipos de iniciativas e projetos que visam desenvolver, promover, incentivar a cibersegurança europeia e, em particular (ECS, [s.d]):

- Fomentar e proteger das ciberameaças o crescimento do Mercado Único Digital Europeu;
- Desenvolver o mercado de cibersegurança na Europa e o crescimento duma indústria competitiva de cibersegurança e TIC;
- Desenvolver e implementar soluções de cibersegurança certas etapas críticas, em aplicações sectoriais em que a Europa é líder.

Em 2017, a ENISA realizou um estudo sobre modelos cooperativos para as PPPs que agrupam informações sobre as melhores práticas e abordagens comuns. Esta investigação analisou o estatuto das PPPs na UE àquela data, os desafios que, entretanto, tanto o sector privado como o setor público enfrentam no processo de criação e desenvolvimento das PPPs e as recomendações para o seu desenvolvimento na Europa. Os principais objetivos desse estudo foram (ENISA, 2017):

- Fornecer informações sobre as PPPs na Europa através da recolha de informações e da análise do estatuto actual das PPPs para identificar os principais modelos deste tipo de colaboração;
- Identificar os desafios actuais que tanto o sector privado como o setor público enfrentam no processo de criação e desenvolvimento das PPPs;
- Formular e propor recomendações para o desenvolvimento das PPPs na Europa.

É importante não esquecer, neste contexto, que um dos principais objetivos da Estratégia Nacional de Cibersegurança Europeia é a aposta na colaboração para aumentar a cibersegurança em diferentes âmbitos como, por

exemplo, informações sobre possíveis ameaças e aumento da sensibilização através da *Informations Sharing and Analysis Centers* (ISAC) e das PPP. Em 2017, a ENISA voltou a elaborar outro estudo sobre os Modelos de Cooperativos para as PPP e sobre as ISACs (ENISA, 2017).

A confiança entre as entidades público-privadas, apenas privadas ou apenas públicas sempre foi díficil e é considerado como um dos maiores desafios das PPPs. Qualquer processo de confiança define-se de forma contínua e pode ser destruído especialmente se houver a entrada de novos membros ou se os membros não forem suficientemente ativos no âmbito dessa parceria e se estiverem "a aproveitar" dos serviços que essa PPP oferece sem contruirbuir com os deveres que foram estabelecidos (ENISA, 2017).

São várias as razões que justificam a importância associada à criação de PPPs (ENISA,2017):

- Intersses económicos: Esta é uma das razões mais fortes para estabelecer uma PPP na UE e a principal motivação para o setor privado entrar na parceria. Pode ser através da vontade de estabelecer um organismo que ajude a identificar as barreiras para o crescimento da indústria de cibersegurança e criar as condições para exportar os seus produtos. Também poderia ser porque a indústria precisa de cooperação com o setor público como, por exemplo, o setor financeiro no campo da luta contra o cibercrime;
- Requisitos regulamentares: As PPPs são criadas tal e qual como uma lei específica. A administração decide que uma PPP será a melhor maneira fazer um determinado papel e entre em acordo com o setor privado para dar-se ínicio a uma parceria. Os requisitos também podem incluir uma lei específica para as PPPs, que fornecem um quadro claro para a cooperação e colaboração público-privada. Estas leis são criadas, normalmente, com o objectivo de estimular a economia, mas devido ao crescente aumento da importância da cibersegurança

têm vindo a tornar-se, cada vez mais, uma questão pertinente na agenda política;

- Relações Públicas: Neste caso, o Governo permite que o setor privado contribua para a nova legislação O governo e as PPPs trabalham também em conjunto para desenvolver uma estratégia nacional de cibersegurança. Para o setor privado, a motivação está no trabalho que desenvolve com o Governo e com outras entidades privadas, com as quais compartilham conhecimento;
- Interesses sociais: Para a indústria, é crucial promover a cibersegurança em geral, para que o mercado possa evoluir sem interrupção. Geralmente existe mais do que apenas um motivo para se criar uma PPP. Os motivos mais comuns associados à criação de uma PPP surgem associados a interesses económicos e sociais que são acompanhados por um novo regulamento. Isso requer troca de informações e cooperação entre entidades públicas e privadas;
- Outras razões: Nesta categoria, os especialistas destacam, nomeadamente, os novos regulamentos da UE (a Directiva NIS e o Regulamento Geral de Protecção de Dados), que impõem novas exigências por parte do setor privado. Por esta razão, os governos dos Estados-Membros podem decidir criar uma PPP para ajudar a indústria a implementar os novos regulamentos.

Existe um objetivo comum para a participação das PPPs, tanto do setor privado quanto do público: aumentar o nível de cibersegurança. No entanto, existem também outras motivações como mostra a seguinte tabela:

Tabela 2 - Motivação para a participação das PPP

PRIVATE SECTOR REASONS TO PARTICIPATE IN A PPP	PUBLIC SECTOR REASONS TO PARTICIPATE IN A PPP
Access to public funds	Better understanding of Critical Infrastructure Information Protection (CIIP) and industry in general
Opportunity to influence national legislation and obligatory standards	Possibility to create synergies between different initiatives of private sector
Access to public sector knowledge and confidential information (EU legislation, fighting cybercrime)	Access to private sector resources (e.g. valuable experts), which makes it is easier to set up standards and good practices
Assurance that the products delivered through PPP are of good quality, as it is guaranteed by the government	
Sharing knowledge, experiences and good practices	
Helping to achieve resilience in the cyber ecosystem	
Increase the trust between public-public, private-private and public-private – PPP allows to meet different people and get to know them; because of that, it allows to have better information and proactive attitude in case of crisis	
Getting direct and credible contacts with other organisations	

Fonte: (ENISA, 2017)

As PPPs podem oferecer diversos serviços aos Estados-Membros. É o caso da *Cyber Securtiy Platform* (CSP) na Áustria que desenvolve linhas orientadoras sobre a cibersegurança e destina-se a promover a partilha de conhecimentos e informações entre a administração pública e os operadores das infraestruturas críticas. A CSP define também o trabalho conjunto entre os operadores da infraestrutura crítica e o setor público que desenvolve normas de segurança com vista à implementação da diretiva da *Network and Information Security* (NIS) (European Parliament, 2016). Podemos invocar, também, o caso do *Informations System Authority* na Estónia que providencia avisos sobre ciberameaças, oferece formação para entidades de setor privado, ajuda na triagem dos seus parceiros, elabora planos de resiliência para o seu país, oferece *benchmarking* das suas infraestruturas críticas aos seus operadores, desenvolve estatísticas sobre os incidentes no ciberespaço, de entre outras contribuições (Andersen, Cao, Tvarnø, & Wang, 2010).

6.4 Os diferentes modelos de PPPs que existem atualmente

6.4.1 PPPs orientadas para um só objetivo

A partir do momento em que a cibersegurança passou a ser entendida como um objetivo distinto e específico da economia que precisa de apoio suplementar e interesse do Governo são criados certos tipos de PPPs com determinados objetivos. Estes tipos de PPPs focam-se em soluções a nível estratégico de forma a apoiar o mercado das Tecnologias de Informação e criar uma estrutura capaz de desenvolver a cibersegurança no país. De Estado para Estado, as PPPs têm diferentes objetivos e metas e as suas especificações advêm das diferenças culturais dos Estados-Membros. Muitas vezes os Estados-Membros têm os mesmos objetivos, muito embora os mesmos sejam alcançados através de diferentes abordagens (Bank, 2012).

