INSTITUTO SUPERIOR DE CIÊNCIAS POLICIAIS E SEGURANÇA INTERNA

Enquadramento concetual, estratégico e normativo da Segurança do Ciberespaço: subsídios para a definição de uma estratégia institucional da Polícia de Segurança Pública

Relatório Final do Curso de Comando e Direção Policial

Autor: Nuno Miguel Alves e Silva

Orientador: Rui Filipe Resende Coelho de Moura

Lisboa, 20 de junho de 2016

AUTOR

NUNO MIGUEL ALVES E SILVA

Comissário

Consultor no Centro Nacional de Cibersegurança

Presidência do Conselho de Ministros

Gabinete Nacional de Segurança

ORIENTADOR

MESTRE RUI FILIPE RESENDE COELHO DE MOURA

Intendente

Direção Nacional da Polícia de Segurança Pública

Diretor do Gabinete de Estudos e Planeamento

“Ser modesto no êxito, digno na adversidade e confiante face às dificuldades”

Código de honra dos alunos do Colégio Militar

AGRADECIMENTOS

O presente Relatório Final representa o culminar do Curso de Comando e Direção Policial ministrado pelo Instituto Superior de Ciências Policiais e Segurança Interna.

Gostaria de agradecer àqueles que, direta ou indiretamente, contribuíram para a realização do trabalho de investigação apresentado, em especial:

Ao Sr. Intendente Rui Filipe Resende Coelho de Moura pela confiança depositada ao ter acedido ao convite para orientar a realização do Relatório Final, pela sua manifesta dedicação e disponibilidade, assim como pela sua competente direção e exigência de método e rigor.

Ao Dr. José Carlos Martins, primeiro Coordenador do Centro Nacional de Cibersegurança, com quem tive o gosto, privilégio e honra de trabalhar diretamente e aprender durante dois anos, pelo seu contributo inestimável na elaboração do presente trabalho.

Aos restantes colaboradores do Centro Nacional de Cibersegurança pela disponibilidade manifestada e pela prestimosa colaboração, em diferentes níveis, na persecução dos objetivos do trabalho.

Aos representantes nacionais do *Grupo de Trabalho do Conselho da União Europeia para Assuntos Ciber*, meus congéneres, cujo apoio durante a fase de recolha bibliográfica permitiu arrecadar um manancial de informação que em muito contribuiu para a execução do Relatório Final.

RESUMO

A estruturação em rede das sociedades e a criação do ciberespaço, assumido hodiernamente como o quinto domínio de geoestratégia, constituem caraterísticas fundamentais da conjuntura estratégica hodierna, decisivamente condicionada pela disponibilidade e acessibilidade aos recursos de informação. O ciberespaço é por natureza um espaço aberto, desprovido de fronteiras tangíveis, onde o setor público e privado, atores nacionais e internacionais, interagem simultânea, interdependente e interligadamente, imergindo numa verdadeira plataforma de comunicação global que compreende bens, serviços, modelos de negócio, infraestruturas e dinâmicas sociais próprias. Assim, transpõe a vida real para um mundo virtual, sendo palco do desenvolvimento acelerado da sociedade da informação e da crescente dependência das tecnologias da informação e comunicação em funções vitais do funcionamento dos Estados. Tal, vem aumentar, de forma significativa, os riscos sociais e materiais decorrentes desta dependência e da quantidade e qualidade da informação armazenada e em circulação, expondo os Estados, as empresas e os cidadãos a práticas e ameaças de pendor criminal, belicista e subversiva. Com efeito, a sua natureza aduz características particulares à sua governação e regulação, que colocam em equação o entendimento de dois conceitos estruturantes e axiomáticos da ordem internacional e na conceção de Estado, a soberania e a segurança. Definimos como âmbito de estudo e campo geral de investigação, a segurança do ciberespaço, delimitando-o, por motivos de amplitude do trabalho, à compreensão e equação de uma estratégia institucional da PSP em matéria de Segurança do Ciberespaço, perspetivando o respetivo enquadramento estratégico, concetual e normativo nacional e internacional. Para alcançar as respostas pretendidas, recorremos ao método qualitativo, consubstanciado num estudo de caso do tipo de exploração e nas técnicas de recolha de dados, análise documental e entrevista do tipo semiestruturada, aplicada a uma amostra não-probabilística ou empírica de tipo intencional, sendo que adotámos a análise de conteúdo enquanto técnica de investigação.

Palavras-chave: Ciberespaço; Segurança do Ciberespaço; Ameaça; Cibercriminalidade; Capacidade de ciberdefesa.

ABSTRACT

The structuring of societies in a network and the creation of cyberspace, assumed nowadays as the fifth domain of geostrategy, are key characteristics of today's strategic context, decisively conditioned by the availability and the time of access to information resources. Cyberspace is by nature an open space, devoid of tangible boundaries, where sectors, both public and private, and actors, both national and international, interact in a simultaneous, interdependent and intertwined manner, immersing together in a truly global communicational platform including goods, services, business models, infrastructures and its own social dynamics. So, real life is transposed to a virtual world, setting stage to the accelerated development of the information society and to the increasing dependence on information and communication technologies in vital functions of States around the world. This increases significant risks, social, material, and concerning quantity and quality of information thus available, exposing States, businesses and citizens to practices and threats of criminal, warmongering and subversive bent. Indeed, this nature adds specific features to its governance and regulation, which place in equation the understanding of two concepts, structuring and axiomatic, in international order and in State conception, sovereignty and security. We establish as scope of study and general field of research, security in the field of cyberspace, delimiting it, for reasons of breadth of work, to understanding and equating an institutional strategy for PSP regarding Cyberspace Security, describing the corresponding strategic, conceptual and legal framework, national and international. To achieve the required answers, we use the qualitative method, embodied in an explorative case study and on data collection technique, semi-structured interview, applied to a non-probabilistic sample or of empirical intentional character, and we adopted content analysis as technique of research.

Keywords: Cyberspace; Cyberspace Security; Threat; Cyberspace Criminality; Cyberspace Defense Capability.

ÍNDICE

Índice de Apêndices

Índice de Figuras

Índice de tabelas

INTRODUÇÃO

A estruturação em rede das sociedades e a criação do ciberespaço, assumido hodiernamente como o quinto domínio de geoestratégia, constituem caraterísticas fundamentais da conjuntura estratégica dos séculos XX e XXI, decisivamente condicionada pela disponibilidade e acessibilidade aos recursos de informação.

Com efeito, o ciberespaço é por natureza um espaço aberto, desprovido de fronteiras tangíveis, onde setor público e privado, atores nacionais e internacionais, interagem simultânea, interdependente e interligadamente, porquanto inexoravelmente mais complexo e abrangente do que a internet em sentido estrito, imergindo numa verdadeira plataforma de comunicação global que compreende bens, serviços, modelos de negócio, infraestruturas e dinâmicas sociais próprias.

Assim, o ciberespaço transpõe a vida real para um mundo virtual, sendo palco do desenvolvimento acelerado da sociedade da informação e da crescente dependência das tecnologias da informação e comunicação (TIC) em funções vitais do funcionamento dos Estados.

Contudo, se as TIC trazem claros benefícios, sendo vulneráveis, aumentam significativamente os riscos sociais e materiais decorrentes da sua dependência e da quantidade e qualidade de informação armazenada e em circulação, expondo Estados, empresas e cidadãos a ameaças de pendor criminal, belicista e subversiva.

Assim, a segurança do ciberespaço é um conceito cada vez mais presente nas agendas dos mais variados atores e instituições ao nível político dos países da comunidade internacional. A necessidade de proteger as áreas que materializam a soberania nacional, assegurando a autonomia política, económica e estratégica dos países, em contraponto com o crescente número de incidentes e ataques maliciosos, impõe a segurança do ciberespaço como uma prioridade nacional, europeia e internacional.

O espectro de atribuições e competências no quadro da segurança do ciberespaço, afigura conveniente que, à atuação dos organismos e serviços setorialmente envolvidos na prossecução de relações internas e externas inerentes, seja

fomentada a cooperação e coordenação indispensáveis para garantir a unidade, coerência e a continuidade da ação do Estado de forma a potenciar o conhecimento e maturidades necessárias à proteção dos sistemas de informação nacionais, não olvidando a transversalidade que o conceito de segurança aporta a todos os domínios do ciberespaço, sendo igualmente condição *sine qua non*.

Definimos como âmbito de estudo e campo geral de investigação, a segurança do ciberespaço. Tratando-se de um tema abrangente, por motivos de amplitude do trabalho, procedemos à delimitação da nossa investigação à compreensão e equação da necessidade de uma estratégia institucional da Polícia de Segurança Pública (PSP) em matéria de Segurança do Ciberespaço, perspetivando o respetivo enquadramento concetual, estratégico e normativo nacional e internacional.

A rápida evolução intrínseca ao ciberespaço e, consequentemente, a crescente evolução das ameaças, dos processos e das infraestruturas, bem como dos modelos de segurança, económicos, sociais e culturais que assentam na sua utilização, leva-nos a formular a seguinte pergunta de partida (PP): A Polícia de Segurança Pública deve definir uma estratégia institucional de Segurança do Ciberespaço?

Sendo necessário delimitar as variáveis de investigação e enunciar os aspetos alvo de desenvolvimento durante a investigação, por forma a melhor responder à questão central, decorrem a seguintes perguntas derivadas (PD):

PD1: Como pode ser definido o quadro concetual da segurança do ciberespaço?

