Departamento de Ciência Política e Políticas Públicas

A Cibersegurança em Portugal: A ação política nacional em matéria de cibersegurança

Daniela Gonçalves Guerreiro Santos

Dissertação submetida como requisito parcial para obtenção do grau de

Mestre em Políticas Públicas

Orientador:
Coronel Fernando José Vicente Freire, Investigador,
Instituto da Defesa Nacional

Co-orientadora:
Doutora Maria Helena Chaves Carreiras, Professora Auxiliar,
ISCTE – Instituto Universitário de Lisboa

Setembro, 2014

i. Agradecimentos

Agradeço a todos os que me dispensaram o seu tempo e partilharam comigo o seu conhecimento, que tão útil foi para a conclusão deste trabalho.

Agradeço especialmente ao meu orientador, Coronel Fernando Freire, todo o tempo, conhecimento e contatos que me facultou para que pudesse realizar este projeto, assim como o seu apoio incondicional.

Agradeço à minha co-orientadora, Professora Helena Carreiras, a prontidão e disponibilidade, mesmo sem ter sido em normais circunstâncias, para co-orientar a elaboração deste trabalho.

Agradeço à minha família e todos os que me estão mais próximos pelo apoio e esforço para que hoje pudesse concluir esta fase dos meus estudos.

Agradeço-te, amor, a paciência, carinho e força que me deste, sempre que precisei.

ii. Resumo

No presente trabalho é mapeada e sumariamente analisada a ação política em matéria de cibersegurança em Portugal, desde que as questões da segurança das redes e dos sistemas de informação surgiram na agenda política até a atualidade, com a implementação do Centro Nacional de Cibersegurança.

Para o levantamento e mapeamento dos atores e das medidas políticas adotadas em Portugal nesta área, utiliza-se como modelo de análise o ciclo das políticas públicas.

A relevância desta investigação prende-se, por um lado, com o facto de, apesar de já existir noutros países e das orientações europeias e internacionais apontarem nesse sentido, ainda não existe em Portugal uma política pública de cibersegurança e, por outro lado, se considerar que este domínio deve ser um fator estratégico nas políticas públicas dos países desenvolvidos (aqueles cujo normal funcionamento dos serviços que mantêm a sociedade como a conhecemos, dependem de infraestruturas suportadas por redes e sistemas de informação).

Deste modo, pretende-se alertar para a importância desta questão e vir, de alguma forma, a contribuir para a criação dessa política pública, que urge em Portugal.

Palavras-chave: cibersegurança; ação política; ciclo das políticas públicas; Portugal.

iii. Abstract

In this work we briefly mapped and analyzed political action in the field of cybersecurity in Portugal, since the subject of security of networks and information systems have emerged on the political agenda to the present, with the implementation of the National Cybersecurity Centre.

To the survey and mapping of actors and policy measures taken in Portugal in this field, we use the public policy cycle as model of analysis.

The relevance of this research is related to, on one hand, the fact that despite already exists in other countries and European and international guidelines so indicate, in Portugal there is not yet a cybersecurity public policy and on the other hand, we consider that this should be a strategic factor in public policies of developed countries (those whose normal functioning of services that keep society as we know, depend on infrastructures supported by networks and information systems).

Thus, with this project we intend to draw attention to the importance of this issue and come, somehow, to contribute to the development of that public policy, which urges in Portugal.

Keywords: cybersecurity; political action; public policy cycle; Portugal.

iv. Índice

v. Índice de Quadros

vi. Índice de Figuras

vii. Glossário de Siglas

AMA: Agência para a Modernização Administrativa
ANACOM: Autoridade Nacional de Comunicações
ANPC: Autoridade Nacional de Proteção Civil
ANS: Autoridade Nacional de Segurança
APDSI: Associação para a Promoção e Desenvolvimento da Sociedade da Informação
APTs: Advanced Persistent Threats
ARN: Autoridade Reguladora Nacional
BIS: Department for Business Innovation & Skills (Reino Unido)
CC-CRISI: Centro de Coordenação da CRISI-FA
CCD CoE: NATO Cooperative Cyber Defence Centre of Excellence/Centro de Excelência Cooperativo de Ciberdefesa da OTAN
CEGER: Centro de Gestão da Rede Informática do Governo
CEMGFA: Chefe de Estado-Maior-General das Forças Armadas
CEPOL: European Police College
CERT: Computer Emergency Response Team
CET: Capability, Armament & Technology
CGCiber: Curso de Cibersegurança e Gestão de Crises no Ciberespaço (leccionado no IDN)
CITIUS: plataforma informática do Ministério da Justiça, que permitiu a desmaterialização dos processos nos tribunais
CNCseg: Centro Nacional de Cibersegurança
CNEL: Coordenador Nacional da Estratégia de Lisboa
CNPCE: Conselho Nacional de Planeamento Civil de Emergência
CNPD: Comissão Nacional de Proteção de Dados
CPNI: Centre for the Protection of National Infrastructure (Reino Unido)
CRISI-FA: Capacidade de Resposta a Incidentes de Segurança Informática das Forças Armadas
CRP: Constituição da República Portuguesa
CSIRT: Computer Security Incident Response Team
CT 163: Comissão Técnica 163 (comissão especializada em normalização da área da segurança da informação)
DGIDC-CRIE: Equipa de Missão Computadores, Redes e Internet na Escola, no âmbito da Direção-Geral de Inovação e de Desenvolvimento Curricular
DICSI: Divisão de Comunicações e Sistemas de Informação (do EMGFA)
ECEE: Entidade de Certificação Eletrónica do Estado – Infraestrutura de Chaves Públicas
EC3: Centro Europeu de Cibercrime
EDA: European Defence Agency

eGovernment: Governo eletrónico

EM: Estados-Membros

EMGFA: Estado-Maior-General das Forças Armadas

ENISA: European Network and Information Security Agency

ENSI: Estrutura Nacional de Segurança da Informação

EUROPOL: European Police Office

FCCN: Fundação para a Computação Científica Nacional

FCT: Fundação para a Ciência e a Tecnologia

FFAA: Forças Armadas

GCHQ: Government Communications Headquarters (Reino Unido)

GECENI: Grupo de Estudos sobre Contributos para uma Estratégia Nacional de Informação

GNS: Gabinete Nacional de Segurança

GPTIC: Grupo de Projeto para as Tecnologias de Informação e Comunicação

GRISI: Grupo de Resposta a Incidentes de Segurança Informática

GSSI: Grupo Segurança na Sociedade da Informação (da APDSI)

IDN: Instituto da Defesa Nacional

IPDJ: Instituto Português do Desporto e Juventude

IPQ: Instituto Português da Qualidade

ISO: International Organization for Standardization

ISP: Internet Service Provider

*it*SMF: Associação Portuguesa de Gestores de Serviços de Tecnologias de Informação

I&D: Investigação e Desenvolvimento

LCE: Lei das Comunicações Eletrónicas

MP: Ministério Público

NSA: National Security Agency

OCDE: Organização para a Cooperação e Desenvolvimento Económico

OCSIA: Office of Cyber Security and Information Assurance

OECD: The Organisation for Economic Co-operation and Development

OTAN: Organização do Tratado do Atlântico Norte

PCM: Presidência do Conselho de Ministros

PCSD: Política Comum de Segurança e Defesa

PJ: Polícia Judiciária

PNACE: Programa Nacional de Ação para o Crescimento e o Emprego

PRACE: Programa de Reestruturação da Administração Central do Estado

PSD: Partido Social Democrata

PSP: Polícia de Segurança Pública

RCM: Resolução do Conselho de Ministros

RCTS: Rede Ciência, Tecnologia e Sociedade (da FCCN)

SCADA: Supervisory Control and Data Aquisition

SCEE: Sistema de Certificação Eletrónica do Estado

SEGNAC 4: instruções sobre a segurança informática

SGSSI: Secretário-Geral do Sistema de Segurança Interna

SIRP: Sistema de Informações da República Portuguesa

SSI: Sistema de Segurança Interna

TIC: Tecnologias de Informação e Comunicação

UE: União Europeia

UMIC: Unidade de Missão Inovação e Conhecimento (2002-2005); Agência para a Sociedade do Conhecimento (2005-2012)

UTI: Unidade de Telecomunicações e Informática (da PJ)

INTRODUÇÃO

A evolução tecnológica, principalmente o aparecimento da internet e a generalização do seu uso, veio alterar por completo as sociedades e o seu funcionamento. Passámos das Sociedades Industriais para a Sociedade da Informação - uma sociedade globalizada, caraterizada pela partilha e o acesso fácil a todo o tipo de informação.

Estados, indivíduos e organizações passaram a depender do uso das tecnologias de informação e comunicação (TIC), especialmente da internet, para realizar as suas tarefas diárias.

Os Estados, para garantirem o correto funcionamento das atividades e serviços da Administração Pública, das funções de defesa e soberania, da Economia, das infraestruturas críticas (que permitem o abastecimento de energia e água, o funcionamento de hospitais, aeroportos…), entre outros, dependem de uma rede interdependente baseada na internet.

Quanto aos indivíduos, a maioria dos cidadãos, de quase todas as partes do mundo, têm os seus dados pessoais e bancários na internet, mesmo os que não são utilizadores da mesma e muitos dependem dela para as suas tarefas diárias, incluindo o próprio trabalho[1].

No que concerne às organizações, a Sociedade da Informação trouxe novas formas de relacionamento e paradigmas de organização. Algumas organizações existem, praticamente, apenas virtualmente, outras têm uma descentralização nunca antes vista, permitindo que as diferentes componentes de produção estejam em qualquer parte do mundo e mesmo assim se produzam produtos e se forneçam serviços a clientes noutros locais ainda, muitas vezes em simultâneo (ex. a indústria automóvel; cada vez mais a indústria de desenvolvimento tecnológico).

Neste ambiente, começaram a surgir ataques a este sistema global de informação, onde a informação já não se encontra armazenada num espaço específico e restrito, tendo passado a estar num local - ciberespaço - que, devido à sua amplitude, torna mais difícil o controlo do acesso à informação, podendo torná-la mais acessível a indivíduos mal intencionados, dotados de determinadas competências informáticas (*hackers*). Portanto, este sistema pode deixar os Estados, as organizações e os cidadãos mais vulneráveis a (ciber)ataques, geralmente realizados com o intuito de proporcionar benefícios económicos ao atacante, a disrupção e desestabilização de Estados e/ou indivíduos, etc.

Segundo informação do Centro Europeu de Cibercrime (EC3) e da Comissão Europeia, o cibercrime está a aumentar rapidamente, representando um desafio considerável para as agências de aplicação da lei e um custo significativo para a sociedade no geral: um relatório recente sugere que, todos os anos, no mundo inteiro, as vítimas perdem cerca de 290 biliões de euros, como resultado do cibercrime, tornando-o mais rentável que o comércio mundial de marijuana, cocaína e heroína, juntas[2].

---

[1] Muitas profissões surgiram com o aparecimento das TIC (ex. técnico de informática; *web designer*; informático; gestor de conteúdos *web*; gestor de tecnologias de informação e comunicação), sem as quais não haveria uma Economia à escala que atualmente existe, nem se conseguiria produzir conhecimento à velocidade que é hoje possível (OECD, 2008; JOIN(2013) 1 final).

[2] Consultar https://www.europol.europa.eu/ec/cybercrime-growing (consultado a 05/04/14).

De acordo com os Eurobarómetros 390 e 404, sobre Cibersegurança (2012 e 2013), estima-se que, todos os dias, mais de um milhão de pessoas no mundo sejam vítimas de cibercrimes e as perdas representem biliões de euros por ano. E, conforme uma notícia publicada na plataforma Internet Segura, um estudo da empresa de *sofware* Panda Security sugere que são detetados diariamente, em média, 160.000 de novos tipos de *malware*[3], i.e., 160.000 novos tipos de *software* especificamente desenhado para perturbar ou provocar danos num sistema informático (Oxford Dictionary, 2014).

Tendo como pano de fundo esta realidade, considera-se fundamental contribuir para a consciencialização e para a ação política para fazer frente a estas ameaças.

Posto isto, o presente trabalho consiste num levantamento e mapeamento da ação política em matéria de cibersegurança em Portugal, bem como dos atores intervenientes naquilo a que podemos chamar de sistema nacional de cibersegurança, desde o surgimento da necessidade de apostar nesta questão, até a atualidade.

Este texto encontra-se dividido em cinco partes: introdução; capítulo 1 "Enquadramento"; capítulo 2 "A cibersegurança na União Europeia"; capítulo 3 "A cibersegurança em Portugal"; capítulo 4 "Estudo de casos"; conclusão.

Na introdução é apresentado, de uma maneira geral, o impacto da evolução tecnológica, principalmente a internet, na sociedade e o conteúdo deste projeto.

No capítulo 1 apresenta-se a razão da escolha deste tema e o objetivo deste estudo, assim como as metodologias, de investigação e de análise, utilizadas para a realização deste projeto.

No capítulo 2 faz-se uma sumária apresentação dos atores e do seu papel, bem como das iniciativas na área da cibersegurança que se destacam ao nível europeu e da sua importância para o desenvolvimento das políticas públicas nesta matéria, ao nível doméstico.

No capítulo 3 são levantadas e mapeadas as iniciativas, as medidas políticas e os atores intervenientes na garantia da cibersegurança em Portugal. Para a apresentação desta informação utiliza--se o ciclo das políticas públicas como modelo de análise.

No capítulo 4 são analisadas duas medidas políticas em matéria de cibersegurança em Portugal (as duas medidas consideradas mais relevantes), à luz de duas teorias de análise das políticas públicas: a criação do Sistema de Certificação Eletrónica do Estado é analisada de acordo com a teoria dos fluxos múltiplos e a criação do Centro Nacional de Cibersegurança é analisada com base no neo-institucionalismo da escolha racional.

Finalmente, na conclusão é feita uma síntese da informação recolhida, levantadas algumas questões e deixadas algumas sugestões como forma de contributo para a cibersegurança em Portugal, nomeadamente para o desenvolvimento de uma política pública neste domínio.

[3]Consultar http://www.internetsegura.pt/noticias/milhares-de-novos-softwares-maliciosos-sao-detetados-todos-os-dias#.U52ARfmSyPb (consultado a 6 de Junho de 2014).

CAPÍTULO 1. ENQUADRAMENTO CONCETUAL E METODOLÓGICO

1.1 Enquadramento concetual

1.1.1 Ciberameaças

Para além do cibercrime, já mencionado, há outros tipos de ameaças colocadas pelo massivo uso das TIC ligadas em rede, como o *hacktivismo*, a ciberespionagem, o ciberterrorismo ou a ciberguerra[4].

O *hacktivismo* é caracterizado pela utilização de meios informáticos e da própria internet para passar uma mensagem relacionada com a ideologia defendida pelo *hacktivista*, seja ela política, religiosa ou outra, ou seja, é o uso das novas TIC, incluindo a internet para disseminar uma mensagem, chamando a atenção da opinião pública para determinado assunto (Santos, 2011: 27).

Os *hacktivistas* fazem uso dos seus conhecimentos informáticos para explorar vulnerabilidades dos sistemas informáticos e penetrar em *websites* de empresas e governamentais, para passar a sua mensagem ao maior número possível de pessoas, em jeito de protesto. As suas ações geralmente passam pelo *graffiti* (em forma de imagem ou mensagem) deixado na página principal dos *websites* atacados ou o bloqueio dos mesmos, através de ações de disseminação de *spam*, i.e., *emails* não solicitados[5].

A ciberespionagem caracteriza-se pela exploração das vulnerabilidades encontradas em *websites* (geralmente governamentais e de empresas) para ter acesso a informação sensível e, muitas vezes, roubar informação sobre projetos (principalmente industriais) em desenvolvimento ou segredos de negócio. As motivações que estão por detrás da ciberespionagem costumam ser a vantagem competitiva de Estados sobre Estados ou de empresas sobre outras empresas que desenvolvam projetos na mesma área ou ainda os benefícios financeiros provenientes da venda da informação roubada[6].

O ciberterrorismo pode ser genericamente definido como o uso das TIC para a realização de ameaças ou a organização (incluindo a troca de informação, angariação de seguidores e financiamento) e execução de ataques com grande impacto nas redes e sistemas informáticos e nas infraestruturas críticas, motivadas por ideologias políticas ou religiosas, fomentando o medo e o terror, com o intuito

---

[4] Nenhum destes tipos de ação estão legalmente definidos na legislação nacional, pelo que as definições propostas se baseiam no que é comummente entendido como cada um destes tipos de ação.

[5] O grupo de *hackers* Anonymous identifica-se publicamente com este tipo de ação. Consultar http://www.tugaleaks.com/banco-de-portugal-bes-ataque-informatico.html , http://www.tugaleaks.com/hackers-atacam-aguas-de-portugal.html , http://www.tugaleaks.com/ataque-sites-bancos-anonymous.html , http://www.tugaleaks.com/nomes-telemoveis-procuradores-republica.html , etc (consultado a 07/09/2014).

[6] Exemplos deste tipo de ações são as realizadas entre a China e a Rússia sobre os Estados Unidos da América e vice-versa ou entre estes últimos e a União Europeia, como divulgou o antigo agente da NSA (National Security Agency norte americana), Edward Snowden. O principal foco de espionagem são organizações governamentais, laboratórios e centros de investigação e desenvolvimento científico e tecnológico, empresas na área da indústria da defesa, empresas de setores vitais como a energia. Consultar http://portuguese.ruvr.ru/2012_11_08/Caca-chines-de-quinta-geracao-sera-resultado-de-ciberespionagem/ , http://www.publico.pt/mundo/noticia/uniao-europeia-e-alvo-prioritario-da-espionagem-norteamericana-1602758 , http://moraisvinna.blogspot.nl/2013/05/ciberespionagem-volta-confrontar-china.html , http://expresso.sapo.pt/eua-acusam-china-e-russia-de-ciberespionagem=f685470 , http://www.rtp.pt/noticias/index.php?article=619426&tm=7&layout=121&visual=49 (consultado a 20/05/2014).

de despoletar determinadas ações políticas[7].

Com base nesta definição, verifica-se que o espectro da atuação dos terroristas no ciberespaço é enorme, à semelhança do seu campo de atuação no espaço físico, mas com algumas agravantes: o facto dos ciberataques realizados por um conjunto muito limitado de "ciberguerreiros"[8] terem efeitos semelhantes aos ataques físicos realizados por dezenas de terroristas; o facto da utilização da internet facilitar a disseminação da mensagem que os grupos terroristas pretendem veicular e a angariação de seguidores, bem como o financiamento para suas causas; o facto de tudo isto poder ser feito de forma anónima, dificultando a interseção e o desmantelamento destes grupos.

A ciberguerra é o último tipo de ameaça apresentado, por ser aquele ao qual se atribui menor possibilidade de vir a acontecer, enquanto ação completamente autónoma porém, é uma possibilidade real, não podendo deixar de ser considerado na elaboração de uma política de cibersegurança.

Esta consiste na "luta ou conflito entre duas ou mais nações ou entre diferentes fações dentro de uma nação onde o ciberespaço é o campo de batalha" (Freire, Nunes, Davara e Acosta, 2013: 23). "No plano militar, a ciberguerra concentra as capacidades de defesa das redes, dos sistemas e da informação de caráter militar e as capacidades ofensivas de espionagem militar e de retaliação a ataques"[9] (Santos, 2011: 39). Enquanto no plano civil deverá concentrar as capacidades de defesa das infraestruturas críticas, i.e., as infraestruturas essenciais ao normal funcionamento da sociedade, tal como a conhecemos, como o armazenamento e abastecimento de energia, água, comida ou a utilização dos meios eletrónicos para a realização de transferências bancárias.

Os protagonistas destas ações são geralmente Estados, embora estes possam contratar estes serviços a *"ciberguerreiros"*, para se poderem desresponsabilizar, em caso de conflito, por possíveis problemas, incluindo questões legais ou de legitimidade.

O *worm* Stuxnet constituiu a primeira ciberarma conhecida, que pode ser usada em caso de ciberguerra e que muitos autores defendem que o seu uso constituiu o início da ciberguerra, como modo autónomo de fazer guerra, com recurso a ciberarmas.

Stuxnet provou que não é preciso que os sistemas informáticos estejam ligados à internet para estarem vulneráveis a possíveis ataques, uma vez que o sistema informático da central de enriquecimento de urânio de Natanz (Irão) não se encontrava ligado à internet, mas sim a uma rede interna, considerada segura e fisicamente protegida por elementos militares.

Este *worm* (tipo de vírus informático), desenhado especificamente para se camuflar e espalhar facilmente pelos vários computadores e sistemas que comandam o funcionamento das centrais nucleares iranianas, com o intuito de alterar as suas definições, danificando-os, foi introduzido nos sistemas da

[7] Definição baseada na transposição da atividade terrorista no espaço físico, para o ciberespaço.

[8] Por ciberguerreiros entendemos elementos de um grupo organizado que realizam ciberataques a alvos estratégicos (ex. sistemas informáticos de infraestruturas críticas, *websites* governamentais que disponibilizem *online* serviços essenciais para o normal funcionamento da sociedade), por questões políticas ou religiosas, assim como defendem os seus sistemas de informáticos.

[9] Às quais se acrescenta a capacidade de defesa do sistema de redes de emergência e segurança nacional.

Central de Natanz, através da introdução de uma *pen usb* num dos seus computadores, tendo mesmo vindo a atrasar a inauguração da usina de Bushehr[10].

Este exemplo demonstra a necessidade de proteger os sistemas e redes que suportam as infraestruturas vitais ao normal funcionamento da sociedade.

Em Portugal, o primeiro tipo de ameaça apresentado - cibercrime - tem sido o mais frequente[11], o terceiro tipo de ameaça - ciberespionagem - também tem afetado o Estado[12], empresas e instituições académicas[13], mas o *hacktivismo* parece ser o tipo de "ataque" mais mediatizado. As notícias de ataques a *websites* governamentais e a empresas privadas, nomeadamente instituições bancárias, onde são deixadas mensagens de protesto, têm sido frequentes nos últimos anos[14].

O Relatório de Segurança Interna de 2013 também faz alusão ao ciberterrorismo. Contudo, não se encontra facilmente informação sobre este tipo de ameaça, provavelmente porque a sua prevenção compete aos serviços de informações nacionais, cujas funções e atividades são caracterizadas pelo sigilo.

1.1.2 Escolha do tema e objetivo

Tendo em consideração o contexto apresentado, a Comissão Europeia tem vindo, principalmente desde 2001, a emitir orientações e a adotar diretivas no sentido dos Estados-Membros (EM) desenvolverem capacidades e políticas públicas de cibersegurança[15]. Todavia, esse objetivo ainda não foi alcançado em alguns EM, como é o caso de Portugal, onde ainda não existe uma política pública nacional de cibersegurança.

Deste modo, considera-se pertinente a realização de um levantamento e mapeamento das ações políticas que se possam considerar como parte de um processo de produção de uma política pública de cibersegurança em Portugal, dos seus atores, bem como a identificação dos problemas inerentes a esse processo, tendo como limites temporais o momento em que a questão da cibersegurança surgiu na praça pública portuguesa e a atualidade.

Repare-se que, apesar das ameaças ao ciberespaço nacional e da pressão nacional (de atores intervenientes na garantia da cibersegurança em Portugal) e internacional (ex. Organização para a

---

[10] Stuxnet é um vírus informático que explora as vulnerabilidades dos sistemas informáticos que utilizem os sistemas SCADA (Supervisory Control And Data Aquisition), geralmente utilizados em infraestruturas industriais.

[11] De acordo com declarações do subdiretor da PJ, grande parte da criminalidade informática continua a estar associada ao *home-banking*, ao *phishing*, à violação de privacidade e à pedofilia (Consultar http://www.dn.pt/politica/interior.aspx?content_id=4166630&page=1 – consultado a 11/10/14).

[12] Em 2013, Portugal sofreu "tentativas de infiltração de sistemas informáticos do Estado, ocorridas no contexto de campanhas internacionais (…) visando a informação privilegiada" (Sistema de Segurança Interna, 2013: 32).

[13] De acordo com as declarações de um elemento do SIS, no simpósio "Globalização, Inovação e Segurança na Era da Informação, que teve lugar no Funchal, em 2007.

[14] Consultar http://www.tugaleaks.com/nomes-telemoveis-procuradores-republica.html , http://www.tugaleaks.com/partidos-politicos-2014.html , http://www.tugaleaks.com/enderecos-emaic-camaras-municipais.html , http://www.tugaleaks.com/ataque-sites-bancos-anonymous.html , entre outros (consultado a 08/09/2014). Grande parte destes ataques são reivindicados pelo grupo Anonymous, cujos membros se autointitulam como *hacktivistas* e defendem a liberdade de expressão e o uso livre da internet.

[15] Ex. COM(2001) 298; Diretiva 2009/140/CE; COM(2010) 245 final; COM(2010) 673 final; COM(2011) 163 final; JOIN(2013) 1 final; COM(2013) 48 final.

Cooperação e Desenvolvimento Económico - OCDE -, UE, Organização do Tratado do Atlântico Norte - OTAN) para o desenvolvimento de capacidades e políticas nesta área, não estão legalmente definidos em Portugal, os conceitos de cibersegurança e ciberdefesa, por exemplo.

No entanto, já existem algumas medidas nesta área, como uma proposta de Estratégia Nacional de Cibersegurança[16] publicada no *website* do Gabinete Nacional de Cibersegurança - GNS - (que não define claramente o conceito de cibersegurança), um despacho do Ministro da Defesa Nacional, com uma Orientação Política para a Ciberdefesa[17], que não define o conceito de ciberdefesa, um Centro Nacional de Cibersegurança (CNCseg), sem estar legalmente definido o conceito de cibersegurança, com base no qual se deve basear a ação nesta matéria, entre outros.

Uma vez que não estão legalmente definidos os conceitos de cibersegurança e de ciberdefesa, em Portugal, para o desenvolvimento deste estudo baseámo-nos no conceito de cibersegurança como as precauções e ações tomadas "para proteger o ciberespaço, tanto nos domínios civil como militar, contra as ameaças decorrentes da interdependência das suas redes e infraestruturas informáticas"[18] e ciberdefesa como "os meios para alcançar e executar medidas defensivas para combater ciberataques e mitigar os seus efeitos e, ainda, preservar e restaurar a segurança da comunicação, informação e outros sistemas eletrónicos ou a informação que é guardada, processada ou transmitida nesses sistemas"[19], embora tomemos a liberdade de acrescentar que esses meios devem ser utilizados para proteger a soberania e segurança nacional, ao contrário do que acontece com a cibersegurança que deve ser garantida em qualquer situação.

A escolha destes conceitos prende-se com o facto de serem os conceitos disseminados pela União Europeia e pela OTAN (respetivamente), das quais Portugal faz parte e deve estar em consonância.

Dada a frequência da ocorrência de incidentes de cibersegurança em Portugal[20], apesar de não existir uma política pública de cibersegurança, têm sido implementadas algumas medidas que contribuem para a cibersegurança nacional, embora um pouco dispersas e descoordenadas.

Para resolver este problema, foi recentemente implementado o Centro Nacional de Cibersegurança, que deverá coordenar toda a ação nacional em matéria de cibersegurança. Esta medida tardou a ser aprovada[21], dado que a proposta para a sua constituição foi entregue ao Primeiro-Ministro

---

[16] Consultar http://www.gns.gov.pt/media/1247/PropostaEstrat%C3%A9giaNacionaldeCiberseguran%C3%A7aPortuguesa.pdf (Consultado a 20/05/2014).

[17] Consultar https://dre.pt/application/dir/pdf2sdip/2013/10/208000000/3197631979.pdf (Consultado a 17/06/2014).

[18] Conceito definido pela Comissão Europeia, na Estratégia da UE para a cibersegurança (JOIN (2013) 1 final).

[19] Em AC/322-N(2014)0072, da OTAN, um documento oficial classificado da OTAN.

[20] De acordo com informação do CERT.PT, os incidentes de *phishing*, i.e., a prática fraudulenta de envio de *emails* que pretendem ser de fontes fidedignas, para induzir as pessoas a revelar informações pessoais, como senhas e números de cartão de crédito, entre outros, *online*, acontecem todas as semanas e as infeções no geral podem chegar a um milhão por mês.

[21] O CNCseg foi aprovado em maio de 2014, pelo Decreto-Lei nº 69/2014, de 9 de maio, tendo, desde então, instalações designadas e alguns elementos afetos, embora o responsável tivesse sido nomeado apenas em setembro e o centro tenha entrado em funções em outubro.

em julho de 2012. Proposta que foi elaborada por elementos de vários setores da sociedade (ex. Administração Pública, academia, setor militar), que parecem ter chegado a um consenso, especialmente no que toca à urgência da implementação de um Centro Nacional de Cibersegurança em Portugal[22].

É neste contexto de, por um lado, alguma descoordenação e inércia da parte dos decisores políticos competentes e, por outro lado, a implementação da primeira autoridade competente na área, que se verifica a necessidade de analisar o que já existe e o que está a ser desenvolvido em Portugal, nesta matéria, para perceber como tem sido o processo político até então e o que se poderá melhorar.

Portanto, o objetivo do presente trabalho é fazer o levantamento e o mapeamento das diferentes iniciativas, medidas, atores e recursos envolvidos no processo de produção daquilo que chamaremos uma política pública de cibersegurança em Portugal, desde o surgimento do problema, i.e., o momento em que se verificou a necessidade de garantir a cibersegurança em Portugal, até a atualidade, bem como identificar os problemas associados a tal processo (problemas que podem estar relacionados com a falta de implementação de uma política pública nacional de cibersegurança).

Considera-se que este mapeamento poderá contribuir para alcançar alguma coerência, que poderá ajudar no processo do desenho de uma política pública nacional de cibersegurança, procurando informar os decisores políticos e racionalizar a sua ação, assim como informar o debate público nesta matéria.

Desta forma, a opção pelo tema da cibersegurança deveu-se ao facto de se ter constatado que este se afigura como um tema muito pouco abordado pelos investigadores que desenvolvem atividades na área das políticas públicas (principalmente em Portugal), traduzindo-se essa falta de investigação na necessidade de desenvolvimento de uma política pública nacional de cibersegurança eficiente e coerente, bem como de canais adequados de comunicação, que devem ser implementados, de acordo com as orientações da UE para o seu desenvolvimento e os esforços internacionais para alcançar a segurança do ciberespaço ao nível global.

Os esforços internacionais nesta área prendem-se com o facto do ciberespaço ter características próprias, diferentes do mundo físico, que propiciam a realização de (ciber)crimes, tais como: sem fronteiras, impacto imediato das ações realizadas através da internet, possibilidade da sua utilização para fins maléficos, de fácil acesso, possibilidade da realização de ações de forma anónima, etc.