Embora existam diversos exemplos de PPPs, iremos analisar em pormenor as CSP na Áustria e a *Cyber Security Commission* (CSC) na Eslováquia por serem por um lado como o caso da CSP ser uma PPP inovadora à data da sua criação e a CSC por contribuir em grande escala para o plano estratégico do Estado Esloveno (ENISA, 2017).

A CSP foi criada em 2011 quando o governo austríaco se apercebeu que a cibersegurança era uma questão muito importante. Esta CSP foi a primeira a implementar uma estratégia de cibersegurança nacional. Verificou-se, nesse contexto, existirem relações de cooperação em que estiveram envolvidos os diversos setores contributivos para as infraestruturas críticas e que participaram na elaboração da lei de cibersegurança. Esta iniciativa constituiu uma nova abordagem do Governo austríaco, uma vez que até esse momento, geralmente era o próprio Governo que instruía a indústria sobre como proceder (ENISA, 2017).

A CSC, por sua vez, foi criada em 2016 pelo Conceito e Plano de Ação de Cibersegurança Eslovaca. O CSC é um órgão consultivo do Diretor da Autoridade Nacional de Segurança. É uma plataforma criada sob o governo da

National Security Agency (NSA) eslovaca e resulta do contributo conjunto de representantes do setor público e do setor privado sob a forma de uma plataforma de segurança eficiente e eficaz, que apoia o diretor da NSA na sequência da prévia discussão política das questões estratégicas, contribuindo para o plano estratégico do Estado (ENISA, 2017).

A CSC, tal como a CSP e as PPPs deste género têm um papel bastante ativo no fornecimento de orientação estratégica e na consulta aos seus governos sobre (ENISA, 2017):

- Ideias de inovação sobre a estratégia de cibersegurança;
- Fornecimento de conhecimento, orientação e recomendação para a criação de novas leis;
- Apoio no desenvolvimento da indústria de cibersegurança.

Assim, as PPPs envolvem diferentes partes interessadas:

- As indústrias de cibersegurança: estão incluídas empresas de cibersegurança, de TI e operadores de infraestruturas críticas;
- Governo: conforme as suas necessidades cria uma PPP para uma cooperação mútua de forma a atingir os seus objetivos;
- Parte académia: tem como papel criar e desenvolver soluções juntamente com o Governo e a indústrias de forma a mitigar os problemas da cibersegurança.

6.4.2 Outsourcing cybersecurity services

Outro papel fundamental das PPPs é o *Outsourcing Cybersecurity Services* (OSC). Este tipo de PPPs aparecem quando o Governo reconhece as necessidades da indústrias mas através dos seus meios não consegue colmatar essas lacunas. Neste caso, a PPP é uma organização autónoma que pode oferecer os seus serviços a um terceiro, neste caso o Governo, atendendo às necessidades. Por exemplo, pode apoiar o Governo na criação de políticas como a implementação da *Network and Information Security* (NIS)

ou de estratégias nacionais de cibersegurança. A principal função do OSC é aumentar a consciencialização sobre a cibersegurança e o nível da mesma, tanto por parte do Governo como das empresas (ENISA, 2017).

A ENISA elaborou, em 2017, um estudo sobre diversas empresas que praticavam OSC. Uma das empresas era a *Kuratorium Sicheres Österreich* (KSO) que está sediada na Áustria. Foi criada em 1975 e era uma associação privada mas financiada pelo governo austríaco. Mais recentemente, em 2010, tornou-se uma organização independente com estreitas relações com Estado. Em 2011 foi quando a KSO, que até aí estava focada na segurança nacional e física, passou a cooperar com o Ministério do Interior para um aumento da cibersegurança. O objetivo principal era aumentar a consciência da população nesse domínio. O conhecimento e a experiência desta organização foi usada para elaborar a Estratégia Nacional de Cibersegurança e atualmente contribui para a elaboração da lei de cibersegurança. Em 2015, a KSO criou o "Fórum de Cibersegurança" onde se discutem novas e melhores práticas e desafios nesse âmbito. Em 2018 o Fórum foi transformado numa "Segurança Digital da Plataforma de Segurança" para incluir mais empresas do setor privado (ENISA, 2017).

Os OSC estão particularmente relacionados com a proteção da infraestrutura crítica, oferecendo suporte para essa infraestrutura para aumentar o nível de cibersegurança em setores críticos (ENISA, 2017).

Todos os sectores de infraestruturas críticas estão envolvidos nas PPPs do OCS juntamente com instituições governamentais, tais como autoridades nacionais competentes e agências de cibersegurança. Esse trabalho em conjunto cria condições para troca de conhecimento e desenvolvimento de possíveis soluções para novos desafios (ENISA, 2017).

Na Áustria, este tipo de organizações que têm iniciativas de cibersegurança como é o caso da KSO não pagam qualquer imposto ao Estado, isto para promover a evolução da ciberdefesa. Este tipo de PPPs são extremamente importantes ao avisar os governos para a criação de novas, ou alterar as existentes, leis e políticas sobre o ciberespaço (ENISA, 2017).

6.4.3 PPPs Institucionais

Este tipo de PPPs são direcionadas para as instituições públicas que a elas recorrem em questões relacionadas com a proteção de infraestruturas críticas. Estes tipos de PPPs são chamadas a intervir em tarefas críticas como gestão de crises ou atos de emergência. Isso obriga o setor público a ser mais sensível às necessidades e desafios do setor privado. Sendo a PPP designada para proteger a infraestrutura crítica, as instituições públicas são obrigadas a estabelecer uma cooperação forte e eficiente com o setor privado para atender às suas necessidades. Dois exemplos de PPPs institucionais são o *Information System Authority* (*Riigi Infosusteemi Amet*, RIA) na Estónia e o *Government's Centre for Security* (*Rządowe Centrum Bezpieczeństwa*, RCB) na Polónia (ENISA, 2017).

A RIA, criada em 2011, é responsável pela cibersegurança nacional e pela supervisão dos sistemas de informação usados pelo Estado para fornecer serviços vitais e cibersegurança a nível nacional. A própria CERT da Estónia faz parte da RIA (ENISA, 2017).

O RCB, por sua vez, é uma instituição governamental e é responsável pela gestão e proteção de infraestruturas na Polónia em alturas de crise (ENISA, 2017).

Estes tipos de PPPs institucionais tendem a ser muito dependentes. O seu forte compromisso determina o seu sucesso e o nível de cooperação com o setor privado. Estas PPPs ajudam a aumentar a cibersegurança e a implementação de requisitos regulatórios como, por exemplo, recomendações desenvolvidas em conjunto pelo governo e pela organização. Também são cruciais no apoio para estabelecer uma rede eficaz em alturas de emergência/crise. As PPPs institucionais podem fornecer vários serviços dos quais se destacam, regulamento de boas práticas, planeamento estratégico, aumento da resiliência e troca de conhecimento (ENISA, 2017).

As PPPs institucionais envolvem muitas organizações do setor público e privado. Por parte da indústria, todos os setores considerados críticos estão

envolvidos como é o caso da energia, abastecimento e distribuição de água potável, saúde, infraestruturas, transportes, distribuição, entre outros. Existem uns setores em que as PPPs são mais importantes que noutros, como é o caso do setor energético e financeiro que está sujeito a inúmeras ciberameaças e é importante que reconheça a cibersegurança como uma prioridade de elevada relevância, razão pela qual estão usualmente dispostos a participar em qualquer tipo de atividade relacionada com o ciberespaço (ENISA, 2017).

As PPPs estão também envolvidas com a Administração Pública como é o caso das *National Competent Authorities* (NCAs) que se encarrega de setores críticos e que suportas as PPPs providenciando regulação e recomendações especiais para aumentar o nível de cibersegurança. Essas recomendações também são desenvolvidas através de uma cooperação público-privada. As agências de cibersegurança contribuem, igualmente, com conhecimento nessa área para as PPPs, tal como as agências que aplicam as leis a elas estão diretamente ligadas para que possam operar estando melhor protegidas contra o cibercrime (ENISA, 2017).