PD2: Qual a importância estratégica da segurança do ciberespaço?

PD3: O enquadramento legal nacional e internacional aplicável à segurança do ciberespaço é suficiente para a definição de uma estratégia institucional da Polícia de Segurança Pública?

PD4: O quadro de atuação e de cooperação da Polícia de Segurança Pública no domínio da segurança do ciberespaço impele à definição de uma estratégia institucional?

PD5: Deve ser equacionada a criação na estrutura da Polícia de Segurança Pública de um órgão autónomo, especifico e especializado em matérias de Segurança do Ciberespaço?

Tendo em consideração a pergunta de partida e derivadas, propomo-nos atingir o seguinte objetivo geral (OG):

OG. Equacionar a definição de uma estratégia da Polícia de Segurança Pública em matéria de segurança do ciberespaço, perspetivando o respetivo enquadramento estratégico, concetual e normativo.

Por forma a ser possível a cabal satisfação do objetivo geral é de todo importante precisar e restringir as linhas orientadoras da investigação. Assim sendo, estabelecem-se os seguintes objetivos específicos (OE):

OE1. Ancorar concetualmente a segurança do ciberespaço.

OE2. Compreender a importância estratégica da segurança do ciberespaço.

OE3. Analisar o enquadramento normativo da segurança do ciberespaço, nacional e internacionalmente.

OE4. Sistematizar o quadro de intervenção e de cooperação da Polícia de Segurança Pública no âmbito da segurança do ciberespaço.

OE5. Equacionar a criação na Polícia de Segurança Pública de um órgão autónomo, especifico e especializado em matérias de segurança do ciberespaço.

Na prossecução dos objetivos propostos e para alcançar as respostas às questões de investigação, recorremos ao método qualitativo, consubstanciado num estudo de caso do tipo de exploração e nas técnicas de recolha de dados, análise documental e entrevista do tipo semiestruturada, aplicada a uma amostra não-probabilística ou empírica de tipo intencional, sendo que adotámos a análise de conteúdo enquanto técnica de investigação. Para a revisão de literatura, baseamo-nos numa análise documental recorrendo a autores nacionais e internacionais, sem prejuízo do levantamento e sistematização do enquadramento legal e normativo essencial da segurança do ciberespaço.

Com efeito, o trabalho segue um procedimento de escrita e de organização em cinco capítulos, contemplando o procedimento metodológico e alinhando objetivos e questões de investigação, tendo presente que a finalidade de uma investigação impõe um desenvolvimento, iminentemente interpretativo e correlativo, sobre a revisão da literatura e sobre os dados obtidos e analisados em sede de estudo de caso.

Assim, no primeiro capítulo definimos a ancoragem concetual da investigação do tema, alicerçando-o na neutralidade epistemológica, sem prejuízo da complexidade de processos que são fenomenológicos, e na completude, unidade e coerência face ao ordenamento jurídico.

No segundo capítulo abordamos a caracterização estratégica da segurança do ciberespaço, perspetivando a regulação e governação do ciberespaço, num mundo crescentemente dependente, interligado e em rede; o domínio sobre a informação e consequentemente sobre o conhecimento; a sociedade em rede; a sociedade de risco; bem como a forma como o ciberespaço coloca em equação dois princípios axiomáticos da ordem internacional e nucleares do conceito de Estado: a soberania e a segurança.

No terceiro capítulo caraterizamos o enquadramento normativo da segurança do ciberespaço, apresentando, no âmbito do quadro comunitário, as principais organizações e normas e subsequentemente no quadro nacional, expomos os normativos jurídicos, atores e orientações estratégicas mais relevantes neste domínio.

No quarto capítulo sistematizamos o quadro de atuação e de cooperação da PSP no âmbito da segurança do ciberespaço, correlacionando as suas atribuições e competências com o escopo da Estratégia Nacional de Segurança do Ciberespaço, caracterizando ainda o seu ambiente e clientes, internos e externos, de forma a permitir um diagnóstico institucional atual que concorra para a compaginação das opções, dos objetivos e, consequentemente, da definição de estratégias de atuação.

No quinto capitulo apresentamos e discutimos os resultados obtidos no estudo exploratório, aprofundando igualmente as opções e procedimentos metodológicos como meio de direcionar a investigação para os seus objetivos e para o esclarecimento das perguntas de partida e derivadas.

O trabalho de investigação termina com a apresentação de conclusões, limitações do estudo e sugestões de investigações futuras.

CAPÍTULO I

ANCORAGEM CONCETUAL DA SEGURANÇA DO CIBERESPAÇO

O grau de complexidade subjacente à ideia de ciberespaço tem a sua raiz conceptual no prefixo ciber, que nos projeta numa dimensão imagética, indissociável da artificialidade do pensamento cibernético. Assim, o termo ciberespaço, pode ser pensado enquanto espaço disponível para estruturas que podem ser definidas a partir de redes dinâmicas de relações de gestão e de organização entre sistemas, que se servem da capacidade conectora do espaço para a sua atividade (McLuhan, 1962).

O conceito de cibernética, criado e popularizado por Norbert Wiener (1948) no seu livro *Cybernetics, or Control and Communication in the Animal and the Machine,* sustenta uma teoria de comando e comunicação aplicável tanto à máquina como ao homem. A cibernética pode então ser definida como a disciplina que estuda as regulações e a comunicação nos seres vivos e nas máquinas construídas pelos homens (Rosnay, 1995, p. 89), englobando as teorias que explicam os mecanismos de controlo de informação e da comunicação quer quanto aos organismos vivos, às máquinas ou às estruturas sociais, ou mais resumidamente, que se debruçam sobre os mecanismos de regulação dos sistemas, qualquer que seja a sua natureza (Benoit, Malarewicz, Beaujean, Colas & Kannas, 1988).

O conceito de ciberespaço[1] surgiu do ideário de William Gibson (1984), autor do livro de ficção científica *cyberpunk*[2] - *Neuromancer* (Neuromante), no qual esboça a ideia posteriormente apropriada pela comunidade científica internacional[3] como

[1] Espaço cibernético, espaço virtual, mundo virtual, esfera da informação e reino eletrónico são sinónimos comummente usados para ciberespaço.

[2] Cyberpunk é o termo que denomina uma corrente literária de ficção científica que caracteriza a cibercultura das décadas de 80 e 90, da qual fazem parte William Gibson, Bruce Sterling, John Shirley, Mark Dery, Michael Swanwick e Walter Jon William. Cyberpunk está também associado à identificação de um movimento essencialmente informático com posicionamento de contracultura fortemente sustentado.

[3] Esta estratégia tornou-se mais visível e conhecida nos Estados Unidos da América, concretizando-se através de projetos como a ARPA - Advanced Research and Projects Agency, (1957) da NASA - Nacional Aeronautics and Espace Administration (1958) ou da ARPANET (1969) e no envolvimento de algumas universidades - na UCLA - University of California, Los Angeles, SRI - Stanford Research Institute/Stanford University, UCSB - University of California Santa Barbara e a UTHA - University of Utha, - com o objetivo de organizar oceanos de dados, realizar o seu tratamento de forma a que a informação resultante permitisse reagir rapidamente em caso de ataque nuclear. Em 1990, o Departamento de Defesa dos Estados Unidos da América desmantelou a ARPANET a qual foi

potencial campo-espaço cibernético, no qual confluem os media digitalizados, libertando uma memória coletiva incomensurável de um rigor inatingível humanamente. Antevendo a crescente dependência da sociedade relativamente às TIC, que suportariam um universo virtual eletrónico, ficciona e define ciberespaço como uma representação física e multidimensional do universo abstrato da informação.

Assim, por um lado, de uma forma marcadamente material e arquitetural[4], o ciberespaço é caracterizado como um novo e paralelo universo ilimitado, sem restrições de tempo e lugar, criado e mantido por computadores e linhas de comunicação, consubstanciando-se numa realidade virtual que depende da eletricidade para a exploração de uma quantidade ilimitada de informação e de dados disponíveis que se caracterizam pela sua intemporalidade (Benedikt 1991:1-3). Concomitantemente, é um domínio global dentro do ambiente de informação, que consiste na rede interdependente de infraestruturas de tecnologia de informação, incluindo a internet, redes de telecomunicações, sistemas de computadores e os inerentes processadores e controladores (JP 1-02, 2010:83).

Por outro lado, o termo não só especifica a infraestrutura material da comunicação digital, como o universo das informações que ele abriga, assim como os seres humanos, que navegam e alimentam esse universo, sendo o espaço psicológico onde ocorre a comunicação mediada por computador, pelo que o neologismo cibercultura, entronca o conjunto de técnicas materiais e intelectuais, de práticas, de atitudes, de modos de pensamento e de valores que se desenvolvem juntamente com o crescimento do ciberespaço (Lévy, 2000).

Destarte, se entendermos o ciberespaço como o espaço ou território que integra as redes eletrónicas ou de comunicação que constituem a infraestrutura sobre a qual são criados, tratados, armazenados e distribuídos fluxos de informação, bem como os utilizadores que o exploram e suportam, então o conceito de segurança do ciberespaço ou de cibersegurança deve ser de igual modo entendido como todas

substituída pela rede da NSF, rebatizada NSFNET que se popularizou, em todo o mundo, com a denominação Internet. Para expansão da utilização da Internet foi decisiva a criação da www – World Wide Web – criada por dois engenheiros do CERN – Centre Européen pour la Recherche Nucléaire – Robert Caillaiu e Tim Berners-Lee.