1.2 Metodologia

1.2.1 Metodologia de Investigação

Para realizar este projeto procedeu-se a uma análise documental da literatura, legislação e outros documentos de caráter político, produzidos, em Portugal, sobre esta matéria, documentação proveniente dos órgãos da UE (ex. orientações, directivas, comunicações), tal como literatura e documentos de cariz político de outros países (não) membros da UE (ex. estratégias nacionais de cibersegurança).

[22] Consultar http://www.asjp.pt/2013/12/02/militares-querem-fazer-ataques-pela-internet/ (consultado a 12/05/2014 15:50).

Foram também efetuadas dezassete entrevistas a atores chave na área da cibersegurança em Portugal (um elemento que desempenha funções de topo no GNS, um elemento da direção do CERT.PT (da Fundação para a Computação Científica Nacional - FCCN), um elemento com funções de topo em matéria de segurança na Autoridade Nacional de Comunicações (ANACOM), elementos do recém--criado CNCseg, um elemento da Polícia Judiciária - PJ -, com funções na área da cibersegurança, um elemento com funções de topo na Divisão de Comunicações e Sistemas de Informação - DICSI -, do Estado-Maior-General das Forças Armadas - EMGFA -, um elemento com funções de topo em matéria de proteção de infraestruturas críticas, da Autoridade Nacional de Proteção Civil - ANPC -, o responsável pela segurança de uma empresa que fornece serviços de segurança informática para privados, para o Estado português e outros Estados estrangeiros (AnubisNetworks), um elemento que já dirigiu o Centro de Gestão da Rede Informática do Governo - CEGER -, um elemento que já dirigiu a Agência para a Modernização Administrativa - AMA -, um perito em políticas públicas na área da sociedade da informação, que participou na elaboração do Livro Verde para a Sociedade da Informação em Portugal, da Estrutura Nacional de Segurança da Informação, foi presidente da FCCN, foi representante de Portugal no Conselho de Administração da Agência Europeia para a Segurança das Redes e da Informação - ENISA -, entre outras funções, o presidente da Comissão Técnica 163 (CT 163), entre outros[23].

1.2.2 Metodologia de Análise

Partindo da questão "Qual tem sido a ação política em matéria de cibersegurança em Portugal?", procurou-se perceber quais têm sido as iniciativas, decisões e medidas políticas implementadas em Portugal nesta matéria, tal como os atores envolvidos nesse processo.

Procurou-se ainda perceber se existem adequados mecanismos de comunicação entre esses atores e o tipo de recursos aos quais têm acesso.

Uma vez que se têm desenvolvido algumas iniciativas e têm sido implementadas algumas medidas de política pública relacionadas com a cibersegurança, em Portugal, para além do facto dos atores intervenientes nesta área serem vários e uns participam em várias iniciativas, enquanto outros apenas em determinada área de atuação do Governo (ex. AMA), escolheu-se o ciclo das políticas públicas ou modelo das etapas das políticas públicas, como modelo de análise a utilizar nesta investigação.

Este modelo de análise das políticas públicas foi introduzido por Lasswell, em 1956, no seu livro *The Decision Process: Seven Categories of Functional Analysis*[24] .

[23] As entrevistas tiveram lugar entre julho e outubro de 2014 e revelaram-se essenciais para o desenvolvimento deste projeto, pois a cibersegurança envolve decisões estratégicas e o tratamento de informação classificada e sensível, à qual os cidadãos em geral não têm acesso, tendo, por isso, sido uma fonte muito rica de informação à qual não seria possível aceder de outra forma.

[24] Segundo Lasswell, o processo político compreende sete fases: o conhecimento; a promoção; a prescrição; a invocação; a aplicação; a conclusão; a avaliação.

Porém, deste então, este modelo tem vindo a ser utilizado por diversos autores e sofrido alterações, sendo atualmente mais comum considerar apenas quatro ou cinco, ao invés das sete fases consideradas por Lasswell, em 1956[25].

Para a realização deste estudo restringimo-nos a cinco fases: o surgimento do problema; o agendamento; o planeamento; a implementação; e a avaliação das políticas públicas.

Apesar de diretamente relacionados, separamos o surgimento do problema da cibersegurança em Portugal, do agendamento, i.e., a introdução dessa questão na agenda política nacional, porque nos parece ser pertinente uma explicação algo detalhada das circunstâncias em que esta questão entra na sociedade portuguesa.

O surgimento do problema, como a própria designação indica, consiste no momento em que determinada questão é definida como sendo um problema que necessita de intervenção política.

O agendamento consiste no reconhecimento, pelos decisores políticos, desse problema e da sua colocação na lista de questões que afetam a sociedade e devem ser tidas em consideração para uma possível intervenção política, i.e., a introdução na agenda política nacional.

O planeamento das medidas políticas consiste na definição dos objetivos a alcançar para resolver esse problema e na consideração de diferentes alternativas de ação[26].

A fase da implementação consiste na aplicação das medidas políticas, pelos atores responsáveis por essa implementação, tal como foram desenhadas. Esta tende a ser uma fase difícil de analisar, pelo menos em Portugal, uma vez que os planos de muitas das medidas políticas não discriminam claramente os objetivos, os atores responsáveis pela implementação, os instrumentos a utilizar, os orçamentos, etc.

Esta falta de objetividade na formulação das medidas políticas pode resultar na distorção das intenções dos decisores políticos e ainda no atraso ou bloqueio da implementação das medidas (Jann e Wegrich, 2007: 51).

Quanto à avaliação, embora possa estar presente em diversas fases do ciclo de uma política pública, este modelo considera-a como a última fase do ciclo. Esta fase consiste na análise e avaliação do que foi realizado, do processo de implementação das medidas e dos instrumentos políticos e na confrontação com os objetivos predefinidos.

Esta é uma fase muito importante, porque permite avaliar o desempenho dos atores envolvidos no processo pelo qual passam as políticas públicas, assim como justificar a ação política em determinada área (ex. se um projeto-piloto teve muito êxito, justifica-se o seu alargamento a um público mais vasto ou vice-versa) (Jann e Wegrich, 2007: 54).

[25] Exemplos de autores que utilizam quatro ou cinco, ao invés das sete fases, para a análise das políticas públicas são: Brewer e deLeon (1983); May e Wildavsky (1978); Anderson (1975); Jenkins (1978); Hill (2009); Rodrigues (2014).

[26] Para um correto planeamento de uma política pública deverão ficar claramente definidos: os objetivos (mensuráveis), os instrumentos de política a utilizar, os orçamentos, os atores envolvidos, as suas funções e como as devem cumprir, o público-alvo, a calendarização, etc.

No entanto, neste estudo não será dado grande enfoque à fase da avaliação, por um lado, por se tratar de uma área de intervenção política à qual, apesar da sua importância, não tem sido dada grande prioridade, tendo sido apenas implementadas algumas medidas políticas dispersas, que não foram alvo de avaliações e, por outro lado, porque algumas das medidas implementadas não parecem ter sido desenhadas da melhor forma, ou seja, sem uma clara discriminação de objetivos mensuráveis, dos orçamentos, dos recursos, dos atores e das suas funções, entre outros - fatores essenciais, não só, para uma eficaz e eficiente implementação, mas também para a avaliação das medidas[27].

O ciclo das políticas públicas, como modelo de análise, tem algumas vantagens e desvantagens.

Algumas das desvantagens são: o facto do processo pelo qual passa uma política pública nem sempre ter todas as fases aqui apresentadas ou nem sempre de acordo com a sequência definida; o facto de ser um modelo que tem implícita uma perspetiva *top-down*, i.e., a ideia de que uma política pública começa no topo da hierarquia política (o Governo) e acaba, ou seja, é implementada e avaliada, por elementos de entidades públicas ou privadas, que se encontram hierarquicamente abaixo dos primeiros; o facto de não ter em consideração a influência que a relação entre as diversas leis, programas políticos, normas, entre outros, tem sobre as políticas públicas; o facto de não ter em conta as relações entre os vários atores e entidades intervenientes na mesma área de política, neste caso a cibersegurança (Jann e Wegrich, 2007: 57-58 e Rodrigues, 2014: 31).

Contudo, apesar das desvantagens apresentadas, este modelo apresenta diversas vantagens, daí o facto de ter vindo a ser usado e aprimorado desde a década de 50, quando foi introduzido em exercícios de análise de políticas públicas, por Lasswell.

Algumas das vantagens do modelo são: o facto de permitir identificar quem são e qual o papel dos diversos atores intervenientes no processo pelo qual passa uma política pública, bem como a sua relevância em cada fase; o facto de permitir focarmo-nos numa única política pública ou medida de política pública, sem nos dispersarmos com informação considerada secundária, o que demonstra ser muito útil para investigações académicas, por exemplo; o facto de ser de tal forma flexível que permite a introdução de diferentes teorias para analisar e responder a questões relacionadas com determinada fase, por exemplo; o facto de permitir identificar e perceber dinâmicas internas e peculiaridades do processo de elaboração das políticas públicas, como os fatores que propiciam ou condicionam a ação política, etc (Jann e Wegrich, 2007: 57-58 e Rodrigues, 2014: 31).

Além destas razões e, contrapondo algumas das desvantagens apresentadas, como, por exemplo, o facto deste modelo ter implícita uma perspetiva *top-down*, este modelo parece adequar-se à análise de modelos políticos de representação democrática[28], como acontece em Portugal. O facto deste modelo não ter em conta a relação entre as diversas leis, programas políticos, normas e outros, também se pode

[27] Uma possível justificação para o desenho de medidas pouco detalhadas é o *blame-avoidance*, i.e., a necessidade que os políticos têm de evitar a culpa sobre ações pouco populares, em vez de tentar reivindicar o mérito pelas ações mais populares (Weaver, 1986: 371; *apud.* Hill, 2009: 164).

[28] Os modelos políticos de representação democrática caracterizam-se por ser modelos em que os políticos tomam as decisões, os legisladores traduzem-nas em leis e outros atores implementam-nas (Jann e Wegrich, 2007: 49).

mostrar como uma vantagem no estudo aqui apresentado, pois o intuito é limitar a análise às medidas políticas mais diretamente relacionadas com a cibersegurança, evitando a dispersão. O facto de não ter em consideração as relações entre os diversos atores intervenientes na garantia da cibersegurança em Portugal, também não se apresenta aqui como um problema, uma vez que este é um modelo bastante flexível, que permite a introdução da informação necessária para completar a análise.

Posto isto, considerando que este modelo permite decompor em fases o processo político que envolve a cibersegurança em Portugal, possibilitando perceber as dinâmicas que estão por detrás das iniciativas e dos bloqueios à ação política, que têm acontecido em Portugal, no âmbito da cibersegurança e tendo em mente que este modelo deve ser sempre completado com outras teorias explicativas e informação pertinente, assim como a noção de que nem sempre acontecem todas as fases e nem sempre sucedem segundo a sequência pré-definida[29], este modelo apresenta-se como uma opção adequada para se começar a estudar determinada área das políticas públicas, para daí se puder avançar para análises mais detalhadas e teorias mais complexas para o estudo dessas mesmas medidas ou políticas públicas[30].

Além disso, este modelo permite ainda "combinar a análise de políticas públicas para fins académicos com as preocupações em racionalizar a ação política", que é precisamente o caso do trabalho aqui apresentado[31] (Rodrigues, 2014: 31).

[29] Citando Friedrich "Public policy is being formed as it is being executed and it is likewise executed as it is being formed" (Friedrich, 1940: 6). Esta citação adequa-se à ação política em matéria de cibersegurança em Portugal.
[30] Pretende-se que este trabalho seja o início de um estudo mais aprofundado da ação política nacional, em matéria de cibersegurança.
[31] Considera-se que o facto deste modelo possibilitar a decomposição do processo político em fases é de extrema utilidade no caso da cibersegurança, em particular, pois, por um lado essa decomposição facilita, numa fase posterior, a perceção da totalidade do processo político e, por outro lado, a ação política nesta área tem sido pautada pela falta de coerência e dispersão, como se pode verificar na Figura 1, na página 16, que documenta a ação política em matéria de cibersegurança em Portugal.

CAPÍTULO 2. A CIBERSEGURANÇA NA UNIÃO EUROPEIA

Ao nível europeu, existem algumas entidades com responsabilidades em matéria de cibersegurança e ciberdefesa, que têm contribuído bastante para o desenvolvimento do conhecimento e das políticas públicas nesta área. Entre essas entidades estão a ENISA, a Agência Europeia de Defesa (EDA), o Centro Europeu de Cibercrime (EC3), o Centro de Excelência Cooperativo de Ciberdefesa da OTAN (CCD CoE)[32], a Comissão Europeia, o Conselho da Europa, a OCDE, entre outras.

Em 2004, no seguimento da transformação das redes de comunicação e dos sistemas de informação num "fator essencial no desenvolvimento económico" e do aumento do número de brechas de segurança, que geraram "substanciais danos financeiros, minando a confiança dos utilizadores e prejudicando o desenvolvimento do *e-commerce*", foi criada a ENISA, com sede na ilha de Creta, que tem tido um papel essencial na evolução do conhecimento em matéria de cibersegurança (Regulamento nº 460/2004, do Parlamento Europeu e do Conselho).

Entre as funções da ENISA estão: "contribuir para uma segurança das redes e da informação de alto nível entre a comunidade (europeia) e o desenvolvimento de uma cultura de segurança das redes e da informação (…), contribuindo (…) para um bom funcionamento do mercado interno"; promover a cooperação entre os diferentes atores intervenientes na segurança das redes e da informação; "ajudar os Estados-Membros a desenvolver as suas capacidades para prevenir (…) e responder a problemas de segurança de informação"; "contribuir para a consciencialização das questões de segurança das redes e da informação (…) promovendo a troca de boas práticas (…) e procurando sinergias"[33] (Regulamento nº 460/2004, do Parlamento Europeu e do Conselho).

Esta agência tem promovido a cooperação entre os diversos atores envolvidos nesta área, funcionando como facilitador das suas relações e promovendo a troca de informação e partilha de boas práticas, promovendo também a consciencialização e a formação na área da cibersegurança (ex. através dos diversos estudos realizados e publicações sobre esta matéria[34] ou da organização e colaboração em eventos de consciencialização para a temática da cibersegurança, como é o caso das iniciativas relacionadas com o mês europeu da cibersegurança[35]).

---

[32] Apesar do CCD CoE não ser um organismo da UE, mas sim da OTAN, decidimos incluí-lo por estar sediado e contribuir também para o desenvolvimento do conhecimento sobre matérias relacionadas com a ciberdefesa, na comunidade europeia.

[33] A atuação desta agência baseia-se numa lógica de mercado, procurando contribuir para o bom funcionamento do mercado interno, sem interferir nas competências relacionadas com a segurança pública, defesa e segurança nacional (Regulação nº 460/2004, do Parlamento Europeu e do Conselho).

[34] Consultar http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-an-implementation-guide , http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/cyber-security-strategies-paper/at_download/fullReport , http://www.enisa.europa.eu/activities/cert/support/guide , http://www.enisa.europa.eu/activities/cert/support/exercise, http://www.enisa.europa.eu/ (consultado a 28/10/14).

[35] No âmbito das comemorações do mês europeu da cibersegurança, este ano, entre os dias 6 e 10 de outubro, tiveram lugar no GNS uma série de conferências e *workshops* sobre cibersegurança (iniciativa que contou com a participação da ENISA).

A Agência Europeia de Defesa (EDA), sensivelmente desde 2010, tem vindo a contribuir para a ciberdefesa da comunidade europeia, através do seu esforço para o desenvolvimento de capacidades neste domínio, no âmbito da Política Comum de Segurança e Defesa (PCSD)[36].

Entre as iniciativas da EDA nesta área, destacamos alguns projetos na área de treino e exercícios (ex. o *Digital Forensics Pilot Course* ou o *Decision Making Course and Exercise*), outros na área da investigação (ex. a criação de um *road map* para os próximos 10 anos, a criação de um projeto para o desenvolvimento de soluções para a deteção e o combate às APTs - Advanced Persistent Threats) e outros no âmbito da criação de capacidades de ciberdefesa (ex. um projeto de transferência do conhecimento académico de criptografia para produtos inovadores, inclusive para uso militar)[37].

No âmbito destes projetos, a EDA não só promove o aproveitamento da investigação académica para o desenvolvimento das capacidades de ciberdefesa, como também desempenha um papel de facilitador das relações entre os diversos atores intervenientes nesta área, como se verificou ter sido o caso do curso e exercício piloto, que teve lugar em Portugal, entre os dias 11 e 14 de maio de 2014, que permitiu o contacto, o trabalho conjunto e a criação de laços entre esses atores.

Devido ao crescente número de cibercrimes e a pouca confiança no uso da internet, por parte de muitos cidadãos europeus[38], em 2013 foi criado o Centro Europeu de Cibercrime (EC3), integrado na Polícia Europeia (EUROPOL), em Haia (Holanda).

Este organismo europeu tem cinco funções principais: cruzamento de dados (recolhe dados das autoridades nacionais competentes dos vários Estados-Membros (EM) da UE e apoia-os na aplicação da lei nesta matéria); operações (apoia os EM na investigação de cibercrimes e facilita a cooperação internacional com parceiros não europeus, em casos de investigação mais complexos); estratégia (produz análises sobre a tendência dos cibercrimes e da sua execução); investigação e treino (desenvolve ferramentas forenses a ser usadas pelos EM na investigação de cibercrimes e colabora com a Academia Europeia de Polícia - CEPOL - no treino dos elementos policiais); divulgação (desenvolve iniciativas de consciencialização conjuntas com a sociedade civil, o setor privado, a academia, as CERTs nacionais, a ENISA, etc).

O CCD CoE, sedeado em Tallinn (Estónia), criado em 2008, sensivelmente um ano após os ciberataques aos sistemas informáticos daquele país, foi o resultado do primeiro esforço conjunto para a criação de um pólo de conhecimento sobre ciberdefesa, baseado na investigação, no treino e no ensino dessa matéria. Este é um centro aberto a todos os membros da OTAN, onde são treinados todos os anos diversos militares dos países membros da aliança, incluindo Portugal.

---

[36] A ciberdefesa, ao nível da comunidade europeia, está integrada na "*Capability, Armament & Technology - CET*", uma das áreas de atuação da EDA.

[37] Consultar http://www.eda.europa.eu/docs/default-source/eda-factsheets/2014-03-24-factsheet_cyber_defence_high- (consultado a 9/10/14).

[38] 61% dos europeus estão preocupados com a possibilidade de experienciarem o roubo de identidade, 49% estão preocupados com a fraude *online* e 43% estão preocupados por poder não conseguir aceder a serviços *online* devido a ciberataques (Comissão Europeia, 2012: 5).

Este Centro de Excelência tem promovido o desenvolvimento do conhecimento, ao nível mundial, sobre ciberdefesa, destacando-se, para além do já referido treino, a criação de um Manual do Direito Internacional aplicável à Ciberguerra ("*Tallinn Manual on the International Law Applicable to Cyber Warfare*") que, apesar de não ser considerado um documento legal, informa o pensamento de juízes, legisladores, entre outros, sobre a aplicação da lei a atos que possam ser considerados como ciberguerra.

A UE, principalmente a Comissão Europeia, tem estimulado os EM a desenvolverem determinadas capacidades de cibersegurança, como: a criação de um enquadramento regulamentar e político, no âmbito da segurança dos sistemas de informação e de comunicação; o desenvolvimento de operações de simulação de ciberataques em grande escala; o estabelecimento de linhas diretas de denúncia de conteúdos *online* ofensivos ou prejudiciais; a criação de plataformas nacionais de alerta; ministrar formação em segurança das redes e da informação nas escolas; a criação de equipas de resposta a emergências informáticas (CERTs) e o estabelecimento de redes nacionais de CERTs; o desenvolvimento das capacidades nacionais para a sensibilização e formação nesta área; a instituição de centros de excelência em matéria de cibersegurança a nível nacional ou com outros EM; a criação, juntamente com a ENISA, de planos de contingência e de cooperação, nacionais e europeus, em matéria de resposta a incidentes e recuperação em caso de catástrofes; a definição de estratégias nacionais de cibersegurança; a criação de autoridades nacionais competentes nessa matéria, etc[39].

Dada a importância desta matéria, a UE publicou, em 2013, a "Estratégia da União Europeia para a cibersegurança: Um ciberespaço aberto, seguro e protegido", que define cinco prioridades para a ação política nesta área: a garantia da resiliência do ciberespaço; a redução drástica da cibercriminalidade; o desenvolvimento das políticas e das capacidades no domínio da ciberdefesa, no quadro da PCSD; o desenvolvimento de recursos industriais e tecnológicos para a cibersegurança; o estabelecimento de uma política internacional coerente em matéria de ciberespaço para a UE, que promova os valores fundamentais da mesma (JOIN(2013) 1 final).

Em alguns casos por iniciativa própria, embora grande parte no seguimento dessas orientações da UE, vários têm sido os países a desenvolver as suas capacidades de cibersegurança, como: estratégias nacionais de cibersegurança (que orientam a ação política neste domínio), a criação de autoridades nacionais competentes em cibersegurança (que devem coordenar a ação nesta área) ou a criação de CERTs, responsáveis por uma resposta rápida aos incidentes de segurança informática[40].

Por esta razão, considera-se que o trabalho de consciencialização e as orientações emanadas dos órgãos da UE têm sido da maior importância para (acelerar) o desenvolvimento das políticas públicas de cibersegurança dos EM. Embora ainda não tenham tido o efeito desejado em Portugal, uma vez que

[39] Consultar COM(93) 700 final; COM(96) 592 final; COM(2001) 298 final; COM(2006) 251 final; Diretiva do Parlamento Europeu e do Conselho 2009/140/CE, de 25 de novembro de 2009; COM(2010) 245 final; COM(2010) 673 final; JOIN(2013) 1 final, COM(2013) 48 final, entre outros.

[40] Incidentes de segurança informática são os eventos ou as ações que podem comprometer a disponibilidade, autenticidade, integridade e/ou confidencialidade dos dados armazenados ou transmitidos pelas redes e sistemas de informação e os serviços conexos oferecidos através dessas redes e sistemas (COM(2001) 298 final).

não tem uma estratégia nacional de cibersegurança e até maio de 2014 ainda estava em incumprimento com a data limite, avançada pela Comissão Europeia, para a constituição de uma CERT nacional[41].

Apesar da criação desse organismo ter sido aprovada em maio de 2014, pelo Decreto-Lei nº 69/2014, de 9 de maio (embora com uma maior abrangência e denominado por Centro Nacional de Cibersegurança), entrou em funcionamento apenas no dia 7 de outubro de 2014.

O Conselho da Europa também contribui para o desenvolvimento da cibersegurança na UE, destacando-se a realização da Convenção sobre Cibercrime, a 23 de novembro de 2001, em Budapeste[42].

Destacamos também a OCDE, porque contribui para o desenvolvimento de capacidades de cibersegurança ao nível internacional, incluindo na UE, através da publicação de diretivas e orientações relacionadas com este tema, mesmo que o intuito seja o crescimento económico[43].

Durante a elaboração do estudo aqui apresentado, não foi possível apurar como decorreu o processo de elaboração das estratégias nacionais, nem das medidas políticas de cibersegurança dos EM da UE, exceto Portugal, sobre o qual se foca o interesse deste trabalho[44]. No entanto, foram analisadas algumas estratégias e comparadas com a proposta portuguesa de Estratégia Nacional de Cibersegurança, tendo como resultado o seguinte quadro[45].

---

[41] Uma CERT nacional consiste numa capacidade de resposta a emergências informáticas, à qual compete: a monitorização e resposta a incidentes informáticos ao nível nacional; a ativação de mecanismos de alerta rápido em caso de incidente; a sensibilização para os perigos do uso desprotegido da internet; a divulgação de informação considerada relevante sobre riscos e incidentes às partes interessadas; a análise do nível do risco associado às ciberameaças, entre outros (COM(2013) 48 final).

[42] A Convenção sobre Cibercrime, do Conselho da Europa, pode ser considerada o primeiro e mais importante trabalho realizado ao nível internacional em matéria de cibersegurança, reconhecendo a criminalidade informática como um problema transfronteiriço, que requer a partilha de esforços e soluções coletivas, traduzindo-se num exemplo de partilha de conhecimentos e esforços e de promoção do consenso, com o intuito de se alcançar melhores políticas de combate à cibercriminalidade, entre os Estados-Membros da UE.

[43] Consultar: http://www.oecd.org/sti/ieconomy/informationsecurityandprivacy.htm , http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm , http://www.oecd.org/internet/ieconomy/2002-security-guidelines-review.htm , http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf (consultado a 17/09/2014).

[44] Considera-se que seria pertinente a realização desse estudo comparativo, num próximo trabalho, para tentar perceber as diferenças neste processo, os atores envolvidos e os impactos que possam ter tido no processo de (não) aprovação das mesmas, assim como no processo de elaboração das próximas estratégias nacionais de cibersegurança desses mesmos países, pois já vários implementaram mais do que uma estratégia nesta área (ex. Reino Unido, Holanda) e outros encontram-se em processo de revisão das atuais estratégias (Estónia).

[45] Na elaboração do quadro foram considerados os EM da UE com avançadas respostas de cibersegurança ou estratégias nacionais consideradas avançadas (de acordo com o Cyber Power Index, 2011 - consultar http://www.boozallen.com/content/dam/boozallen/media/file/Cyber_Power_Index_Findings_and_Methodology.pdf) e os EM considerados exemplos de boas práticas nesta matéria (consultar http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/cyber-security-strategies-paper/at_download/fullReport), aos quais se juntou Portugal, sobre o qual esta análise se foca, bem como Espanha, seu Estado vizinho, com quem desenvolve diversas iniciativas conjuntas em matéria de segurança (projetos na área da cibersegurança, desenvolvidos pelo Instituto da Defesa Nacional e a Escuela de Altos Estudios de la Defensa, do Centro Superior de Estudios de la Defensa Nacional de Espanha; a IBERGRID, i.e., uma iniciativa conjunta dos dois Governos, com o objetivo de integrar, numa só rede, as infraestruturas de computação GRID de ambos os países, aumentando as capacidades e reforçando a cooperação de instituições e investigadores dos dois países, que desenvolvam atividades nesta área, nomeadamente na segurança informática).

Quadro 1: Sistemas de Cibersegurança na União Europeia

País	Ano de publicação da estratégia	Ciberameaça	Nível de prioridade dada à ciberameaça	Autoridades com competências na matéria
Estónia	2008 (em processo de revisão)	Foco nos efeitos das ameaças	Alta/Elevada	A Autoridade Estoniana para os Sistemas de Informação (RIA) é a autoridade última em matéria de cibersegurança, coordenando a resposta a incidentes, a proteção de infraestruturas críticas de informação e servindo de plataforma de cooperação e integração de esforços. A ciberdefesa compete essencialmente ao setor militar, que trabalha em estreita colaboração com a NATO, através do *Cooperative Cyber Defence Centre of Excellence*, com sede na Estónia.
Finlândia	2013	Não há referência	Não há referência	Uma vez que não existe uma autoridade nacional com competência em matéria de cibersegurança, essa é partilhada por diversos ministérios, de acordo com as suas responsabilidades (ex. o Ministério das Finanças é responsável pela direção e desenvolvimento da segurança da informação do governo, o Ministério da Defesa pela segurança dos seus próprios sistemas de informação, o Ministério dos Transportes e Comunicações pela segurança das infraestruturas críticas, o Ministério do Interior pela segurança interna).
França	2011	Não há referência	Grande ameaça	A Agence Nationale de la Sécurité des Systèmes d'Information é a autoridade última em matéria de cibersegurança (organização sob dependência direta do Primeiro-Ministro, à qual estão subordinadas outras com competências na matéria, como o Ministério da Defesa Nacional, a Direção-Geral de Armamento, a Direção de Proteção e da Segurança da Defesa, o Ministério do Interior, o Gabinete da luta contra a criminalidade, entre outros).
Alemanha	2011	Ciberterrorismo, cibercrime e ciberguerra; desastres naturais; falhas humanas ou técnicas	Não há referência	Liderança dividida entre o Ministério do Interior e o Centro de Ciberdefesa, sendo o primeiro responsável pelo desenvolvimento e implementação das políticas públicas nesta matéria e o Centro de Ciberdefesa um pólo de recursos de diferentes organismos governamentais, incluindo os serviços policiais e de inteligência.
Reino Unido	2009/2011	Criminosos; Estados; *hackers* patrióticos; grupos terroristas; hacktivistas	A mais alta prioridade	O Gabinete de cibersegurança e segurança da informação (OCSIA) é a autoridade última em matéria de cibersegurança (parte integrante do gabinete do Primeiro-Ministro), à qual compete mobilizar a cooperação e coordenar a ação dos vários atores governamentais (Centro de Operações de Cibersegurança, *Home Office*, Ministério da Defesa Nacional, GCHQ, entre outros), bem como promover uma abordagem política comum.

Dinamarca	Não há referência	Prejuízos financeiros; Disrupção ou controlo da infraestrutura de IT e ciberguerra; espionagem; ciberterrorismo	Altamente provável	A liderança da política de cibersegurança é partilhada pelos Serviços de Inteligência e Segurança, responsáveis pela análise, deteção e prevenção de cibercrimes, bem como pelo Centro Nacional de Crimes de Alta Tecnologia, que coopera com as unidades nacionais de investigação e o Ministério Público na investigação e aplicação da lei. Para além destas entidades, em caso de emergência aplica-se o princípio da "responsabilidade do setor", i.e., a instituição que normalmente é responsável por determinada área é também responsável por essa área em caso de acidente grave ou catástrofe.
Holanda	2011/2013	Estados; organizações privadas; criminosos profissionais; terroristas; hactivistas; *script kiddies*; ciberinvestigadores; atores internos	Alta/Elevada prioridade	O Centro Nacional de Cibersegurança é a autoridade última em matéria de cibersegurança (este centro encontra-se sob a dependência do Ministério da Justiça, é apoiado por um Conselho de Cibersegurança que define as prioridades no combate às ciberameaças, considera a necessidade de mais investigação e estabelece as melhores formas de partilha do seu conhecimento com as várias partes envolvidas, sejam públicas ou privadas) e desenvolve as suas competências nesta matéria com a colaboração da Equipa de Crimes de Alta Tecnologia da polícia nacional, da Cyber *Taskforce* do Ministério da Defesa Nacional e dos serviços de inteligência civis e militares.
Espanha	2013	Estados; fenómenos naturais; ameaças internas; sabotagem; espionagem; organizações terroristas; cibercrime; falhas técnicas; crime organizado, etc.	Não há referência	O Conselho de Segurança Nacional é a autoridade última em matéria de cibersegurança (esta entidade encontra-se sob dependência direta do Primeiro-Ministro, apoiando-o na direção da política de segurança nacional), sob a qual se encontram o Comité Especializado de Cibersegurança, cuja composição reflete o espectro das entidades envolvidas na garantia da cibersegurança em Espanha, bem como o Comité Especializado de Situação. Ao primeiro comité referido compete apoiar o Conselho de Segurança Nacional, nomeadamente através da promoção das relações de cooperação entre as entidades governamentais com competências na matéria e outras organizações dos setores público e privado, enquanto ao Comité Especializado de Situação compete a gestão de crises no âmbito da cibersegurança, garantindo a interconexão entre os centros operativos implicados, facilitando o controlo e a transmissão das decisões políticas e operacionais, de forma a assegurar uma adequada resposta em situações de crise.