Nas PPPs institucionais é o setor privado que toma as decisões estratégicas, contudo são financiadas pelo setor público e geralmente são parcerias de longo prazo (2-3 anos) (ENISA, 2017).

6.4.4 PPPs Híbridas

A PPP híbrida é, na verdade, uma combinação do OSC e das PPPs institucionais. Este tipo de PPPs cria-se quando o governo não dispõe de recursos suficientes para fornecer as soluções de cibersegurança necessárias a nível nacional e inicia uma cooperação com uma entidade privada que possui o conhecimento adequado e pode fornecer essas soluções. As PPPs híbridas estão fortemente ligadas à prestação de serviços de CSIRT (ENISA, 2017).

Dois exemplos de PPPs híbridas são o caso do *Governmental* CERT na Áustria e o CSIRT.CZ *national* CERT na República Checa (ENISA, 2017).

As atividades principais das organizações são os serviços de CSIRT nacionais e governamentais. Além disso, este tipo de PPPs híbridas trabalham para um aumento da consciencialização dos Estados sobre a cibersegurança e apoiam as autoridades policiais na investigação do cibercrime. Estas equipas CSIRTs, na UE, são usualmente usadas para proteger o ciberespaço de instituições governamentais como é o caso das infraestruturas críticas, bem como para garantir a gestão do cibercrime (ENISA, 2017).

Estas PPPs, ao contrário das anteriores, são financiadas por uma organização e não pelo governo. A organização que financia pode assim participar nessa PPP sem custos adicionais. A par das PPPs institucionais, estas parcerias são enlaces de longo prazo com o objetivo de aumentar o nível de cibersegurança, participando na elaboração da regulamentação da diretiva NIS bem como de estudos sobre incidentes relacionados com o ciberespaço e apresentação de posteriores medidas de resolução (ENISA, 2017).

6.4.5 Visão global da inclusão das PPPs na Europa

Um dos maiores desafios associado à existência das PPPs é a criação de confiança entre entidades público-privadas, privadas-privadas e públicas-públicas. A maioria dos PPPs tem a visão de que o ganho da confiança é um processo contínuo, que envolve relações pessoais e pode demorar algum tempo. A confiança numa PPP nem sempre é contínua e na maioria das vezes não é estável, o que pode não ser positivo para a cibersegurança (ENISA, 2017).

Existem vários mecanismos que fazem aumentar a confiança nas PPPs sendo que aqueles que são considerados como mais eficazes são (ENISA, 2017):

- Encontros presenciais: interação considerada ideal para a troca de informações entre parceiros pois o meio de coordenação é ‘cara a cara’;

- Reuniões regulares: através da regularidade de encontros o compromisso por parte dos membros aumenta
- . Eventos sociais: fundamental para a construção de laços entre os membros da parceria e para se conhecerem mutuamente.

As PPPs com alto nível de confiança são obviamente mais eficientes, visto que reconhecem as necessidades dos setores público e privado e são capazes de resolvê-las através da cooperação (ENISA, 2017).

Desde 2011, um maior número de Estados-Membros tem investido na colaboração para melhorar a cibersegurança nacional. Em 2011 a ENISA elaborou o *Good Practice Guide* (GPG), que explicava como criar uma parceria, fornecendo informação e orientação para formalizar essas parcerias (Dupré, Falessi, & Liveri, , 2011). Em 2011, apenas 12 Estados-Membros possuíam uma estratégia nacional sobre cibersegurança enquanto hoje em dia já todos possuem uma estratégia nacional nesse domínio. No campo das PPPs, entre 2011 e 2018 verificou-se um aumento no número de Estados-Membros a desenvolverem uma PPP oficial (15) (Dupré, Falessi, & Liveri, , 2011). Em muitos casos, as parcerias são criadas para realizar um projeto específico: por exemplo, um exercício nacional de cibersegurança ou uma campanha de sensibilização sobre cibersegurança (Mês Europeu da Cibersegurança) (Dupré, Falessi, & Liveri, , 2011).

O cenário da cibersegurança é muito volátil e passou por muitas mudanças nos últimos anos. Se as organizações acompanharem de maneira correta essas mudanças, as PPPs poderiam ser uma mais-valia para o aumento da cibersegurança europeia.

Análise Crítica

Este Capítulo visa analisar de forma construtiva o percurso das PPPs no que toca à regulamentação das Políticas Europeias de Segurança no Ciberespaço. Numa primeira abordagem iremos analisar os desafios que enfrentam atualmente seguindo-se algumas recomendações para uma PPP mas efetiva (ENISA, 2017).

7.1 Desafios que as PPPs enfrentam

As PPPs apesar de serem fundamental para a sustentação das Políticas de Segurança Europeia no Ciberespaço enfrentam alguns desafios (ENISA, 2017):

Falta de recursos humanos no setor público e privado

Um dos maiores desafios das PPPs é a falta de recursos humanos para dar continuidade ao seu desenvolvimento e evolução. As PPPs em alguns Estados-Membros ainda não são vistas como uma prioridade, logo o Governo por norma não envolve um número suficiente de pessoas no projeto. Esta é uma das causas para que algumas PPPs não sejam tão eficazes quanto poderiam ser (ENISA, 2017).

O orçamento e os recursos por parte do setor público estão abaixo das expectativas esperadas pelo setor privado

Este desafio não se aplica só as PPPs. Os recursos que o setor privado necessita têm que ser primariamente identificados, tal como o respetivo orçamento a ser afeto (ENISA, 2017).

Uma vez que parece verificar-se uma tendência generalizada para uma evidente desorçamentação em múltiplos setores (alguns deles críticos), esta falha por parte do setor público (por exemplo, o governo) é um dos principais desafios das PPPs contribuindo, também, para diminuir a confiança por parte dos privados (ENISA, 2017).

O estabelecimento de um nível comum de entendimento e diálogo entre os setores público e privado

O setor privado é muito distinto do setor público e por vezes não há um entendimento claro entre as duas partes. Existem dificuldades em criar uma linguagem comum para se comunicar quando estes setores estabelecem uma parceria pois diferentes organizações usam diferentes linguagens. Por vezes, surgem mal entendidos entre as diferentes organizações e torna-se muitas vezes difícil de resolver. A cultura organizacional de Empresas/Organizações do setor privado tende a ser significativamente diferente de um governo, pelo que também na identificação do que é estratégico, operacional ou técnico se pode verificar haver ambiguidade (ENISA, 2017).

Incluir o conceito de PPP nas PME

As PMEs não possuem, usualmente, recursos nem experiência para participar em PPPs. No entanto, considera-se relevante encorajar as PMEs a participar nessas parcerias, por exemplo através da concessão de incentivos financeiros, pois seria benéfico para as mesmas uma vez que ganhariam experiência nesse campo e estar-se-ia a promover a participação de importantes 'franjas' da sociedade num problema de interesse nacional (ENISA, 2017).

Falta de liderança

A hesitação por parte do setor privado em assumir a liderança da parceria e o desinteresse do governo em algumas fases de edificação e concretização da mesma desencoraja os privados na participação numa PPP. Além disso, as instituições públicas entram, muitas vezes e sucessivamente em desacordo, o que conduz ao atraso na tomada de decisões e a um descontentamento e desmotivação por parte do setor privado porque tem que esperar sempre pelo governo para agir. O ideal nestas situações poderia ser a elaboração de um acordo por escrito onde cada parte envolvida na parceria conhecesse exatamente e de forma inequívoca o seu papel e responsabilidades (ENISA, 2017).