[4] A organização fundamental do sistema, ligada às suas componentes, as relações destas entre si e com o ambiente, bem como os princípios que regem a sua conceção e evolução.

as dimensões de segurança que o afetam, direta ou indiretamente (Caldas, 2011, p. 94).

Refutando o nevoeiro terminológico que concorre na segurança do ciberespaço, por entendermos que põe em causa, não só, o Estado de Direito Democrático[5], a Segurança Interna[6] e a Defesa Nacional[7], mas também as premissas da estabilidade internacional[8], pela inevitabilidade globalizante da sua natureza, adotamos, rigorosamente, o conceito de segurança do ciberespaço plasmado na Estratégia da União Europeia para a Cibersegurança: *Um espaço aberto, seguro e protegido*, definindo-o como as "precauções e ações que podem ser utilizadas para proteger o ciberespaço, tanto nos domínios civil como militar, contra as ameaças decorrentes da interdependência das suas redes e infraestruturas informáticas, procurando manter a sua integridade, disponibilidade e a confidencialidade das informações nelas contidas, ou que as possam danificar." (p.3). A própria Estratégia Nacional de Segurança do Ciberespaço[9] edifica o conceito como "parte integrante da segurança nacional[10], referindo-o como essencial para o funcionamento do Estado, para o desenvolvimento económico e a inovação, bem como para a confiança dos cidadãos no mercado digital[11] e no ciberespaço".

[5] Encontra-se consagrado constitucionalmente no art.º 2 da CRP que a República Portuguesa é um Estado de direito democrático, baseado na soberania popular, no pluralismo de expressão e organização política democráticas, no respeito e na garantia de efetivação dos direitos e liberdades fundamentais e na separação e interdependência de poderes, visando a realização da democracia económica, social e cultural e o aprofundamento da democracia participativa.

[6] Nos termos do n.º 1, do art.º 272.º da CRP, a Segurança Interna é garantida pela Polícia, sendo que o art.º 1.º da Lei n.º 53/2008, de 29 de agosto, que aprova a Lei de Segurança Interna, define segurança interna como a atividade desenvolvida pelo Estado para garantir a ordem, a segurança e a tranquilidade públicas, proteger pessoas e bens, prevenir e reprimir a criminalidade e contribuir para assegurar o normal funcionamento das instituições democráticas, o regular exercício dos direitos, liberdades e garantias fundamentais dos cidadãos e o respeito pela legalidade democrática

[7] Conforme o n.º 2, do art.º 273.º da CRP, que refere que a defesa nacional tem por objetivos garantir, no respeito da ordem constitucional, das instituições democráticas e das convenções internacionais, a independência nacional, a integridade do território e a liberdade e a segurança das populações contra qualquer agressão ou ameaça externas. O n.º 1, do Art.º 275.º da CRP refere ainda que compete às Forças Armadas a defesa militar da República.

[8] Conforme art.ºº 7 e 8 da CRP.

[9] Consta do anexo à Resolução do Conselho de Ministros n.º 36/2015, de 28 de maio de 2015, e que dela faz parte integrante

[10] O conceito de Segurança Nacional integra, por conseguinte, "duas noções fundamentais: a de Segurança Interna e a de Segurança Externa ou Defesa Nacional, conceitos histórica e juridicamente autónomos na lei portuguesa, reconhecidos enquanto diferentes funções do Estado, aqui fundidos numa perspetiva de salvaguarda mais eficiente do Interesse Nacional.(…) Particularmente, porque é, atualmente, cada vez mais difícil gerir a separação entre Defesa Nacional e Segurança Interna, em concreto no que concerne à caracterização das ameaças". (Carvalho, Jorge Silva, 2006)

[11] O Mercado Único Digital tem por base o conceito de mercado comum, que visa "a supressão das barreiras comerciais entre os Estados-Membros com o objetivo de aumentar a prosperidade

Impõe-se, decorrentemente, uma clara definição do conceito de ameaça, podendo esta ser caracterizada como "qualquer acontecimento ou ação, de variada natureza, em curso ou previsível, que contraria a consecução de um objetivo e que, normalmente, é causador de danos, materiais ou morais, sendo o produto de uma possibilidade por uma intenção." (Couto, 1988a, p. 329). Outrora estático, previsível, homogéneo, rígido, hierarquizado e resistente à mudança, o quadro atual de ameaças à segurança do ciberespaço pode ser caracterizado por uma natureza dinâmica, difusa, intrincada, multidirecional, imprevisível, polimorfa, evolutiva e desterritorializada.

Concetualmente, as ameaças que impendem sobre a segurança do ciberespaço podem assumir a configuração de intervenção social - ciberativismo ou hacktivismo, a tipologia de ilícitos criminais - *hacking*, *cracking*, cibercrime ou ciberterrorismo, ou mesmo a forma de atos de guerra (ciberguerra ou guerra eletrónica) (Denning, 1999).

Concordando com Klimburg (2011, p. 41), entendemos que "cibercrime, ciberterrorismo e ciberguerra partilham uma base tecnológica comum, ferramentas, logística e instrumentos. As diferenças entre categorias de ciberatividades são frequentemente ténues ou estão apenas nos olhos de quem as vê". Assim, numa perspetiva substantiva, assumimos como uma etapa prévia e incontornável, a definição e consolidação doutrinária do conceito de segurança no ciberespaço, impondo-se agora a clarificação concetual de capacidade de ciberdefesa, de cibercriminalidade, de infraestrutura crítica e de prevenção da segurança do ciberespaço por enformarem a Segurança do Ciberespaço enquanto eixos de intervenção[12].

Cabe então, em termos pragmáticos, definir claramente a articulação da capacidade de ciberdefesa, evitando sobreposições e duplicações nocivas que ponham em causa fatalmente a agilidade dos processos e a governação do

económica e contribuir para uma união cada vez mais estreita entre os povos da Europa, passando a ter por base o conceito de mercado interno, definido como um espaço sem fronteiras internas no qual é assegurada a livre circulação de mercadorias, pessoas, serviços e capitais". Comunicação da Comissão "Estratégia para o Mercado Único Digital na Europa" (COM(2015)0192). Vide igualmente os documentos adicionais publicados em: http://europa.eu/rapid/press-release_IP-15-4919_pt.htm. Informações sobre as consultas públicas relevantes (abertas, previstas e encerradas) encontram-se em: https://ec.europa.eu/digital-agenda/en/consultations.

[12] Na definição dada pela Estratégia Nacional de Segurança do Ciberespaço.

ciberespaço. Com efeito, acautelando, liminarmente, o envolvimento de meios militares no ciberespaço à sua atividade subsetorial do esforço nacional de cibersegurança, aos objetivos da Defesa Nacional[13], à incumbência da defesa militar da República pelas Forças Armadas, bem como às condições do emprego das Forças Armadas quando se verifiquem situações de estado de sítio e de estado de emergência declarados pela forma prevista na CRP, regendo-se pelas normas constitucionais aplicáveis e pelo disposto na lei, acolhemos o conceito de capacidade de ciberdefesa da OTAN[14], como os "meios para alcançar e executar medidas defensivas para conter ciberataques e mitigar os seus efeitos e ainda preservar e restaurar a segurança dos sistemas de informação e comunicação e outros sistemas eletrónicos, ou a informação que é armazenada, processada ou transmitida nesses sistemas".[15]

Quanto à prática de crimes no ciberespaço, tal assume várias denominações[16], não existindo consenso quanto à expressão, definição, tipologia e classificação destes ilícitos criminais. Independentemente da sua designação, a criminalidade informática, cibercriminalidade ou cibercrime, é uma realidade incontornável, em permanente mutação e num processo evolutivo constante que consiste em "todo o ato em que o computador serve de meio para atingir um objetivo criminoso ou em que o computador é o alvo desse ato ou em que o computador é objeto do crime" (Marques, Garcia & Martins, Lourenço, 2000). Contudo, o crime informático pode também categorizar-se diferentemente, inserindo-se os crimes onde o bem jurídico protegido é a informática no conceito de criminalidade-digital em sentido próprio (Rodrigues, 2009). Assim, considerando que o conceito não encontra definição legal no ordenamento jurídico português, recorremos novamente à definição patente na Estratégia da União Europeia para a Cibersegurança, que a refere,

[13] Considerando o disposto na CRP, na Lei Orgânica n.º 1-B/2009 de 7 de Julho, que aprova a Lei de Defesa Nacional, na Lei n.º 44/86 de 30 Setembro, que aprova o Regime Estado de Sítio e de Emergência, parece-nos que a mera aposição do prefixo ciber não permite que se possa extravasar os limites constitucionalmente consagrados no âmbito da defesa nacional relativamente à atuação das Forças Armadas.

[14] No que concerne à ciberguerra, o documento de terminologia conjunta dos Estados Unidos para as operações cibernéticas define-a como "um conflito armado conduzido somente ou em parte, por meios cibernéticos. As operações militares conduzidas para negar à força opositora a utilização eficaz dos sistemas de ciberespaço e de armas no conflito. Inclui ataques cibernéticos, ações de defesa e facilitação de cibernética" (*U.S. Department of Defense, Joint Chiefs of Staff, 2011*).

[15] AC/322-N(2014)0072, da OTAN, Enclosure 1, documento oficial classificado da OTAN.