Portugal	Proposta publicada em 2012	Ciberataques em larga escala às infraestruturas críticas	"uma prioridade nacional" (Proposta de Estratégia Nacional de Cibersegu--rança)	O Centro Nacional de Cibersegurança (CNCseg), criado no âmbito do Gabinete Nacional de Segurança, é a autoridade última em matéria de cibersegurança, relativamente ao Estado e aos operadores de infraestruturas críticas e deve promover e assegurar a articulação e a cooperação entre os vários intervenientes na garantia da cibersegurança nacional, assim como coordenar e assegurar a resposta a incidentes de informática. Esta autoridade deve coordenar a sua ação com outras entidades como: a ANACOM (autoridade nacional reguladora das comunicações); o CEGER (a autoridade responsável pela proteção da rede e sistemas de informação e comunicação dos elementos de topo do Governo); o GNS (responsável pela proteção da informação classificada em Portugal); o Secretário-Geral do Sistema de Segurança Interna, que é responsável pela garantia da articulação das forças e dos serviços necessários à gestão de incidentes táctico-policiais (ex. ciberataques a infraestruturas críticas); a ANPC (responsável pelo planeamento civil de emergência para fazer face a situações de crise); o CEMGFA, que é a autoridade última em matéria de ciberdefesa, a qual deve ser coordenada com as políticas públicas de cibersegurança; o Serviço de Informações da República Portuguesa, responsável pela recolha e análise da informação necessária à previsão de incidentes e proteção da infraestrutura nacional de informação, bem como da própria informação em Portugal; entre outros.

Fonte: Adaptado de Robinson, N. *et al.*, 2013, págs vii-viii.

É de salientar que não fez parte dos objetivos deste exercício analisar as relações nem identificar ao pormenor os atores intervenientes na proteção do ciberespaço dos restantes Estados-Membros (EM) da UE, pelo que esse tipo de análise se foca apenas no caso português.

Com base na comparação realizada, verifica-se que a maioria dos EM da UE considera as ciberameaças como estando entre o tipo de ameaças mais prioritárias.

Verifica-se também que a maioria dos EM optaram por um modelo interdepartamental de resposta à cibersegurança, ou seja, as competências e responsabilidades atribuídas a cada setor ou entidade governamental no mundo físico, são transpostas para o "mundo virtual" (ex. aos serviços policiais e judiciais compete gerir as investigações criminais relativas aos cibercrimes, aos serviços de informações compete a investigação relacionada com a ciberespionagem) (Robinson, N. *et al.*, 2013: ix).

A natureza das autoridades nacionais competentes em matéria de cibersegurança difere entre países, sendo, em alguns, órgãos de coordenação criados no âmbito das orientações da UE para a adoção de determinadas medidas em matéria de cibersegurança (como acontece na Estónia - Estonian Authority for Information Systems -, em França - Agence Nationale de la Sécurité des Systèmes d'Information -, ou mesmo, em Portugal - CNCseg[46]), enquanto noutros, órgãos, ou melhor, departamentos, criados no seio de organismos governamentais já existentes, como é o caso do Office of Cyber Security and Information Assurance (OCSIA), inserido no Gabinete do Primeiro-Ministro do Reino Unido.

O próprio organismo com competências políticas nesta área difere entre países, sendo em alguns, o gabinete do Primeiro-Ministro (Reino Unido), noutros o equivalente ao Ministério da Administração Interna português (Alemanha), noutros o Ministério da Defesa Nacional (Dinamarca) e noutros ainda o Ministério das Finanças (Finlândia) (Robinson, N. *et al.*, 2013: ix)[47].

Quanto à natureza da autoridade do CNCseg, é semelhante à autoridade congénere francesa, uma vez que, embora no âmbito do GNS, constitui-se um novo organismo, na dependência da Presidência do Conselho de Ministros.

Verifica-se que a importância dada às CERTs nacionais também difere entre os EM e nem todos têm este tipo de serviço[48], apesar dos órgãos da UE terem publicado orientações no sentido de todos virem a criar CERTs nacionais até 2012 (ex. COM(2010) 673 final).

Verifica-se também que, em Portugal, à semelhança do que acontece na Alemanha, onde foi adotado o modelo de separação de "ciberpoderes" entre o setor civil e o setor militar, existe uma autoridade com competências em matéria de cibersegurança - o CNCseg - e outra com competências em

[46] No que concerne a Portugal, à semelhança do que aconteceu em França, foi criada uma autoridade nacional com competências na área da cibersegurança - o Centro Nacional de Cibersegurança, designado por CNCseg - antes ainda da aprovação de uma estratégia nacional de cibersegurança.

[47] É de referir que esta falta de harmonização no que toca à liderança política em matéria de cibersegurança, entre EM pode refletir-se em alguma dificuldade na harmonização dos procedimentos ou mesmo no aumento da cooperação entre países pelo que, tal como sugere Robinson N. *et al.* (2013), seria interessante mapear os decisores políticos em matéria de ciberespaço nos vários países, como tentativa de se obter mais conhecimento sobre a cooperação internacional neste domínio.

[48] Consultar https://www.enisa.europa.eu/activities/cert/background/inv/certs-by-country-interactive-map (consultado a 08/10/14).

matéria de ciberdefesa - o CEMGFA. Também à semelhança do que existe na Alemanha, ou seja, uma estratégia nacional de cibersegurança e outra de ciberdefesa, em Portugal foi publicada em 2012 uma proposta de Estratégia Nacional de Cibersegurança e em 2013 foi apresentado, um documento orientador de uma Política Nacional de Ciberdefesa (Despacho nº 13692/2013 do Ministro da Defesa Nacional).

Esta separação de funções coincide com a ideia tradicional e que está patente na Constituição da República Portuguesa (CRP), de que os militares se ocupam das ameaças externas ao Estado (sem incluir tarefas de gestão e manutenção da ordem pública) e o setor civil, neste caso as polícias civis, se ocupam das ameaças internas, i.e., a segurança pública face a ameaças internas. Ideia proveniente da época das guerras e da necessidade de proteger os Estados e garantir a soberania nacional[49].

Porém, esta ideia tem vindo a ser questionada, porque o tipo de ameaças que se põem aos Estados, especialmente os ocidentais, são diferentes (ex. as ciberameaças). As ciberameaças são caracterizadas pela grande dificuldade de atribuição e pelo impacto imediato e elevado, com poucos recursos (financeiros, humanos e materiais), entre outros. Este tipo de ameaças não reconhece fronteiras entre os setores civil e militar, levando a uma necessidade de repensar o paradigma da segurança externa e da segurança interna, pelo menos nesta área.

Outra questão que se põe no caso das ciberameaças é o facto do mesmo tipo de vírus informático servir para atacar tanto a soberania de um país como a sua segurança pública ou interna, por exemplo. Desta forma, o essencial é a garantia da cooperação[50] e da articulação e interoperabilidade das funções e capacidades destes setores, o que, aliás, está previsto, tanto no documento que estabelece os termos do funcionamento do CNCseg, prevendo que "O CNCseg atua (…) em estreita articulação e estreita cooperação com as estruturas nacionais responsáveis pela ciberespionagem, ciberdefesa, cibercrime e ciberterrorismo"[51]), como no Despacho nº 13692/2013, de 11 de outubro, do Ministro da Defesa Nacional, que prevê o desenvolvimento de "um sistema de partilha de informação aos vários níveis e patamares de decisão (…) e de colaboração com a rede nacional de serviços de resposta a incidentes de segurança informática (CSIRT)", entre outras entidades.

Deve-se ainda referir que uma das caraterísticas da esmagadora maioria das estratégias de cibersegurança (europeias e internacionais) é a aposta na investigação neste domínio, uns baseados numa lógica mais virada para a garantia da superioridade do conhecimento ou tecnológica (ex. França,

[49] Segundo Robinson, N. *et al.* (2013), esta separação constitucional entre responsabilidades civis e militares pode constituir um desafio a uma abordagem integrada de cibersegurança, uma vez que, especialmente no meio militar, a autorização para a partilha de informação tem que vir de superiores hierárquicos, pelo que essa partilha pode acontecer tardiamente ou nem sempre acontecer (Robinson, N., *et al.*, 2013: 19).

[50] Esta cooperação não poderá acontecer apenas ao nível nacional, pois, pela razão acima apresentada, o mesmo vírus poderá ter como alvo Estados diferentes. Logo, é essencial a criação de plataformas e mecanismos de comunicação rápidos, através dos quais os vários países aliados possam partilhar informação relevante para proteção e resposta a ciberataques. Estas plataformas estão previstas em algumas estratégias de cibersegurança de países europeus e a Estratégia da União Europeia para a cibersegurança prevê o apoio financeiro à criação das mesmas, através do Mecanismo Interligar a Europa (CEF).

[51] É importante salientar que o "ciberterrorismo" e a "ciberespionagem" ainda não estão legislados, não havendo assim entidades responsáveis e que sejam responsabilizadas pelo seu combate e, possivelmente, nem recursos e/ou instrumentos adequados ao seu combate.

Holanda), outros com o intuito de tirar proveitos económicos desse investimento (ex. Espanha, Reino Unido), por exemplo. Contudo, analisando a proposta portuguesa de Estratégia Nacional de Cibersegurança, conclui-se que ainda não nos debruçámos sobre a relevância de um plano estratégico para a investigação nesta área, pois a única referência à investigação circunscreve-se à criação de tecnologias de segurança que deverão ser desenvolvidas nas Universidades e Centros de Investigação nacionais, sem qualquer alusão a um plano nacional para a investigação desta matéria, nem a sua extensão a outras áreas, igualmente importantes para a cibersegurança (ex. *awareness*, direito do ciberespaço).

Ainda relativamente à investigação, verificou-se que a Fundação para a Ciência e a Tecnologia (FCT), que gere o financiamento para a investigação científica em Portugal e é responsável pela "mobilização das políticas públicas para a Sociedade da Informação", nomeadamente por meio do desenvolvimento de atividades na área de I&D em "Infraestruturas e Segurança" (incluindo a cibersegurança) e cujo próprio *website* faz referência ao facto de que "o futuro da I&D e Inovação em TIC em Portugal passará sobretudo pela (sua) capacidade para potenciar e alavancar o potencial identificado", particularmente através da "promoção da liderança internacional das equipas de I&D portuguesas (…) em áreas onde a sua capacidade e qualidade são reconhecidas", não parece estar a fazê-lo[52].

[52] Este ano um laboratório de investigação na área da segurança das infraestruturas de informação críticas (do Prof. Paulo Veríssimo - um perito em cibersegurança, internacionalmente reconhecido) foi chumbado. Ao mesmo projeto foram atribuídos cinco milhões de euros, pela congénere luxemburguesa, da FCT. Consultar http://www.publico.pt/ciencia/noticia/paulo-verissimo-portugal-ainda-nao-concretizou-a-sua-estrategia-de-ciberseguranca-1668772 (consultado a 09/09/14).

CAPÍTULO 3. A CIBERSEGURANÇA EM PORTUGAL

Com base no ciclo das políticas públicas[53], seguidamente apresentam-se os atores intervenientes e as iniciativas que têm vindo a ser adotadas em Portugal, em matéria de cibersegurança.

3.1 O Problema

O problema da cibersegurança, tal como as restantes questões sujeitas a intervenção política, é um problema socialmente construído, dependendo de diversos fatores para ser entendido como "problema" (ex. o nível de consciencialização dos cidadãos e dos decisores políticos para a questão; as orientações e políticas das organizações regionais e internacionais, das quais, neste caso Portugal, faz parte, como a UE, OTAN ou a OCDE; o contexto social, económico e político vigente).

Ao nível da UE e, por inerência, assumimos que em Portugal também, como já foi referido, a cibersegurança é caracterizada pelas "precauções e ações (…) utilizadas para proteger o ciberespaço, tanto nos domínios civil como militar, contra as ameaças decorrentes da interdependência das suas redes e infraestruturas informáticas" (JOIN(2013) 1 final: 3).

Desta forma, o problema que aqui se trata é a necessidade de garantir a segurança da informação dos cidadãos, das organizações e do Estado, que circula e está alojada nos sistemas e nas redes informáticas e dos próprios sistemas e redes. Informação, redes e sistemas de informação que asseguram o funcionamento da sociedade portuguesa como a conhecemos, dado que as infraestruturas críticas nacionais (ex. rede de abastecimento de água, electricidade, gás, sistema bancário, serviços de emergência) dependem deles para funcionar com normalidade.

Até meados dos anos 90, esta questão não constituiu um problema para a sociedade portuguesa ou, pelo menos, não suscitava a necessidade de intervenção política, possivelmente porque, até então, poucos eram os cidadãos portugueses com computador pessoal e pouca era a informação de cidadãos, organizações e do próprio Estado a circular nas redes e nos sistemas informáticos, pois só em finais dos anos 90 se começou a informatizar os serviços da Administração Pública.

Posto isto, uma vez que, por um lado, os decisores políticos não sentiam necessidade de investir mais na cibersegurança e, por outro, os cidadãos também não sentiam essa necessidade e não pressionavam o Governo para que agisse nesse sentido, além do facto da própria UE só ter começado a demonstrar preocupações com esta matéria em 1989, através da R (89)9 do Conselho da Europa, sobre criminalidade informática (nove anos após a primeira orientação da OCDE, relacionada com a cibersegurança[54]), não tinha havido necessidade, por parte do Governo, de adotar medidas nesta área.

[53] Relembrar que as fases do ciclo das políticas públicas abordadas neste estudo são: o surgimento do problema, o agendamento, o planeamento, a implementação e a avaliação.
[54] Consultar http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (consultado a 20/09/2014).

Só após essa recomendação do Conselho da Europa, foi publicada a SEGNAC 4 (Resolução do Conselho de Ministros nº 5/90, de 28 de fevereiro), que define as instruções sobre segurança informática, no tratamento de matérias classificadas. Pouco tempo depois surgiu a Lei da Proteção de Dados Pessoais face à Informática (Lei nº 10/91, de 29 de abril) e a Lei da Criminalidade Informática[55] (Lei nº 109/91, de 17 de agosto), que demonstram preocupações com a informação informatizada.

Todavia, estas medidas - excluindo o SEGNAC 4, que diz respeito apenas ao tratamento de informação classificada - não previam concretamente a segurança das redes e dos sistemas de informação, mais comummente designada por cibersegurança.

Ao nível europeu, após a R (89)9 do Conselho da Europa, a Comissão Europeia elaborou e publicou, a 5 de dezembro de 1993, o Livro Branco sobre "Crescimento, Competitividade e Emprego: Os Desafios e as Pistas para Entrar no Século XXI"[56], que introduziu na agenda política da UE a preocupação com a normalização dos processos relacionados com as TIC e com a segurança dos sistemas de informação e de comunicação.

Em 1996, no seguimento desse e doutros trabalhos e orientações dos órgãos da UE, foi publicada a Resolução do Conselho de Ministros nº 16/96, de 7 de março, que cria uma Equipa de Missão para a Sociedade da Informação. Esta equipa teria a responsabilidade de apoiar o Ministro da Ciência e Tecnologia na elaboração de um Livro Verde para a Sociedade da Informação em Portugal.

O Livro Verde para a Sociedade da Informação em Portugal, apresentado em 1997, foi o primeiro documento político que visou as questões da proteção, integridade e autenticidade dos dados informáticos[57] (incluindo os dados classificados e não classificados).

À semelhança da lógica da UE, também as propostas do referido Livro Verde, em matéria de cibersegurança, tinham implícita uma lógica de mercado - orientada para um aumento da confiança dos utilizadores do comércio eletrónico, considerado como fonte de aumento de competitividade e emprego.

Assim, considera-se que o surgimento deste problema em Portugal consistiu num processo de transferência voluntária e convergência de questões da agenda política europeia para o nível doméstico.

De acordo com esta abordagem, as instituições, neste caso em particular a UE é entendida como uma fonte de normas ou quadros cognitivos e sistemas simbólicos que orientam a ação humana e política, assim como *scripts* culturais e esquemas difundidos pelos ambientes organizacionais, que servem propósitos simbólicos e não apenas propósitos utilitários (Schmidt, 2006).

Segundo esta teoria, as perceções, crenças e normas partilhadas pelos indivíduos sobre o que é socialmente aceite, moldam as suas identidades, influenciam os seus interesses e afetam o que é entendido como um problema e possíveis soluções. Portanto, quando confrontado com uma situação,

[55] Este documento introduziu na legislação nacional crimes como a falsidade e a sabotagem informáticas, o acesso e a interceção ilegítimas ou a reprodução ilegítima de programa protegido.
[56] Consultar COM(93) 700 final.
[57] Em nosso ver, a proteção, integridade e autenticidade dos dados informáticos só se alcançam eficaz e eficientemente através de uma política integrada de cibersegurança, ou seja, uma política que inclua não só segurança da informação mas também a proteção das redes e sistemas informáticos onde ela circula e está alojada.

um indivíduo ou um Governo procura identificá-la e reagir, consoante os quadros cognitivos e conhecimentos de que dispõe previamente, numa lógica de adequação. Assim, as orientações da UE para que os EM desenvolvam capacidades e intervenham na área da Sociedade da Informação, nomeadamente na cibersegurança, estão relacionadas com crenças partilhadas.

Pode-se então considerar que o surgimento do problema da cibersegurança em Portugal adveio de um processo de "aprendizagem social" resultante da internacionalização, particularmente da presença de Portugal em redes transnacionais e da consequente comunicação transnacional.

A comunicação transnacional consiste num conjunto de mecanismos de comunicação entre países, usados para o desenho de resoluções para problemas transnacionais e promoção transnacional de modelos políticos. A própria resolução de problemas transnacionais é baseada na aprendizagem social, através do desenvolvimento, em conjunto, de perceções sobre problemas comuns e soluções para problemas internos semelhantes, utilizando as experiências que conhecem.

Portanto, a comunicação transnacional consiste na difusão de políticas que, muitas vezes, resulta na convergência transnacional, resultante da aquisição de novos quadros cognitivos e crenças partilhadas, adquiridas por meio de aprendizagem social.

Outros fatores que se podem apontar como impulsionadores desta transferência são: a existência de obrigações, por parte dos EM, de acompanhar a agenda política da UE; o desejo de manter uma boa imagem externa de Portugal, por acompanhar as tendências e preocupações da UE, principalmente se considerarmos que Portugal teria entrado na União Europeia, havia apenas uma década, etc.

Considerando que a apresentação do referido Livro Verde constituiu o "surgimento do problema" da cibersegurança em Portugal, os atores intervenientes nesta fase do ciclo daquilo que designamos uma política pública de cibersegurança em Portugal, foram os elementos da Unidade de Missão para a Sociedade da Informação, através da apresentação pública do documento, em 1997.

Esta questão foi problematizada em Portugal numa época marcada por alguma estabilidade social, política e financeira e sem grandes debates públicos específicos sobre cibersegurança (provavelmente porque os cidadãos, no geral, ainda não estavam muito sensibilizados para esta questão).

3.2 Agendamento

Apesar da apresentação do Livro Verde ter consubstanciado o momento da introdução do problema da cibersegurança em Portugal (excluindo a SEGNAC 4, que respeitava apenas ao tratamento da informação classificada), constituiu também a introdução do tema na agenda política nacional, uma vez que, por um lado, o referido documento foi elaborado a pedido do Governo e, por outro, os elementos que o elaboraram eram representantes de vários Ministros portugueses (RCM nº 16/96).

A criação da Equipa de Missão para a elaboração do Livro Verde afigura-se como tendo provindo de um processo de difusão de orientações políticas da UE, com especial atenção para o Livro Branco sobre "Crescimento, Competitividade e Emprego" e, possivelmente, os documentos relacionados com a preparação do Programa Comunitário Plurianual de Instauração da Sociedade da Informação na

Europa[58] - programa que teve início em 1997 e visava, entre outras, a questão da segurança da informação informatizada -, que incentivava o Governo a empenhar-se nestas matérias, com o intuito de vir a beneficiar de fundos financeiros comunitários.

Posto isto, também o agendamento desta questão parece ter consistido num processo convergência de políticas públicas europeias, através da transferência de uma das questões que faziam parte da agenda política da UE, para a agenda política nacional, por meio do próprio Livro Verde, apresentado em 1997.

Face ao apresentado, os atores que conduziram à introdução da cibersegurança na agenda política nacional (como parte integrante de uma proposta mais abrangente, de medidas políticas para a sociedade da informação), foram também os elementos da Equipa de Missão para a Sociedade da Informação.

Este agendamento ocorreu no mesmo contexto social e económico que o surgimento do problema.

Posteriormente, em 1998, foi criada a Iniciativa Nacional para o Comércio Eletrónico, que volta a introduzir a questão da cibersegurança na agenda política nacional, prevendo a "Definição de um quadro base de regras harmonizadas, respeitantes à segurança das transacções efectuadas por via electrónica, à protecção das informações de carácter pessoal e da vida privada" (Resolução do Conselho de Ministros nº 115/98, de 1 de setembro).

Em 2002, o Programa do XV Governo Constitucional voltou a introduzir esta questão na agenda política, prevendo a criação de um Plano de Segurança Digital Nacional e o desenvolvimento de uma Estratégia de *eGovernment*[59],que deveria garantir, entre outros, a segurança dos *websites* do Governo.

Também em 2002, entra na agenda política nacional a questão da ciberdefesa, através do acordo realizado entre os Chefes de Estado dos membros da OTAN, para a "necessidade de fortalecer as capacidades da Aliança na defesa contra ataques informáticos", no âmbito da Declaração de Praga de 21 de novembro de 2002 (Freire, Nunes, Davara e Acosta, 2013: 57).

Em 2004, o Programa do XVI Governo Constitucional volta a referir a criação do Plano de Segurança Digital Nacional, como um dos seus objetivos, colocando-o de novo na agenda política.

No âmbito do trabalho desenvolvido pela, entretanto criada, Unidade de Missão Inovação e Conhecimento - UMIC[60], verificou-se a necessidade da criação de "um projecto autónomo e transversal para a segurança da informação"[61], à parte das iniciativas já desenvolvidas pela UMIC.

Para o desenvolvimento desse projeto, semelhante à criação de um Plano de Segurança Digital Nacional, já previsto nos programas dos XV e XVI Governos Constitucionais, foi criado um grupo de

[58] Consultar A4-0164/97 - COM(96) 592 final.
[59] O *eGovernment* ou governo eletrónico consiste na utilização das TIC, da parte dos organismos governamentais, para a interação com os cidadãos, como forma de prestação de serviços de um modo mais rápido e eficiente (http://web.worldbank.org/WBSITE/EXTERNAL/TOPICS/EXTINFORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/EXTEGOVERNMENT/0,,contentMDK:20507153~menuPK:702592~pagePK:148956~piPK:216618~theSitePK:702586,00.html).
[60] Criada pela Resolução do Conselho de Ministros nº 135/2002, de 20 de novembro.
[61] Consultar http://conferenciashiperion.files.wordpress.com/2012/11/ciberseguranc3a7a-uma-visc3a3o-do-estado-universidade-lusc3b3fona-21nov2012.pdf (consultado a 20/05/14).

trabalho (constituído pela UMIC, o GNS, a ANACOM e a FCCN), para a criação de uma Estrutura Nacional de Segurança da Informação (ENSI), que veio introduzir mais uma vez a questão na agenda.

Ainda em 2005, o Programa do XVII Governo Constitucional volta a introduzir este tema na agenda política, referindo a necessidade de consolidar iniciativas em curso e preencher lacunas, através do reforço da privacidade, segurança e fiabilidade e de um planeamento estratégico dos sistemas de informação na Administração Pública (Presidência do Conselho de Ministros, 2005: 13).

Depois da divulgação de diversas orientações dos órgãos da UE, para que os EM criassem determinadas capacidades de cibersegurança[62] e do trabalho desenvolvido pela ENISA, de partilha de boas práticas em matéria de estratégias nacionais de cibersegurança[63], a Resolução do Conselho de Ministros nº 12/2012, de 7 de fevereiro, que aprova o plano global estratégico de racionalização e redução de custos com as TIC na Administração Pública, apresentado pelo Grupo de Projeto para as Tecnologias de Informação e Comunicação (GPTIC)[64], constituiu mais um documento que se traduziu no agendamento da cibersegurança, através da proposta medida 4, que previa a "definição e implementação de uma estratégia nacional de segurança da informação", que deveria incluir a "criação, instalação e operacionalização de um Centro Nacional de Cibersegurança".

3.3 Planeamento

O Livro Verde para a Sociedade da Informação em Portugal foi também o primeiro documento publicado no âmbito do planeamento de medidas políticas nessa área, em Portugal, designadamente através da previsão da revisão da política de segurança da informação.

Porém, apesar de conter propostas de medidas políticas, faltava-lhe informação relativa aos instrumentos a utilizar, o calendário para a implementação, os agentes e o custo da concretização, entre outros, exemplificando como as propostas de políticas públicas tendem a ser desenhadas de forma abstrata, possivelmente para desresponsabilizar os intervenientes, caso os objetivos não sejam cumpridos (*blame-avoidance*[65]).

Em 1999, foi aprovado o documento orientador da Iniciativa Nacional para o Comércio Eletrónico. Nesse documento foram propostas algumas medidas na área da cibersegurança (ex. "Transpor para a legislação nacional a Directiva da União Europeia nº 96/9/CE, de 11 de março, sobre a proteção de bases de dados e direitos (…) da propriedade intelectual"; "Proceder ao enquadramento jurídico da assinatura electrónica e dos prestadores de serviços de certificação"; "Definir a política

[62] Exemplos dessas comunicações são: a COM(2001) 298; a Diretiva 2009/140/CE; a COM(2010) 245 final; a COM(2010) 673 final; a COM(2011) 163 final; JOIN(2013) 1 final ou a COM(2013) 48 final.

[63] Consultar http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/cyber-security-strategies-paper/at_download/fullReport (consultado a 20/04/2014).

[64] O GPTIC foi criado pela Resolução do Conselho de Ministros nº 46/2011, de 14 de novembro.

[65] Conceito de *blame-avoidance* explicado na página 10 deste texto.

nacional de criptografia"), ainda que, mais direcionadas para o desenvolvimento do comércio eletrónico (Resolução do Conselho de Ministros nº 94/99, de 25 de agosto)[66].

Em meados do ano 2000, os elementos da FCCN[67] verificaram um aumento do número de incidentes de segurança informática[68] na Rede Ciência, Tecnologia e Sociedade (RCTS)[69] e constataram que as redes académicas de países estrangeiros já tinham equipas de resposta a estes incidentes, enquanto em Portugal não existia nenhuma[70].

Assim, no enquadramento da RCTS, a FCCN formou e treinou de um conjunto de funcionários, para a criação uma equipa de resposta a incidentes de segurança informática (CERT) para desenvolver atividades no âmbito da RCTS - o CERT.PT.

À primeira vista, esta medida parece ter sido uma iniciativa totalmente privada, uma vez que a FCCN era uma instituição privada sem fins lucrativos. Todavia, considerando as características da FCCN que, apesar de, até 2013, quando foi inserida na FCT, ter sido uma instituição privada, os seus fundadores eram entidades públicas (Instituto Nacional de Investigação Científica, Conselho de Reitores das Universidades Portuguesas e Laboratório Nacional de Engenharia Civil), o que lhe atribuía, mesmo que fosse informalmente, um estatuto um pouco diferente.

Com base na história da FCCN, consideramos que esta foi uma iniciativa *bottom-up*, que pode ter começado como uma iniciativa de um grupo de operacionais do setor privado, mas acabou por ser aceite e assumida pelo setor público, tendo-se tornado uma CERT nacional *de facto*, em 2005.

Em 2003, no âmbito das medidas previstas no Programa do XV Governo Constitucional, nomeadamente a elaboração de um Plano Estratégico Info 2005 e o desenvolvimento de uma estratégia de *eGovernment*, foi aprovado o Plano de Ação para a Sociedade da Informação.

Este plano incluía medidas de cibersegurança, como: a promoção do "reforço da unidade de combate ao crime informático da Polícia Judiciária"; a criação de "marcas de confiança reconhecidas, que atestem a genuinidade (…) e segurança dos *sites*"; a promoção de "um *standard* de chaves públicas por parte das entidades públicas" (Resolução do Conselho de Ministros nº 107/2003, de 12 de agosto).

[66] As medidas propostas neste documento não apresentam objetivos claros e mensuráveis, os instrumentos e atores envolvidos na sua implementação, uma calendarização, nem um orçamento para a sua implementação.
[67] Entidade nacional com responsabilidades sobre o domínio .pt.
[68] Um incidente de segurança informática consiste em "qualquer acção ou conjunto de acções desenvolvidas contra um computador ou rede de computadores e que resulta, ou pode resultar, na perda da confidencialidade, integridade ou desempenho de uma rede de comunicação de dados ou sistema informático, designadamente, o acesso não autorizado, a alteração ou remoção de informação, a interferência ou a negação de serviço em sistema informático" (http://cert.pt/index.php/servicos/tratamento-de-incidentes).
[69] A RCTS consiste numa plataforma de comunicação avançada para a comunidade académica e científica nacional (Universidades, Laboratórios públicos, Institutos Politécnicos, entre outros), onde são disponibilizados diversos serviços de conectividade e aplicações relacionadas com a área da segurança.
[70] Existia, desde a década de 90, resposta a este tipo de incidentes, no âmbito da FCCN, embora funcionasse ainda de forma rudimentar e morosa, com recurso a uma caixa de correio eletrónico para a qual os queixosos deveriam enviar um *email* a reportar o sucedido e esperar por um contato com orientações.

No mesmo dia, a Resolução do Conselho de Ministros nº 108/2003 aprovou o Plano de Ação para o Governo Eletrónico, que previa, entre outros, a criação de um Plano Nacional de Segurança Digital, que deveria incluir uma infraestrutura nacional de chaves públicas.

Embora as RCM nºs 107/2003 e 108/2003 definissem os atores envolvidos no planeamento das medida e a data limite para a sua implementação, não previam informação relativa aos objetivos, instrumentos a utilizar, o custo ou os meios de concretização.