7.2 Recomendações para uma melhor efetividade das PPPs

Para se conseguir uma melhor efetividade das PPPs há algumas considerações e recomendações que seria relevante tomar em consideração (ENISA, 2017).

1ª Recomendação: Ao estabelecer-se uma PPP a prioridade deverá ser a motivação do setor privado

Nos diferentes tipos de modelos de PPPs que analisamos, bem como nos exemplos que foram dados, para criar uma PPP bem-sucedida e eficiente é necessário garantir estarem reunidos os recursos de que o setor privado necessita para trabalhar. Este tipo de cooperação não será 100% se apenas se fornecer dinheiro e incentivos. Para uma PPPs ser bem-sucedida é necessário que se possa contar, também, com os recursos humanos. É vital que exista um conjunto de pessoas que possa levar a cabo de forma eficiente as suas tarefas de modo a assegurar a eficácia sob a forma dos resultados esperados (e necessários). Uma PPP precisa de alguém que interaja com os restantes membros da parceria, marque as reuniões necessárias com vista a manter a perspetiva estratégica, prepare planos de ação e que trabalhe tanto com as organizações privadas como com a administração pública (ENISA, 2017).

As PPPs mais bem-sucedidas são geralmente as *Non-Governmental Organisations* (NGOs) ou instituições que são apenas criadas para fortalecer a cooperação e colaboração entre os setores público e privados (ENISA, 2017).

2ª Recomendação: Os participantes devem concordar com base num documento jurídico ao criar um PPP

Enquanto não houver um documento jurídico que possa regular os termos da cooperação entre o setor público e o setor privado, todo o processo de criação e desenvolvimento de uma PPP será lento e pouco eficiente e irá sempre levar ao descontentamento por parte do setor privado. Esse documento jurídico pode ser, por exemplo, um Memorando de Entendimento entre ambas as partes. A cibersegurança é uma área em que muitas entidades públicas são geralmente envolvidas em conjunto com várias empresas privadas. Devido a este facto, é fundamental haver regras específicas aplicáveis a todas as partes

– deve-se estabelecer um quadro de toda a cooperação, e cada membro deve saber que tipo de informação deve fornecer e que tipo de benefícios pode esperar dessa PPP.

3ª Recomendação: As instituições públicas devem liderar a PPP

É desanimador para o setor privado que por vezes haja desacordo entre as principiais instituições públicas. É o governo que tem que atuar nestes casos. Se o setor público pudesse concordar com o contrato da PPP, iria ser benéfico para essa parceria.

Como a cibersegurança é altamente interdisciplinar baseando-se em várias áreas, há bastantes órgãos de cariz público envolvidos na PPP como o Ministério da Economia, da Defesa, do Mar e do Ambiente, dos Assuntos Internos entre outros dependendo da parceria estabelecida. Para que haja esse envolvimento é crucial que a Administração Pública comunique de forma clara e objetiva as suas necessidades bem como as suas limitações, quer sejam a nível financeiro ou logístico, ao setor privado. Antes de se estabelecer qualquer parceria, o setor público, que é quem inicia o contacto, tem que definir de forma exata qual é o seu objetivo, o que quer alcançar com uma possível parceria e qual o contributo do setor privado. Por outras palavras, tem que definir a sua estratégia antes mesmo de iniciar a parceria.

4ª Recomendação: As PPPs devem investir numa colaboração interna privado-privado e pública-pública

A PPP trata da cooperação privado-privado, público-público e privado-público. Quando a parceria se foca apenas nos relacionamentos entre o setor público e o setor privado, tal pode revelar-se insuficiente para criar uma política eficaz. É necessário haver um diálogo e um entendimento entre as agências públicas pois por vezes é fundamental para o sucesso da parceria. O mesmo se aplica ao setor privado. Uma PPP bem-sucedida integra não apenas a administração privada e indústria, mas também diferentes entidades da indústria (por exemplo, empresas de energia, bancos, telecomunicações). Por esta razão, seria relevante que as PPPs em toda a UE pudessem centrar-se na

cooperação privado-privado e público-público, para além de colaborarem entre si.

5ª Recomendação: Os membros da PPP devem investir numa comunicação aberta

Se os membros das PPPs não comunicarem de forma clara e aberta podem não se entender e deteriorar as suas expectativas. É crucial que tanto o setor público como o privado sejam pragmáticos e vejam o objetivo mais amplo – no âmbito do objeto em análise, aumentar o nível de cibersegurança - para que a PPP tenha mais sucesso. Normalmente, o privado, assim como o setor público, têm expectativas diferentes. É fundamental uma comunicação aberta entre ambos para que se entendam de forma clara para que consigam atender às expectativas do outro, o que geralmente requer comprometimento.

6ª Recomendação: Os representantes do governo devem poder participar nas reuniões com acordo de não divulgação

O desinteresse do governo bem como a sua hesitação na tomada de decisão em nada abona para a confiança de uma PPP. Para a PPP funcionar e desenvolver-se de forma eficiente, os servidores públicos não devem apenas participar nas reuniões, mas também partilhar a sua experiência com os privados e participar abertamente na discussão de soluções. Deve-se estabelecer a regra da reciprocidade. Se o setor privado participar e fornecer conhecimento/recursos, o setor público também deve fazer o mesmo.

7ª Recomendação: As PMEs também devem participar das PPPs

Normalmente, apenas as grandes empresas estão envolvidas nas PPPs. As PMEs não dispõem de recursos suficientes para se envolverem e não reconhece que uma PPP pode ser útil para o seu crescimento. Seria útil também, de uma perspetiva social, envolver outros tipos de partes interessadas, como PMEs e *start-ups* nas PPPs, para ajudá-las a ganhar experiência neste caso no campo da cibersegurança. A inclusão do conceito das PPPs entre as PMEs seria também muito benéfica para aumentar o nível de SRI na Europa e ainda se torna mais importante quando essas PMEs prestam serviços de *outsourcing* a organizações de maior dimensão.

Conclusão e Contribuições Futuras

Este capítulo é o corolário do trabalho de investigação que se realizou onde se irá recordar a pergunta de partida e as hipóteses de trabalho que se levantou na Nota Metodológica. Procurar-se-á, consequentemente, responder à questão e demonstrar a validade das hipóteses formuladas. Além disso, serão igualmente apresentadas as mais relevantes conclusões relacionadas com os três capítulos centrais. Por último, deixaremos um pequeno contributo para o desenvolvimento de trabalhos de investigação futuros no âmbito do ciberespaço e das PPPs.

8.1 Conclusão

A presente dissertação teve como foco principal a cibersegurança europeia através da análise de documentos provenientes de instituições e organizações que têm vindo a auxiliar a UE a adotar medidas, políticas e estratégias de cibersegurança. De modo a chegar a estas conclusões, foi apresentado um capítulo de introdução, outro de enquadramento teórico e outro de metodologia que serviram de fio condutor, onde foram apresentadas as motivações para o desenvolvimento desta investigação, assim como a metodologia pela qual este trabalho se regeu.

Atualmente, assiste-se a uma sociedade que vive rodeada de tecnologia pelo que o mundo cibernético está presente todos os dias na vida da população mundial, podendo afirmar-se que tem havido um crescimento tanto dos recursos a ela associados como do simples acesso à *internet.* Apesar do aumento de pessoas ligadas à *internet* poder aparentar ser um aspeto de evolução na sociedade, daí advêm questões complexas que suscitam importantes riscos e ameaças. O facto de a *internet* se apresentar como cada vez mais acessível às pessoas, transforma-a num meio e num instrumento que permite aos menos bem-intencionados (por exemplo os *hackers*) o acesso a um poder maior.