[16] Designadamente, crime digital, crime informático, crime informático-digital, *high technology crimes*, *computer related crime*.

geralmente, a um "amplo leque de diferentes atividades criminosas que envolvem os computadores e os sistemas informáticos, quer como instrumentos quer como alvos principais, incluindo as infrações tradicionais, as infrações relativas aos conteúdos e crimes respeitantes exclusivamente a computadores e sistemas informáticos." (p. 3).

Concebemos, ainda, o conceito de Infraestrutura crítica[17] como "a componente, sistema ou parte deste situado em território nacional que é essencial para a manutenção de funções vitais para a sociedade, a saúde, a segurança e o bem-estar económico ou social, e cuja perturbação ou destruição teria um impacto significativo, dada a impossibilidade de continuar a assegurar essas funções".[18]

Definimos, por fim, o conceito de prevenção da segurança do ciberespaço enquanto a(s) atividade(s) que contribui(em) para a sua concretização e fazer cessar ou reduzir a conflitualidade decorrente do respetivo fenómeno social, tanto quantitativa como qualitativamente, quer através de medidas de cooperação permanente e estruturada, quer através de iniciativas informais, envolvendo os agentes suscetíveis de desempenhar um papel preventivo.[19]

[17] A Diretiva 2008/114/CE identificou o setor das TIC como um setor prioritário no futuro, embora não tenha sido classificado de per si como uma infraestrutura crítica. Não obstante, desde 2005, a Comissão Europeia tem realçado a necessidade de coordenar esforços no sentido de criar confiança nas telecomunicações eletrónicas(1). Para esse efeito, foi adotada uma estratégia para uma sociedade da informação segura, em 2006, cujos elementos principais foram aprovados na Resolução 2007/068/01 do Conselho da União Europeia.

[18] A proteção de infraestruturas críticas ganhou sustento legal em Portugal aquando da publicação do Decreto-Lei 62/2011, de 09 de maio, o qual transpôs para o quadro jurídico nacional a Diretiva 2008/114/CE. O diploma legal define procedimentos relativos à identificação e designação de infraestruturas críticas europeias, estabelece a obrigatoriedade de elaboração de planos de segurança por parte dos operadores e determina a existência de planos de segurança externos, da responsabilidade das forças de segurança e da proteção civil. Embora vocacionado para as infraestruturas críticas europeias dos sectores do transporte e da energia, o Decreto-Lei 62/2011 prevê igualmente a aplicação dos mesmos procedimentos às infraestruturas críticas nacionais, com exceção das fases correspondentes à componente transfronteiriça.

[19] A atividade de prevenção da cibersegurança poderá conceptualmente ser estruturada em três dimensões, a saber: primária, secundária e terciária. As mesmas situam-se, respetivamente, ao nível (i) das Causas (Comunidade, Família, Escola e Trabalho); (ii) dos Autores (forças e serviços de segurança, autoridades e estruturas judiciárias e entidades reguladoras) e (ii) dos alvos (objetos, espaços e situações).

CAPÍTULO II

CARACTERIZAÇÃO ESTRATÉGICA DA SEGURANÇA DO CIBERESPAÇO

Wegener (1929) teorizou que os cinco continentes que hodiernamente conhecemos estiveram inicialmente unidos num único que designou de Pangea[20]. O movimento de deriva continental, primeiro por partição e depois por separação, provocou, inevitável e forçosamente, um maior afastamento entre as espécies, acentuando e impelindo distâncias oceânicas. Hoje, cerca de trezentos milhões de anos depois, surgem e ampliam-se fenómenos que parecem contrariar o afastamento tectónico e a atual geografia, sendo o ciberespaço o seu palco primordial e o seu universo paradigmático e pandectista.

Esta contradição adensa-se com Schäfer (2003, p.76-82), que aborda a história contemporânea através de uma noção verdadeiramente globalizante. Distinguindo a história geofísica não-linear, que alternadamente vai unindo e dividindo o mundo-continente denominado de Pangeia Um, e a história tecnocientífica revolucionária da Pangeia Dois, onde sugere que a confluência de interesses e capacidades, como a rápida comunicação, ramificação de redes de comunicação e transporte que surgem com base na tecnociência, estão a criar uma unidade civilizacional.

O ciberespaço reequaciona indelevelmente as noções de espaço, tempo, individual e coletivo, remetendo-nos para o arquétipo de Aldeia Global proposta por Mcluhan (1962), que teorizou como os meios de comunicação em massa permitiriam a abolição de fronteiras, reduzindo distâncias e garantindo um processo de comunicação mais rápido e de escala planetária, emergindo um processo de retribalização da sociedade e uma uniformização sociocultural que nega o isolamento e o individualismo, unindo a humanidade.

Decorre então que ação, espaço e tempo são as dimensões que as TIC visam suplantar (Parenty, 2003).

Ao significado que a terra detinha na Era Agrícola - Primeira Vaga - ou o carvão e o petróleo na Era Industrial - Segunda Vaga - a Era da Informação – Terceira Vaga

[20] Etimologicamente o conceito deriva do grego Pan — toda + Gea — Terra

- consubstancia-se no domínio sobre a informação, encarada enquanto matéria-prima e fator de produção e consequentemente sobre o conhecimento (Toffler, 2003).

Castells (2011) refere que "uma revolução tecnológica, centrada nas tecnologias de informação, começou a remodelar, de forma acelerada, a base material da sociedade" (p. 1), sendo que "no novo modo informacional desenvolvimento, a fonte de produtividade encontra-se na tecnologia de produção de conhecimentos, de processamento de informação e de comunicação de símbolos" (p. 20).

Consequentemente, surgiu, no fim dos anos sessenta e meados da década de setenta, a sociedade em rede, cujo motor de desenvolvimento assentou na internet, que tem origem na coincidência histórica de três processos independentes: a "revolução da tecnologia da informação, a crise económica do capitalismo e do estatismo e a consequente reestruturação de ambos. A interação entre esses processos e as reações desencadeadas fizeram surgir uma nova estrutura social dominante, a sociedade em rede; uma nova economia, a economia informacional/global; e uma nova cultura, a cultura da virtualidade real." (Castells, 1999, p. 411).

Atinente a uma profunda reflexão sociológica sobre o atual período da humanidade, a sociedade de risco, Ulrich Beck e Anthony Giddens rotulam o período contemporâneo de modernização reflexiva ou segunda modernidade, em que o desenvolvimento da ciência e da tecnologia já não permitem prever e controlar efetivamente os riscos[21] que contribuíram para criar.

Num contexto de pós-Guerra Fria e de globalização em marcha, desvanecido o mundo bipolar, "passámos de um mundo de inimigos a um mundo de perigos e de riscos, sendo que o conceito de risco e de sociedade de risco combina o que em tempos se excluía mutuamente: sociedade e natureza, ciências sociais e ciências

[21] "Risco é o enfoque moderno da previsão e controlo das consequências futuras da ação humana, das diversas consequências não desejadas da modernidade radicalizada. É uma tentativa (institucionalizada) de colonizar o futuro, um mapa cognitivo. Toda a sociedade, obviamente, experimentou perigos. Todavia, o regime do risco é uma função de ordem nova: não é nacional, mas global. Está intimamente relacionado com o processo administrativo e de decisão. Anteriormente, essas decisões eram tomadas com normas fixas de calculabilidade, ligando meios e fins, causas e efeitos. A "sociedade de risco global invalidou precisamente essas normas." (Beck, 2002, p. 5)

da matéria, construção discursiva do risco e materialidade das ameaças" (Beck, 2002, p. 5).

Com efeito, o *ethos* da Era digital, densificado por uma utopia libertária ou até de anarquia do ciberespaço[22], está a dar lugar, a nível internacional, a crescentes mecanismos de afirmação da soberania estadual e de mecanismos de controlo do ciberespaço marcados por interesses económicos-comerciais e por um crescente uso profissional feito por múltiplos organismos públicos e privados.

Chris Demchak e Peter Dombrowski (2011), antecipam uma nova era de afirmação vestefaliana, de declaração do poder dos Estados sobre o ciberespaço, em nome da segurança e da sustentabilidade económica, argumentando que "uma ciberfronteira nacional é tecnologicamente possível, psicologicamente confortável, sendo também sistemática e politicamente gerível".

Assim, o ciberespaço alterou o entendimento de dois conceitos estruturantes da ordem internacional: a soberania e a segurança. Em alguns Estados[23], materializou-se num território não só de afirmação de soberania estadual, como de controlo securitário e das atividades dos cidadãos, sendo que o ciberespaço, entendido como espaço de liberdade, não é uma inevitabilidade tecnológica mas, fundamentalmente, uma opção política de outros Estados.

De facto, soberania e segurança são nucleares no conceito de Estado e, concomitantemente, princípios axiomáticos onde se baseia o direito internacional. Numa perspetiva jusinternacional, cabe destacar que é com base, precisamente, no princípio da soberania territorial que se admite que um Estado possa regular, para o seu território, as suas próprias atividades da internet ou aquelas que os estrangeiros possam desenvolver nos seus países, mas que tenham efeitos no seu território. Em alternativa, a governação e regulação focam-se na elaboração de um conjunto de *cyber-confidence measures*[24], baseadas na proteção da confiança de

[22] Visto como lugar de realização do ideal libertário-anárquico, o ciberespaço, encarado enquanto espaço social global, tem em *A Declaration of the Independence of Cyberspace* (1996) uma proclamação contracultural em que não cabe aos Estados o direito moral de governar, regular ou legislar. (Barlow, 1996)
[23] Note-se o caso da *Great Firewall of China*.
[24] Confidence Building Measures for Cyberspace – Legal Implications (2013), CCDCOE – NATO Cooperative Cyber Defence Centre of Excelence, Tallinn; p. 90.

que os Estados irão agir e adotar normas num determinado sentido (Castro, Raquel, 2016, p. 211).