Entre 2004 e 2005 o grupo criado para desenhar a ENSI elaborou o projeto e apresentou-o ao Governo em 2005. A elaboração da ENSI[71] baseou-se no levantamento das entidades nacionais e internacionais relevantes para a segurança da informação e, por inerência, a cibersegurança em Portugal e na análise de Planos Nacionais de Segurança Digital de países estrangeiros e culminou na criação de uma estrutura baseada na Segurança da Informação, tendo em conta a preservação da confidencialidade, integridade, disponibilidade e autenticidade da informação (UMIC, *et al.*, 2005: 6).

Entre os seus objetivos destacamos: a criação de uma equipa de resposta a incidentes de segurança informática (CSIRT); o desenvolvimento de "uma infra-estrutura electrónica nacional de autenticação"; a proteção da privacidade e dos interesses pessoais do consumidor na Sociedade da Informação, através da atualização da legislação nesta área.

A ENSI baseava-se numa lógica de mercado, à semelhança do discurso e iniciativas europeias (ex. ENISA[72]), que diferia da lógica americana, que procurava garantir a segurança e defesa nacionais[73].

Considera-se que a ENSI constituiu a primeira tentativa de definição de uma política nacional de cibersegurança (apesar da referência à segurança da informação), porque diz respeito à segurança da informação informatizada e dos sistemas informáticos. Embora, como proposta de política pública, apresentasse algumas lacunas (ex. a falta de: objetivos que fossem mais facilmente mensuráveis; definição de orçamentos claros; definição dos instrumentos a utilizar na implementação; definição clara dos atores envolvidos na implementação e as suas funções, bem como a forma como as deveriam desempenhar; definição da calendarização da implementação e, idealmente, da avaliação, etc).

No entanto, a elaboração da ENSI colocou Portugal entre os primeiros países da UE a realizar esforços na área da cibersegurança.

Também em 2005, o Programa Nacional de Ação para o Crescimento e o Emprego (PNACE) 2005/2008, criado no âmbito da Estratégia de Lisboa, incluiu duas medidas de cibersegurança: a "Criação da Autoridade de Certificação Electrónica do Estado", (necessária para o desenvolvimento dos

[71] Consultar Figura 2, em anexo, página 82.

[72] Entre as atribuições da ENISA está contribuir "para um alto nível de segurança das redes e da informação entre a comunidade e o desenvolvimento de uma cultura de segurança das redes e da informação (…) contribuindo (…) para um bom funcionamento do mercado interno" (Regulação nº 460/2004 do Parlamento Europeu e do Conselho, de 10 de março).

[73] Discurso patente na Estratégia Nacional para Segurar o Ciberespaço, onde se refere que "a principal preocupação é a ameaça dos ciberataques organizados capazes de causar uma disrupção debilitante das infraestruturas nacionais (…) ou segurança nacional" (The White House, 2003: viii).

processos de certificação digital e assinatura eletrónica e outros projetos em desenvolvimento, como a criação do Passaporte electrónico, também previsto neste documento) (CNEL, 2005: 15).

Apesar de não terem ficado claramente definidos os objetivos (mensuráveis), as entidades envolvidas na implementação das medidas, nem as suas funções ou o orçamento, considera-se que eram medidas essenciais, pois rapidamente foram implementadas (junho e julho de 2006, respetivamente)[74].

Ainda em 2005, o Plano Tecnológico também integrou uma proposta de medida nesta área: "Desenvolver uma política de segurança informática", a ser implementada até 2006 (Unidade de Coordenação do Plano Tecnológico, 2005: 23). Para permitir o desenvolvimento e implementação desta política, foi criada "a UMIC - Agência para a Sociedade do Conhecimento, I.P., um veículo institucional facilitador dos procedimentos requeridos para fazer chegar aos cidadãos as mudanças desejadas". Este novo instituto público era dotado de personalidade jurídica e autonomia administrativa e financeira, o que lhe permitia a prossecução dos objetivos por si traçados, coisa que não era possível para a UMIC, a Unidade de Missão (Decreto-Lei nº 16/2005, de 18 de janeiro).

Também em 2005, depois de proposta em vários momentos[75], é aprovada a criação da Entidade de Certificação Eletrónica do Estado - Infraestrutura de Chaves Públicas (ECEE), pela Resolução do Conselho de Ministros nº 171/2005, de 3 de novembro, para a qual é criado um grupo de trabalho. Este sistema seria necessário para a implementação de projetos já programados (ex. cartão do cidadão, passaporte eletrónico português ou a "desmaterialização dos processos intra e interorganismos do Estado"[76]), que requeriam "autenticação digital forte de identidades e assinaturas electrónicas".

No planeamento desta entidade que, aquando da sua implementação, lhe foi atribuída a designação de Sistema de Certificação Eletrónica do Estado (SCEE), constava o objetivo ("assegurar a (…) autenticação digital forte nas relações electrónicas de pessoas singulares e colectivas com o Estado e entre entidades públicas"), a definição do responsável pela coordenação do processo de instalação (o então Secretário de Estado da Presidência do Conselho de Ministros) e dos restantes elementos do grupo de trabalho que iria acompanhar o seu processo de instalação, uma calendarização e ainda a definição dos responsáveis pelos encargos orçamentais (a Secretaria-Geral da Presidência do Conselho de Ministros), a quem competia também o apoio administrativo e logístico, necessários (Resolução do Conselho de Ministros nº 171/2005).

O facto desta medida estar relativamente bem definida, i.e., com os atores intervenientes e as suas funções e responsabilidades definidas, tal como o facto do grupo ter sido coordenado por um elemento nomeado pelo então Secretário de Estado da Presidência do Conselho de Ministros e ter tido todo o

[74] De acordo com a Resolução do Conselho de Ministros nº 77/2001, de 5 de julho, o cartão do cidadão já estaria a ser preparado. Quanto ao passaporte eletrónico, acredita-se que a rapidez na sua implementação se deveu ao facto de já haverem orientações europeias nesse sentido (COM(2004) 116 final).

[75] Proposta no Plano de Ação para a Sociedade da Informação, no Plano de Ação para o Governo Eletrónico, no Plano Tecnológico e na ENSI.

[76] Consultar RCM nº 77/2001, RCM nº 68/2003, de 7 de agosto, RCM nº 171/2005 e https://www.oa.pt/Conteudos/Artigos/detalhe_artigo.aspx?idc=1365&idsc=31626&ida=45432 (consultado a 20/10/2014).

apoio administrativo e logístico da Secretaria-Geral da Presidência do Conselho de Ministros, que assegurou a publicação de toda a regulação necessária, permitiu o seu rápido desenvolvimento e implementação, que aconteceu cerca de sete meses após a sua aprovação.

Em 2005 ainda, foi criada a Equipa de Missão Computadores, Redes e Internet na Escola, no âmbito da Direção-Geral de Inovação e de Desenvolvimento Curricular (DGIDC-CRIE), que teria "como missão a concepção, desenvolvimento, concretização e avaliação de iniciativas (…) no domínio do uso dos computadores, redes e Internet nas escolas e nos processos de ensino-aprendizagem" e que desenvolveu, no âmbito do programa *Safer Internet Plus*[77], o Projeto Seguranet, que promove uma utilização esclarecida e segura da internet, entre os estudantes dos ensinos básico e secundário.

A este projeto seguiu-se a criação de um projeto mais abrangente, também no âmbito do programa *Safer Internet Plus*, o Projeto Internet Segura[78], que viria a contribuir para "assegurar a segurança e a privacidade no uso da Internet" (uma das orientações estratégicas do Programa de Ação Ligar Portugal, integrado no Plano Tecnológico), garantindo que todos, em particular as famílias, dispusessem de instrumentos de proteção contra os riscos associados ao uso da internet e informação sobre como os utilizar (Ministério da Ciência, Tecnologia e Ensino Superior, 2005: 27).

Infelizmente, não foi possível aceder aos documentos relativos ao planeamento destes projetos e analisá-los. Porém, acredita-se que estivessem corretamente desenhados, pois foram aprovados e o Projeto Internet Segura, em particular, é co-financiado pela Comissão Europeia.

No que toca à ciberdefesa, em 2005, na sequência da publicação do PEMGFA/CSI/004, de 14 de fevereiro de 2005, que definia determinados requisitos de segurança, criou-se uma capacidade de Resposta a Incidentes de Segurança Informática das Forças Armadas (CRISI-FA), no âmbito do Grupo de Resposta a Incidentes de Segurança Informática (GRISI), do EMGFA, que deve "promover a implementação da política conjunta de segurança da informação, de forma a garantir a autonomia, sobrevivência e interoperabilidade dos sistemas das FFAA" (Freire, Nunes, Davara e Acosta, 2013: 57).

Além destas capacidades, também se prevê a criação de um Centro de Coordenação da CRISI (CC-CRISI), para fazer a ligação com a estrutura nacional de cibersegurança, neste caso o recém-criado CNCseg (Freire, Nunes, Davara e Acosta, 2013: 57).

No que concerne ao *eGovernment*, em 2006, a Resolução do Conselho de Ministros nº 39/2006, de 27 de abril, aprovou o Programa de Reestruturação da Administração Central do Estado (PRACE), que previa a criação da Agência para a Modernização Administrativa, I.P. (AMA), que viria assumir "a definição das linhas estratégicas e das políticas transversais à Administração Pública, nomeadamente quanto às regras de interoperacionalidade e de acessibilidade, taxonomias, normas de segurança e normalização da informação" (Resolução do Conselho de Ministros nº 39/2006, de 21 de abril)[79].

[77] Um programa da Comissão Europeia, que tinha como linhas estratégicas o combate aos conteúdos ilegais, a reação aos conteúdos não desejados ou nocivos e a promoção da segurança no uso da internet.
[78] Projeto criado por um consórcio constituído pela FCT, a Direção-Geral de Educação, a FCCN, o Instituto Português do Desporto e Juventude (IPDJ) e a Microsoft Portugal.
[79] Não foi possível aceder a qualquer documento do planeamento da AMA e analisá-lo.

Em 2012 foi apresentado e aprovado o plano de ação para a redução de custos com as TIC na Administração Pública. Este plano previa algumas medidas relacionadas com a cibersegurança (ex. o estabelecimento de "uma arquitectura de sistemas de informação de referência" para os "sistemas de informação na AP"; a definição e implementação de uma Estratégia Nacional de Segurança da Informação), sendo mesmo o primeiro documento político nacional a fazer referência ao termo "cibersegurança", com a previsão da criação de um Centro Nacional de Cibersegurança, embora até hoje não exista um conceito de cibersegurança, legalmente definido, em Portugal (RCM nº 12/2012).

Na proposta da primeira medida referida, são apresentados os atores responsáveis e a calendarização para a sua implementação, mas falta a definição de um orçamento, de objetivos claramente mensuráveis, assim como os instrumentos políticos a utilizar na sua implementação. Na proposta de criação de uma Estratégia Nacional de Segurança da Informação, prevê-se que se venham a definir os objetivos, os agentes da implementação e a estrutura de segurança de informação, incluindo os serviços fornecidos a nível nacional. Esta proposta parece, então, prever o planeamento daquilo que poderíamos considerar uma política pública nacional de cibersegurança, uma vez que se refere essencialmente à segurança da informação informatizada.

Na sequência do referido plano de ação, que previa a definição de uma Estratégia Nacional de Segurança da Informação, que deveria incluir um Centro Nacional de Cibersegurança, ao invés de se ter iniciado o processo de desenho da estratégia, foi criada a Comissão Instaladora do Centro Nacional de Cibersegurança, cuja missão seria "definir as medidas e os instrumentos necessários à criação, instalação e operacionalização de um Centro Nacional de Cibersegurança"[80] (RCM nº 42/2012, de 13 de abril).

A comissão era composta por representantes das entidades mais relevantes na área da cibersegurança e ciberdefesa em Portugal e alguns elementos que, embora desempenhem cargos de destaque em entidades relevantes nesta matéria, foram nomeados pelo Primeiro-Ministro, a título individual, pelo seu consagrado conhecimento e experiência na área[81], não tendo contado com outros atores que pudessem contribuir para uma a definição desta entidade.

Apesar do âmbito da sua missão, os elementos da comissão entenderam que a criação, instalação e operacionalização do centro, pressupunha a elaboração prévia de um esboço do que entendiam que deveria ser uma Estratégia Nacional de Cibersegurança (como proposto pelo GPTIC), enquadradora da ação política nessa matéria, pelo que o fizeram, embora muito baseado nas estratégias estrangeiras.

Contudo, apesar daquele ter sido apenas um exercício de enquadramento da missão da comissão, esse esboço de proposta de Estratégia Nacional de Cibersegurança foi publicado no *website* do GNS -

[80] O relatório da Comissão Instaladora do Centro Nacional de Cibersegurança contou com a especificação de: os objetivos, os atores envolvidos na implementação, uma calendarização e uma estimativa do orçamento necessário.
[81] Alguns elementos da comissão consideram que esta deveria ter sido constituída por representantes das entidades, ao invés de peritos a título individual (que desempenham funções em entidades relevantes na matéria), representando um maior número de atores.

que estava a coordenar o processo de "definição e implementação de uma estratégia nacional de segurança da informação" -, como suposta proposta oficial de Estratégia Nacional de Cibersegurança[82].

A publicação desta proposta poderá ter sido uma tentativa do GNS para pressionar e alertar a tutela para a necessidade de definição de uma Estratégia Nacional de Cibersegurança. Porém, de acordo com as orientações da ENISA, que promove as boas práticas nesta matéria, a elaboração de uma estratégia nacional de cibersegurança é um processo complexo, passando pela realização de uma revisão da literatura e das iniciativas já realizadas nessa área, tanto ao nível nacional, como internacional (ex. estratégias nacionais e outros documentos políticos), pelo debate, partilha de boas práticas e coordenação de esforços de um conjunto abrangente de entidades, incluindo a sociedade civil e o setor privado, pois a maior parte das infraestruturas críticas de informação pertencem a empresas privadas (ex. os fornecedores de serviços de internet), entre outros, devendo o Estado funcionar como facilitador desta colaboração (ENISA, 2012: 13-14).

Uma iniciativa que se assemelhou ao proposto pela ENISA foi o processo de elaboração do Conceito Estratégico de Defesa Nacional de 2013, que terá durado meses, contando com diversos debates e reuniões, abertas e fechadas ao público, que tiveram lugar no Instituto da Defesa Nacional (IDN), onde muitos dos atores intervenientes na defesa nacional foram convidados a participar, até se alcançar o documento final: a Resolução do Conselho de Ministros n.º 19/2013, de 5 de abril.

Do mesmo modo, pode considerar-se que o trabalho desenvolvido no âmbito do Grupo de Estudos sobre Contributos para uma Estratégia Nacional de Informação (GECENI), do IDN, esteve mais próximo de um processo de elaboração de uma Estratégia Nacional de Cibersegurança, do que o trabalho desenvolvido pela Comissão Instaladora do CNCseg. No âmbito do GECENI, sob o "chapéu" da segurança da informação, dentro do qual estava a cibersegurança, desenvolveram-se reuniões (algumas delas abertas ao público) protagonizadas por alguns dos atores intervenientes na segurança do ciberespaço, debates e *working papers* e procurou-se acompanhar as iniciativas desenvolvidas nesta área até então, tanto ao nível nacional como internacional, analisar os desafios e necessidades existentes, assim como o papel dos diversos intervenientes na proteção do ciberespaço, com o intuito de contribuir para o desenho de uma Estratégia Nacional da Informação integrada, esclarecida e participada.

Embora revelando abrangência, esta iniciativa parece não ter tido grande adesão por parte de alguns atores intervenientes na cibersegurança em Portugal. Algumas das razões atribuídas para essa falta de adesão da parte de alguns convidados foram: o facto de considerarem que essa função não fazia parte das atribuições do IDN, pensando que essa instituição estaria a estudar uma área que já estaria "nas mãos" de outras entidades (ex. GNS, FCCN, UMIC, ANACOM); o facto de entenderem que o tema já

[82] A proposta de Estratégia Nacional de Cibersegurança publicada no *website* do GNS reflete a abordagem pouco aprofundada que a comissão adotou na sua elaboração, sendo bastante semelhante às estratégias estrangeiras de cibersegurança, especialmente a francesa. Consultar http://www.gns.gov.pt/media/1247/PropostaEstrat%C3%A9giaNacionaldeCiberseguran%C3%A7aPortuguesa.pdf e http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/France_Cyber_Security_Strategy.pdf (Consultado a 20/06/2014).

estaria suficientemente estudado, pelo que não traria grande benefício a participação na iniciativa, faltando apenas a iniciativa dos decisores políticos para se avançar com medidas concretas[83].

Nós adicionaríamos outra justificação: o facto do IDN ser percecionado como sendo uma instituição de cariz militar e haver alguma clivagem entre o discurso dos elementos civis e o dos militares, o que faz sentido, uma vez que o "setor civil" tem preocupações diferentes do setor militar, nesta área. Enquanto a Administração Pública procura garantir a disponibilidade e o normal funcionamento dos serviços de governo eletrónico e a proteção dos dados dos cidadãos e das empresas nacionais e as empresas procuram garantir que a informação está sempre disponível aos consumidores, por exemplo, o setor militar procura explorar e garantir a segurança do ciberespaço, enquanto "espaço nacional", incluindo as infraestruturas que o sustentam, o que pode resultar em alguma dificuldade na concertação entre estes atores[84].

Posteriormente, na sequência da publicação da Estratégia da UE em matéria de cibersegurança (JOIN(2013) 1 final), que estabelece como prioridade estratégica o desenvolvimento de uma política e de capacidades de ciberdefesa, no âmbito da Política Comum de Segurança e Defesa (PCSD), foi publicada a Orientação Política para a Ciberdefesa, em outubro de 2013, pelo Despacho nº 13692/2013, do Ministro da Defesa Nacional. Neste documento são identificados os objetivos - "Garantir a proteção, a resiliência e a segurança das redes (…) da Defesa Nacional"; "Assegurar a liberdade de ação do País no ciberespaço"; "Contribuir de forma cooperativa para a cibersegurança nacional" - e as linhas orientadoras de uma Política Nacional de Ciberdefesa - a criação de uma estrutura de ciberdefesa nacional, o planeamento da defesa militar, a criação de uma capacidade para conduzir operações militares em redes de computadores, a partilha de informação relacionada com a ciberdefesa, o desenvolvimento da sensibilização, formação e de exercícios de ciberdefesa e a promoção de uma cultura de gestão do risco para a aquisição de *software* e *hardware* (Despacho nº 13692/2013, do Ministro da Defesa Nacional).

Para a consecução destes objetivos, prevê-se: a criação de um Centro de Ciberdefesa, "uma estrutura de comando e controlo da ciberdefesa nacional (…), contemplando (…) um órgão com caráter de orientação estratégica-militar das atividades de ciberdefesa e uma capacidade militar de resposta operacional a ciberataques e a incidentes informáticos"; o desenvolvimento de "um sistema de partilha de informação (…) e de colaboração com a rede nacional de (…) CSIRT, instituições privadas, universidades e organizações internacionais como a OTAN e a UE"; a definição de "uma estratégia de ciência e tecnologia no domínio da ciberdefesa, sendo para esse efeito implementadas linhas de investigação (…), orientadas para o desenvolvimento de capacidades nesta área"; a centralização da formação e do treino em ciberdefesa e a constituição de "um pólo de excelência neste domínio, evitando

[83] Opiniões recolhidas no âmbito das entrevistas realizadas.
[84] Segundo depoimentos dos entrevistados.

duplicações e aproveitando as competências e os recursos já existentes nas Forças Armadas" (Despacho nº 13692/2013, do Ministro da Defesa Nacional).

Este planeamento de uma Política de Ciberdefesa apresenta objetivos claros e mensuráveis, alguns instrumentos a ser utilizados na sua implementação (ex. atualização da legislação, formação de pessoal, definição dos atores envolvidos, especialmente os atores que irão coordenar a ação em matéria de ciberdefesa[85]), embora não seja apresentada a calendarização, nem o orçamento para a implementação.

Ainda no que concerne à ciberdefesa, é de salientar que é prática comum a consulta de peritos para o planeamento de medidas políticas, como aconteceu no processo de elaboração do atual conceito estratégico de Defesa Nacional. No entanto, em relação à cibersegurança não foi possível apurar a existência dessa prática[86].

3.4 Implementação

Desde os anos 90, têm vindo a ser implementadas algumas medidas políticas no âmbito daquilo a que se poderia chamar de política nacional de cibersegurança, se tais medidas estivessem relacionadas entre si e as decisões fossem tomadas de forma coordenada, com base numa estratégia política.

Em 1991, como já foi referido, foram publicadas algumas leis.

Em 1998, o Governo considerou que o Centro de Gestão da Rede Informática do Governo (CEGER)[87] não satisfazia as necessidades existentes e para colmatar tais necessidades, pelo Decreto-Lei nº 184/98, de 6 de julho, foi alargado o seu âmbito de atuação, que passou a abranger, não só a gestão da rede informática do Governo, mas também a garantir a "concepção, desenvolvimento (…) e exploração de sistemas de informação de utilização comum para os gabinetes dos membros do Governo", entre outros.

Em 1999, como previsto no documento orientador da Iniciativa Nacional para o Comércio Eletrónico, foi publicado o Decreto-Lei nº 290-D/99, de 2 de agosto, que aprova o regime jurídico dos documentos eletrónicos e da assinatura digital e acolhe as orientações da UE nesse sentido[88].

Em 2002, foi criado o CERT.PT (da FCCN), constituindo-se como a primeira CERT em Portugal e a primeira CERT portuguesa acreditada internacionalmente[89].

---

[85] "As atribuições de orientação estratégica-militar da ciberdefesa deverão recair sobre o Conselho de Chefes de Estado-Maior". O Centro de Ciberdefesa ficará sob a dependência do Chefe de Estado-Maior-General das Forças Armadas (Despacho nº 13692/2013, do Ministro da Defesa Nacional).

[86] Nenhum dos peritos entrevistados foi consultado no âmbito do desenho de medidas políticas nesta área.

[87] O CEGER foi criado em 1989, pelo Decreto-Lei nº 429/89, de 15 de dezembro, sendo uma das suas atribuições a garantia da "segurança e confidencialidade da informação, promovendo a realização de auditorias periódicas". A decisão de implementação deste organismo já demonstra alguma preocupação com a cibersegurança em Portugal, embora ainda numa fase muito embrionária, apenas direcionada para a segurança da informação presente na rede informática do Governo.

[88] Também no âmbito do regime jurídico dos documentos eletrónicos e da assinatura digital, em 2000, o Decreto-Lei nº 146/2000, de 18 de julho, atribuiu ao Instituto das Tecnologias de Informação na Justiça a competência de "autoridade credenciadora", que passou depois a ser assistido por um Conselho Técnico de Credenciação (Decreto-Lei nº 234/2000, de 25 de setembro).

[89] O CERT.PT é, desde 2004, acreditado pelo serviço europeu *Trusted Introducer for CSIRT in Europe*.

Apesar da criação do CERT.PT não ter derivado concretamente de uma decisão governamental, uma vez que a FCCN era, em 2002, uma instituição privada sem fins lucrativos, é extremamente relevante apresentá-la no ciclo das políticas públicas relacionadas com a cibersegurança pois, devido à sua importância na garantia da cibersegurança em Portugal, veio a assumir o papel de CERT nacional *de facto* e foi inserida no âmbito do Estado, através da inclusão da FCCN na FCT.

É de referir que, ainda antes da inclusão da FCCN na FCT, já o CERT.PT tinha assumido o papel de CERT nacional *de facto*, informando a "tutela" da FCCN, o então Ministério da Ciência, Tecnologia e Ensino Superior, que "aceitou" ou melhor, não rejeitou esse papel, assumindo-o.[90]

Como exposto atrás, o CERT.PT foi criado no âmbito da RCTS. No entanto, por um lado, por não haver um serviço destes ao nível nacional[91] e, por outro porque, de acordo com declarações do ex--diretor do CERT.PT, cerca de 95% dos pedidos de colaboração e avisos da existência de atividade maliciosa ou da ocorrência de incidentes em *websites* de entidades portuguesas têm sido feitos por entidades estrangeiras, o CERT.PT sentiu essa necessidade e assumiu, desde 2005, um papel típico de CERT nacional - passando a funcionar como elo de ligação entre Portugal e as CERTs estrangeiras, respondendo aos pedidos de ajuda de outras entidades nacionais, além da academia, desenvolvendo estudos estatísticos sobre as ciberameaças, números e tipos de ciberataques em Portugal, dando formação na área de segurança das redes e sistemas de informáticos, etc.

Paralelamente, a equipa do CERT.PT conseguiu construir um conjunto de relações de confiança, que levaram à criação de uma rede nacional de CERTs, para potenciar a cooperação e partilha de boas práticas nesta matéria e promover uma cultura de segurança[92].

Portanto, na prática, existe oficiosamente, desde 2005, uma CERT nacional em Portugal - o CERT.PT -, que tem realizado um trabalho reconhecido como exemplar[93]. Todavia, nunca obteve um mandato do Governo para desempenhar essa função, pelo que, embora já tenha o respeito e a confiança de uma larga rede de entidades intervenientes na cibersegurança (ao nível nacional e internacional), não tem um orçamento adequado a uma CERT nacional, nem canais formais e instrumentos (ex. legais) para desempenhar, o mais eficaz e eficientemente possível, as funções de CERT nacional.

---

[90] Este tipo de atuação da parte do Governo, i.e., não maximizar as iniciativas (não atribuindo um mandato a um organismo que necessitávamos, que já estava implementado e com provas de sucesso) pode demonstrar pouca relevância atribuída à cibersegurança em Portugal (o que poderá ser justificado pelo facto de ser uma área tão abrangente e que poderá ser mais interessante e prioritária para aqueles que têm responsabilidades na área da segurança e defesa, por exemplo).

[91] Entre os serviços que uma CERT nacional deve oferecer estão: a análise e gestão de vulnerabilidades de *software* e *hardware*, o desenvolvimento de ferramentas de segurança, a deteção e o alerta de intrusões, a disseminação de informação de segurança informática, a consciencialização dos utilizadores, a avaliação de impactos dos incidentes, entre outros (Consultar https://www.enisa.europa.eu/activities/cert/support/guide/files/csirt-setting-up-guide e http://run.unl.pt/bitstream/10362/7341/1/Santos_2011.PDF - consultado a 20/04/2014).

[92] Atualmente, a rede nacional de CERTs conta com cerca de 20 CERTs dos setores académico, bancário, da defesa, energético, de telecomunicações, dos transportes e dos provisores de serviços de comunicações (consultar http://cert.pt/index.php/rede-nacional-csirt/directorio - consultado a 20/04/2014).

[93] O CERT.PT encontra-se em processo de certificação e poderá, brevemente, ser a 8º CERT europeia certificada pela *Trusted Introducer* (consultar https://www.trusted-introducer.org/directory/country_certification_Z.html - consultado a 13/10/14).

Fica então a dúvida sobre as razões para não ter sido atribuído um mandato político ao CERT.PT para o desempenho dessas funções, cumprindo assim as datas impostas pela Comissão Europeia, para os EM criarem este tipo de equipas.

Possíveis respostas para esta questão são: a falta de consenso entre os diversos atores intervenientes na garantia da cibersegurança em Portugal; o *lobbying* realizado por outras entidades com acesso a determinados recursos e instrumentos, nomeadamente a proximidade dos decisores políticos, para que não fosse atribuído tal mandato; a própria postura do CERT.PT, que não insistiu para a atribuição desse mandato, mantendo uma posição mais distanciada e imparcial, talvez mais propícia à criação de laços de confiança com o setor privado, por exemplo; o facto do CERT.PT ter sido criado no seio de uma fundação privada e não ter sido proveniente de uma decisão governamental (podendo ter ferido, de algum modo, o orgulho de decisores políticos com responsabilidades nesta área); falta de sensibilidade da parte do poder político para a importância deste tipo de entidades, entre outras[94].

Também em 2002, por força do Decreto-Lei nº 128/2002, de 11 de maio, foi criada, no seio do Conselho Nacional de Planeamento Civil de Emergência (CNPCE), uma Comissão de Planeamento de Emergência do Ciberespaço, que deveria "identificar as «potencialidades» a explorar e as «vulnerabilidades» a colmatar ou a minimizar, prevendo (…) os ajustados «planos de contingência»" para esta área. Porém, só por volta de 2008/2009 é que o Primeiro-Ministro nomeou alguém para a operacionalizar, que chegou a fazer uma proposta para a composição e o mandato da Comissão. Contudo, como o próprio referiu, esta "acabou por nunca funcionar na prática", tendo sido extinta em 2012, pelo Decreto-Lei 73/2012, de 26 de março, que transfere as atribuições do CNPCE para a ANPC (embora sem referência específica às funções das Comissões de Planeamento de Emergência setoriais).

Como vimos, a apresentação da ENSI, em 2005, colocou Portugal na vanguarda em matéria de cibersegurança. Todavia, até hoje, poucas das suas propostas foram implementadas e as que o foram (o SCEE e a CERT nacional), aconteceram dispersas no tempo e pelo âmbito de atuação de diversas entidades, sem a existência uma entidade com autoridade para coordenar a ação nesta matéria.

Das propostas da ENSI, a única medida que foi plenamente implementada, foi a infraestrutura eletrónica nacional de autenticação (SCEE), implementada em 2006, estando no topo deste sistema a ANS[95], como "autoridade credenciadora (…) das entidades certificadoras compreendidas no SCEE" e o CEGER, como "entidade certificadora do Governo" (Decreto-Lei nº 116-A/2006, de 16 de julho e Decreto-Lei nº 116-B/2006, de 16 de julho).

Apesar do SCEE, à primeira vista, parecer ser apenas o resultado do seu planeamento (em vários momentos), através de uma análise mais aprofundada, pode-se constatar que poderão haver outras razões para a sua implementação, neste caso razões que podem ter acelerado o processo da sua implementação, como projetos que estariam em desenvolvimento, mas necessitavam do funcionamento prévio deste tipo

[94] De acordo com alguns testemunhos recolhidos.
[95] A ANS substituiu o, já referido, Instituto das Tecnologias na Justiça, nas funções de autoridade credenciadora.

de sistema de certificação para a garantia dos adequados níveis de segurança para a sua utilização (ex. o cartão do cidadão, o passaporte eletrónico português, o Diário da República Eletrónico).

Mais recentemente, a 7 de outubro de 2014, é implementada a CERT nacional, no âmbito do CNCseg. No entanto, esta implementação ainda não foi plenamente concluída, estando previstas as suas capacidades iniciais para janeiro de 2015 e as capacidades finais para 2017. Logo, avizinha-se a implementação de mais uma medida proposta na ENSI, embora tenham passado cerca de dez anos[96].

Verifica-se então que, apesar das várias propostas apresentadas na ENSI, poucas vieram a ser implementadas. Possivelmente devido a fatores conjunturais pois, cerca de um mês após a apresentação da ENSI o Governo foi dissolvido, ou por não terem ficado desenhados de forma clara.