Devido a este facto, o Mundo em geral e a Europa em particular têm-se visto forçados a desenvolver medidas para contrariar esses aspetos, através da criação de políticas, estratégias, e meios como as PPPs para buscar aumentar o nível e a qualidade da cibersegurança e ciberdefesa. Verificaram-se casos de ciberataques tais como os da Estónia em 2007 e da Geórgia em 2008 que constituíram os dois primeiros grandes exemplos de ataque no âmbito do ciberespaço (se ignorarmos o caso registado nos Balcãs em 1999).

Depois disso, tanto a NATO em 2002 como a UE logo a seguir em 2008 começaram a reconhecer uma muito significativa relevância ao ciberespaço, promovendo o desenvolvimento de mecanismos de proteção de forma a auxiliar os seus Estados-Membros no desiderato da Cibersegurança e da Ciberdefesa. Hoje em dia é possível observar essa evolução através da definição de políticas e estratégias, bem como de realização de cimeiras onde o ciberespaço é abordado como uma preocupação de amplitude mundial. Nessas cimeiras procura-se arranjar soluções e medidas para diminuir a eficácia dos ciberataques. A criação de organizações como a ENISA representou, por isso, um passo muito significativo para a União Europeia tendo em vista a diminuição dos ciberataques.

A criação de PPPs, por sua vez, foi vista como desempenhando um papel crucial na Política Europeia de Segurança do Ciberespaço pois foi através dessas parcerias que os governos dos Estados-Membros conseguiram impor as suas ideias e promover o desenvolvimento de sistemas de ciberdefesa capazes de enfrentar o *statu quo* do desafio no tempo presente.

Assim, a pergunta de partida que fez espoletar esta investigação e da qual apresentamos os respetivos resultados foi:

Qual a importância do papel dos privados na Política Europeia de Segurança do Ciberespaço?

Conforme analisado no capítulo 3, os privados têm um papel crucial na Política Europeia de Segurança do Ciberespaço. Quando estabelecem parcerias com o Governo em matéria de Cibersegurança, os Privados têm

como principal intuito aumentar essa mesma Cibersegurança e com ela a confiança nacional.

A UE, na sua estratégia de cibersgurança faz referência à cooperação dos privados com os setores públicos através de parcerias que estimulem o setor da cibersegurança ajudando os vários setores críticos a desenvolver soluções susceptíveis de serem aplicadas ao domínio da energia, saúde, transportes, entre outros.

Assim, pode dizer-se que os privados adquiriram uma importância significativa neste contexto, de tal modo que a própria UE investiu quase quatrocentos e cinquenta milhões de euros numa parceria ao abrigo do programa Horizonte 2020, destinada à inovação e investigação e da qual a cibersegurança faz parte.

No entanto, e apesar do papel crucial que os privados têm vindo a desempenhar numa perspetiva evolutiva, do âmbito da cibersegurança, nem sempre há um perfeito entendimento entre as entidades público-privadas pelo que se terá que avançar para a adoção de algumas medidas destinadas a aumentar a confiança entre ambas de modo a que a opção estratégica possa ser sustentável.

Por outro lado, e no que diz respeito à primeira hipótese - “As Parcerias Público-Privadas têm demonstrado ser determinantes na criação de infraestruturas críticas de cibersegurança na EU.” , é um facto que as Organizações Internacionais e os Estados já reconhecem a importância de uma PPP para criar infraestruturas que ajudem ao crescimento da confiança da população e ao aumento da cibersegurança. O melhoramento das infraestruturas críticas é uma das principais razões que justificam a cooperação entre o setor público e o setor privado. Organizações como a CSP na Áustria e o *Gorvernment Center for Security* na Polónia prepararam um programa nacional de infraestruturas críticas que contém várias práticas e diretrizes que os operadores dessas infraestruturas podem seguir de modo a aumentar o nível e a qualidade da cibersegurança do seu país. O aumento da

cibersegurança de um país da UE equivale ao aumento do nível de proteção face aos ciberataques de e em toda a Europa.

Relativamente à segunda hipótese de trabalho “As Parceria Público-Privadas contribuem para potenciar a Cibersegurança na UE”, os Estados Membros atualmente já se socorrem dos privados para aumentar a sua segurança mas a falta de recursos humanos e financeiros por parte do Estado põe os privados de “pé atrás” na hora de estabelecer um acordo. O facto do setor público e do setor privado não terem os mesmos objetivos nem expectativas pode ser algo prejudicial numa parceria.

Na terceira hipótese de trabalho “Parcerias público-privadas têm mais força sendo lideradas instituições privadas.” é algo que investigámos e concluímos que não deve acontecer pois é desanimador para o setor privado que por vezes haja desacordo entre as principiais instituições públicas. Tem que ser o governo a atuar nestes casos e para isso tem que liderar a PPP. Como concluímos na hipótese anterior, antes de se estabelecer uma parceria, é o setor público que tem uma necessidade e posteriormente socorre-se do setor privado, já com o seu objetivo definido. Ou seja, é ele que tem que liderar essa parceria. Neste caso, consideramos que esta terceira hipótese terá que ser refutada.

Em relação à quarta e última hipótese de trabalho “A Participação de PMEs aumenta significativamente a cibersegurança na UE.” considera-se também validada porque apesar das PMEs não disporem de recursos suficientes, uma PPP poderia ser fundamental para o seu crescimento. Seria também útil para aumentar o nível de SRI na Europa e ainda se torna mais importante quando essas PMEs prestam serviços de *outsourcing* a organizações de maior dimensão.

Conseguimos concluir que o mundo do ciberespaço é um dos maiores desafios que se colocam à escala mundial em geral, e à União Europeia em particular – e que vai continuar a sê-lo no futuro. As principais Organizações Internacionais bem como os Estados-Membros têm convidado empresas do setor privado para desenvolver as suas capacidades de ciberdefesa e

cibersegurança, bem como as suas estratégias e políticas de forma a mitigar os ciberataques e as ciberameaças a que se assiste no tempo presente.

Neste sentido, os privados têm uma grande importância na Política Europeia de Segurança no Ciberespaço uma vez que a sua cooperação com os Estados ajuda-os a desenvolver estratégias, facultando informações sobre as ciberameaças e partilha de conhecimento, o que é crucial nesta área.

Em conclusão, a resposta contra as ciberameaças reside na prevenção, cooperação do setor público e privado, bem como no investimento na cibersegurança por parte das instituições públicas, assim como na sensibilização da população para que seja possível combater este desafio que o mundo e Europa atualmente enfrentam.

8.2 Recomendações e Contribuições futuras

O mundo do ciberespaço está em profunda transformação e desenvolvimento, assim como as ameaças e riscos a que está sistematicamente sujeito. Assim, é fundamental continuar a investir em pesquisa e investigação contínua sobre a cibersegurança para que possa ser possível avançar mais e mais profundamente no conhecimento e na consequente definição de Políticas e Estratégias, assim como meios e instrumentos sucessivamente mais eficientes e eficazes.

No seguimento desta dissertação, surgiram ideias que poderão ser objeto de reflexão e estudo em futuras dissertações, nomeadamente:

- Institucionalização de um documento jurídico de criação de uma PPP;
- Análise do investimento e recursos necessários por parte do setor público para a criação de uma PPP (estudos de caso).

Referências Bibliográficas

AC - NATO´s Cyber Capabilities: Yesterday, Today, and Tomorrow. (2012). Antlantic Council, Ideas.