A necessidade de proteger as áreas que materializam a soberania nacional, assegurando a autonomia política e estratégica dos países, bem como o crescente número de incidentes[25] e ataques maliciosos no ciberespaço, impõe então a segurança do ciberespaço como prioridade estratégica de qualquer país.

Para além disso, a própria difusão da internet e a digitalização da economia geram riscos e vulnerabilidades, de que se destacam a possibilidade de ciberataques a organismos públicos ou empresas privadas ou até de ciberguerra, envolvendo, direta ou indiretamente, atores estaduais, casos indeléveis da Estónia em 2007, Lituânia em 2007, Geórgia em 2008, Quirguistão em 2009 ou mais recentemente na Ucrânia.

De facto, o ciberespaço aduz uma série de características particulares que é necessário ponderar cuidadosamente, de forma a podermos identificar a sua relevância no âmbito da segurança. Com efeito, apresenta uma frequência de mudança e mutação extremamente elevadas em razão dos diferentes sistemas que o sustentam e das suas interligações, bem como das suas vulnerabilidades e riscos emergentes. O seu custo irrelevante de acesso e o seu enorme potencial de crescimento, introduziram profundas alterações na forma como os cidadãos, as organizações e os Estados se relacionam entre si, sendo que dados da Internet World Stats[26] apontam um mundo crescentemente dependente, interligado e em rede. Assim, numa população mundial estimada de cerca 7 mil milhões de pessoas, o número de utilizadores da internet acerca os 4 mil milhões de utilizadores ativos em todo o mundo, destes 48.2% na Ásia, 18% na Europa, 10.2% na América Latina e Caraíbas, 9.8% na África, 9.3% na América do Norte, 3.7% no Médio Oriente e 0.8% na Oceânia. Mais, tendo aumentado 832.5% no período de 2000 a 2015, a taxa atual de penetração da internet a nível global é de 46.4%, na Europa de 73.5% e em Portugal[27] de 67.6%. É também marcado por uma alta capacidade de

[25] Adotamos a taxonomia do Centro Nacional de Cibersegurança para classificar observáveis de eventos de segurança e da Rede Nacional CSIRTS para classificação de incidentes de segurança. Vide: http://www.cncs.gov.pt/media/2015/06/Taxonomia_pt.pdf.
[26] Conforme sítio da Internet World Stats, em http://www.internetworldstats.com/stats.htm [acedido em 28/05/2016], cujos dados são referentes a Novembro de 2015.
[27] Dados que apontam uma população portuguesa de 10,374,822 pessoas, sendo 7,015,519 destas utilizadoras de internet.

processamento, alicerçado numa elevada procura e de armazenamento de informação. O seu caráter assimétrico consubstancia que conhecimentos rudimentares e capacidades relativamente mínimas, aliadas a intenções subversivas, criminais ou belicistas, podem produzir ações hostis de grande impacto e em diversos domínios da sociedade, nomeadamente na área política, económica, social ou mesmo na segurança e defesa dos Estados. Por fim, o anonimato que caracteriza os ciberataques dificulta a determinação da sua origem, a capacidade de dissuasão e resposta, bem como a sua prevenção e investigação em sede criminal e ulterior prossecução penal.

O conceito de segurança assume então, atualmente, novos contornos, tratando-se de um conceito passível de ser alterado com a evolução da sociedade, pois "a força gravitacional do espaço e do tempo impõe ajustes inerentes à volatilidade dos fatores políticos, económicos e jurídicos conjugados com o contexto social e cultural" (Valente, 2013, p. 115).

Se antes a segurança era entendida como uma competência exclusiva do Estado, hoje em dia assistimos cada vez mais à sua privatização. Para além de haver um número crescente de instituições a oferecer serviços de segurança, temos também de considerar que muitas das infraestruturas críticas dependem do setor privado, logo não podem demitir-se de assumir um papel ativo na demanda da segurança do ciberespaço (Bendiek, 2012).

Note-se, porém, que a concretização da segurança do ciberespaço não se esgota na aplicação de tecnologia. O seu sucesso passa decisivamente pela promoção de uma cultura de segurança que proporcione a todos o conhecimento, a consciência e a confiança necessários para a utilização dos sistemas de informação, reduzindo a exposição aos riscos do ciberespaço.

É, então, indispensável informar, sensibilizar e consciencializar não só as entidades públicas e as infraestruturas críticas, mas também as empresas e a sociedade civil. Concomitantemente, afigura-se fundamental que qualquer país se dote de recursos humanos qualificados e com competências digitais para lidar com os complexos desafios da segurança do ciberespaço.

É igualmente consensual que a garantia da segurança das infraestruturas tecnológicas, das redes e dos sistemas de informação depende da capacidade de

os utilizadores finais saberem tomar medidas que previnam os riscos a que se encontram expostos, atento o vulgar, gradativo e inexorável predomínio da tecnologia digital, relevando-se então, estrategicamente, a educação, sensibilização e prevenção da Segurança do Ciberespaço e uma cultura global de cibersegurança.

CAPÍTULO III

ENQUADRAMENTO NORMATIVO DA SEGURANÇA DO CIBERESPAÇO

3.1 ENQUADRAMENTO DA UNIÃO EUROPEIA

A Comissão Europeia, em colaboração com a Alta Representante da União para os Negócios Estrangeiros e a Política de Segurança, publicou a 7 de fevereiro de 2013, a Estratégia da UE para a Cibersegurança: *Um ciberespaço aberto, seguro e protegido*, define o conceito de segurança do ciberespaço ou cibersegurança como as precauções e ações que podem ser utilizadas para proteger o ciberespaço, tanto nos domínios civil como militar, contra as ameaças decorrentes da interdependência das suas redes e infraestruturas informáticas, procurando manter a sua integridade e disponibilidade e a confidencialidade das informações nelas contidas, ou que as possam danificar. A estratégia pretende (i) reforçar a resiliência e segurança das redes e da informação; (ii) reduzir drasticamente a cibercriminalidade; (iii) desenvolver uma política de ciberdefesa da UE; (iv) desenvolver a política e as capacidades no domínio da ciberdefesa no quadro da política comum de segurança e defesa; (v) promover a investigação e o desenvolvimento; e (vi) reforçar a política internacional da UE em matéria de ciberespaço. Substantivamente, os objetivos da estratégia reforçam-se mutuamente, sendo que o desiderato de resiliência da rede e da segurança das redes e da informação prevê ações que visam reforçar a cooperação e o intercâmbio de informações entre atores relevantes, as parcerias público-privadas e a constituição de equipas nacionais de resposta a emergências informáticas.

Estes objetivos foram densificados ainda numa Proposta de Diretiva, COM (2013) 48 Final, relativa a garantir um elevado nível comum de segurança das redes e da informação, que acompanha a estratégia. O Conselho da União Europeia adotou-a formalmente em maio de 2016, cuja entrada em vigor espera-se para agosto de 2016, após aprovação pelo Parlamento Europeu. O objetivo principal da proposta consiste em garantir o funcionamento correto do mercado interno. Tal implica melhorar a segurança da Internet e das redes e sistemas informáticos privados em que assenta o funcionamento das nossas sociedades e economias. Este propósito

será alcançado exigindo aos Estados Membros que aumentem o seu nível de preparação e melhorem a cooperação entre si e exigindo aos operadores das infraestruturas críticas, bem como às administrações públicas, que adotem medidas adequadas para gerir os riscos de segurança e comunicar os incidentes graves às autoridades nacionais competentes.

As iniciativas da UE no âmbito da Cibersegurança têm-se vindo a focar essencialmente na harmonização da legislação de combate ao cibercrime e na introdução de instrumentos orientados para o desenvolvimento de políticas de proteção das infraestruturas críticas de informação. A "Agenda Digital", o "Programa de Estocolmo" e a "Estratégia de Segurança Europeia", reafirmam a preocupação da UE com este assunto, sublinhando-se o facto de, nas áreas da cibersegurança e, consequentemente, no esforço contra o cibercrime, a segurança interna e externa dos Estados se encontrar interligada de forma indissociável.

O instrumento internacional de maior relevo na área do cibercrime é a Convenção sobre o Cibercrime do Conselho da Europa de 23 de Novembro de 2001, vulgo Convenção de Budapeste, destinada a proteger a sociedade do cibercrime, *inter alia*, através da adoção de legislação adequada e da melhoria da cooperação internacional, de modo a tornar mais eficazes as investigações e os processos penais respeitantes às infrações penais relacionados com sistemas e dados informáticos, bem como permitir a recolha de prova, em formato eletrónico. Sendo o primeiro tratado internacional sobre criminalidade contra sistemas de computadores, redes ou dados, pretende harmonizar as várias legislações nacionais sobre a matéria, propiciar e facilitar a cooperação internacional e facilitar as investigações de natureza criminal. Com este fim, impõe aos Estados signatários que adequem o seu direito penal substantivo e adjetivo interno às especificidades destes crimes, tendo como objetivo a harmonização de legislações, incluindo instrumentos processuais e de produção de prova adequados e simplificar a cooperação internacional policial e judicial.