A 17 de julho de 2004, o então vice-presidente do PSD, Santana Lopes, tornou-se Primeiro--Ministro, porque o eleito Primeiro-Ministro, Durão Barroso, decidira aceitar uma proposta para presidir a Comissão Europeia.

Desde que Santana Lopes integrou o Governo, várias foram as remodelações ministeriais para combater a instabilidade política que se vivia. No entanto, não foram suficientes e o então Presidente da República, Jorge Sampaio, dissolveu o Governo, dando lugar a eleições legislativas e consequente mudança de Governo no mês seguinte à apresentação da ENSI.

Logo após a mudança para o novo Governo, liderado por José Sócrates, à semelhança do que geralmente acontece, as preocupações do novo corpo executivo recaíram mais sobre as reformulações de determinados organismos e consolidação das finanças públicas. Contudo, o XVII Governo Constitucional não abandonou este tema, até porque o seu programa se baseava na aposta na inovação e no desenvolvimento tecnológico, como forma de aumentar o emprego e a competitividade nacional.

O Programa do Governo incluía um "Plano Tecnológico para uma Agenda de Crescimento" para impulsionar a inovação e "vencer o atraso científico e tecnológico", através da consolidação das iniciativas em curso e do preenchimento de algumas lacunas (ex. "acesso e utilização da Internet em todas as escolas (…), combate à fraude; reforço da privacidade, segurança e fiabilidade; planeamento estratégico dos sistemas de informação na Administração Pública") (Presidência do Conselho de Ministros, 2005: 13 e 14).

Posteriormente, em outubro de 2006, foi criada, pelo Decreto-Lei nº 202/2006, de 27 de outubro, a Agência para a Modernização Administrativa, I.P. (AMA), que veio assumir as atribuições da UMIC I.P. no domínio da administração electrónica e tem como atribuições: "Contribuir para a definição das linhas estratégicas e das políticas gerais relacionadas com a administração electrónica"; "estimular actividades de investigação, de desenvolvimento tecnológico e de divulgação de boas práticas, nas áreas da (…) administração electrónica" (Decreto-Lei nº 202/2006, de 27 de outubro).

Porém, com base nas entrevistas realizadas, parece que os próprios (AMA) não consideram ter responsabilidades no que toca à cibersegurança em Portugal, mas sim apenas na garantia da

[96] Na página 42 são apresentadas algumas propostas de justificação para a criação do CNCseg em 2014.

interoperabilidade na Administração Pública. Admitem também que o facto de terem simultaneamente responsabilidades sobre o governo eletrónico e a prestação de serviços presenciais aos cidadãos não facilita as suas funções, não podendo focar-se numa só atribuição.

Segundo este entendimento, a AMA tem demasiadas atribuições, para as capacidades operacionais que dispõe, o que pode ter levado a um certo desleixo em relação às redes e sistemas de informação da Administração Pública, como podemos ver com o recente caso do CITIUS (plataforma informática do Ministério da Justiça) que ficou inoperacional entre setembro e outubro de 2014, devido à falta de cumprimento de determinados requisitos de segurança (a garantia da integridade e disponibilidade da informação), durante o processo de migração para o novo mapa judicial.

Em junho de 2007 foi aprovado e implementado o Projeto Internet Segura, que integra uma plataforma Internet Segura e uma plataforma eletrónica de denúncia de conteúdos ilegais na internet, - Linha Alerta[97] -, onde são publicados conteúdos multimédia com informações sobre segurança na internet, um Guia de Segurança no uso da internet, entre outros.

Em 2008, por força da Lei nº 37/2008, de 6 de agosto (Lei Orgânica da PJ), esta passou a coadjuvar "as autoridades judiciárias em processos relativos a crimes cuja detecção ou investigação lhe incumba realizar ou quando se afigure necessária a prática de actos (…) que requerem conhecimentos ou meios técnicos especiais", uma vez que os magistrados do Ministério Público (MP) não têm esses conhecimentos e meios, delegando funções à polícia criminal competente, que, conforme a Lei nº 49/2008, de 27 de agosto (Lei de Organização da Investigação Criminal)[98], é a PJ, designadamente a Unidade de Telecomunicações e Informática (UTI).

A UTI é responsável "pela realização de "acções de despistagem de intercepções ilegais de comunicações", pela realização de "perícias em equipamentos de telecomunicações e de informática, determinadas pelas autoridades judiciárias e de polícia criminal", entre outros (Decreto-Lei nº 42/2009, de 12 de fevereiro).

Na mesma altura, foi publicada a Lei nº 53/2008, de 29 de agosto (Lei de Segurança Interna), que inclui a política de segurança interna e o Sistema de Segurança Interna (SSI), ambos relevantes quando se trata de cibersegurança.

A política de segurança interna, porque o ciberespaço (com as suas vulnerabilidades) pode apresentar ameaças à segurança interna em Portugal.

O sistema de segurança interna, porque ao Secretário-Geral do Sistema de Segurança Interna (SGSSI), competem as funções de: "coordenação entre as forças e os serviços de segurança, no âmbito da definição e execução de planos de segurança e gestão de crises"; "articulação das forças e dos serviços de segurança necessários (…) à gestão de incidentes táctico-policiais graves", i.e., ataques a "infra-

[97] Que disponibiliza um conjunto de meios para a denúncia de conteúdos ilegais existentes na internet, embora infelizmente se foque em apenas três tipos de conteúdos - pornografia infantil, apologia ao racismo e apologia à violência -, por meio do preenchimento *online* de um formulário de denúncia, da denúncia por telefone e por *email*.
[98] Nos termos desta lei, é da "competência reservada da Polícia Judiciária a investigação" de crimes "informáticos e praticados com recurso a tecnologia informática".

-estruturas destinadas ao abastecimento e satisfação de necessidades vitais da população" (Lei nº 53/2008). Deste modo, os ciberataques a sistemas informáticos que suportem o funcionamento das infraestruturas críticas e dos meios de comunicação podem ser exemplos desse tipo de ataques.

Assim, as entidades constituintes do SSI, i.e., o SGSSI, que intervém em caso de ciberataque, com impactos graves, às infraestruturas críticas ou meios de comunicação e o Conselho de Segurança do SSI, que intervém a um nível mais geral, participando no processo de definição da política de segurança interna, também podem ter um papel importante na cibersegurança em Portugal.

Em 2009 foi publicada a Lei nº 109/2009, de 15 de setembro (Lei do Cibercrime)[99], que ratificou a Convenção sobre Cibercrime, do Conselho da Europa e transpôs a Decisão-Quadro nº 2005/222/JAI, do Conselho, de 24 de fevereiro, relativa a ataques contra sistemas de informação.

A Lei do Cibercrime sistematiza grande parte das normas penais relacionadas com o cibercrime e a recolha de prova em suporte digital e introduz disposições legais adaptadas à nova realidade (capítulos novos sobre "disposições processuais" e "cooperação internacional"[100]). Contudo, esta legislação impede a monitorização do ciberespaço, como forma de prevenção e controlo, através da criminalização do uso de determinadas técnicas e ferramentas que podem ser usadas para esses fins (embora a informação obtida dessa forma possa facilitar a preparação de cibercrimes).

Na sequência das alterações impostas pela Lei do Cibercrime, que implica uma cooperação entre as autoridades competentes em matéria de investigação criminal, de aplicação da lei (MP e PJ) e os fornecedores de internet (ISPs), foi criado o Gabinete Cibercrime[101], que funciona sob a dependência direta do Procurador-Geral da República, constituindo o organismo responsável pela coordenação da atividade do MP, na área da cibercriminalidade.

Entre as funções do Gabinete Cibercrime estão a promoção de formação específica nesta área para magistrados do MP e a promoção de canais de comunicação entre esses magistrados, os elementos da polícia criminal competente (a PJ) e os ISPs, nomeadamente através da celebração de protocolos de cooperação entre os ISPs e a Procuradoria-Geral da República Portuguesa (Despacho do Procurador--Geral da República, de 7 de dezembro de 2011).

Ainda em 2011, a Lei das Comunicações Eletrónicas - LCE - (a então Lei nº 5/2004, de 10 de fevereiro) foi alterada pela Lei nº 51/2011, de 13 de setembro, que introduziu um capítulo relativo à

[99] A Lei nº 109/2009 revogou a Lei nº 109/91, que já se encontrava obsoleta, tendo em conta o avanço tecnológico e das formas de praticar crimes informáticos, desde a sua entrada em vigor (ex. quem produzisse e/ou difundisse um vírus informático, não teria qualquer tipo de punição, pois estes atos não estavam contemplados na anterior legislação).

[100] A cooperação internacional em matéria de cibercriminalidade é essencial, tendo em conta o caráter transfronteiriço do fenómeno, que possibilita a realização de um ataque informático num país, com impacto noutro(s) país(es). A cooperação e harmonização da legislação nesta matéria, entre os diversos países, permite não só, a agilização e maximização da cooperação internacional, mas também, o combate à cibercriminalidade, evitando *"safe havens"* para os cibercriminosos, proporcionados por países sem este tipo de legislação, onde podem ser alojados *websites* com conteúdos ilegais e onde podem ser hospedados servidores que podem ser utilizados por cibercriminosos, para a realização de cibercrimes, mesmo que estes se encontrem fisicamente em países com legislação de combate à cibercriminalidade, por exemplo.

[101] O Gabinete Cibercrime foi criado por Despacho do Procurador-Geral da República, a 7 de dezembro de 2011.

"Segurança e integridade das redes e serviços", onde estão definidas as obrigações, em matéria de segurança e integridade, tanto das empresas que fornecem redes de comunicações públicas ou serviços de comunicações eletrónicas acessíveis ao público, como da própria Autoridade Reguladora Nacional (ARN), i.e., a ANACOM (Lei nº 51/2011).

Deste modo, a ANACOM passou a ser um ator ainda mais relevante em matéria de cibersegurança, do que já era quando tinha apenas funções de regulação e supervisão das comunicações.

Como já vimos, em 2012 a CNPCE[102], responsável pela gestão de crises, foi extinta, tendo as suas funções passado para a ANPC, nomeadamente a garantia do "planeamento e coordenação das necessidades nacionais na área do planeamento civil de emergência (…) face a situações de crise".

Todavia, durante as entrevistas realizadas no âmbito desta investigação, verificou-se que a ideia de que a gestão de crises compete à ANPC não é partilhada por todos os intervenientes na cibersegurança em Portugal. Alguns elementos entrevistados consideram que, com base na Lei nº 53/2008, a função de gestão de crises compete ao SGSSI, pelas suas atribuições, nomeadamente a garantia da "coordenação entre as forças e os serviços de segurança (…), no âmbito da definição e execução dos planos de segurança e gestão de crises", outros elementos, nomeadamente da ANPC, partilham a ideia de que as funções de gestão de crises competem à ANPC, com base no exposto no Decreto-Lei nº 73/2012[103].

Na base desta discrepância de ideias poderá estar, por um lado, uma questão semântica, pois a Lei nº 53/2008 não define claramente o conceito de gestão de crises nem o âmbito da atuação do SGSSI nesta matéria, enquanto, nem o Decreto-Lei nº 73/2012, nem o Decreto-Lei nº 73/2013, definem objetivamente o conceito de "actividade de planeamento civil de emergência para fazer face (…) a situações de (…) crise" e, por outro lado, existir a probabilidade destes documentos legais terem sido elaborados por um grupo restrito de elementos, com informação limitada sobre esta matéria.

Posto isto, caso houvesse uma "cibercrise"[104], poderíamos não conseguir geri-la em tempo útil, devido à falta de coordenação e de adequados meios de comunicação entre os devidos intervenientes.

No entanto, de acordo com o Decreto-Lei nº 69/2014, o novo CNCseg irá também "Assegurar o planeamento da utilização do ciberespaço em situação de crise e de guerra no âmbito do planeamento civil de emergência". Portanto, prevê-se a necessidade de atualizar a legislação nesta matéria, não só para esclarecer possíveis confusões relativamente às competências de cada entidade, mas também para que todo o processo associado à gestão de "cibercrises" seja fluido e célere e os atores intervenientes sejam claramente identificados e responsabilizados pelo desempenho das suas funções.

---

[102] O CNPCE era um "órgão colegial de apoio consultivo", com a função de definir e atualizar as "políticas de planeamento civil de emergência (…) em situação de crise ou em tempo de guerra" (Decreto-Lei nº 279/84, de 13 de agosto) e tinha uma comissão setorial dedicada ao ciberespaço.

[103] Apesar dos elementos da ANPC considerarem que essa função lhes compete, não têm meios suficientes para o efetivo desempenho da mesma, estando a atuar apenas ao nível do planeamento civil de emergência para as infraestruturas críticas de energia e transportes, às quais se refere especificamente a Diretiva do Conselho da Europa 2008/114/EC, de 8 de dezembro de 2008.

[104] Por "cibercrise" entendemos um incidente grave que afete o normal funcionamento dos serviços básicos que suportam a atividade bancária, os serviços da Administração Pública, o fornecimento de energia, os transportes, os serviços de comunicações, etc.

Em maio de 2014, quase dois anos após a entrega da proposta da Comissão Instaladora e, de acordo com os testemunhos recolhidos, após disputas entre algumas entidades para a superintendência do CNCseg, foi publicado o Decreto-Lei nº 69/2014, que estabelece os seus termos de funcionamento.

O CNCseg, que entrou em funções no dia 7 de outubro de 2014, é o mais recente organismo criado na área da cibersegurança em Portugal, já com um atraso de cerca de 2 anos em relação à data limite avançada pelas organizações europeias para a implementação deste tipo de organismos[105].

Este organismo está integrado no GNS, que passou a ter mais um subdiretor, que ficou responsável pela direção do CNCseg.

É de salientar que, por integrar a PCM e estar sob a dependência do Primeiro-Ministro, o GNS tem acesso a recursos e instrumentos aos quais outros atores não têm, o que facilita a possibilidade de fazer prevalecer os seus interesses, em detrimento dos de outros atores, designadamente a superintendência da autoridade nacional em matéria de cibersegurança, tal como da CERT nacional[106].

Para além destes recursos, o GNS também goza da atribuição de coordenar a criação, instalação e operacionalização de um Centro Nacional de Cibersegurança (RCM nº 12/2012).

A missão do CNCseg consiste em contribuir para um uso mais livre, confiável e seguro do ciberespaço, "através da promoção da melhoria contínua da cibersegurança nacional e da cooperação internacional, em articulação com todas as autoridades competentes, bem como da implementação de medidas e instrumentos necessários à antecipação, à deteção, reação e recuperação de situações que, face à iminência ou ocorrência de incidentes ou ciberataques, ponham em causa o funcionamento das infraestruturas críticas e os interesses nacionais" (Decreto-Lei nº 69/2014).

Para isso, o CNCseg é a "autoridade nacional competente em matéria de cibersegurança, relativamente ao Estado e aos operadores das infraestruturas críticas nacionais", sendo responsável por contribuir para a garantia da "segurança dos sistemas de informação e comunicação do Estado e das infraestruturas críticas nacionais", nomeadamente através de: o desenvolvimento de capacidades "nacionais de prevenção, monitorização, deteção, reação, análise e correção destinadas a fazer face a incidentes de cibersegurança e ciberataques"; a "produção de referenciais normativos em matéria de cibersegurança"; o apoio ao "desenvolvimento das capacidades técnicas, científicas e industriais, promovendo projetos de inovação e desenvolvimento na área da cibersegurança"; a promoção da "qualificação de recursos humanos na área da cibersegurança" e da formação de uma cultura nacional de cibersegurança; a garantia da "articulação e a cooperação entre os vários intervenientes (…) nacionais na área da cibersegurança"; a coordenação da "cooperação internacional em matérias da cibersegurança, em articulação com o Ministério dos Negócios Estrangeiros" (Decreto-Lei nº 69/2014).

[105] A COM(2010) 673 final, define 2012 como a data até a qual os EM deveriam ter as suas CERTs nacionais.
[106] Esta proximidade do Primeiro-Ministro resulta, simultaneamente, num aumento de recursos a mobilizar, por parte do GNS e numa forma do próprio Primeiro-Ministro ter um maior "controlo" sobre esta área de atuação, tão estratégica, quer para a soberania, quer para a economia nacional.

O CNCseg foi implementado este ano, sem verbas orçamentais previstas, nem recursos humanos e materiais suficientes para desempenhar as necessárias funções. Essa implementação em 2014 (aparentemente precoce) pode ter-se devido a um conjunto de razões: a pressão proveniente dos órgãos da UE para o estabelecimento de CERTs nacionais e, mais recentemente, de autoridades nacionais nesta matéria; a necessidade de assegurar as melhores condições nesta área, como forma de incentivo à transferência da Escola de Comunicações e Sistemas de Informação da OTAN para Portugal; talvez a forte mediatização de casos de ciberataques a *websites* governamentais, que pode ter levado a uma percepção do aumento do número de ciberataques em Portugal, conduzindo à necessidade de atuação política; a publicação do Despacho nº 13692/2013, do Ministro da Defesa Nacional, relativo a uma "Orientação para a Política de Ciberdefesa", que inclui o planeamento de um Centro de Ciberdefesa em Portugal, que espera aprovação para ser implementado[107], entre outras.

Posto isto, o GNS pode ter feito uso destes e de outros fatores para induzir alguma pressão sobre os decisores políticos, o que em conjunto com o contexto político (haverão eleições em breve) e a proximidade existente entre o GNS e o Primeiro-Ministro (e outros decisores políticos), pode ter constituído o contexto ideal para a implementação do novo CNCseg nesta altura e no seio do GNS.

Para além das medidas apresentadas, diversa foi a legislação publicada, relacionada com a cibersegurança, embora a grande maioria tenha sido fruto da transposição de diretivas e orientações europeias. Algumas áreas específicas, relacionadas com a cibersegurança, sobre as quais se legislou, foram: a proteção de dados e dos direitos de personalidade; a segurança informática; a cooperação internacional; redes e serviços de comunicações eletrónicas; a proteção da propriedade intelectual; o comércio eletrónico; a documentação eletrónica.

Porém, apesar da panóplia de legislação existente nesta área, as autoridades competentes dispõem de poucos instrumentos legais para a efetiva proteção do ciberespaço. De acordo com declarações de um elemento da PJ, compete-lhes não só a investigação como também a prevenção da cibercriminalidade, mas não têm os instrumentos legais necessários para desempenhar eficientemente essas funções, especialmente as de prevenção (ex. interceção de comunicações[108]).

Quanto às capacidades de investigação também se verificam algumas lacunas, nomeadamente o facto das autoridades competentes não conseguirem responder, pelo menos em tempo útil, aos casos de ciberataques a *websites* governamentais, de partidos políticos e instituições bancárias, devido à falta de determinadas competências e de instrumentos adequados para responder àquele tipo de ataques, com consequências para os direitos à privacidade de vários cidadãos[109].

---

[107] A notícia de que estaria pronto para ser implementado um Centro de Ciberdefesa, enquanto a aprovação do CNCseg estaria pendente desde 2012, pode ter fomentado a necessidade de pressionar mais a tutela para a sua aprovação.

[108] A PJ só pode intercetar comunicações em casos extremamente graves e com a autorização de um juiz.

[109] De acordo com uma notícia publicada no Jornal Público, apesar do Governo ter apostado, em 2011, em *software* aberto para a Administração Pública, "até agora não houve nem formação para os funcionários que fazem a gestão dos sistemas nem verbas para a sua atualização para colmatar as vulnerabilidades" dos sistemas. Além disso, apesar da frequência dos ciberataques, "o Departamento de Investigação e Acção Penal de Lisboa continua apenas a ter

Nestes casos, as autoridades competentes desligam o sistema informático, até averiguação da informação acedida e prejuízos causados, o que impede acessos ilegítimos aos sistemas informáticos mas, também impede comunicações legítimas, prejudicando o normal funcionamento dos serviços da Administração Pública que, por si só, devido à sua cultura burocrática, já tendem a ser morosos, particularmente a justiça.

3.5 Avaliação

Como se pode verificar, as medidas políticas adotadas em matéria de cibersegurança em Portugal têm ocorrido de forma dispersa, incoerente e sem uma estratégia na qual se baseie a ação política. Esta falta de coerência e de estratégia reflete-se no próprio planeamento das medidas que, muitas vezes, é de tal forma abstrato que impede a sua avaliação, pelo que, de uma forma geral, as medidas não são avaliadas, de forma a verificar a sua eficiência ou eficácia, bem como o alcance dos objetivos definidos.

Entre as medidas referidas, algumas são avaliadas, como o SCEE, que é avaliado através de um sistema interno de avaliação periódica de todas as entidades certificadoras, para que possam continuar a certificar e o CERT.PT, que faz, periodicamente, avaliações internas e é constantemente submetido a avaliações externas, para a aquisição das certificações europeias, mas pouco mais do que isso.

Quanto ao CNCseg, o Decreto-Lei nº 69/2014 prevê a sua avaliação em 2017. No entanto, não foi possível apurar se já existem métricas definidas para a avaliação, nem quem irá avaliar, parecendo que ainda não se planeou tal avaliação.

Constata-se então que, em Portugal não existe a prática da realização de auditorias e do desenvolvimento de mecanismos de monitorização e avaliação das medidas políticas implementadas, pelo menos nesta área.

Deste modo, o ciclo das políticas públicas de cibersegurança em Portugal não está completo, apesar de, como exposto atrás, algumas preocupações com esta matéria constarem com alguma frequência na agenda política, desde há mais de uma década.

3.6 Outros atores intervenientes no sistema nacional de cibersegurança

Para além das iniciativas e atores identificados ao longo da exposição do ciclo das políticas públicas nacionais relacionadas com a cibersegurança, existem outros atores que, de alguma forma, intervêm na garantia da cibersegurança em Portugal, que são seguidamente apresentados.

A APDSI foi criada no final de 2000, na sequência do final do período de funções da Equipa de Missão criada para a elaboração do Livro Verde para a Sociedade da Informação em Portugal, por alguns dos seus elementos, incluindo o presidente.

A sua criação deveu-se à necessidade de se continuar a trabalhar na emergente área da sociedade da informação e de sensibilizar o poder político e o setor privado, para a importância desta área.

---

um perito informático" (http://www.publico.pt/sociedade/noticia/procuradoria-de-lisboa-desligou-site-para-colmatar-debilidades-do-sistema-atacado-1633719 - consultado a 30/04/2014).

Esta entidade tem tido um papel importante na área da sociedade da informação e, consequentemente, no sistema nacional de cibersegurança, afirmando-se como um grupo de "pressão sobre os poderes públicos, instituições e sector privado no sentido de maximização dos benefícios da Sociedade da Informação", desenvolvendo exercícios de consciencialização, apelo e aconselhamento ao Estado sobre questões políticas e legais relativas à Sociedade da Informação[110].

O seu grupo de estudos dedicado à "Segurança na Sociedade da Informação" (GSSI), através da publicação de trabalhos como um "Guia sobre o tratamento de dados pessoais", de "As TIC para um Mundo mais Seguro" ou de "O Tratamento de Dados Pessoais em Portugal - Breve Guia Prático", tem contribuído para a criação de uma cultura de cibersegurança, entre essa comunidade.

Esta associação tem uma característica particular: os seus sócios estão profissionalmente ligados a instituições públicas e privadas, consideradas estratégicas na área da sociedade da informação (ex. direção de entidades reguladoras, cargos de topo em instituições governamentais), logo, com acesso a determinados recursos que podem ser essenciais para a introdução ou implementação de determinadas medidas políticas nesta área.

Posto isto, consideramos que a existência e o trabalho desenvolvido por esta entidade é bastante relevante para o desenvolvimento de medidas políticas na área da sociedade da informação em Portugal, incluindo a cibersegurança.

A Shadowsec também tem contribuído para a consciencialização sobre a cibersegurança. Esta empresa (privada) tem desenvolvido diversas atividades, abertas ao público em geral, para as quais são convidados atores com responsabilidades neste domínio, tanto do setor privado, como do setor público, para divulgar e informar quem queira assistir e participar nas conferências e debates, sobre o que fazem, o seu âmbito de atuação, o que é feito noutros países, entre outros.

Entre as atividades desenvolvidas pela Shadowsec há que salientar as iniciativas do mês europeu da cibersegurança, que tiveram lugar entre 7 e 11 de outubro de 2013 e entre 6 e 10 de outubro de 2014, com especial destaque para as atividades de 2014, uma vez que foi no âmbito dessas atividades que o CNCseg entrou formalmente em funcionamento, com a apresentação da sua equipa.

Outras entidades que contribuem para a cibersegurança nacional, embora de forma indireta, são as instituições que oferecem formação nesta área. Instituições que ministram formação académica (ex. Academia Militar; Instituto Superior Técnico; Universidade de Lisboa; Instituto Politécnico de Beja). Empresas que oferecem formação certificada (ex. Rumos; Shadowsec). Empresas que oferecem formação profissional (ex. AmbiSig; Galileu; Shadowsec). Entidades que oferecem formação na área da cibersegurança, de cariz político ou estratégico, como o IDN, que disponibiliza formação em diversas áreas específicas relacionadas com a segurança e defesa e realizou este ano o primeiro Curso de Cibersegurança e Gestão de Crises no Ciberespaço (CGCiber) - um curso destinado à formação de

[110] Consultar http://www.apdsi.pt/index.php/portugues/menu-secundario/sobre-nos/missao-visao-e-objectivos (consultado a 04/05/2014).

quadros intermédios e superiores das estruturas do Estado e elementos da sociedade civil -, tal como a realização (conjuntamente com a Academia Militar e *a MTÜ European Cyber Security Initiative*, da Estónia) de um curso-piloto em matéria de cibersegurança e ciberdefesa intitulado *"Strategic Decision Making Course & Exercise on Cyber Crisis Management"*, com vista a dotar representantes civis e militares, dos Estados-Membros da UE, com as capacidades necessárias para uma eficiente gestão de crises no ciberespaço.

As empresas que fornecem produtos e serviços de segurança informática em Portugal, também têm um papel importante nesta matéria, contribuindo para a proteção das redes e sistemas informáticos de empresas, entidades públicas e cidadãos comuns, não só através do fornecimento de serviços e produtos, mas também da consciencialização para os perigos associados ao uso desprotegido das TIC.

A Comissão Nacional de Proteção de Dados (CNPD), criada em 2004 pela Lei nº 43/2004, de 18 de agosto, é outra entidade com um papel importante no âmbito da cibersegurança nacional.

A esta entidade compete o controlo e a fiscalização do cumprimento da lei em matéria de proteção de dados pessoais e, para isso, promove "a difusão dos princípios da protecção da vida privada e dos dados pessoais e dos diplomas legislativos e instrumentos comunitários e internacionais correspondentes", realiza "acções de inspecção e de auditoria informática a sistemas de informação" e colabora "na organização de colóquios, seminários e outras iniciativas de difusão das matérias de protecção da vida privada e dos dados pessoais", incluindo as TIC (Lei nº 43/2004, de 18 de agosto).

Outro organismo que, de alguma forma, contribui para a cibersegurança em Portugal é o Instituto Português da Qualidade, IP (IPQ), i.e., o Organismo Nacional de Normalização, uma vez que tem entre as suas atribuições a promoção da "elaboração de normas e outros documentos normativos portugueses, nomeadamente para a área da segurança da informação (diretamente relacionada com a cibersegurança) (Decreto-Lei nº 71/2012, de 21 de março e na Portaria nº 23/2013, de 24 de janeiro, dos Ministérios das Finanças e da Economia e do Emprego).

Mas, uma vez que este organismo não tem capacidades para realizar tais funções, formou várias comissões técnicas dedicadas a temas específicos e depositou noutras entidades a responsabilidade da coordenação dessas comissões. Uma delas, a Comissão Técnica 163 (CT 163), criada em 2004, tem a função de acompanhar as normas internacionais ISO, em matéria de segurança da informação, sob a coordenação da Associação Portuguesa de Gestores de Serviços de Tecnologias de Informação (*it*SMF).

Do trabalho desenvolvido pela CT 163, destaca-se a tradução e adaptação da norma ISO 27001, para Portugal. A certificação das organizações, segundo essa norma, tornou-se uma boa prática entre as organizações nacionais, como garantia da qualidade e segurança dos seus serviços.

3.7 Síntese

Após uma análise do que ocorreu nas diferentes fases do ciclo das políticas públicas de cibersegurança em Portugal, verifica-se que este ciclo não é linear, as fases não seguem uma sequência pré-estabelecida, podendo um documento ou evento constituir simultaneamente o objeto do surgimento

do problema, do agendamento e até do planeamento, como é o caso do Livro Verde da Sociedade da Informação em Portugal.

A Sociedade da Informação esteve frequentemente na agenda política nacional, embora a cibersegurança, especificamente, tenha sido menos vezes alvo de ponderação pelos decisores políticos.

Podemos dizer que, em matéria de cibersegurança, realizaram-se apenas uma vez esforços concertados no sentido de se criar aquilo que se pode designar por uma política nacional de cibersegurança, quando se planeou a ENSI (2005), que nunca chegou a ser implementada.

Fora isso, alguns atores têm tentado sensibilizar a comunidade interessada nesta área e o poder político para a importância da cibersegurança[111], sugerindo até propostas de estratégias de cibersegurança, como foi o caso do então diretor do CEGER que, em 2010, entregou ao então Primeiro--Ministro uma proposta de Estratégia Nacional de Cibersegurança ou o caso da Proposta de Estratégia Nacional de Cibersegurança publicada pelo GNS no seu *website*, por exemplo.

Constatou-se também que, apesar de Portugal, em 2005, ter estado na vanguarda dos países que desenvolveram iniciativas relacionadas com a cibersegurança (devido à elaboração da ENSI), atualmente está na cauda dos Estados-Membros da UE, no que concerne a iniciativas estratégicas nesta matéria[112].

Em 2006 foi implementado o SCEE, que permitiu a implementação de diversas medidas relacionadas com esta área (ex. o cartão do cidadão, o passaporte eletrónico, o diário da República Eletrónico, a desmaterialização dos procedimentos parlamentares).

Em 2012, possivelmente por pressão da Comissão Europeia[113], a questão da cibersegurança voltou a ser colocada na agenda política, através do plano global estratégico de racionalização e redução de custos com as TIC na Administração Pública, que previa a definição e implementação de uma Estratégia Nacional de Cibersegurança, que deveria incluir, entre outros, a criação de um Centro Nacional de Cibersegurança.

Porém, em 2014 temos apenas mais um Centro Nacional de Cibersegurança que, apesar de ter sido aprovado em maio, só entra em funções em outubro, sem dotações orçamentais concretas atribuídas, tendo apenas um local físico atribuído, alguns funcionários e alguns equipamentos, estando previstas as suas capacidades iniciais, para o início de 2015.