Andersen, H., Cao, F., Tvarnø, C., & Wang, P. (Agostol de 2010). *Public-Private Partnerships: An international analysis - from a legal and economic perspective*. Obtido em 22 de abril de 2019, de EU Asia Inter University Network for Teaching and Research in Public Procurement Regulation: https://openarchive.cbs.dk/bitstream/handle/10398/8422/public-private_partnership.pdf?sequence=1

Andress, J., & Winterfeld, S. (2014). *Cyber Warfare - Technique, Tactics and Tools for Security Practitioners.* USA: Elsevier.

ARON, R. (2002). *Paz e guerra entre as nações.* São Paulo: Universidade de Brasília.

Balão, S. (2014). ENISA e a Estrtégia Europeia de Cibersegurança: Fundamentos Suprenacionais de uma Estratégia Nacional de (Ciber)segurança de Informações. In A. Lara, *Crise, Estado e Segurança* (pp. 127-167). Lisboa: MGI.

Balão, S. (2010). *Geopolítica e Geoestratégia do Ciberespaço: Para uma Estratégia da Informação Nacional.* Lisboa: Proelium.

Bank, A. D. (2012). *Public–private partnership operational plan 2012–2020: Realizing the vision for Strategy 2020—the transformational role of public–private partnerships in Asian Development Bank operations*. Obtido em 22 de abril de 2019, de ADB: https://www.adb.org/sites/default/files/institutional-document/33671/ppp-operational-plan-2012-2020.pdf

Barrinha, A., & Carrapiço, H. (2016). *Segurança Contemporânea.* Lisboa: Pactor.

Batista, G., Ribeiro, C., & Amaral, F. (2003). *Ciberterroismo: A nova forma de crime do Séc XXI como combatê-la=.*

Billo, C., & Chang, W. (2004). *An Analysis of the Means and Motivations of Selected Nations States.* Institute for Security Technology Studies, Dartmouth College.

Bryant, W. (2016). *International Conflict and Cyberspace Superiority: Theory and practice.* Nova Iorque: Routledge.

CAE. (2012). *Resolução do Parlamento Europeu sobre a cibersegurança e ciberdefesa.* Comissão dos Assuntos Externos.

Carta das Nações Unidas. (1945). Obtido em 7 de abril de 2019, de https://www.cm-vfxira.pt/uploads/writer_file/document/14320/Carta_das_Na__es_Unidas.pdf

Carvalho, F. D., & Silva, E. M. (2003). *Cyberwar-Netwar: Security in the Information Age.* Lisboa: IOS Press.

Castells, M. (2012). *A Sociedade em Rede. Era da Informação II: Economia, Sociedade e Cultura.* Fundação Calouste Gulbenkian.

Coleman, K. (2008). *Iranian Cyber Warfare Threat Assessment.*

Conselho Europeu. (20 de fevereiro de 2019). *Aumento da transparência nos negócios realizados por intermédio de plataformas em linha*. Obtido em 13 de abril de 2019, de Conselho Europeu: https://www.consilium.europa.eu/pt/press/press-releases/2019/02/20/increased-transparency-in-doing-business-through-online-platforms/

Conselho Europeu. (23 de novembro de 2001). *Convenção sobre o Cibercrime*. Obtido em 19 de abril de 2019, de https://www.dgpj.mj.pt/sections/relacoes-internacionais/copy_of_anexos/convencao-sobre-o/downloadFile/attachedFile_f0/STE_185.pdf?nocache=1200659879.8

Conselho Europeu. (28 de março de 2019). *Reforma da cibersegurança na Europa*. Obtido em 14 de abril de 2019, de https://www.consilium.europa.eu/pt/policies/cyber-security/

Council on Foreign Relations. (2019). *The Futere of Cybersecurity*. Obtido em 3 de março de 2019, de https://www.cfr.org/conference-calls/future-cybersecurity

Curtis, V. J. (2005). *The theory of Fourth Generation Warfare.* Canadian Army Jounal.

Digital Atatack Map. (2019). *Digital Atatack Map*. Obtido em 9 de Março de 2019, de http://www.digitalattackmap.com/

Dinis, J. A. (2009). Obtido em 2 de abril de 2019, de A Guerra de Informação: Perspectivas de Segurança e Competitividade: www.revistamilitar.pt/modules/article.php?id=401

Dougherty, J., & Pfaltzgraft Jr., R. L. (2003). *Relações Internacionais: As Teorias em Confronto.* Lisboa: Gravida.

Dunne, T., Kurki, M., & Smith, S. (2010). *International Relations theories: Discipline and diversity.* New York: Oxford University Press.

Dupré, L. (Novembro de 2014). *EP3R 2010-2013: Four Years of Pan-European Public Private Cooperation*. Obtido em 20 de abril de 2019, de ENISA: file:///C:/Users/ASUS/Downloads/EP3R%202009-2013%20Future%20of%20NIS%20Public%20Private%20Cooperation.pdf

Dupré, L., Falessi, N., & Liveri, D. (2011). *Cooperative Models for Effective Public Private Partnerships*. (P. O. Union, Editor) Obtido em 20 de abril de 2019, de ENISA: file:///C:/Users/ASUS/Downloads/ENISA_Desktop_Research_report.pdf

ECS. (s.d.). *About the cPPP*. Obtido em 23 de abril de 2019, de ECS: https://ecs-org.eu/cppp

ECS. (s.d.). *Mission & Objectives*. Obtido em 22 de abril de 2019, de ECS: http://ecs-org.eu/about

EDA. (2013). *EDA Study Identifies Cooperation Prospects in Cyber Defence*. Obtido em 12 de março de 2019, de EDA: https://www.eda.europa.eu/info-hub/press-centre/latest-news/2013/05/24/eda-study-identifies-cooperation-prospects-in-cyber-defence

ENISA. (2017). *About ENISA*. Obtido em 5 de abril de 2019, de ENISA: https://www.enisa.europa.eu/about-enisa

ENISA. (4 de abril de 2019). *ENISA supports Portuguese National Exercise on Elections*. Obtido em 14 de abril de 2019, de ENISA: https://www.enisa.europa.eu/news/enisa-news/enisa-supports-portuguese-national-exercise-on-elections

ENISA. (2011). *National Cyber Security Strategies*. Obtido em 17 de abril de 2019, de ENISA: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ppps?tab=details

ENISA. (21 de Março de 2013). *National Cyber Security Strategy of Hungary.* Obtido em 17 de fevereiro de 2019, de National Cyber Security Strategy: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/HU_NCSS.pdf

ENISA. (Novembro de 2017). *Public Private Partnerships: Cooperative models*. Obtido em 19 de abril de 2019, de ENISA: file:///C:/Users/ASUS/Downloads/WP2017%20O-3-1-3%203%20Public%20Private%20Partnerships%20-PPP-%20Cooperative%20models%20(1).pdf

Escravana, N., Lima, J., & Ribeiro, C. (2012). *Ciber(in)segurança da Infraestrutura de Transportes Públicos*. Obtido em 3 de abril de 2019, de IDN: www.idn.gv.pt/publicacoes/nacaodefesa/textointegral/NeD133

EU. (2013). *Comunicação conjunta ao Parlamento Europeu, ao Conselho, ao Comité Económico e ao Comité das Regiões Estratégia da União Europeia para a cibersegurança: Um ciberespaço aberto, seguro e protegido*. Obtido em 12 de abril de 2019, de https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52013JC0001&from=PT

EU. (13 de dezembro de 2011). *Directiva 2011/92/UE do Parlamento Europeu e do Conselho: relativa à luta contra o abuso sexual e a exploração sexual de crianças e a pornografia infantil*. Obtido em 17 de abril de 2019, de https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32011L0093&from=PT