A União Europeia tem dedicado especial atenção ao cibercrime tendo legislado através de diversos instrumentos jurídicos este âmbito. Neste contexto, importa então destacar a Decisão-Quadro 2005/222/JAI do Conselho, de 24 de Fevereiro de 2005, relativa a ataques contra os sistemas de informação tem como objetivos reforçar a cooperação entre as autoridades judiciárias e outras autoridades

competentes, responsáveis pela aplicação da lei nos Estados-Membros, atendendo a uma aproximação do direito penal interno, no que diz respeito aos ataques contra os sistemas de informação; garantir a punibilidade destes ataques através de sanções penais eficazes; possibilitar uma cooperação judiciária neste âmbito; e harmonizar as legislações nacionais através de disposições comuns.

A Diretiva 2013/40/EU, emanada do Parlamento Europeu e Conselho da União Europeia, visa alterar e alargar o âmbito das disposições da Decisão-Quadro 2005/222/JAI do Conselho, de 24 de fevereiro de 2005, relativa a ataques contra os sistemas de informação. Substantivamente, tem como objetivos aproximar o direito penal dos Estados-Membros no domínio dos ataques contra os sistemas de informação, estabelecendo regras mínimas relativas à definição de infrações penais e as sanções aplicáveis, e melhorar a cooperação entre as autoridades competentes, nomeadamente as forças e serviços de segurança e outros serviços especializados dos Estados-Membros responsáveis pela aplicação da lei, bem como as agências e organismos especializados competentes da União, tais como a EUROJUST, a EUROPOL e designadamente o Centro Europeu de Cibercriminalidade e a Agência Europeia para a Segurança das Redes e da Informação. .

Para reforçar o combate ao cibercrime, o Conselho da União Europeia aprovou a criação do *European Cybercrime Centre* (EC3) que constitui o principal instrumento operacional na luta contra o cibercrime, contribuindo para uma resposta cooperativa rápida e eficaz à ocorrência de ciberataques e das ameaças crescentes e complexas suscitadas pela cibercriminalidade. Entre outras áreas de intervenção, o EC3, em estreita cooperação com a EUROJUST, presta assistência às instituições europeias e aos Estados membros no levantamento de uma capacidade operacional e analítica para apoio à investigação criminal e à cooperação internacional, nomeadamente, quando esta envolva parceiros internacionais.

A *European Network and Information Security Agency* (ENISA), constituindo a agência especializada em assuntos relacionados com a segurança da informação nas redes da UE, tem vindo a assumir-se como um centro de competências técnicas na área da segurança do ciberespaço e a desempenhar também um importante papel na coordenação de uma resposta cooperativa dos diversos

Estados membros. Neste contexto, verificam-se grandes discrepâncias registadas nas capacidades operacionais dos *Computer Emergency Response Teams (CERT)* nacionais e governamentais, como o maior obstáculo para a cooperação entre os diferentes Estados-Membros da UE e um potencial risco para a cibersegurança europeia. A necessidade de levantamento de uma rede operacional e funcional de CERT nacionais ou governamentais na Europa – até final de 2012 – foi estabelecido em vários documentos oficiais da UE, mas em muitos países as equipas existentes não apresentam um nível adequado de maturidade.

É com o recrudescimento do terrorismo que a Proteção das Infraestruturas Críticas de Informação entra nas agendas de segurança da UE, introduzindo-se uma diferenciação positiva entre os assuntos relacionados com a *eSociety* e a autonomia de assuntos ligados às Redes e Sistemas de Informação. Inserido no quadro da Diretiva 2008/114/CE relativa à identificação e designação das infraestruturas críticas europeias e à avaliação da necessidade de melhorar a sua proteção, o Programa Europeu de Proteção das Infraestruturas Críticas define o quadro geral para a proteção das infraestruturas críticas na UE. A Diretiva veio assim estabelecer um procedimento de identificação e designação das Infraestruturas Críticas Europeias (ICE) e uma abordagem comum relativa à avaliação da necessidade de melhorar a sua proteção, de modo a contribuir para a proteção das pessoas. A proteção efetiva das ICE requer comunicação, coordenação e cooperação, aos níveis nacional e comunitário, processos mais adequadamente prosseguidos através da existência e intervenção efetiva, em cada país, de pontos de contacto para a proteção de infraestruturas críticas. Os regimes bilaterais de cooperação entre os Estados Membros da UE neste domínio constituem um meio já consagrado de tratar as infraestruturas críticas transfronteiriças, bem como numa participação significativa do setor privado, dada a sua presença significativa na exploração das ICE.

A nível comunitário assiste-se também a uma crescente preocupação de articulação na dicotomia: proteção da privacidade *vs* segurança, sobretudo depois dos atentados terroristas em solo norte-americano e europeu deste século. O desenvolvimento da sociedade da informação, dominado pela globalização da troca de informação e pelo uso de tecnologias cada vez mais intrusivas na vida privada, tem igualmente acarretado desafios constantes neste domínio da proteção da

privacidade.[28] O Tratado de Lisboa, que entrou em vigor em dezembro de 2009, introduziu uma única base jurídica para a proteção de dados pessoais na União Europeia, nomeadamente o artigo 16.º do Tratado sobre o Funcionamento da União Europeia, o que despoletou a reforma global apresentada pela Comissão Europeia em 25 de janeiro de 2012. Atendendo a que evolução tecnológica e a globalização alteraram profundamente a forma como os dados são recolhidos, a reforma visa salvaguardar os dados pessoais na UE, aumentando o controlo dos utilizadores sobre os seus próprios dados e reduzindo os custos para as empresas. A reforma inclui uma comunicação sobre os principais objetivos políticos da mesma, uma proposta de regulamento geral que atualize os princípios consagrados na Diretiva 95/46/CE1, uma proposta de diretiva específica relativa ao tratamento de dados pessoais no domínio da cooperação policial e judiciária em matéria penal e um relatório sobre a aplicação da Decisão-Quadro 2008/977/JAI.

Associado à problemática da segurança e da privacidade, está a necessidade de incrementar a utilização da Sociedade de Informação e a consequente Economia de Conhecimento, como instrumentos de crescimento económico, luta contra a infoexclusão e iliteracia digital. A Agenda Digital para a Europa (2010-2020) traçou o objetivo ambicioso de assegurar um "crescimento inteligente" (*smart growth*), estabelecendo como prioridade a exploração das tecnologias digitais de forma a garantir o desenvolvimento económico e benefícios sociais sustentáveis.

3.2. ENQUADRAMENTO NACIONAL

A Resolução do Conselho de Ministros n.º 12/2012 atribuiu ao Gabinete Nacional de Segurança, no âmbito da quarta medida do plano global estratégico de racionalização e redução de custos com as TIC, a missão de coordenação com as entidades relevantes da definição e implementação, a criação, instalação e operacionalização do Centro Nacional de Cibersegurança, de acordo com as diretrizes comunitárias já afloradas.

Através da Resolução do Conselho de Ministros n.º 112/2012, de 31 de dezembro, foi aprovada a Agenda Portugal Digital com vista ao reforço da competitividade e

[28] Vide Diretiva 95/46/CE1; Regulamento (CE) n.º 45/2001; Diretiva 2002/58/CE; Diretiva 2009/136/CE; e Decisão-Quadro 2008/977/JAI do Conselho da União Europeia.

da internacionalização das empresas nacionais, em especial das pequenas e médias empresas, através da inovação e do empreendedorismo qualificado, relevando a utilização das TIC. A mesma foi posteriormente atualizada pela Resolução do Conselho de Ministros n.º 22/2015 no sentido de reforçar o seu alinhamento com as prioridades estabelecidas na Agenda Digital para a Europa e na Estratégia Europa 2020 e de assegurar a convergência com o período de execução do Acordo de Parceria, 2014-2020.

O Decreto-Lei n.º 69/2014, de 9 de maio, procedeu à segunda alteração ao Decreto-Lei n.º 3/2012, de 16 de janeiro, que aprova a orgânica do Gabinete Nacional de Segurança, estabelecendo os termos do funcionamento do Centro Nacional de Cibersegurança (CNCS), as suas atribuições e competências, adiante plasmadas.

Figura 1 – Missão e competências do Centro Nacional de Cibersegurança
Fonte: Autor

Resulta então que, não tendo sido definidos os poderes do CNCS, enquanto autoridade nacional competente em matéria de cibersegurança, relativamente ao Estado e aos operadores de infraestruturas críticas nacionais, tal competência é juridicamente inconsequente. Entendemos, por um lado, que é na qualidade de autoridade pública que um organismo atua quando está no âmbito do regime jurídico que lhe é próprio, não sendo o objeto ou o fim da atividade que importa, mas o regime jurídico a que está submetida[29]. Por outro, pensamos que tal competência, não sendo densificada, poderá colidir com as do Secretário-Geral do Sistema de Segurança Interna em matéria de infraestruturas críticas, tipificadas na Lei n.º 53/2008, de 29 de agosto, que aprova a Lei de Segurança Interna e no Decreto-Lei n.º 62/2011, de 9 de maio, já abordado.