---

[111] O CERT.PT tem dado formação e ajudado a criar outras CERTs e criou uma rede nacional de CERTs, a APDSI procura fazer *lobbying* para a área da Sociedade da Informação, incluindo a cibersegurança, o IDN procura juntar os atores interessados, para contribuir para o desenho de uma Estratégia Nacional de Informação, etc.

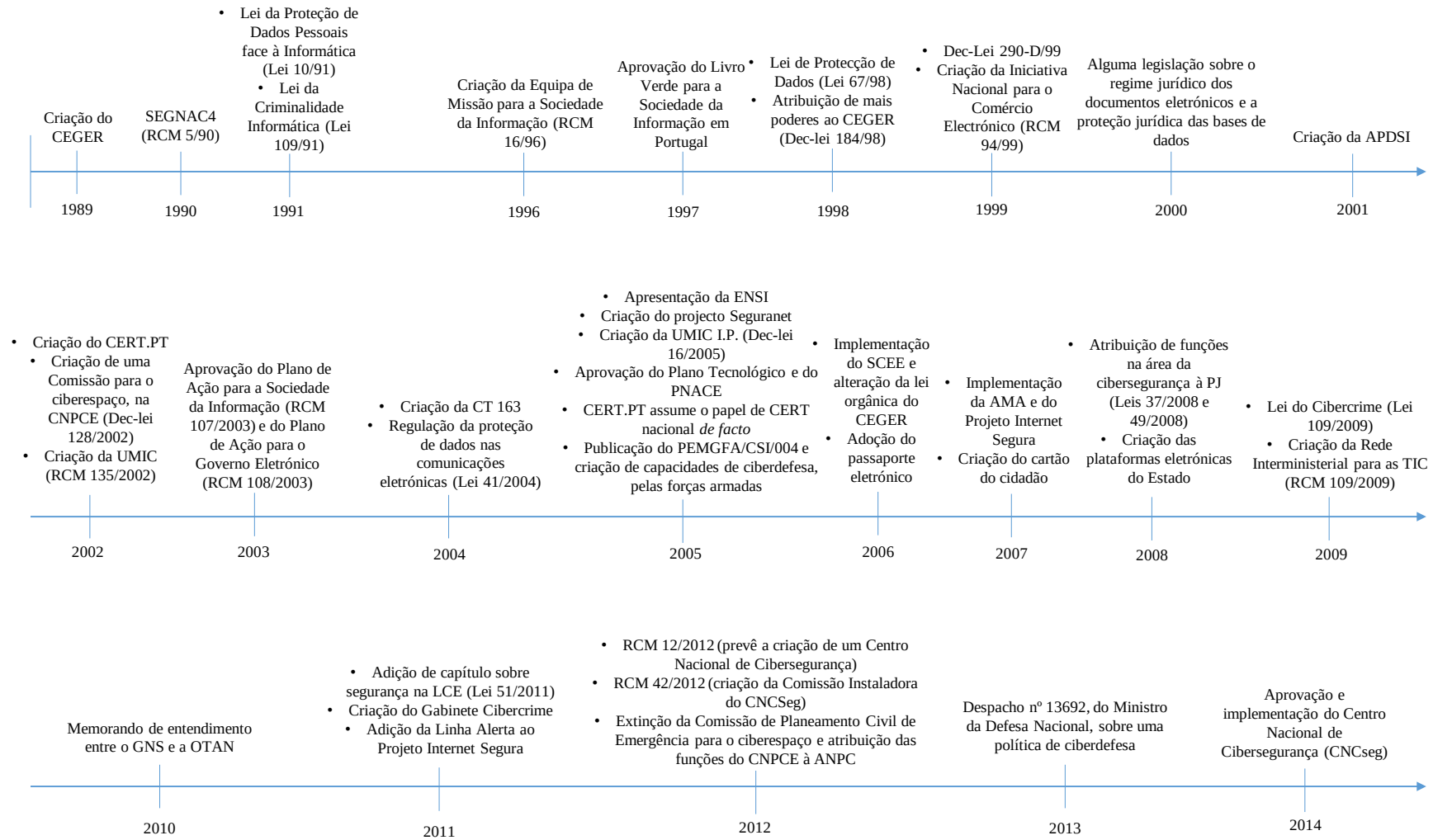
[112] Atualmente 36 países têm as suas estratégias nacionais de cibersegurança, sendo 18 deles da UE. Consultar http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world (consultado a 19/06/2014).

[113] Diretiva do Parlamento Europeu e do Conselho 2009/140/CE, de 25 de novembro de 2009; COM(2010) 245 final; COM(2010) 673 final, entre outros.

Seguidamente apresenta-se uma "linha temporal", onde estão resumidas as iniciativas realizadas em matéria de cibersegurança, ao longo do tempo[114].

[114] Deve-se ressalvar que esta linha temporal foi elaborada com base na informação à qual foi possível aceder, podendo estar incompleta. Por outro lado, devido ao facto do conceito de cibersegurança não estar legalmente definido em Portugal e variar entre pessoas e organizações, é possível que algumas pessoas considerem a linha mais ou menos completa que outras. É também importante referir que esta linha deve ser constantemente atualizada, para se ter uma clara "fotografia panorâmica" das iniciativas desenvolvidas nesta área.

Figura 1: Ação política em matéria de cibersegurança em Portugal



Em anexo, na página 81, apresenta-se uma figura semelhante com informação relativa à União Europeia, no geral.

CAPÍTULO 4. ESTUDO DE CASOS

Após a descrição apresentada da ação política em matéria de cibersegurança, destacam-se duas medidas políticas, que analisaremos com maior pormenor: a criação do Sistema de Certificação Eletrónica do Estado (SCEE) e a criação do Centro Nacional de Cibersegurança (CNCseg).

A seleção destas medidas, em detrimento de outras, deve-se ao facto de as considerarmos das mais relevantes para a garantia da cibersegurança em Portugal. Além disso, as restantes medidas apresentadas baseiam-se, principalmente, em alterações legislativas (ex. atribuição de funções em matéria de cibersegurança à PJ ou a criação da Lei do Cibercrime) ou não foram iniciativas de cariz governamental (ex. a criação do CERT.PT[115] ou do projeto Internet Segura).

A criação do SCEE trouxe um maior nível de segurança ao sistema de *eGovernment* português, através da introdução de certificações de segurança e de sistemas de autenticação seguros na documentação e nas operações *online* realizadas entre o cidadão, as empresas e o Estado e foi uma medida basilar para o desenvolvimento de outras nesta área (ex. a desmaterialização dos procedimentos parlamentares, a implementação do cartão do cidadão ou do passaporte eletrónico).

A implementação do CNCseg poderá traçar o início da criação de uma política integrada em matéria de cibersegurança em Portugal. O CNCseg compreenderá, não só, a autoridade nacional em matéria de cibersegurança relativamente ao Estado e aos operadores de infraestruturas críticas nacionais[116], pelo que se espera que venha atribuir legitimidade e coerência à ação política nesta matéria[117], mas também a CERT nacional, disponibilizando serviços de reação rápida a incidentes informáticos com grande impacto e apoio na gestão de vulnerabilidades.

Para a análise, baseámo-nos nas seguintes teorias de análise das políticas públicas: o modelo *multiple streams framework* ou teoria dos fluxos múltiplos e o neo-institucionalismo da escolha racional. A escolha destas teorias baseou-se no facto de, em comparação com outras (ex. teoria da escolha pública, institucionalismo histórico, *advocacy coalition framework*), considerarmos serem as mais adequadas aos casos em análise, dado o ênfase que dão em determinados fatores.

---

[115] Poderíamos também destacar a criação do CERT.PT que, em nosso ver, é a entidade melhor preparada em Portugal para garantir a cibersegurança em caso de incidentes informáticos. Contudo, não o destacamos, porque não foi uma iniciativa do Governo e, principalmente, por não ter um mandato político para tal.

[116] Embora, o Decreto-Lei nº 69/2014 não seja suficientemente esclarecedor quanto às funções e os poderes do CNCseg, não esclarecendo o que deve/pode e não deve/não pode fazer e em relação a que entidades. Pressupõe-se que em caso de ciberataques que não estejam relacionados com o Estado ou com os operadores das infraestruturas críticas nacionais, o CNCseg não terá autoridade, pelo que o seu papel na resolução desses problemas será diferente de casos de ciberataques que envolvam o Estado, mesmo que os impactos dos primeiros sejam piores que os dos segundos.

[117] Espera-se que a criação do CNCseg leve à elaboração e aprovação de uma coerente Estratégia Nacional de Cibersegurança, em Portugal.

4.1 Criação do Sistema de Certificação Eletrónica do Estado à luz da teoria dos fluxos múltiplos

Para analisar a criação do SCEE recorreu-se à teoria dos fluxos múltiplos. Esta teoria de análise das políticas públicas, introduzida por John Kingdon em 1984, na sua obra *Agendas, Alternatives and Public Policies*, deriva do modelo *Garbage Can*, de Cohen, March e Olsen (1972) que, por sua vez, teve origem no modelo da escolha organizacional, segundo o qual as escolhas resultam de forças estruturais e processos cognitivos e afetivos que dependem do contexto no qual são tomadas.

O modelo *Multiple Streams* foca-se na análise dos processos de colocação de questões na agenda política e na formulação de políticas em contextos de ambiguidade, atribuindo grande relevância aos *timings* e à sequência das escolhas políticas.

Este modelo é constituído por cinco elementos: os problemas; as políticas; a política; as *policy windows*; os *policy entrepreneurs*.

Entre estes cinco elementos estão os três *streams* ou fluxos, essenciais nesta teoria: o fluxo dos problemas; o fluxo das políticas ou soluções; o fluxo da política ou do contexto político.

O fluxo dos problemas consiste nas preocupações que os indivíduos, dentro e fora do sistema político, têm. Essas preocupações estão relacionadas com as condições em que vivem. Pode-se verificar quais são esses problemas através de indicadores, como dados estatísticos, eventos focalizadores, estudos de opinião, peças publicadas nos *media*, *feedback* de políticas anteriores, comparações internacionais, entre outros.

No período anterior à implementação do SCEE, Portugal deparava-se com o facto de, por um lado, já haver diversos serviços da Administração Pública disponibilizados *online* (ex. a criação de empresas ou o pedido e renovação de documentos) e alguns projetos em desenvolvimento (ex. o cartão do cidadão ou a desmaterialização dos procedimentos parlamentares) à espera de um sistema destes que garantisse os adequados níveis de segurança para a sua implementação, nomeadamente assegurar a atribuição de certificados para uma autenticação segura e certificados para assinaturas eletrónicas qualificadas, por outro, se verificar a necessidade de reduzir gastos públicos, o que se podia alcançar com um programa de compras públicas eletrónicas e, por outro ainda, já se terem detetado alguns problemas de segurança que necessitavam a tomada de medidas para os mitigar.

Deste modo, a criação desta entidade viria proporcionar as bases necessárias para a introdução dos projetos em desenvolvimento e garantir um maior nível de segurança dos serviços já disponibilizados *online*, pela Administração Pública.

O fluxo das políticas geralmente inclui uma "sopa primavera" de ideias que lutam por aceitação nas redes de atores políticos. Essas ideias são concebidas por especialistas, no seio das comunidades políticas - redes que integram burocratas, académicos, investigadores, entre outros, que partilham o interesse por determinada área de políticas.

Até se chegar ao SCEE, diversas foram as propostas deste tipo de medida, embora a lógica subjacente a todas elas fosse a mesma - uma entidade que garantisse a certificação e autenticação segura nas operações realizadas entre os cidadãos, as empresas e o Estado.

Ao longo deste processo de planeamento de um sistema de certificação eletrónica do Estado, vários foram os atores e redes intervenientes, tais como o conjunto de atores que elaboraram a ENSI, os que elaboraram os Planos de Ação para o Governo Eletrónico e para a Sociedade da Informação, o PNACE e o grupo responsável pelo acompanhamento do planeamento e implementação do próprio SCEE.

Entre estes atores, destacamos a UMIC, que liderou a elaboração da ENSI, que parece ter estado perto de ter sido implementada e que incluía este tipo de sistema e o então sub-diretor do CEGER que, por delegação do Secretário de Estado da PCM, coordenou o grupo responsável pelo acompanhamento do planeamento e implementação do SCEE, processo que demorou apenas cerca de sete meses (incluindo o desenho do modelo de governação, a criação das instalações, a aquisição do equipamento, o recrutamento de recursos humanos e a produção regulatória necessária).

O fluxo da política é composto por três elementos: o *mood* nacional; as campanhas dos grupos de pressão; a mudança na administração ou no poder legislativo.

O *mood* nacional no período anterior à criação do SCEE caracterizava-se pela estabilidade social e económica, trazida pela mudança de Governo e esperança na mudança, na inovação e no aumento do número de postos de trabalho.

Quanto aos grupos de pressão, em Portugal não existe grande tradição no uso deste tipo de grupos, embora exista a APDSI, que vai desenvolvendo algumas atividades nesse sentido, mas neste caso em particular não se verificou claramente a sua influência na implementação do SCEE.

Relativamente à mudança na administração ou no poder legislativo, verifica-se que a implementação desta medida ocorreu sensivelmente um ano após a queda do XVI Governo Constitucional e a entrada de um novo Governo. Portanto, ocorreu numa altura em que o Governo se esforçava por ganhar popularidade e cumprir as promessas feitas durante a campanha eleitoral, nomeadamente, a implementação do Plano Tecnológico, que tinha como intuito, entre outros, "Convocar Portugal para a Sociedade da Informação" e "Vencer o atraso científico e tecnológico"[118] (Programa do XVII Governo Constitucional).

Quando estes três fluxos (problemas, políticas e política) se juntam, em determinadas condições, surgem as *policy windows*, i.e., janelas de oportunidade para a adoção de novas medidas políticas ou alteração das existentes - neste caso, para a implementação do SCEE.

Segundo Kingdon (1995), as *policy windows* são oportunidades para os defensores de determinadas propostas impulsionarem as suas soluções de estimação ou para chamar a atenção para

[118] Entre os objetivos específicos do Plano Tecnológico estava a introdução do cartão do cidadão, que necessitava, previamente, de um sistema de chaves públicas.

determinados problemas, do seu interesse. O autor defende ainda que estas "janelas de oportunidade" duram pouco tempo abertas.

Estas janelas são muitas vezes abertas pelos *policy entrepreneurs*, i.e., atores individuais ou coletivos (ex. peritos, sindicatos) que procuram acoplar os três fluxos. Estes atores são considerados *power brokers*, na medida em que conseguem captar a atenção dos decisores políticos e influenciar as suas decisões. A sua eficácia depende da persistência e da capacidade de juntar os problemas às soluções e encontrar políticos recetivos às suas ideias, assim como o acesso privilegiado aos decisores políticos.

Neste caso, destacamos dois atores que tiveram papéis importantes em momentos diferentes. A UMIC, através da proposta de criação de um sistema destes no Plano de Ação para o Governo Eletrónico e, principalmente na ENSI que, se na altura se tivessem verificado e juntado todos os fluxos, teria aberto uma *policy window* para a sua implementação. O CEGER, através da coordenação do grupo designado para criar e implementar o SCEE. Sob a coordenação do então sub-diretor do CEGER, este grupo em cerca de sete meses preparou e implementou todo o sistema, desde o *benchmarking* do que seria feito no estrangeiro, passando pela regulação e até a implementação e avaliação[119].

Portanto, não diríamos que o CEGER abriu uma *policy window*, mas aproveitou-a eficientemente e conseguiu criar e implementar em apenas sete meses, o que andava na agenda política desde 2003.

4.2 Criação do Centro Nacional de Cibersegurança à luz do neo-institucionalismo da escolha racional

Para analisar a criação do CNCseg recorremos ao neo-institucionalismo da escolha racional.

Esta teoria retrata o Estado como um ator racional, que age de acordo com uma "lógica de interesses".

Segundo esta teoria, os atores têm um conjunto de preferências e comportam-se de modo absolutamente utilitário para maximizar a satisfação das suas preferências, de forma estratégica e calculista, sendo os seus cálculos fortemente influenciados pelas suas expetativas relativamente ao comportamento provável dos outros atores.

No caso da implementação do CNCseg, considera-se que os cálculos dos decisores políticos foram influenciados pelas suas expectativas relativamente ao comportamento de determinadas entidades como:

1) a UE, de quem Portugal recebe "pressão" e de onde se poderá vir a receber fundos (especialmente, no âmbito do Programa Horizonte 2020[120]) para a implementação e o desenvolvimento deste organismo, dado que Portugal já se encontra há quase dois

[119] Segundo declarações do então responsável pelo grupo, a implementação do SCEE só foi possível devido à determinação e rapidez da ação do grupo, ou então ter-se-ia perdido a oportunidade de o implementar.
[120] O Programa Horizonte 2020 é um Programa-Quadro Comunitário de Investigação e Inovação, desenvolvido para apoiar a investigação desenvolvida na UE entre 2014 e 2020.

anos em incumprimento com a data definida para a criação de uma CERT nacional (mandatada para tal);

2) a OTAN, uma vez que está prevista a instalação da nova Escola de Comunicações e Sistemas de Informação da OTAN, em Portugal, que deverá trazer mais investimento e conhecimento e poderá criar mais postos de trabalho no nosso país, assim como proporcionar uma maior visibilidade da *expertise* dos peritos portugueses nesta área e, sabendo que, enquanto a Escola não estiver efetivamente operacional, não temos a garantia da sua vinda para cá, dado que há vários países interessados neste tipo de investimento, principalmente na atual conjuntura económica. Por esta razão, poder ter-se considerado urgente o estabelecimento de uma autoridade nacional em matéria de cibersegurança e de uma CERT nacional, que estão entre as atribuições do CNCseg;

3) o eleitorado, pois dada a conjuntura económica e social que se tem vivido em Portugal nos últimos anos, é natural que o atual Governo procure deixar "marcas" do trabalho realizado, como pode ser o caso da implementação do CNCseg, cuja proposta de implementação salientava a urgência da sua constituição, mas aguardava uma decisão do Governo, desde 2012.

Por outro lado, as instituições estruturam a interação entre os decisores políticos e os restantes atores, influenciando a possibilidade de introdução e a sequência de alternativas na agenda ou oferecendo informações ou mecanismos que reduzem a incerteza em relação ao comportamento dos outros atores, ao mesmo tempo que propiciam aos atores os "benefícios da troca"[121], incentivando a realização de determinados cálculos e ações (Hall e Taylor, 2003).

A razão para a implementação do CNCseg, pelo menos inicialmente, no âmbito do GNS foi "a transversalidade da (sua) missão e das atribuições do GNS e da Autoridade Nacional de Segurança, bem como a direta dependência destas entidades do Primeiro-Ministro" (Dec-Lei nº 69/2014).

Porém, fica a expectativa deste organismo vir a tornar-se autónomo, mantendo-se na PCM, pois o Decreto-Lei que o aprova, prevê o funcionamento do CNCseg, no âmbito do GNS, até 2017, altura em que será alvo de uma avaliação e se decidirá se permanecerá ali ou não.

Os teóricos desta Escola tendem a considerar a vida política como um conjunto de dilemas de ação coletiva, caracterizados por situações em que os indivíduos que agem de modo a maximizar a satisfação das suas preferências o fazem sob o risco de produzir um resultado sub-ótimo para a coletividade.

Estes dilemas ocorrem porque a ausência de condições institucionais que garantam comportamentos complementares da parte de outros atores impede cada ator de adotar uma linha de

[121] Explicação do que são os benefícios da troca nas páginas 55-56 deste texto.

ação que seria preferível no plano coletivo. Isto acontece porque não há adequados mecanismos de comunicação entre os atores envolvidos, talvez porque quem tem o poder discricionário para o planeamento e a implementação do CNCseg, entenda que deva ser assim ou por não conseguir criar laços de confiança com os restantes atores intervenientes na cibersegurança em Portugal, por exemplo[122].

Esta abordagem propõe uma compreensão um pouco simplista da racionalidade e motivação humanas, perdendo-se as subtilezas dos motivos humanos para agir (Mansbridge, 1990) e os seus pressupostos falham, ao postular a racionalidade instrumental como única motivação para a ação política, uma vez que os decisores políticos, tal como todos os intervenientes numa decisão política, são seres humanos que mudam de ideias, têm hábitos e ideologias, para além de terem acesso a informação limitada, o que lhes limita a racionalidade na ação.

Por exemplo, a maioria dos funcionários do GNS são militares, incluindo a própria ANS e estes têm idiossincrasias próprias, provenientes da sua formação e relacionadas com o tipo de funções que desempenham, como a garantia da soberania nacional. Os militares estão habituados a lidar com segredos de Estado, informação classificada e sensível, entre outras e, arriscamo-nos a dizer que são dos portugueses melhor preparados para definir estratégias, pois estão habituados a defini-las e segui-las.

O facto dos militares estarem habituados e preparados para definir estratégias e agir consoante essas poderá ter levado a que o CNCseg fosse criado (inicialmente) no seio do GNS, pois este último (GNS) parece ter sido um persuasivo *policy entrepreneur* no processo de criação do CNCseg, tendo conseguido mesmo ficar com a sua tutela, pelo menos até 2017.

Esta teoria tende a explicar a criação de uma instituição tendo em conta os seus efeitos, assumindo que os atores racionais (atores que procuram maximizar as suas preferências, principalmente em relação a questões económicas) podem perceber os efeitos das instituições que os afetam, criá-las e controlá-las (Bates, 1987; Hall e Taylor, 1996; *apud* Schmidt, 2006).

Assim, com base nestes fatores (a criação de uma instituição pode ser explicada com base nos seus efeitos; os atores racionais podem perceber os seus efeitos, criar e controlar as instituições; os atores procuram maximizar os seus interesses, nomeadamente os económicos), considera-se que a criação do CNCseg em 2014, mesmo sem dotações orçamentais concretamente previstas para a sua implementação, sem debate político público antes da sua implementação, particularmente sob a alçada do GNS, pode ser explicada com recurso ao neo-institucionalismo da escolha racional.

Considera-se que o principal *policy entrepreneur* interveniente na criação e implementação do CNCseg foi o GNS, que ficou com a sua tutela, apesar de haver outros atores interessados nesse papel.

[122] O facto de não se conseguir criar laços de confiança entre os vários atores intervenientes na cibersegurança (assim como noutras áreas) em Portugal, parece estar relacionado, por um lado, com uma cultura portuguesa, que provém desde a época ditatorial, de não partilha de informação (e, até por vezes, sentimentos) com elementos externos à família e amigos mais chegados e, por outro, o facto das leis não serem claras, permanecendo a dúvida sobre o que será, ou não, segredo de Estado, segredo de negócio, proteção de dados pessoais, entre outros, bem como com quem se pode, ou não, partilhar esse tipo de informação.

Apesar de não ter sido possível confirmar a existência de interesses económicos na implementação do CNCseg no seio do GNS, sabemos que a criação deste tipo de organismo no seio de determinada entidade poderia permitir, juntamente com o alargamento do espectro das suas funções e capacidades, também o aumento do orçamento nacional para essa entidade. Neste caso em concreto, considerando a área de atuação (no âmbito da Sociedade da Informação e das tecnologias), acrescenta-se a possibilidade de obtenção de financiamento externo, no âmbito do Programa Horizonte 2020, que poderá aumentar o "bolo" do orçamento do GNS.

Por outro lado, verifica-se que a criação do CNCseg no seio do GNS pode ser justificada com base nos efeitos que este novo organismo poderá trazer ao primeiro (para além dos fatores económicos), tais como: o facto do GNS coordenar e passar a ter o controlo na área da cibersegurança em Portugal, uma área tão abrangente e cobiçada, dado o seu cariz estratégico, através da superintendência da autoridade nacional de cibersegurança; o facto do GNS poder, dessa forma, vir a criar e melhorar as ligações com outras instituições e até ter um maior controlo sobre o que é feito nesta matéria, através de mecanismos de monitorização e auditoria, entre outros.

Para a criação do CNCseg foram utilizados determinados recursos e mobilizadas vontades, preponderantes para que hoje houvesse esta entidade em Portugal. Entre os recursos aos quais o GNS tem acesso e que foram mobilizados, podemos destacar: o acesso privilegiado aos decisores políticos, nomeadamente o Primeiro-Ministro; a possibilidade de realizar diretamente acordos com a OTAN, (ex. o memorando de entendimento assinado em 2011, que estabelece que o GNS é o ponto de contato nacional com a OTAN, em matéria de ciberdefesa); o facto de lhe ter sido atribuída a responsabilidade de coordenar a criação e instalação de um Centro Nacional de Cibersegurança[123].

Para além destes fatores, houve outros, não relacionados com o GNS, mas que, conjuntamente com os fatores apresentados, podem ter acelerado o processo de implementação do CNCseg.

A perceção do aumento do número de ciberataques, geralmente veiculada pelos *media* e a morosidade e falta de instrumentos adequados para lidar com tais assuntos, parecem ter tido como consequência o aumento da atenção por parte da opinião pública, sobre estas matérias.

O facto da divulgação de ciberataques bem sucedidos a *websites* governamentais, nomeadamente os do Ministério Público e da PSP, poder vir a diminuir a probabilidade da transferência da Escola de Comunicações e Sistemas de Informação da OTAN, para Portugal, o que, em nosso ver, poderia ser danoso, primeiro, porque a transferência deste organismo para Portugal viria compensar a extinção do antigo comando operacional da OTAN, situado em Oeiras, que levou à redução de um significativo número de postos de trabalho e, depois, porque após a extinção deste organismo e sem a transferência de outro organismo da OTAN para Portugal, deixaria de existir no nosso país qualquer organismo desta organização internacional, o que poderia afetar a nossa capacidade de interlocução internacional.

[123] Consoante testemunhos recolhidos.

Outro motivo que se afigura como um fator de pressão para a implementação do CNCseg, nesta altura, foi a notícia de que o Centro de Ciberdefesa já estaria pronto para entrar em funcionamento, sob a tutela do CEMGFA, assim que aprovado.

A sumar a estes fatores existiam as várias orientações da UE para a criação de CERTs nacionais e, desde 2013, para a criação de autoridades nacionais com responsabilidades neste domínio.

Considera-se que este conjunto de fatores pressionaram os decisores políticos a tomarem medidas.

Relativamente à criação de uma CERT nacional mandatada para tal, havia uma hipótese que se afigurava mais económica e eficiente para resolver a questão da falta de existência deste tipo de serviço. Essa solução seria a atribuição de um mandato político ao CERT.PT (que já vinha a desempenhar as funções de CERT nacional *de facto*).

Esse mandato viria facilitar a cooperação e o desenvolvimento de mecanismos de alerta rápido, por exemplo que, muitas vezes, só são possíveis quando existem relações institucionais entre os intervenientes.

Todavia, todos os atores intervenientes no ciclo de uma política pública de cibersegurança, incluindo os decisores políticos, têm as suas perspetivas (que muitas vezes se confundem com os seus interesses particulares), que podem, à primeira vista, não parecer muito racionais. Neste caso em particular, pelas razões já apresentadas, nomeadamente os interesses e recursos mobilizados pelo GNS, o que parece ter-se sobreposto na decisão política foi a influência mobilizada.

Além da poupança de recursos, um dos principais benefícios da atribuição de um mandato político ao CERT.PT seria o cumprimento dos prazos previstos nas orientações provenientes da UE para a criação de uma CERT nacional.

Porém, para acompanhar as mais recentes orientações da Comissão Europeia, nesta área[124], Portugal também teria que criar uma autoridade nacional em matéria de cibersegurança. Desta forma, poderá considerar-se pertinente a criação do CNCseg, que vem cumprir as orientações da UE, não só para a criação de um serviço nacional de resposta a incidentes de informática, mas também de uma autoridade nacional com responsabilidades em matéria de cibersegurança.

Este organismo concentra o poder em matéria de cibersegurança, numa só entidade, não convergindo com uma política de desconcentração do poder, muito em voga até o início da atual conjuntura económica. Contudo, tal concentração de poder, permite, desde que a entidade tenha capacidade para fazê-lo, ter um maior controlo sobre o que se passa no ciberespaço e uma melhor coordenação da resposta, em caso de incidente ou "cibercrise".

Como já foi referido, a aplicação do neo-institucionalismo da escolha racional a uma medida política implica a existência de "benefícios da troca", para se chegar a decisões estáveis. Neste caso, tanto os decisores políticos como a comunidade que desenvolve atividades na área da cibersegurança e os próprios cidadãos usufruem desses benefícios.

[124] Consultar JOIN(2013) 1 final e COM(2013) 48 final.

Os decisores políticos beneficiam na medida em que a implementação do CNCseg pressupõe o aumento da cibersegurança em Portugal, o que poderá proporcionar, a longo prazo, mais investimento externo em Portugal[125] e, possivelmente, uma melhoria da perceção da ação política nesta matéria, considerando a mediatização dos ciberataques a *websites* governamentais, com impacto nos direitos à privacidade de vários cidadãos portugueses.

A comunidade que desempenha funções na área da cibersegurança, que alertou para a necessidade da criação desta entidade e contribuiu para a sua criação vê o seu esforço ser recompensado.

Os cidadãos em geral beneficiam com a implementação do CNCseg através do aumento do controlo e monitorização da atividade *online*, que poderá resultar num aumento do sentimento de segurança e da confiança na utilização da internet, designadamente na execução de transações ou outras operações *online*.

[125] Uma vez que, atualmente, a maioria das empresas se baseiam no uso da internet para o desenvolvimento dos seus negócios, podem vir a preferir sedear-se em países com legislação, autoridades e capacidades operacionais competentes, que garantam esse tipo de segurança, essencial aos seus negócios.

CONCLUSÕES

Todos os dias em Portugal, à semelhança de outros países, ocorrem cibercrimes, principalmente a infeção com vírus e o *phishing*. Paralelamente a este tipo de crimes têm ocorrido campanhas de ciberespionagem e ciberterrorismo, sendo a ciberespionagem especialmente preocupante em Portugal.

Para lidar com este tipo de eventos, desde a década de 90 têm-se adotado algumas medidas que poderíamos considerar como parte de uma política pública de cibersegurança. Algumas dessas medidas provenientes de orientações da UE, já que num ciberespaço sem fronteiras, a sua proteção depende da soma dos esforços realizados por todos os países e cada vez mais os cidadãos, as organizações e a própria Administração Pública (uma vez que, muitos dos seus serviços são disponibilizados *online*) dependem das redes e dos sistemas informáticos para funcionar normalmente.

Não obstante, em 2014, Portugal continua sem ter uma política pública de cibersegurança.

Contudo, entre a década de 90 e a atualidade, a ação política nesta matéria sofreu alterações, principalmente a partir de 2008.