EU. (18 de Novembro de 2014). *EU Cyber Defence Policy Framework*. Obtido em 21 de Janeiro de 2019, de EU: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/sede/dv/sede160315eucyberdefencepolicyframework_/sede160315eucyberdefencepolicyframework_en.pdf

EU. (12 de Dezembro de 2003). *EU Global Strategy*. Obtido em 20 de Janeiro de 2019, de EU: https://europa.eu/globalstrategy/en/european-security-strategy-secure-europe-better-world

EU. (11 de Dezembro de 2008). *EU Global Strategy*. Obtido em 20 de Janeiro de 2019, de EU: https://europa.eu/globalstrategy/en/report-implementation-european-security-strategy-providing-security-changing-world

EU. (2010). *Internal security strategy for the European Union*. Obtido em 12 de março de 2019, de EU: https://www.consilium.europa.eu/media/30753/qc3010313enc.pdf

Euronews. (15 de junho de 2016). *Ciberespaço: O novo teatro de guerra da NATO*. Obtido em 12 de fevererio de 2019, de Euronews: https://pt.euronews.com/2016/06/15/ciberespaco-o-novo-teatro-de-guerra-da-nato

European Commission. (7 de Fevereiro de 2013). *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. Obtido em 21 de Janeiro de 2019, de European Commission: https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf

European Commission. (22 de agosto de 2018). *The EU cybersecurity certification framework*. Obtido em 13 de abril de 2019, de European Commission: https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework

European Council. (15 de Dezembro de 2016). *EU Council Main Results*. Obtido em 21 de Janeiro de 2019, de EU Council: https://www.consilium.europa.eu/en/meetings/european-council/2016/12/15/

Europol. (2017). *European Cybercrime Center- EC3*. Obtido em 12 de abril de 2019, de Europol: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

Eurostat. (3 de janeiro de 2018). *Estatísticas sobre a sociedade da informação - agregados familiares e indivíduos*. Obtido em 8 de abril de 2019, de Eurostat: https://ec.europa.eu/eurostat/statistics-explained/index.php/Archive:Estatísticas_sobre_a_sociedade_da_informação_-_agregados_familiares_e_indivíduos

Fernandes, J. P. (2017). *Cibersegurança*. Obtido em 12 de Março de 2019, de IDN: https://www.idn.gov.pt/publicacoes/nacaodefesa/textointegral/NeD133.pdf

Fernandes, J. (2012). *Utopia, Liberdade e Soberania no Ciberespaço*. Obtido em 3 de março de 2019, de http://www.idn.gov.pt/publicacoes/nacaodefesa/textointegral/NeD133.pdf

Fernandes, M. (4 de Novembro de 2018). *Observador*. Obtido em 31 de Dezembro de 2018, de Observador: https://observador.pt/2018/11/04/cem-anos-do-armisticio-marcelo-elogia-as-forcas-armadas-e-deixa-recado-a-quem-nao-entende-o-seu-papel/

Genest, M. A. (1996). *Conflict and Cooperation: Evolving Theories of International Relations Belmont.* California: Thomson & Wadsworth.

Gibson, W. (1984). *Neuromancer.* Nova Iorque: Ace.

Guedes, A. M. (2009). *A Guerra dos Cinco Dias. A Invasão da Geórgia pela Federação Russa.* Lisboa: IESM e Prefácio.

Haeni, R. (1997). *Information Warfare an Introduction.* Washington DC.

Harding, L. (2016). Obtido em 6 de março de 2019, de What we know about Russia´s interference in the US election: www.theguardian.com/us-news/2016/dec/16/qa-russian-hackers-vladimi-putin-donald-trump-us-presidential-election

Hassan, A. B., Lass, F. D., & Makinde, J. (7 de Agosto de 2012). Obtido em 23 de março de 2019, de Cybercrime in Nigeria: Causes, Effects and the Way Out : http://www.ejournalofscience.org/archive/vol2no7/vol2no7_11.pdf

Hayes, R. E. (2 de maio de 2012). Obtido em março de 23 de 2019, de Cybersecurity and National Cyberdefence: Capability Development, Solutions, and Initiaves, Information Assugurance: www.ebrinc.com/filis/hayes_informations_assurance.pdf

Healey, J. (2013). *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012.* Ashburn : Cyber Conflict Studies Association.

Held, D., & McGrew, A. (2001). *Globalismo e antiglobalismo.* Mulino.

Hewitt, O. (2009). *Information Warfare: Doing Battle in the 21st Century.*

ISC. (2011). *International Strategy for Cyberspace. Prosperity, Security, and Openness in a Netwprked World.*

ITU. (2012). *ITU National Cybersecurity Strategy Guide.* International Union, Switzerland, Geneva.

Kitchin, R. (1998). *Cyberspace:The World in the Wires.* Nova Jersey: John Wiley & Sons.

Koop, C. (2009). *The Analysis of Compound Information Warfare Strategies.* Monash University, Australia.

Lakatos, E. M., & Marconi, M. A. (1994). *Metodologia do Trabalho Científico.* São Paulo: Atlas.

Lee, S.-y. L., & Chomsky, N. (21 de maio de 2015). *Alter Net*. Obtido em 4 de Março de 2019, de https://www.alternet.org/2015/05/noam-chomsky-why-internet-hasnt-freed-our-minds-propaganda-continues-dominate/

Lévy, P. (1999). *Cibercultura.* São Paulo.

Levy´s, P. (1994). *Collective Intelligence: Mankind´s Emerging World in Cyberspace.*

Lewicki, R., & Bunker, B. B. (1996). *Developing and Maintaining Trust in Work Relationships.* Sage .

Libicki, M. (2009). *Cyberdeterrence and Cyberwar.* RAND Corporation.

Lind, W. S. (2004). *Understanding Fourth Generations War.* Military Review.

Lucky, R. W. (1996). *Definition of cyberattack*. Obtido em 9 de abril de 2019, de Meriam-Webster: https://www.merriam-webster.com/dictionary/cyberattack

Mark, P. (Outubro de 1997). Obtido em 29 de março de 2019, de CYBERTERRORISM - Fact or Fancy?: www.cs.georgetown.edu/~denning/infosec/pollitt.html

Martins, M. (2012). *Ciberespaço: uma Nova Relaidade para a Segurança Internacional*. Obtido em 2 de abril de 2019, de IDN: www.idn.gov.pt/publicacoes/nacaodefesa/textointegral/NeD133.pdf

Mashable. (janeiro de 2014). *Mashable*. Obtido em 12 de abril de 2019, de https://www.shortlist.com/news/pete-cashmore

McGuinness, D. (27 de Abril de 2007). *BBC News*. Obtido em 20 de Janeiro de 2019, de BBC News: https://www.bbc.com/news/39655415

McGuinness, D. (27 de abril de 2017). *How a cyber attack transformed Estonia*. Obtido em 3 de abril de 2019, de BBC news: https://www.bbc.com/news/39655415

MDN. (2013). *Conceito Estratégico de Defesa Nacional*. Obtido em 3 de abril de 2019, de www-idn.gov.pt/conteudos/documentos/CEDN_2013.pdf

Miller, R. (2000). *Digital Tradecraft: Espionage and Security in the Informations Age.* Virgínia: Farifax.

Molander, r. C., Riddile, A. S., & Wilson, P. A. (1996). *Statregic Informations Warfare.* RAND.

Moreira, A. (2014). *Teoria das Relações Internacionais.* Coimbra: Edições Almedina.

Moreira, A. (2014). *Teoria das Relações Internacionais.* Coimbra: Almedina.