A Estratégia Nacional de Combate ao Terrorismo, que consta do anexo à Resolução do Conselho de Ministros n.º 7-A/2015, e da qual faz parte integrante, funda-se no compromisso de combate ao terrorismo em todas as suas manifestações, sendo alicerçada nos objetivos estratégicos: Detetar, Prevenir, Proteger, Perseguir e Responder. Com especial relevância para a segurança do ciberespaço, afirma no pilar de "Proteção" a necessidade de implementar um plano de ação nacional para a proteção contra as ciberameaças, bem como de avaliar as vulnerabilidades dos sistemas de informação críticos e manter e acompanhar a adoção das medidas de correção face a ciberataques. O objetivo estratégico "Perseguir", impele ao reforço da colaboração e articulação ente os vários intervenientes e responsáveis nas áreas da cibersegurança, ciberespionagem, ciberdefesa e ciberterrorismo, nos termos da Constituição e da lei. Já o eixo de intervenção "Responder" firma o desiderato de executar ações que permitam exercitar os procedimentos e a articulação entre os diversos atores e desenvolver os mecanismos de interoperabilidade que permitam uma resposta pronta e eficaz a ocorrências terroristas, incluindo sistemas de informação críticos face a ciberataques.

A Segurança do Ciberespaço é edificada, pela respetiva Estratégia Nacional, Resolução do Conselho de Ministros n.º 36/2015, de 28 de maio, como "parte integrante da segurança nacional, referindo-a como essencial para o

[29] Conforme Acórdão do Supremo Tribunal Administrativo, 2ª Secção, de 12-03-2014, N.º de Processo: 01060/13.

funcionamento do Estado, para o desenvolvimento económico e a inovação, bem como para a confiança dos cidadãos no mercado digital e no ciberespaço".

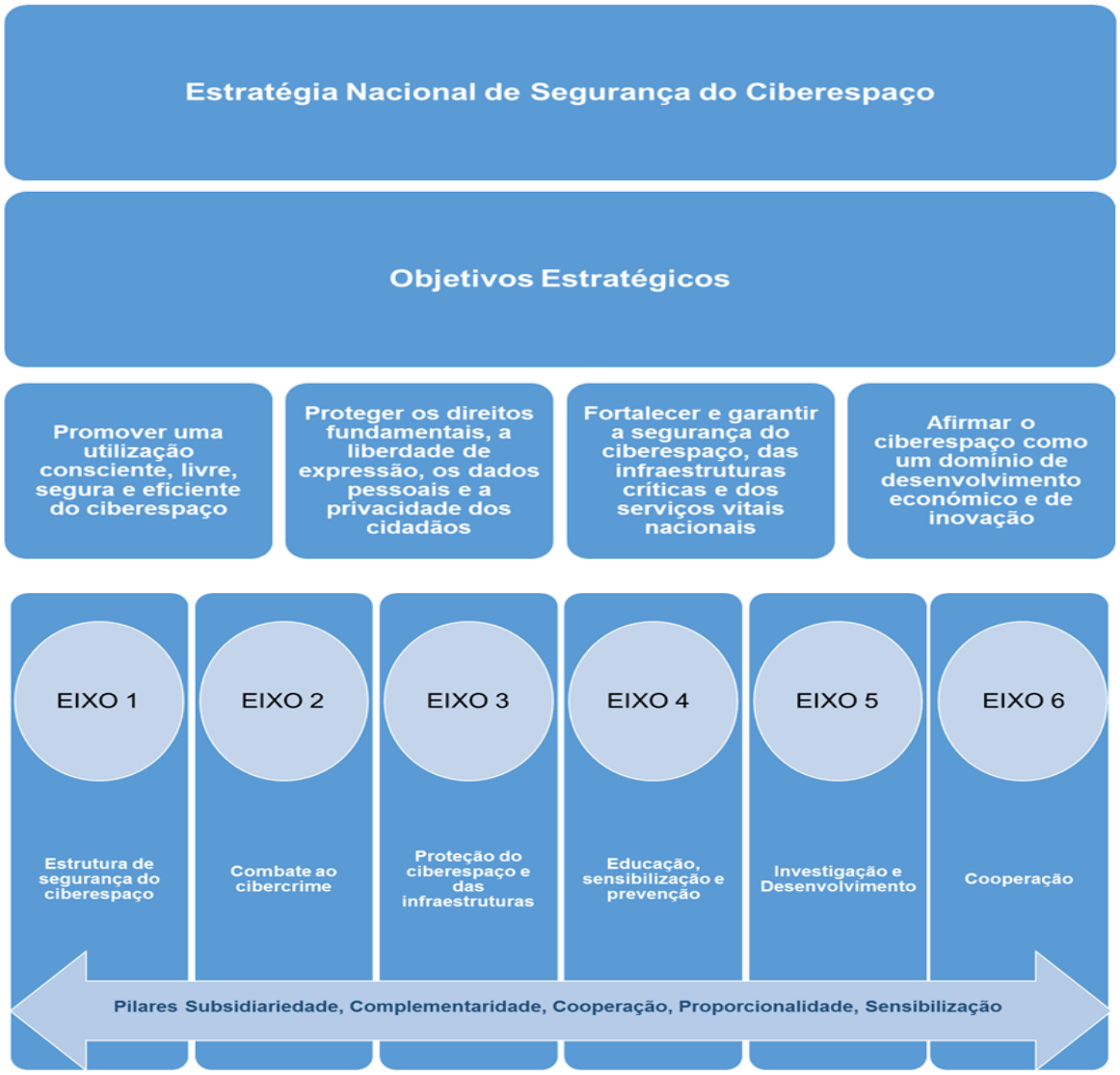

Figura 2 – Sistematização da Estratégia Nacional de Segurança do Ciberespaço

Fonte: Autor

Do seu escopo, resultam objetivos e linhas de ação, consubstanciados em seis eixos de intervenção, com vista a uma eficaz gestão de crises, a uma coordenação da resposta operacional a ciberataques, a um desenvolvimento das sinergias nacionais e a uma intensificação da cooperação nacional, europeia e internacional neste domínio, assentando em princípios de subsidiariedade, complementaridade e cooperação entre públicos e privados, que se resumem na figura adiantes plasmada.

Eixos de intervenção	Principais medidas e respetivas linhas de ação
Eixo 1 - Estrutura de segurança do ciberespaço	✓ Estabelecer a coordenação político-estratégica para a segurança e defesa do ciberespaço. ✓ Consolidar o papel de coordenação operacional e de autoridade nacional em matéria de cibersegurança, relativamente às entidades públicas e às infraestruturas críticas, do Centro Nacional de Cibersegurança. ✓ Desenvolver a capacidade de Ciberdefesa. ✓ Desenvolver a capacidade nacional de resposta a Incidentes. ✓ Estabelecer um gabinete para gestão de crises no Ciberespaço. ✓ Definir e implementar processos de governação da segurança do ciberespaço.
Eixo 2 - Combate ao cibercrime	✓ Revisão e atualização da legislação tendo em vista uma eficaz aplicação no ciberespaço. ✓ Agilizar as capacidades da Polícia Judiciária.
Eixo 3 - Proteção do ciberespaço e das infraestruturas	✓ Avaliar a maturidade e a capacidade das entidades públicas e privadas que administrem infraestruturas críticas ou serviços vitais de informação. ✓ Incluir medidas de segurança do ciberespaço nos planos de proteção de infraestruturas críticas nacionais, seguindo uma abordagem baseada na gestão de risco. ✓ Promover a utilização de normas de segurança da informação nas infraestruturas e sistemas de informação e de comunicação das entidades públicas. ✓ Promover uma política de segurança da informação para as entidades públicas das entidades públicas.
Eixo 4 - Educação, sensibilização e prevenção	✓ Promover campanhas de informação e alerta, tendo como alvos principais os cidadãos e as empresas. ✓ Promover uma cultura de segurança do ciberespaço. ✓ Promover a utilização segura das TIC e do ciberespaço, dando particular importância à capacitação de adolescentes e pessoas idosas e outros grupos de risco.
Eixo 5 - Investigação e desenvolvimento	✓ Promover a investigação científica e o desenvolvimento nos vários domínios da segurança do ciberespaço. ✓ Apoiar a participação da academia e das empresas nacionais em projetos de investigação e desenvolvimento internacionais. ✓ Apoiar a participação nacional em projetos internacionais.
Eixo 6 - Cooperação	✓ Participação em exercícios do ciberespaço que permitam a avaliação e o desenvolvimento de capacidades doutrinárias e operacionais neste domínio. ✓ Participar e cooperar nos diversos fora de CSIRT. ✓ Desenvolver iniciativas de cooperação em áreas ligadas à segurança dos sistemas de informação. ✓ Cooperar e colaborar multilateralmente no quadro das organizações internacionais de que Portugal é parte.

Figura 3 – Principais medidas e respetivas linhas de ação da Estratégia Nacional de Segurança do Ciberespaço
Fonte: Autor

Ora, intervindo-se de forma global no âmbito da segurança do ciberespaço e assentando a estratégia precisamente na subsidiariedade, complementaridade e cooperação entre atores estatais e privados, parece-nos igualmente pertinente dotá-lo de um quadro jurídico completo e estável da reserva de lei, porquanto a positivação da opção política numa mera Resolução do Conselho de Ministros assume-se manifestamente insuficiente e inconsequente no plano das garantias jurídico-constitucionais (Castro, Raquel, 2016).

Admitindo a estratégia que a responsabilidade pela segurança do ciberespaço nacional encontra-se distribuída por diferentes atores com missões e objetivos diversos, não existindo um fio condutor nem a coerência necessária nas políticas e iniciativas desenvolvidas por cada um deles, cabe ainda definir claramente a execução e articulação da capacidade de ciberdefesa, evitando-se sobreposições e duplicações que ponham em causa a agilidade dos processos e o pleno respeito do Estado de Direito Democrático e dos princípios enformadores das diferentes funções do Estado[30].