Até meados de 2007 não se tinha ouvido falar de casos de ciberataques de grande escala que tivessem afetado o funcionamento de qualquer país. Mas, em 2007 os *websites* governamentais e de setores críticos da Estónia e em 2008 os da Geórgia sofreram ciberataques tendo ficado bloqueados. Estes eventos chamaram a atenção para os impactos que os ciberataques podem ter, não só no comércio eletrónico (um dos fatores de competitividade de um país e elemento sobre o qual recaía muito a lógica nacional, pelo menos até 2005), mas também no normal funcionamento dos serviços que sustentam as sociedades e na segurança nacional.

Posteriormente, verificou-se que estes ataques tiveram impacto nas decisões e ações de diversos Governos e organizações internacionais[126].

Ao nível nacional também se verificaram algumas alterações, nomeadamente o facto das medidas políticas adotadas nesta matéria, desde 2008, não se terem prendido tanto com questões relacionadas com a disponibilidade e a acessibilidade da informação, mas mais com a investigação criminal de cibercrimes e a proteção do ciberespaço (ex. a criação da UTI, da PJ, a assinatura do memorando de entendimento entre o GNS e a OTAN, a criação do Gabinete Cibercrime, a criação do CNCseg).

Neste projeto tentou-se dar uma perspetiva abrangente da ação política nacional em matéria de cibersegurança. Essa informação está dispersa por vários atores e fontes, o poderá ter resultado na falta de referência a determinados atores ou iniciativas adotadas nesta área.

O principal intuito deste estudo é criar uma base (documento), certamente a atualizar e corrigir, que agregue, de forma cronológica, as iniciativas e as capacidades de cibersegurança existentes em Portugal. Tal facilitará futuros estudos de políticas públicas de cibersegurança em Portugal.

[126] Em 2008 a Estónia e a Eslováquia publicaram as suas estratégias nacionais de cibersegurança, foi criado o CCD CoE da OTAN e a OCDE publicou uma recomendação sobre a proteção das infraestruturas críticas de informação (C(2008)35), em 2009 o Reino Unido e a Austrália também criaram as suas estratégias nesta área, entre outros.

Procedeu-se à análise da ação política em matéria de cibersegurança em Portugal, utilizando como modelo de análise o ciclo das políticas públicas, uma variante do processo das políticas públicas, de Lasswell (1956). Assim, descreve-se o que aconteceu nas cinco etapas desse ciclo: o surgimento do problema, o agendamento, o planeamento, a implementação e a avaliação[127].

Até hoje, foram implementadas em Portugal algumas medidas políticas e criadas algumas capacidades de cibersegurança, embora não exista uma política pública nesta área, o que pode ser explicado com uma citação de Friedrich: "Public policy is being formed as it is being executed and (…) executed as it is being formed" (Friedrich, 1940: 6).

Considera-se que o Livro Verde para a Sociedade da Informação em Portugal (1997) constituiu, simultaneamente, o surgimento do problema e o primeiro agendamento e planeamento da cibersegurança em Portugal. Mas, a cibersegurança é um tema que, apesar de ter sido, por algumas vezes, introduzido na agenda política, poucas vezes foi debatido publicamente (possivelmente, porque os cidadãos no geral estão pouco sensibilizados para esta questão).

Muitas das medidas previstas têm vindo a ser implementadas, embora passe muito tempo entre o seu planeamento e implementação. Porém, falta a implementação de determinadas medidas, previstas já há alguns anos, como: uma política de criptografia; uma política de segurança informática; a revisão do quadro legal para a segurança das matérias classificadas, incluindo a segurança dos sistemas de comunicação e informação, entre outras.

No entanto, com a entrada em funcionamento do CNCseg e o estabelecimento de adequados mecanismos de comunicação entre os intervenientes na área, bem como o estabelecimento de adequados mecanismos de consulta dos interessados (ex. sociedade civil, setor privado), espera-se que fiquem criadas as condições necessárias para o planeamento e implementação daquelas medidas.

Entre as iniciativas adotadas, destacamos a criação do CERT.PT, que tem tido um papel importante no desenvolvimento da cibersegurança em Portugal, acompanhando as orientações da ENISA e funcionando como CERT nacional *de facto* e elo de ligação entre Portugal e o exterior, no que respeita a proteção de redes e sistemas de informação e resposta a incidentes.

O CERT.PT também criou uma rede de CSIRTs que junta entidades de vários setores, que desenvolveram laços de confiança entre si e passaram a cooperar para um maior nível de segurança das suas redes e sistemas de informação, tendo impacto na cibersegurança nacional.

Quanto às iniciativas governamentais, distinguimos a proposta de criação de uma ENSI, a criação do SCEE e a recente criação do CNCseg que, embora publicados os termos do seu funcionamento no Decreto-Lei nº 69/2014, ainda está em fase de formação do pessoal e com um orçamento muito reduzido, proveniente de várias fontes, para fazer justiça à sua implementação, em outubro.

[127] Sobre a avaliação não foi possível aprofundar os conhecimentos, porque, por um lado, as medidas políticas implementadas em Portugal tenderam a não ser avaliadas e, por outro, não existe, concretamente, uma política pública de cibersegurança em Portugal, uma vez que o conhecimento e o ciclo das políticas públicas de cibersegurança ainda está em desenvolvimento.

O CNCseg é a primeira entidade criada em Portugal cuja designação refere concretamente "cibersegurança" e com competências nessa matéria. É, simultaneamente, a "autoridade nacional (…) de cibersegurança", a CERT nacional e a terá competências ao nível da gestão de crises, em caso de ciberataque (Decreto-Lei nº 69/2014, de 9 de maio).

A implementação do CNCseg foi um passo muito importante e prevê-se que seja o passo antecedente à formulação de uma política pública nacional integrada de cibersegurança, embora ainda não estejam reunidas as condições necessárias para este organismo funcionar eficaz e eficientemente.

A legislação nacional não permite uma efetiva monitorização do ciberespaço, pelo que a prevenção do cibercrime e de outro tipo de ciberataques e incidentes de cibersegurança em Portugal não é eficazmente conseguida. O novo CNCseg deverá "exercer os poderes de autoridade nacional (…) de cibersegurança, relativamente ao Estado e aos operadores de infraestruturas críticas nacionais", todavia, não estão previstos os mecanismos de coordenação entre esta autoridade e as restantes com responsabilidades sobre as infraestruturas críticas nacionais (ex. ANACOM)[128]. A função de "Assegurar a produção de referenciais normativos em matéria de cibersegurança" poderá colidir com as atribuições do, já referido, IPQ, pelo que é necessário estabelecer claramente as funções de cada um. Quanto às funções de CERT nacional atribuídas ao CNCseg, podem colidir com as funções do CERT.PT, que desempenhava o papel de CERT nacional *de facto*, contudo a saída do antigo diretor do CERT.PT para liderar a "mandatada" CERT nacional parece obviar o problema. É ideia partilhada pela comunidade nacional interessada nesta matéria, que o CERT.PT, como CERT nacional, era encarnada no seu ex--diretor[129]. Assim, esta transferência deverá retornar o CERT.PT às funções de CERT académica.

Outro aspeto positivo do CNCseg, além do facto do ex-diretor do CERT.PT liderar a CERT nacional, é o facto de metade do seu pessoal vir do setor privado (e ser civil), o que pode facilitar o estabelecimento de laços e confiança entre o CNCseg e esse setor e com a própria sociedade civil.

Durante a realização deste projeto verificou-se a existência de uma variável comum entre as iniciativas governamentais que considerámos mais relevantes - a proximidade entre os *policy entrepreneurs* e os decisores políticos, neste caso a PCM. Note-se que, tanto os principais *policy entrepreneurs* da ENSI, como do SCEE e do CNCseg têm em comum alguma proximidade com a PCM.

A ENSI foi promovida e iniciada pela UMIC (criada no seio da PCM) e esteve perto da implementação, antes do Governo ter sido dissolvido e o seguinte não a ter implementado.

O SCEE demorou muito pouco tempo desde o seu planeamento e a sua plena implementação (cerca de sete meses). O elemento que coordenou o grupo de trabalho responsável pelo planeamento e implementação do SCEE (o então sub-diretor do CEGER) foi nomeado pelo Secretário de Estado da PCM para essas funções, em sua representação.

[128] Estes mecanismos de coordenação e clara identificação e responsabilização dos atores por determinadas funções são fundamentais para uma efetiva execução dessas funções.

[129] O ex-diretor do CERT.PT procurou sempre acompanhar as boas práticas europeias nesta área, lutou por fazer do CERT.PT uma CERT nacional *de facto*, para colmatar as necessidades nacionais e criou uma rede nacional de CERTs, através do estabelecimento de laços de confiança com entidades de vários setores da sociedade.

Aquele que identificámos como o principal *policy entrepreneur* para a criação e implementação do CNCseg - o GNS -, faz parte da própria PCM.

Uma vez que a proximidade da PCM foi uma variável comum nestes casos, verifica-se que essa, juntamente com o acesso a determinados recursos e mobilização de vontades, parece ser a razão para algum avanço nesta matéria, pois o interesse e ação política nesta área têm sido poucos.

A realização desta investigação permitiu compreender que: passados, pelo menos, treze anos desde o início das preocupações, da parte da UE, com a criação de CERTs nacionais[130], só este ano é que Portugal criou uma entidade com um mandato do Governo para essa função; passaram-se onze anos desde a publicação da primeira estratégia de cibersegurança (dos Estados Unidos da América)[131] e seis desde a publicação da primeira Estratégia de Cibersegurança de um EM da UE (Estónia) e, atualmente já dezoito EM têm as suas estratégias publicadas, enquanto Portugal continua sem ter qualquer estratégia nesta área; a ANPC não tem atuado no âmbito do planeamento civil de emergência em situação de "cibercrise" (por falta de recursos), dedicando-se apenas ao desenvolvimento de planos de emergência para as infraestruturas críticas de energia e transportes; as autoridades competentes não dispõem de instrumentos de ação adequados para o desempenho das suas funções (ex. a legislação existente não permite a PJ fazer prevenção do cibercrime, através da monitorização da atividade *online*, nem permite que a CERT nacional monitorize o ciberespaço, como previsto no Decreto-Lei nº 69/2014 ou corte determinadas comunicações *online*, quando necessário); alguns princípios legais de Direito, como o princípio da proporcionalidade e o da igualdade, estão desadequados da "realidade virtual"[132], dificultando um melhor desempenho das autoridades competentes.

De acordo com os depoimentos recolhidos, à dissemelhança do pressuposto, segundo o ciclo das políticas públicas, os *policy-makers*, i.e., quem desenha as políticas públicas e os *decision-makers*, ou seja, os decisores políticos, em Portugal são os mesmos atores, porque as medidas políticas nesta matéria tendem a ser desenhadas e a sua implementação decidida, nos gabinetes dos respetivos ministros.

Esta prática poderá não ser a ideal pois, uma vez que, como os próprios defensores da teoria da escolha racional proclamam, quanto maior a quantidade e qualidade de informação à qual os decisores políticos têm acesso, melhores as suas decisões. Por outro lado, consultar a maioria dos atores intervenientes em determinada área de atuação política, incluindo o setor público, o setor privado, a sociedade civil e peritos[133], poderá trazer mais legitimidade, qualidade e coerência às decisões políticas

[130] Consultar COM(2001) 298 final (embora se tenha a informação que existem CERTs na Europa desde os anos 90). Consultar http://www.enisa.europa.eu/activities/cert/background/inv/certs-by-country-interactive-map (consultado a 20/9/2014).

[131] Consultar https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf (Consultado a 16/08/2014).

[132] Por um lado, segundo o princípio da proporcionalidade a legislação deve ser necessária, adequada e proporcional ao facto e ao ambiente, por outro lado, segundo o princípio da igualdade, o que é diferente deve ser tratado de forma diferente. Portanto, uma vez que o ciberespaço é um espaço diferente, onde a atribuição é muito difícil e os impactos das ações são imediatos, por exemplo, dever-se-ia adequar a legislação ao mesmo (segundo testemunho recolhido).

[133] Como vimos anteriormente, as próprias orientações da ENISA vão nesse sentido.

- desde que a participação de todos esses atores seja tida em consideração na tomada de decisão e não sirva apenas para transmitir à opinião pública a ideia de que as decisões políticas são o resultado do contributo de todos os atores envolvidos na fase de planeamento das políticas públicas.

Constatou-se também que as medidas políticas de cibersegurança tendem a ser desenhadas com pouca clareza e objetividade, com objetivos pouco mensuráveis, sem orçamentos, nem calendarizações definidas, sem uma clara definição dos atores envolvidos, das suas funções e formas de *accountability*[134], nem os termos das relações entre eles.

Uma vez que são os decisores políticos (ou elementos dos seus gabinetes) a desenhar as medidas políticas, parece que o modo de as desenhar, de forma algo abstrata, tem algum propósito - um propósito ao qual diversos autores designam por "blame-avoidance" (conceito explicado anteriormente).

Apesar de alguma pressão interna (da comunidade interessada), a maioria das medidas de políticas públicas implementadas em matéria de cibersegurança, têm sido fruto da pressão externa (ex. UE, OTAN, OCDE) e da transposição de diretivas e orientações da UE.

Aliás, houve, por duas vezes, propostas de medidas consideradas importantes, para a comunidade interveniente, que parecem não ter sido consideradas como tão importantes para os decisores políticos (a ENSI não chegou a ser implementada e o CNCseg demorou dois anos a ser aprovado)[135].

No decorrer desta investigação, surgiu a questão "Porque não temos uma política pública de cibersegurança em Portugal?", à qual pode ser atribuído um conjunto de razões possíveis, como: a pouca sensibilidade do Governo para a importância da cibersegurança, em conjugação com outras preocupações, principalmente na atual conjuntura económica; uma grande divergência de opiniões sobre este tema, possivelmente por ser relativamente novo; interesses e opiniões divergentes da parte de diversas entidades que pretendem tutelar esta área, possivelmente para daí tirar determinados proveitos, como um maior financiamento, por exemplo e não haver mecanismos de coordenação entre os papéis dessas entidades; o facto dos cidadãos estarem pouco sensibilizados para os efeitos da cibersegurança na soberania nacional e na segurança das instituições, organizações e dos próprios cidadãos, etc[136].

Em suma, podemos apontar três razões principais para a inexistência de uma política pública nacional de cibersegurança: a falta de governança desta área e descoordenação entre as entidades competentes; a existência de competências localizadas que, sem os adequados mecanismos de comunicação e coordenação, não conseguem atuar melhor; a ausência de política estratégica, i.e., a cibersegurança não é entendida como um factor estratégico para a segurança e prosperidade nacionais[137].

[134] As formas de *accountability* são essenciais nos sistemas de governação em múltiplos níveis, como é o caso português. Neste tipo de governação, se as responsabilidades e formas de *accountability* não estiverem previa e claramente definidas, pode haver quem não cumpra as suas funções, sem que seja, por isso, responsabilizado, resultando num desperdício de recursos públicos.
[135] Na página 42 são mencionadas possíveis explicações para a implementação do CNCseg em 2014.
[136] De acordo com os depoimentos recolhidos.
[137] Segundo testemunho recolhido.

Considerando os factos apresentados, julgamos que com algum esforço é possível virmos a ter uma política e um eficaz sistema nacional de cibersegurança em Portugal, se: se tiverem em conta e retirarem contributos das boas práticas disseminadas ao nível internacional, principalmente as orientações da ENISA; se chamar a contribuir o maior número possível de atores intervenientes nesta área e restantes atores que pretendam contribuir para a definição de uma política nacional nesta matéria.

Os ciberataques não implicam grandes recursos financeiros ou materiais, bastando um indivíduo com os adequados conhecimentos informáticos e um dispositivo ligado à internet, enquanto os efeitos desses ataques podem ser desastrosos, pelo que a garantia da cibersegurança deveria ser entendida como um fator estratégico e prioridade nacional. Portanto, facilitaria, se: se aproveitassem os laços de confiança existentes entre alguns atores nesta área; se atribuíssem os instrumentos necessários às entidades competentes (ex. atribuir às autoridades competentes, instrumentos legais para a monitorização do ciberespaço, atribuir instrumentos legais ao CNCseg para atuar rapidamente em caso de necessidade de corte de determinadas comunicações consideradas maliciosas ou inspecionar as instalações de determinadas infraestruturas críticas)[138]; se desenvolvesse o conhecimento sobre a interdependência e a segurança das infraestruturas críticas, que suportam o normal funcionamento da nossa sociedade; se clarificassem os papéis, as funções e as formas de responsabilização de todos os atores intervenientes na cibersegurança em Portugal, assim como os mecanismos de comunicação e coordenação entre eles[139]; se adjudicasse numa entidade a função de elaboração de estatísticas sobre este tema, essenciais para a aquisição de conhecimento sobre a realidade portuguesa e a partir daí se desenharem melhores medidas políticas na área da cibersegurança e de combate ao cibercrime, por exemplo[140]; se apostasse na I&D nesta área tão estratégica para o desenvolvimento económico e a soberania nacional (ex. através de um plano nacional de investigação neste domínio); se investisse na formação e na criação de uma cultura nacional de cibersegurança (através da formação e consciencialização dos portugueses, desde os jovens estudantes, até aos governantes)[141].

Para criar esta cultura nacional de cibersegurança, poder-se-ia criar uma plataforma virtual de discussão, onde os interessados pudessem contribuir para a definição de uma política pública de cibersegurança e realizar debates públicos nas principais cidades do país e mesmo na televisão, onde os

[138] Neste momento, o CNCseg não tem instrumentos legais para inspecionar as estruturas de rede dos ISPs nacionais, nem para cortar a ligação com determinado IP que considere maliciosa, por exemplo.
[139] A falta de adequados mecanismos de comunicação e de coordenação entre os vários intervenientes nesta área, bem como a falta de mecanismos de responsabilização desses atores, pode ter levado ao atual impasse numa política pública de cibersegurança em Portugal.
[140] Segundo o Relatório de Atividade, de 2013, do Gabinete Cibercrime, "Não existem estatísticas englobantes da cibercriminalidade em Portugal".
[141] O CNCseg terá uma equipa de formação e consciencialização, que deverá desenvolver planos e atividades de formação e consciencialização ao público em geral. Porém, considera-se importante que o trabalho desta equipa seja coordenado com outros projetos em desenvolvimento na mesma área, nomeadamente o Projeto Internet Segura ou o Projeto "Educar para uma Cidadania Digital" (consultar http://www.academiamilitar.pt/images/ficheirosPDF/8ein3painelbrigidamoucho_1.pdf - consultado a 12/07/2014).

espectadores pudessem questionar e opinar (sendo importante a consideração dessas opiniões e contributos para o desenho dessa política pública).

Poder-se-ia também criar um *think tank* nacional, juntando os elementos dos vários grupos desta área, como o GSSI, o GECENI e outros, bem como mais alguns peritos e pessoas que pudessem contribuir para a definição e atualização de uma política pública de cibersegurança em Portugal.

Outra iniciativa que poderia ajudar neste processo seria a organização da legislação relacionada com este assunto, uma vez que os documentos legais encontram-se muito dispersos, o que dificulta o trabalho de investigadores, *policy-makers* e todos os que procurem leis por temas.

Seria também benéfico que a discussão destes assuntos integrasse os vários partidos políticos com representação parlamentar, pois as políticas públicas previamente debatidas por todos os partidos (representantes dos cidadãos) ou pela sua maioria seriam, à partida, políticas do interesse da maioria dos cidadãos portugueses.

Algumas das dificuldades com as quais nos deparámos durante a realização deste estudo, foram: a dispersão da informação por diversos atores e fontes, dificultando a investigação, por um lado, porque poucos atores têm uma visão holística do processo nacional no âmbito da cibersegurança[142] e, por outro porque esses atores têm interesses diferentes, podendo interferir na imparcialidade dos seus testemunhos, o que, em conjunto, pode resultar em alguma falha na informação apresentada neste trabalho, que procurámos evitar; o facto de não estarem legalmente definidos, em Portugal, os conceitos de cibersegurança e ciberdefesa, dificultando a perceção do que é entendido em Portugal como cibersegurança e ciberdefesa e levando a alguma divergência entre os atores intervenientes nessas áreas[143]; a dificuldade em acompanhar os acontecimentos (já no final da realização deste estudo foi implementado o CNCseg, uma medida muito importante no que toca ao desenvolvimento da ação política em matéria de cibersegurança em Portugal).

Salientamos que a informação apresentada neste trabalho pode ter algumas lacunas, face ao exposto e ao facto da investigação de questões como a segurança pública e a defesa nacional, implicarem uma dificuldade acrescida, comparativamente a outras áreas da atuação política, pois muita da informação não está disponível ao público e é de difícil acesso, dada a sua natureza sensível.

Este trabalho constitui uma "gota de água" no "oceano" das políticas públicas e da cibersegurança (embora saibamos que todas são importantes). Portanto, para se perceber melhor as políticas públicas nesta matéria, seria muito importante e interessante a realização de um *benchmarking* às políticas

[142] Os entrevistados demonstraram ter uma visão parcial do que se tem passado em Portugal, demonstrando alguma falta de comunicação e partilha de informação entre eles, o que se traduz na morosidade do processo de criação de uma política pública integrada e de um sistema nacional de cibersegurança, tal como a duplicação de esforços por parte de algumas entidades, nomeadamente a realização de conferências sobre temas idênticos com datas próximas ou a criação de diversos grupos de trabalho em áreas relacionadas com a cibersegurança, a trabalhar sobre o mesmo assunto, etc.

[143] Repare-se que já existe em Portugal um Centro Nacional de Cibersegurança, o qual inclui uma autoridade nesta matéria, assim como foi publicada no *website* do GNS uma proposta de Estratégia Nacional de Cibersegurança. Contudo, não se encontra legalmente definido em lado algum (nem no documento de cria o CNCseg, nem na proposta de estratégia ou qualquer outro documento legal) o conceito de cibersegurança.

públicas de cibersegurança e ciberdefesa noutros EM da UE[144] e até fora da UE, com especial atenção para os que são considerados como modelos[145] e os mais semelhantes a Portugal, no que toca à cultura e preocupações nesta matéria, como Espanha, por exemplo, de forma a tentar retirar alguns contributos - baseados na análise dos processos das políticas públicas e da forma como foram resolvidos problemas semelhantes aos que enfrentamos em Portugal, como disputas entre diferentes atores, por exemplo - para melhorar o "sistema nacional de cibersegurança"[146].

Seria também interessante avaliar a evolução do desempenho do CNCseg, no que concerne à garantia dos adequados mecanismos de comunicação e consequente interoperabilidade dos atores envolvidos em Portugal, no momento (antes da entrada em plenas funções) e 6 ou 12 meses depois.

Neste estudo não foi apresentada muita informação sobre a ciberdefesa em Portugal porque essas capacidades estão ainda em desenvolvimento e porque se trata de informação delicada, de difícil acesso.

Espera-se que este trabalho desperte o interesse dos investigadores que se dedicam ao estudo das políticas públicas em Portugal, para que um dia possa haver mais investigação na área da segurança e defesa, nomeadamente contributos para o desenho de uma (eficiente e coerente) política pública de cibersegurança em Portugal.

A cibersegurança diz respeito a todos os portugueses e deveria ser dada abertura a quem pretenda estudar esta área da ação política, facilitando o acesso à informação necessária para a realização e o desenvolvimento de estudos íntegros, aceitando os contributos de investigadores de diversas áreas - sociologia, economia, políticas públicas, psicologia, engenharia, direito, etc - e incrementando o que tem sido feito neste campo. A abertura a estes investigadores poderia facilitar o desenvolvimento de mais e melhores políticas públicas neste domínio e alcançar mais elevados níveis de transparência, conduzindo ainda a processos decisórios mais democráticos, através do escrutínio da ação política neste campo.

[144] Nesse estudo poder-se-ia considerar a existência de diferenças nos sistemas políticos, institucionais, culturais, bem como ambientes políticos, económicos e sociais, entre os diferentes países, como variáveis explicativas para as diferenças nos processos políticos. Poderíamos considerar apenas os Estados-Membros da UE, porque estão sujeitos a pressões específicas para o desenvolvimento de determinadas capacidades de cibersegurança, nomeadamente através das orientações e diretivas dos órgãos da União.

[145] Nomeadamente os países considerados como modelos, pela ENISA (ex. Canadá, França, Alemanha, Holanda, o Reino Unido e os Estados Unidos da América). Consultar http://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR235/RAND_RR235.pdf - consultado a 20/04/2014.

[146] Propomo-nos a chamar sistema ou estrutura nacional de cibersegurança ao conjunto de atores, capacidades e legislação nacionais para garantir a cibersegurança em Portugal.

FONTES

Comunicações e outros documentos dos órgãos da União Europeia:

Comissão Europeia (2000), *eEurope 2002 - Uma sociedade da informação para todos*, Bruxelas.

Comissão Europeia (2002), *eEurope 2005 - Uma sociedade da informação para todos*, Bruxelas.

Comissão Europeia (2005), *i2010 - Uma sociedade da informação europeia para o crescimento e o* emprego, Bruxelas, *s.n*.

Comissão Europeia (2010), *EUROPA 2020 - Estratégia para um crescimento inteligente*, sustentável e inclusivo, Bruxelas, *s.n*.

COM (93) 700 final (Livro Branco sobre competitividade e emprego)

A4-0164/97 - COM(96) 592 final (Programa Comunitário Plurianual de Instauração da Sociedade da Informação na Europa)

COM(2001) 298 final (Proposta para uma política europeia de segurança da informação e das redes)

COM(2004) 116 final (Proposta de Regulação do Conselho, sobre os standards de segurança para os passaportes de cidadãos europeus)

COM(2006) 251 final (Uma estratégia para uma Sociedade da Informação Segura)

COM(2010) 245 final (Agenda Digital para a Europa)

COM(2010) 517 final (Proposta de diretiva sobre ataques a sistemas de informação)

COM(2010) 673 final (Uma estratégia europeia para a segurança interna em cinco passos)

COM(2011) 163 final (Comunicação sobre proteção de infraestruturas críticas de informação)

JOIN(2013) 1 final (Estratégia de Cibersegurança da União Europeia)

COM(2013) 48 final (Proposta de diretiva sobre a segurança das redes e da informação na União Europeia)

Convenção sobre Cibercrime, do Conselho da Europa, de 23 de novembro de 2001, Budapeste

Decisão-Quadro nº 2005/222/JAI, do Conselho, de 24 de fevereiro, relativa a ataques contra os sistemas de informação

Diretiva nº 2002/19/CE, relativa ao acesso e interligação de redes de comunicações eletrónicas e recursos conexos

Diretiva nº 2002/20/CE, relativa à autorização de redes e serviços de comunicações eletrónicas

Diretiva nº 2002/21/CE, relativa a um quadro regulamentar comum para as redes e serviços de comunicações eletrónicas

Diretiva nº 2002/22/CE, relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações eletrónicas

Diretiva do Conselho da Europa 2008/114/EC, de 8 de dezembro de 2008, relativa à identificação e designação das infra-estruturas críticas europeias e à avaliação da necessidade de melhorar a sua proteção

Diretiva nº 2009/136/CE, do Parlamento Europeu e do Conselho, de 25 de novembro, relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações electrónicas

Diretiva do Parlamento Europeu e do Conselho 2009/140/CE, de 25 de novembro de 2009, sobre redes e serviços de comunicações eletrónicas

Diretiva nº 2006/24/CE, do Parlamente Europeu e do Conselho, sobre a conservação de dados de comunicações eletrónicas

Regulamento nº 460/2004, do Parlamento Europeu e do Conselho (criação da ENISA)

R (89)9 do Conselho da Europa, sobre criminalidade informática

Estratégias de Cibersegurança:

ANSSI (2011), Information systems defence and security – France's strategy, Paris. Disponível em http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/France_Cyber_Security_Strategy.pdf

Cabinet Office (2009), Cyber Security Strategy of the United Kingdom – safety, security and resilience in cyber space, London. Disponível em https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228841/7642.pdf

Cabinet Office (2011), The UK Cyber Security Strategy – Protecting and promoting the UK in a digital world, London. Disponível em http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/UK_NCSS.pdf

Estonian Ministry of Defence (2008), *Cyber Security Strategy*, Tallinn. Disponível em http://www.kmin.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf

GNS (2012), Proposta de Estratégia Nacional de Cibersegurança, Lisboa. Disponível em http://www.gns.gov.pt/media/1247/PropostaEstrat%C3%A9giaNacionaldeCiberseguran%C3%A7aPortuguesa.pdf

Ministry of Justice (2011), The National Cyber Security Strategy (NCSS) – Strength through cooperation, The Hague. Disponível em https://english.nctv.nl/Images/cyber-security-strategy-uk_tcm92-379999.pdf

Ministry of Security and Justice (2013), National Cyber Security Strategy 2 – From awareness to capability, The Hague. Disponível em http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/NCSS2Engelseversie.pdf

Não identificado (2011), *Cybersecurity Strategy of the Czech Republic for the 2011-2015 period*, *s.l.* Disponível em http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/CzechRepublic_Cyber_Security_Strategy.pdf

Não identificado (2011), Cyber Security Strategy for Germany, s.l. Disponível em http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/Germancybersecuritystrategy20111.pdf

Não identificado (2011), Cyber Security Strategy, *s.l.* Disponível em http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/AGCyberSecurityStrategyforwebsite.pdf

Presidencia del Gobierno (2013), Estrategia de Ciberseguridad Nacional, Madrid. Disponível em http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/ES_NCSS.pdf

Secretariat of the Security and Defence Committee (2013), Finland's Cyber security Strategy, Helsinki. Disponível em http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/FinlandsCyberSecurityStrategy.pdf

The White House (2003), *The National Strategy to Secure Cyberspace*, Washington. Disponível em https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf

The White House (2011), International Strategy for Cyberspace – Prosperity, Security, and Opennes in a Networked World, Washington. Disponível em http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/international_strategy_for_cyberspace_US.pdf

Legislação nacional:

Conselho de Ministros (2006), Comunicado do Conselho de Ministros de 4 de maio de 2006. Disponível em https://www.oa.pt/Conteudos/Artigos/detalhe_artigo.aspx?idc=1365&idsc=31626&ida=45432

Constituição da República Portuguesa, Coimbra, Edições Almedina.

Decreto-Lei nº 279/84, de 13 de agosto (criação do CNPCE)

Decreto-Lei nº 429/89, de 15 de dezembro (criação do CEGER)

Decreto-Lei nº 184/98, de 6 de julho (alteração das atribuições do CEGER)

Decreto-Lei nº 290-D/99, de 2 de agosto (aprovação do regime jurídico dos documentos eletrónicos e da assinatura digital)

Decreto-Lei nº 146/2000, de 18 de julho (atribuição ao Instituto das Tecnologias de Informação na Justiça, do Ministério da Justiça, a competência de "autoridade credenciadora")

Decreto-Lei nº 234/2000, de 25 de setembro (criação do Conselho Técnico de Credenciação como estrutura de apoio ao Instituto das Tecnologias da Informação na Justiça no exercício das suas funções de autoridade credenciadora das entidades certificadoras de assinaturas digitais)

Decreto-Lei nº 128/2002, de 11 de maio (criação de uma Comissão para o ciberespaço, no CNPCE)

Decreto-Lei nº 16/2005, de 18 de janeiro (criação da UMIC – Agência para a Sociedade do Conhecimento I.P.)