NATO. (3 de Abril de 2008). *Bucharest Summit Declaration*. Obtido em 20 de Janeiro de 2019, de NATO: https://www.nato.int/cps/us/natohq/official_texts_8443.htm

NATO. (20 de Maio de 2012). *Chicago Summit Declaration* . Obtido em 20 de Janeiro de 2019, de NATO: https://www.nato.int/cps/en/natohq/official_texts_87593.htm?selectedLocale=en

NATO. (2010a). *"Cyber Coalition 2010" to exercise collaboration in cyber defence* . Obtido em 20 de Março de 2019, de NATO: https://www.nato.int/cps/en/natohq/news_68205.htm?selectedLocale=en

NATO. (16 de Julho de 2018). *Cyber Defence*. Obtido em 20 de Janeiro de 2019, de NATO: https://www.nato.int/cps/en/natohq/topics_78170.htm

NATO. (2012b). *Internal security strategy for the European Union*. Obtido em 20 de março de 2019, de NATO: https://www.consilium.europa.eu/media/30753/qc3010313enc.pdf

NATO. (20 de Novembro de 2010). *Lisbon Summit Declaration*. Obtido em 20 de Janeiro de 2019, de NATO: https://www.nato.int/cps/em/natohq/official_texts_68828.htm

NATO. (2012a). *NATO Computer Incident Response Capabality*. Obtido em 20 de março de 2019, de NATO: https://www.northropgrumman.com/Capabilities/Cybersecurity/Documents/Literature/NATO_CIRC.pdf

NATO Parliamentary Assembly. (s.d.). *NATO Parliamentary Assembly*. Obtido em 20 de março de 2019, de NATO Parliamentary Assembly: https://www.nato-pa.int/

NATO. (5 de Setembro de 2014). *Wales Summit Declaration*. Obtido em 21 de Janeiro de 2019, de NATO: https://www.nato.int/cps/en/natohq/official_texts_112964.htm

Nunes, P. V. (2016). *Ciberameaças e Quadro Legal dos Conflitos no Ciberespaço. Em BORGES, João V.; RODRIGUES, Teresa F., coord. Ameaças e Riscos Transnacionais no novo Mundo Global.* Porto: Fronteira do Caos.

Nunes, P. V. (Abril de 2018). *Contributos para uma Estratégia de Defesa Nacional*. Obtido em 12 de abril de 2019, de https://www.idn.gov.pt/publicacoes/cadernos/idncadernos_28.pdf

Nunes, P. V. (2015). *Sociedade em Rede, Ciberespaço e Guerra de Informação: Contributos para o enquadramento e Construção de uma Estratégia Nacional da Informação.* Lisboa.

Nye, J. S., & Keohane, R. O. (1977). *Power and Interdependence: World Politics in Transition.* Boston: Little, Brown & Co.

Obama, B. (29 de Maio de 2009). *Obama's Remarks on Cyber-Security*. Obtido em 10 de abril de 2019, de The New York Times: https://www.nytimes.com/2009/05/29/us/politics/29obama.text.html

Parks, R. C., & Duggan, D. P. (2001). *Princioles of Cyber-Warfare.* United States Military Academy NY: Information Assurance and Security.

Parliament, E. (6 de julho de 2016). *Concerning measures for a high common level of security of network and information systems across the Union*. Obtido em 8 de março de 2019, de https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN

Pernik, P. (2014). *Improving Cyber Security : NATO and the EU* . Obtido em 5 de abril de 2019, de https://www.icds.ee/fileadmin/media/icds.ee/failid/Piret_Pernik__Improving_Cyber_Security.pdf

Pernik, P. (Setembro de 2014). *Improving Cyber Security: NATO and the EU*. Obtido em 21 de Janeiro de 2019, de Improving Cyber Security: NATO and the EU: https://icds.ee/wp-content/uploads/2010/02/Piret_Pernik_-_Improving_Cyber_Security.pdf

Quivy, R., & Campenhout, L. V. (2008). *Manual de Investigação em ciênciais sociais.* Lisboa: Gravida Publicações.

Raínho, P. (12 de dezembro de 2016). *Observador*. Obtido em 7 de abril de 2019, de Observador: https://observador.pt/2016/12/10/cia-denuncia-envolvimento-russo-na-eleicao-de-donald-trump/

Rana, W. (2015). *Theory of Complex Interdependence: A Comparative Analysisof Realist and Neoliberal Thoughts.* Internacional Journal of Business and Social Science.

RAND Corporation. (s.d.). *Olympic-caliber cybersecurity: lessons for safeguarding the 2020 games and other major events*. Obtido em 7 de março de 2019, de Rand Corporation: https://www.rand.org/randeurope/research/projects/olympic-caliber-cybersecurity-2020.html

RAND Corporation. (24 de maio de 2016). *The Hackers' Bazaar: Markets for Cybercrime Tools and Stolen Data*. Obtido em 7 de Março de 2019, de Rand Corporation: https://www.rand.org/events/2016/05/24.html

RAND Corporations. (30 de junho de 2015). *Internet Freedom Software Tools Developed by the United States Do Not Facilitate Cybercrime*. Obtido em 8 de março de 2019, de Rand Corporation: https://www.rand.org/news/press/2015/06/30/index1.html

RFA 390-6 Política de Ciberdefesa da Força Aérea. (2011). DUVCSI, Estado-Maior da Força Aérea.

Roseiro, B. (14 de Setembro de 2018). *Observador*. Obtido em 11 de abril de 2019, de Observador: https://observador.pt/2018/09/14/o-que-se-sabe-de-rui-pinto-o-pirata-informatico-do-football-leaks-que-tera-desviado-os-emails-do-benfica/

Rustici, R. M. (2011). *Cyberweapons: Leveng the International PlayingField.*

Shayles, L. (2002). *Deciphering Cyberspace: Making the Most of Digital Communication Technology.* California: Sage.

Silva, T. D. (2019). *A Autonomia Estratégica e a Defesa Europeia*. Obtido de Revista Cientifica da Academia Militar: https://academiamilitar.pt/images/site_images/Revista_Proelium/Ficheiro_1.pdf

Silveira, F. L. (1989). Obtido em 20 de março de 2019, de AFilosofia de Karl Popper e as Suas Implicações no Ensino da Ciência:

https://www.lume.ufrgs.br/bitstream/handle/10183/84999/000014819.pdf?sequence=1

Stein, J. C. (1995). *Prices and trading Volume in the Housing Market: A Model with Down-Payment Effects.* Oxford University Press.

Taylor, H. (21 de setemro de 2018). *What Are Cyber Threats: How They Affect You and What to Do About Them*. Obtido em 3 de abril de 2019, de Prey Nation: https://preyproject.com/blog/en/what-are-cyber-threats-how-they-affect-you-what-to-do-about-them/

UNIDIR. (20 de Janeiro de 2013). *The Cyber Index International Security Trends and Realities*. Obtido de The Cyber Index International Security Trends and Realities: http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf

University of Twente. (2019). *Medium Theory*. Obtido em 4 de Março de 2019, de Communications Theories: (https://www.utwente.nl/en/bms/communication-theories/sorted-by-cluster/Media-Culture-and-Society/Medium_theory-1/).

US DHS. (2016). *Cyber Safety.* Obtido em 23 de março de 2019, de Homeland Securty: www.dhs.gov/cyber-safety

Verton, D. (4 de Abril de 1999). *The Business of Federal Technology.* Obtido em 2019 de Janeiro de 20, de The Business of Federal Technology: https://fcw.com/articles/1999/04/04/serbs-launch-cyberattack-on-nato.aspx

Waltz, E. (1998). *Informations Warfare: Principles and Operations.* Boston: Artech House.