Decreto-Lei nº 116-A/2006, de 16 de julho (criação do SCEE)

Decreto-Lei nº 116-B/2006, de 16 de julho (atribuição de funções ao CEGER, no âmbito do SCEE)

Decreto-Lei nº 116-C/2006, de 16 de julho (estabelece como serviço público o acesso universal e gratuito ao Diário da República)

Decreto-Lei nº 202/2006, de 27 de outubro (criação da Agência para a Modernização Administrativa, I.P.)

Decreto-Lei n.º 143-A/2008, de 25 de julho (regime jurídico que rege atualmente a disponibilização e a utilização das plataformas eletrónicas de contratação pública)

Decreto-Lei nº 42/2009, de 12 de fevereiro (estabelece as competências das unidades da PJ)

Decreto-Lei nº 309/2011, de 7 de dezembro (Estatutos da ANACOM)

Decreto-Lei nº 71/2012, de 21 de março (Lei orgânica do IPQ)

Decreto-Lei 73/2012, de 26 de março (alteração da Lei Orgânica da ANPC)

Decreto-Lei nº 73/2013, de 31 de maio (aprovação da Lei Orgânica da ANPC)

Decreto-Lei nº 69/2014, de 9 de maio (estabelece os termos de funcionamento do Centro Nacional de Cibersegurança)

Despacho do Procurador-Geral da República, de 7 de dezembro de 2011 (criação do Gabinete Cibercrime)

Despacho nº 13692/2013 do Ministro da Defesa Nacional (Orientação Política para a Ciberdefesa). Disponível em https://dre.pt/application/dir/pdf2sdip/2013/10/208000000/3197631979.pdf

Lei nº 10/91, de 29 de abril (Lei da Proteção de Dados Pessoais face à Informática)

Lei nº 109/91, de 17 de agosto (Lei da Criminalidade Informática)

Lei nº 144/99, de 31 de agosto (Lei da cooperação judiciária internacional em matéria penal)

Lei nº 104/2001, de 25 de agosto (alteração da Lei nº 144/99, de 31 de Agosto)

Lei nº 48/2003, de 22 de agosto (segunda alteração à Lei nº 144/99, de 31 de Agosto)

Lei nº 5/2004, de 10 de fevereiro, alterada pela Lei nº 51/2011, de 13 de setembro (Lei das Comunicações Eletrónicas)

Lei nº 43/2004, de 18 de agosto (criação da CNPD)

Lei nº 32/2008, de 17 de julho (regula a conservação e a transmissão dos dados de tráfego e de localização relativos a pessoas singulares e a pessoas colectivas)

Lei nº 37/2008, de 6 de agosto (Lei Orgânica da PJ)

Lei nº 49/2008, de 27 de agosto (Lei de Organização da Investigação Criminal)

Lei nº 53/2008, de 29 de agosto (Lei de Segurança Interna)

Lei nº 109/2009, de 15 de setembro (Lei do cibercrime)

Lei nº 83-C/2013, de 31 de dezembro (Orçamento de Estado 2014)

Portaria n.º 701-G/2008, de 29 de julho (define os requisitos e condições a que deve obedecer a utilização de plataformas electrónicas)

Portaria nº 23/2013, de 24 de janeiro, dos Ministérios das Finanças e da Economia e do Emprego (aprovação dos estatutos do IPQ)

Resolução do Conselho de Ministros nº 5/90, de 28 de fevereiro (SEGNAC 4 – normas para a segurança nacional, salvaguarda e defesa das matérias classificadas, segurança informática)

Resolução do Conselho de Ministros nº 16/96, de 7 de março (atribuição de competências sobre a área da Sociedade da Informação, ao Ministro da Ciência e Tecnologia)

Resolução do Conselho de Ministros nº 115/98, de 1 de setembro (criação da Iniciativa Nacional para o Comércio Electrónico)

Resolução do Conselho de Ministros nº 94/99, de 25 de agosto (aprovação do Documento Orientador da Iniciativa Nacional para o Comércio Eletrónico)

Resolução do Conselho de Ministros nº 77/2001, de 5 de julho (sobre o cartão do cidadão)

Resolução do Conselho de Ministros nº 135/2002, de 20 de novembro (criação da Unidade de Missão Inovação e Conhecimento UMIC)

Resolução do Conselho de Ministros nº 68/2003, de 7 de agosto (define o novo regime de publicação exclusivamente electrónica do Diário da Assembleia da República e novas regras para o uso de novas tecnologias de informação e comunicação no trabalho parlamentar)

Resolução do Conselho de Ministros nº 107/2003, de 12 de agosto (aprovação do Plano de Ação para a Sociedade da Informação)

Resolução do Conselho de Ministros nº 108/2003, de 12 de agosto (aprovação do Plano de Ação para o Governo Electrónico)

Resolução do Conselho de Ministros nº 92/2005, de 20 de maio (estabelece o regime da Unidade de Coordenação do Plano Tecnológico)

Resolução do Conselho de Ministros nº 171/2005, de 3 de novembro (aprovação da criação da Entidade de Certificação Eletrónica do Estado)

Resolução do Conselho de Ministros nº 39/2006, de 27 de abril (aprovação do Programa de Reestruturação da Administração Central do Estado (PRACE))

Resolução do Conselho de Ministros nº 109/2009, de 2 de outubro (criação da Rede Interministerial TIC)

Resolução do Conselho de Ministros nº 46/2011, de 14 de novembro (criação do GPTIC)

Resolução do Conselho de Ministros nº 12/2012, de 7 de fevereiro (Plano global estratégico de racionalização e redução de custos com as TIC na Administração Pública)

Resolução do Conselho de Ministros nº 42/2012, de 13 de abril (constituição da Comissão Instaladora do Centro Nacional de Cibersegurança)

Resolução do Conselho de Ministros n.º 19/2013, de 5 de abril (Conceito Estratégico de Defesa Nacional)

Programas dos Governos:

Conselho de Ministros (1991), Programa do XII Governo Constitucional, Lisboa, Presidência do Conselho de Ministros.

Conselho de Ministros (1995), Programa do XIII Governo Constitucional, Lisboa, Presidência do Conselho de Ministros.

Conselho de Ministros (1999), Programa do XIV Governo Constitucional, Lisboa, Presidência do Conselho de Ministros.

Conselho de Ministros (2002), Programa do XV Governo Constitucional, Lisboa, Presidência do Conselho de Ministros.

Conselho de Ministros (2004), Programa do XVI Governo Constitucional, Lisboa, Presidência do Conselho de Ministros.

Conselho de Ministros (2005), Programa do XVII Governo Constitucional, Lisboa, Presidência do Conselho de Ministros.

Conselho de Ministros (2009), Programa do XVIII Governo Constitucional, Lisboa, Presidência do Conselho de Ministros.

Conselho de Ministros (2011), Programa do XIX Governo Constitucional, Lisboa, Presidência do Conselho de Ministros.

Outra documentação:

AC/322-N(2014)0072, da OTAN (documento oficial classificado da OTAN)

CNEL (2005), Programa Nacional de Ação para o Crescimento e o Emprego 2005/2008, Lisboa, *s.n.*

Comissão Europeia (2012), *Special Eurobarometer 390 – Cyber Security*, *s.l*, *s.n.*

Comissão Europeia (2013), *Special Eurobarometer 404 – Cyber Security*, *s.l*, *s.n.*

Despacho n.º 11509-A/2014 (designação do responsável pela coordenação do Centro Nacional de Cibersegurança)

GCHQ, BIS and CPNI (2012), Ten Steps to Cyber Security, London, Crown Copyright.

Ministério da Ciência, Tecnologia e Ensino Superior (2005), *Ligar Portugal – Um programa de acção integrado no Plano Tecnológico do XVIII Governo: Mobilizar a Sociedade da Informação e do Conhecimento*, Lisboa.

OECD (1980), *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Disponível em http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

OECD (2002), Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security (revision). Disponível em http://www.oecd.org/sti/ieconomy/2002-security-guidelines-review.htm

OECD (2013), *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (2013)*. Disponível em http://www.oecd.org/sti/ieconomy/privacy.htm#newguidelines

Procuradoria-Geral da República (2013), Gabinete Cibercrime - Relatório de Atividade de 2013, Lisboa, *s.n.*

SISTEMA DE SEGURANÇA INTERNA (2013), Relatório Anual de Segurança Interna, Lisboa.

UMIC, *et al.* (2005), *ENSI - Política Nacional de Segurança da Informação*, Lisboa, *s.n.*

UMIC, *et al.* (2005a) *ENSI - Carta Nacional de Segurança da Informação*, Lisboa, *s.n.*

Unidade de Missão para a Sociedade da Informação em Portugal (1997), Livro Verde para a Sociedade da Informação em Portugal, Lisboa, *s.n.*

Unidade de Coordenação do Plano Tecnológico (2005), Plano Tecnológico, Lisboa, *s.n.*

BIBLIOGRAFIA

Almeida, Paulo (2008), "Políticas de Segurança: Visão de Futuro", em *Segurança & Defesa*, nº 8, Out-Dez, 2009, Lisboa, *s.n*. pp. 50-55.

Almeida, Paulo (2009), "OSCOT – Observatório: Qualificar a Segurança", em *Segurança & Defesa*, nº 9, Jan-Mar, 2009, Lisboa, *s.n*. pp. 50-51.

Anderson, J. (1975), *Public Policymaking*, New York, Praeger.

Berger, P. e Luckmann, T. (2004), *A Construção Social da Realidade: Um livro sobre sociologia do conhecimento*, Lisboa, Dinalivro.

Brewer, G. e Deleon, P. (1983), *The Foundations of Policy Analysis*, Monterey, Brooks, Cole.

Caldas, Alexandre (2010), "Uma Estratégia Nacional de Cibersegurança", em *Segurança & Defesa*, nº 16, Jan-Mar., 2011, Lisboa, *s.n*. *s.p*.

Casimiro, Sofia (2014), "Os aspetos legais da cibersegurança e ciberdefesa", em *Advocatus*. Disponível em: http://www.advocatus.pt/opini%C3%A3o/10711-os-aspetos-legais-da-ciberseguran%C3%A7a-e-ciberdefesa.html

Caupers, João (2002), *Introdução à Ciência da Administração Pública*, Lisboa, Âncora.

Claudino, Fátima (2007), "Inteligência Económica: Protecção dos Interesses Económicos Nacionais", comunicação apresentada no Simpósio *Globalização, Inovação e Segurança na Era da Informação*, Universidade da Madeira, 14 de junho de 2007, Funchal.

Cohen, M., March, J. e Olsen, J. (1972), "A Garbage Can Model of Organizational Choice", em *Administrative Science Quarterly*, Vol. 17, nº 1 (Mar.), pp. 1-25.

Comissão Europeia (2003), *Para uma Europa do Conhecimento - A União Europeia e a Sociedade da Informação*, Bruxelas, *s.n*. Disponível em http://ec.europa.eu/archives/publications/booklets/move/36/pt.pdf

Corfee-Morlot, Jan, *et al*. (2009), "Cities, Climate Change and Multilevel Governance", OECD Environmental Working Papers, n° 14, 2009, OECD publishing.

Dias, Manuel (2001), *Liberdade, Cidadania e Segurança*, Coimbra, Almedina.

Dye, Tomas (2010), *Understanding Public Policy*, Boston, Longman.

ENISA (2012), *National Cyber Security Strategies: Setting the course for national efforts to strengthen security in cyberspace*, Greece, ENISA.

ENISA (2012a), *National Cyber Security Strategies: Practical Guide on Development and Execution*, Greece, ENISA.

Fonseca, Francisco (2010), *A Evolução Das Políticas Públicas De Segurança Interna Em Portugal, Na Era Da Globalização*, Lisboa, Tese de Mestrado, Instituto Superior de Ciências Sociais e Políticas, Universidade Técnica de Lisboa.

Freire, F. e Caldas, A. (2013), "O Ciberespaço: Desafios à Segurança e à Estratégia", em Nunes, Isabel (coord.) (2013), *Segurança Internacional - Perspetivas Analíticas*, Lisboa, INCM e IDN.

Freire, F., Nunes, P., Davara, F. e Acosta, O. (2013), "Estratégia da Informação e Segurança no Ciberespaço", em *Cadernos IDN*, nº 12, Lisboa, INCM e IDN.

Friedrich, C. (1940), "Public Policy and the Nature of Administrative Responsibility", em Friedrich, C. e Manson, E. (eds.), *Public Policy*, Cambridge, Harvard University Press.

Garfinkel, Harold (1984 [1967]), *Studies in Ethnometodology*, Cambridge, Polity Press.

Giddens, Anthony (1984), *The constitution of society: Outline of the theory of structuration*, Cambridge, Polity Press.

Hall, P. e Taylor, R. (2003), "The three versions of neo-institutionalism", em *Lua Nova*, nº 58, São Paulo, *s.n*, pp. 193-223.

Hill, Michael (2009), *The Public Policy Process*, London, Pearson/Longman.

Inácio, Carina (2010), *Políticas Públicas de Segurança – novo paradigma*, Aveiro, Tese de Mestrado, Universidade de Aveiro.

Jann, W. e Wegrich, K. (2007), "Theories of the Policy Cycle", em *Handbook of Public Policy Analysis: Theory, Politics and Methods*, *s.l*, CRC Press, Taylor & Francis Group.

Jenkins, W., (1978), *Policy-Analysis. A Political and Organisational Perspective*, London, Martin Robertsen.

Kingdon, John (1995), *Agendas, Alternatives and Public Policies*, New York, Longman.

Lasswell, Harold (1956), *The Decision Process: Seven Categories of Functional Analysis*, College Park, University of Maryland Press.

Mansbridge, J. (ed.) (1990), *Beyond Self-Interest*, Chicago, University of Chicago Press.

Martins, Jorge (2011), *Políticas Públicas de Segurança em Portugal: Aplicação ao Caso da Imigração, 1992-2009*, Lisboa, Tese de Mestrado, Instituto Superior de Ciências Sociais e Políticas, Universidade Técnica de Lisboa.

May, J. e Wildavsky, A. (ed.) (1978), *The Policy Cycle*, Beverly Hills, Sage.

Não identificado (2011), *Cyber Power Index - Findings and Metodology*, *s.l*, Booz Allen Hamilton, Inc. Disponível em http://www.boozallen.com/content/dam/boozallen/media/file/Cyber_Power_Index_Findings_and_Methodology.pdf

OECD (2008), *Shaping Policies for the Future of the Internet Economy*, *s.l*, *s.n*.

OECD (2009), *Lobbyists, Governments and Public Trust: Increasing Transparency through Legislation*, vol. 1, *s.l*, OECD Publishing.

Oxford Dictionary, 2014. Disponível em http://www.oxforddictionaries.com/definition/english/phishing

Robinson, N. *et al.* (2003), *Cyber-security threat characterisation: A rapid comparative analysis*, Santa Monica, RAND Corporation. Disponível em http://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR235/RAND_RR235.pdf

Rodrigues, M. (coord.) (2014), *Exercícios de Análise de Políticas Públicas*, Lisboa, INCM e ISCTE-IUL.

Sagan, Scott D. (1996), "Why Do States Build Nuclear Weapons? Three Models in Search of a Bomb", em *International Security*, Vol. 21, nº 3 (Winter, 1996-1997), pp.54-86, Massachussets, The MIT Press.

Santos, Lino (2011), *Contributos para uma melhor governança da cibersegurança em Portugal*, Lisboa, Tese de Mestrado, Faculdade de Direito da Universidade Nova de Lisboa. Disponível em http://run.unl.pt/bitstream/10362/7341/1/Santos_2011.PDF

Schmidt, V. (2006), "Institutionalism", em Hay, C., Lister, M. e Marsh, D., *The State - Theories and Issues*, New York, Palgrave Macmillan.

Schmitter, Philippe (1974), "Still the Century of Corporatism?", em F.B. Pike and T. Stritch (eds.), *The New Corporatism*, Notre Dame, Notre Dame University Press, pp. 85-131.

Silvestre, Hugo Consciência (2009), *Gestão Pública - Modelos de Prestação no Serviço Público*, Lisboa, Escolar Editora.

Williams, Paul (ed.) (2013), *Security Studies – An introduction*, London, Routledge, Taylor & Francis Group.

Websites

APDSI: http://www.apdsi.pt/index.php/portugues/menu-secundario/sobre-nos/missao-visao-e-objectivos

http://www.apdsi.pt/uploads/news/id706/Conclus%C3%B5es%20F%C3%B3rum%20Arr%C3%A1bida%202013_4016-12_20131011.pdf

AP2SI: https://ap2si.org

CEGER:
http://www.ceger.gov.pt/
http://www.ceger.gov.pt/certificacao-eletronica.aspx

Centro Europeu de Cibersegurança: https://www.europol.europa.eu/ec/cybercrime-growing

CERT.PT:
http://cert.pt/index.php/rede-nacional-csirt/directorio
http://cert.pt/index.php/rede-nacional-csirt/objectivos
http://www.cert.pt/index.php/recomendacoes/1732-quem-e-quem-na-ciberseguranca-nacional-mes-europeu-da-ciber-seguranca-2013
http://cert.pt/images/docs/rfc2350_ptV2.2.3.txt
http://cert.pt/index.php/servicos/tratamento-de-incidentes

CNPD: http://www.cnpd.pt/bin/cnpd/acnpd.htm

ECEE: http://www.ecce.gov.pt/

EDA: http://www.eda.europa.eu/docs/default-source/eda-factsheets/2014-03-24-factsheet_cyber_defence_high-

eGovernment:
http://web.worldbank.org/WBSITE/EXTERNAL/TOPICS/EXTINFORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/EXTEGOVERNMENT/0,,contentMDK:20507153~menuPK:702592~pagePK:148956~piPK:216618~theSitePK:702586,00.html
http://europa.eu/rapid/press-release_IP-13-466_en.htm

ENISA
http://www.enisa.europa.eu/
http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world
http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-an-implementation-guide
http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/cyber-security-strategies-paper/at_download/fullReport
http://www.enisa.europa.eu/activities/cert/support/guide
http://www.enisa.europa.eu/activities/cert/support/exercise

http://www.enisa.europa.eu/activities/cert/background/inv/certs-by-country-interactive-map

https://www.enisa.europa.eu/activities/cert/support/guide/files/csirt-setting-up-guide

https://www.enisa.europa.eu/activities/cert/background/inv/files/inventory-of-cert-activities-in-europe

FCCN:

http://www.fccn.pt/pt/a-fccn/

https://www.fccn.pt/fotos/editor2/pdfmedidascontroloincidentes.pdf

FCT: http://www.fct.pt/fct

IDN:

http://www.idn.gov.pt/index.php

http://www.idn.gov.pt/index.php?mod=022&cod=12052014x1#sthash.R3ODEoFY.dpbs

IPQ: http://www1.ipq.pt/PT/IPQ/Pages/IPQ.aspx

*it*SMF: http://www.itsmf.pt/

ITU:

http://www.itu.int/pub/S-CONF-WCIT-2012/en /

http://www.itu.int/osg/wcit-12/highlights/signatories.html

http://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx

Linha Alerta: http://linhaalerta.internetsegura.pt/index.php

OCDE:

http://www.oecd.org/sti/ieconomy/informationsecurityandprivacy.htm

http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

http://www.oecd.org/internet/ieconomy/2002-security-guidelines-review.htm

http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf

Polícia Judicária:

http://www.policiajudiciaria.pt/PortalWeb/content?id={EBB2E68F-5A55-4141-B20D-88F35A0BD89B}

http://www.policiajudiciaria.pt/PortalWeb/content?id={BEC245A2-A9E2-478E-9982-6FD004DC3B3B}

http://www.policiajudiciaria.pt/PortalWeb/page/%7BF2B1FEAA-D25F-4654-9377-F4A1304DD2A6%7D

https://www.policiajudiciaria.pt/PortalWeb/page/%7BDD12D9E1-1D4A-472C-9518-167624C98F8E%7D

Plataforma Linha Alerta: https://linhaalerta.internetsegura.pt/index.php?option=com_content&view=article&id=61&Itemid=63&lang=pt

Programa Horizonte 2020: http://www.gppq.fct.pt/h2020/h2020.php

Programa Internet Segura: http://www.internetsegura.pt/noticias/milhares-de-novos-softwares-maliciosos-sao-detetados-todos-os-dias#.U5c2Z_mSyPZ

Programa Seguranet: http://www.seguranet.pt/blog/

Projeto "Educar para uma Cidadania Digital": http://www.academiamilitar.pt/images/ficheirosPDF/8ein3painelbrigidamoucho_1.pdf

SCEE:
http://www.scee.gov.pt/ecee/pt/
http://www.scee.gov.pt/ECEE/pt/autcred/

SIRP: http://www.sirp.pt/cms/view/id/90/

SIS: http://www.sis.pt/ciberameaca.html

TF-CSIRT: https://www.trusted-introducer.org/directory/country_certification_Z.html

TSF:
http://www.tsf.pt/paginainicial/interior.aspx?content_id=770177&page=1
http://www.tsf.pt/PaginaInicial/Portugal/Interior.aspx?content_id=2309984

UMIC:
http://www.umic.pt/index.php?option=com_content&task=view&id=2821&Itemid=335
http://www.umic.pt/index.php?option=com_content&task=category&sectionid=18&id=106&Itemid=190
http://www.umic.pt/images/stories/osic/SI_2010/SIP%202010_apresentao%20e%20sintese_2010.pdf
http://www.umic.pt/index.php?option=com_content&task=view&id=3034&Itemid=408

II Conferência de Hiperon - Cibersegurança em Portugal: Aonde nos encontramos? Disponível em http://conferenciashiperion.files.wordpress.com/2012/11/ciberseguranc3a7a-uma-visc3a3o-do-estado-universidade-lusc3b3fona-21nov2012.pdf

Notícias sobre cibercrime:
http://www.internetsegura.pt/noticias/milhares-de-novos-softwares-maliciosos-sao-detetados-todos-os-dias#.U52ARfmSyPb
http://www.tugaleaks.com/banco-de-portugal-bes-ataque-informatico.html

http://www.tugaleaks.com/hackers-atacam-aguas-de-portugal.html
http://www.tugaleaks.com/ataque-sites-bancos-anonymous.html
http://www.tugaleaks.com/nomes-telemoveis-procuradores-republica.html
http://www.tugaleaks.com/partidos-politicos-2014.html
http://www.tugaleaks.com/enderecos-emaic-camaras-municipais.html
http://www.efe.com/efe/noticias/portugal/portugal/hackers-atacam-site-procuradoria-lisboa/6/60016/2303044
http://www.ionline.pt/artigos/portugal/informacao-descarregada-hackers-site-da-pgdl-ainda-esta-online/pag/-1
http://www.noticiasaominuto.com/pais/207564/e-mail-de-general-pirateado-a-conta-de-esquema-de-burla-online
http://exameinformatica.sapo.pt/noticias/internet/2013-09-10-hackers-portugueses-atacaram-cia-nsa-fbi-e-departamento-de-estado-dos-eua
http://www.tugaleaks.com/ataque-informatico-europeias-2014.html
http://www.websegura.net/mais-2-sites-governamentais-hackados/
http://www.tugaleaks.com/torre-do-tombo.html
http://www.ionline.pt/artigos/portugal/hackers-atacam-pgina-da-procuradoria-distrital-lisboa
http://www.dinheirovivo.pt/Buzz/Artigo/CIECO341193.html
http://www.dn.pt/inicio/economia/interior.aspx?content_id=1888752
http://www.jn.pt/PaginaInicial/Interior.aspx?content_id=682803
http://techonlline.blogspot.pt/2014/04/hackers-divulgam-contatos-de.html
http://www.publico.pt/sociedade/noticia/contactos-pessoais-de-todos-os-procuradores-estao-na-net-e-piratas-informaticos-entraram-no-sistema-do-mp-1633938
http://www.publico.pt/sociedade/noticia/procuradoria-de-lisboa-desligou-site-para-colmatar-debilidades-do-sistema-atacado-1633719

Notícias sobre ciberespionagem:

http://portuguese.ruvr.ru/2012_11_08/Caca-chines-de-quinta-geracao-sera-resultado-de-ciberespionagem/
http://www.publico.pt/mundo/noticia/uniao-europeia-e-alvo-prioritario-da-espionagem-norteamericana-1602758
http://moraisvinna.blogspot.nl/2013/05/ciberespionagem-volta-confrontar-china.html
http://expresso.sapo.pt/eua-acusam-china-e-russia-de-ciberespionagem=f685470
http://www.rtp.pt/noticias/index.php?article=619426&tm=7&layout=121&visual=49~
http://codinomeinformante.blogspot.nl/2013/02/apesar-de-alerta-de-obama.html
http://www.publico.pt/mundo/noticia/alemanha-cancela-acordo-de-espionagem-com-eua-e-reino-unido-1602125

http://www.publico.pt/politica/noticia/hackers-chineses-atacaram-ministerio-dos-negocios-estrangeiros-de-portugal-1615718

http://www.computerworld.com.pt/2014/04/01/ciberespionagem-economica-fragiliza-portugal/

Notícias sobre a cibersegurança em Portugal:

http://www.tudomudou.com/2012/04/17/o-estado-da-ciber-seguranca-em-portugal/

http://www.asjp.pt/2013/12/02/militares-querem-fazer-ataques-pela-internet/

http://www.mynetpress.com/pdf/2013/dezembro/201312023524f6.pdf

http://www.computerworld.com.pt/2012/04/13/centro-nacional-de-ciberseguranca-definido-ate-julho/

http://www.computerworld.com.pt/2013/05/29/centro-nacional-de-ciberseguranca-continua-a-ser-para-breve/

http://tek.sapo.pt/noticias/telecomunicacoes/portugal_entre_os_paises_que_nao_subscreveram_1287775.html

http://www.dn.pt/politica/interior.aspx?content_id=4166630&page=1

http://www.computerworld.com.pt/2013/10/01/articular-quadros-legais-e-desafio-na-ciberseguranca/

http://www.publico.pt/ciencia/noticia/paulo-verissimo-portugal-ainda-nao-concretizou-a-sua-estrategia-de-ciberseguranca-1668772

http://www.cmjornal.xl.pt/detalhe/noticias/ultima-hora/governo-aprova-funcionamento-do-centro-nacional-de-ciberseguranca

http://www.computerworld.com.pt/2005/05/31/portugal-j-tem-estrutura-nacional-de-segurana-da-informao/

ANEXOS

Figura 1.1: Ação política em matéria de cibersegurança na União Europeia

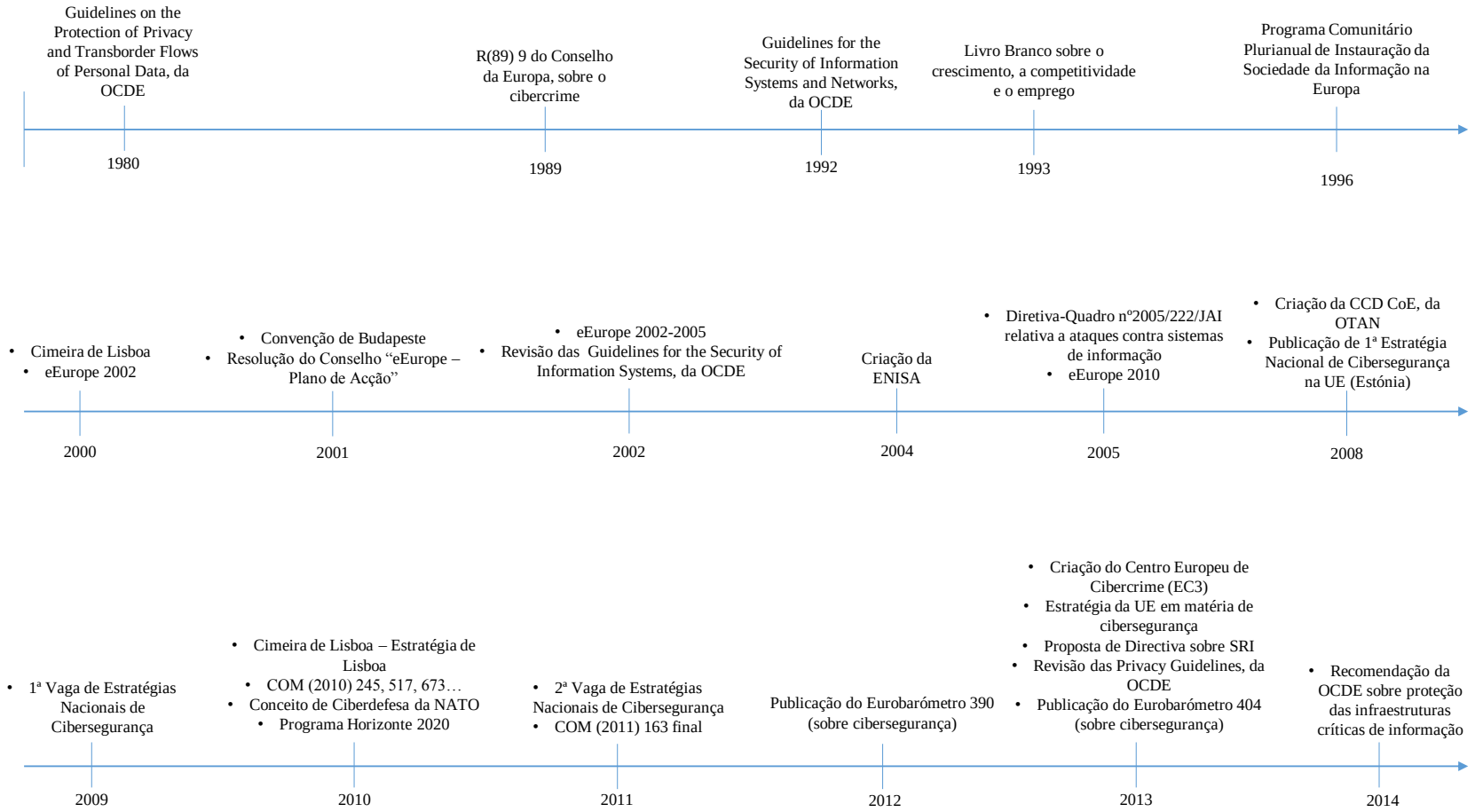


Figura 2: Estrutura Nacional de Segurança da Informação (ENSI)

Fonte: Carta de Segurança da Informação – ENSI, p. 13.