Com efeito, a ordem jurídica portuguesa é marcada por uma indefinição legal de conceitos neste domínio, agravado pela urgência da clarificação do conceito de cibersegurança ou de segurança do ciberespaço e pela identificação rigorosa do seu objeto e do âmbito de aplicação do respetivo regime jurídico (Castro, Raquel, 2016).

No que ao cibercrime diz respeito, do ordenamento jurídico, distinguem-se entre quatro grupos a criminalidade relacionada com a utilização de computadores e em especial no ciberespaço. Primeiro, os crimes que recorrem a meios informáticos, não alterando o tipo penal comum e que correspondem a uma especificação ou qualificação deste[31]. Segundo, os crimes relativos à proteção de dados pessoais ou da privacidade.[32] Terceiro, os crimes informáticos em sentido estrito, sendo o bem ou meio informático o elemento próprio do tipo de crime, também classificados como vertical use of high-tech[33]. Quarto e por último, os crimes relacionados com o conteúdo[34]. Releva-se ainda que o âmbito de aplicação da Lei nº 109/2009, de

[30] A própria Orientação Política para a Ciberdefesa, anexa ao despacho Despacho n.º 13692/2013, de 11 de outubro de 2013, publicado no Diário da República, 2.ª série — N.º 208 — 28 de outubro de 2013, refere que "muitos dos serviços de ciberdefesa baseiam-se funcionalmente nas capacidades técnicas, tradicionalmente associadas à cibersegurança, que passam pela prevenção, deteção e recuperação dos Sistemas de Informação e Comunicações (SIC) face à ocorrência de ataques cibernéticos." e que "As ações e operações militares conduzidas no âmbito da ciberdefesa são executadas no respeito do quadro legal em vigor, obedecendo à mesma lógica e fundamentos que caracterizam a Segurança e a Defesa Nacional."

[31] São exemplo a devassa por meio de informática (art.º 193.º do Código Penal), o crime de burla informática e o crime de burla informática nas telecomunicações (art.º 221.º do Código Penal).

[32] Tipificados na Lei nº 67/98, de 26 de outubro, e na Lei nº 69/98, de 28 de outubro.

[33] Inserindo-se neste grupo os crimes previstos na Lei nº 109/2009 de 15 de setembro, que transpõe para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa, a saber, a Falsidade informática, o Dano relativo a programas ou outros dados informáticos, a Sabotagem informática, o Acesso ilegítimo, a Interceção ilegítima e a Reprodução ilegítima de programa protegido.

[34] Destacam a violação do direito de autor, a difusão de pornografia infantil [art.º. 172º, nº 3, alínea d)] ou a discriminação racial ou religiosa [art.º. 240º, nº 1, alínea a)].

15 de outubro - Lei do Cibercrime - exorbita a criminalidade informática, dispondo igualmente para os crimes cometidos por meio de um sistema informático ou daqueles em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico, excetuando-se as interceções de comunicações e as ações encobertas (Ascensão, 2001). Note-se, por fim, que Lei n.º 49/2008, de 27 de agosto, que aprova a Lei da Organização e Investigação Criminal estabelece, nos termos da alínea l), do n.º 3, do art.º 7, ser da competência reservada da Policia Judiciária a investigação dos crimes informáticos e praticados com recurso a tecnologia informática, sem prejuízo da possibilidade de competência deferida a outro órgão de polícia criminal. É efetivamente assim, desde que tal se afigure, em concreto, mais adequado ao bom andamento da investigação e, nos exatos termos do seu art.º 8, quando existirem provas simples e evidentes, ou estejam verificados os pressupostos das formas especiais de processo, ou tratando-se de crime sobre o qual incidam orientações sobre a pequena criminalidade, nos termos da Lei de Política Criminal em vigor, ou que a investigação não exija especial mobilidade de atuação ou meios de elevada especialidade técnica.[35]

Figura 4 – Enquadramento normativo principal da segurança do ciberespaço
Fonte: Autor

[35] Nos termos do Relatório de Atividades do Gabinete Cibercrime da PGR "não tem sido claro o resultado da delegação de competência, nos termos da lei processual penal, para a investigação de inquéritos na área da cibercriminalidade ou que suponham o uso de meios informáticos ou de redes de comunicações. Em regra, os magistrados têm delegado a competência na Polícia Judiciária, dada a sofisticação técnica e as exigências específicas da investigação. Porém, por vezes, a Policia Judiciária não tem desenvolvido as diligências de inquérito, devolvendo os processos sem investigação, por não se achar competente quanto a ela. Assim tem acontecido, por exemplo, com casos de injúrias ou difamações por meios tecnológicos. Neste tipo de situações, frequentemente, os magistrados acabam assumir diretamente a direção da investigação, uma vez que nem sempre se afigura viável a delegação de competência na PSP ou na GNR. Na origem desta questão estão diferentes interpretações da Lei n.º 49/2008, de 27 de Agosto (Lei de Organização da Investigação Criminal). No Artigo 7º deste diploma descreve-se a competência da Polícia Judiciária em matéria de investigação criminal, dizendo-se, no nº 3, alínea l), que é da competência reservada da Polícia Judiciária a investigação dos crimes "informáticos e praticados com recurso a tecnologia informática". Esta disposição não tem interpretações unívocas, desde logo porque deixou de existir, após a entrada em vigor da Lei nº 109/2009, de 15 de Setembro, conteúdo legal para a expressão "crimes informáticos", que foi substituída na lei pela expressão "cibercrime", (…) tanto mais que existe a perceção de que, no presente momento, aquela polícia não tem meios humanos capazes de dar resposta às inúmeras diligências de investigação."

CAPÍTULO IV

SISTEMATIZAÇÃO DO QUADRO DE ATUAÇÃO E DE COOPERAÇÃO DA POLÍCIA DE SEGURANÇA PÚBLICA NO ÂMBITO DA SEGURANÇA DO CIBERESPAÇO

Nos termos da Lei n.º 53/2007, de 31 de agosto, que aprova a sua orgânica, a Polícia de Segurança Pública é uma força de segurança que tem por missão assegurar a legalidade democrática, garantir a segurança interna e o livre exercício dos direitos fundamentais dos cidadãos, bem como o normal funcionamento das instituições democráticas, no quadro da Constituição e da lei.

Com efeito, é um serviço público policial, com atribuições específicas e uma orgânica própria, dotado de pessoal com funções policiais e funções não policiais e de recursos materiais próprios, prosseguindo a sua missão, essencialmente, no meio urbano e em proximidade com o cidadão

Figura 5 – Missão da Polícia de Segurança Pública
Fonte: Autor

Das suas atribuições[36], com inevitável, indelével e imprescindível repercussão, direta ou indireta, nos princípios e eixos enformadores da segurança do ciberespaço, em razão da Estratégia Nacional, destacamos:

[36] Cfr. Lei n.º 53/2007, de 31 de agosto, que aprova a orgânica da Polícia de Segurança Pública.

Atribuições da PSP	Estratégia Nacional de Segurança do Ciberespaço			
	Pilares	Objetivos estratégicos	Eixo de intervenção	Principais medidas e respetivas linhas de ação
Garantir as condições de segurança que permitam o exercício dos direitos e liberdades e o respeito pelas garantias dos cidadãos, bem como o pleno funcionamento das instituições democráticas, no respeito pela legalidade e pelos princípios do Estado de Direito.	Complementaridade Cooperação	Proteger os direitos fundamentais, a liberdade de expressão, os dados pessoais e a privacidade dos cidadãos.	Eixo 2 – Combate ao Cibercrime Eixo 6 - Cooperação	Desenvolver iniciativas de cooperação em áreas ligadas à segurança dos sistemas de informação e cibercrime.
Garantir a ordem e a tranquilidade públicas e a segurança e a proteção das pessoas e dos bens.	Complementaridade Cooperação	Fortalecer e garantir a segurança do ciberespaço, das infraestruturas críticas e dos serviços vitais nacionais.	Eixo 6 – Cooperação	Desenvolver iniciativas de cooperação em áreas ligadas à segurança dos sistemas de informação e cibercrime.
Prevenir a criminalidade em geral, em coordenação com as demais forças e serviços de segurança.	Complementaridade Cooperação	Promover uma utilização consciente, livre, segura e eficiente do ciberespaço.	Eixo 6 - Cooperação	Desenvolver iniciativas de cooperação em áreas ligadas à segurança dos sistemas de informação e cibercrime. Cooperar e colaborar multilateralmente no quadro nacional e da UE.
Desenvolver as ações de investigação criminal e contraordenacional que lhe sejam atribuídas por lei, delegadas pelas autoridades judiciárias ou solicitadas pelas autoridades administrativas.	Complementaridade Cooperação	Promover uma utilização consciente, livre, segura e eficiente do ciberespaço.	Eixo 2 - Combate ao cibercrime	Robustecer as suas estruturas e as suas capacidades técnicas e humanas para o combate ao cibercrime, assim como reforçar as competências técnicas e forenses para conduzir investigações.
Contribuir para a formação e informação em matéria de segurança dos cidadãos.	Complementaridade Cooperação Sensibilização	Promover uma utilização consciente, livre, segura e eficiente do ciberespaço.	Eixo 4 - Educação, sensibilização e prevenção	Promover campanhas de informação e alerta, tendo como alvos principais os cidadãos e as empresas. Promover uma cultura de segurança do ciberespaço, através da promoção de campanhas e iniciativas de sensibilização para a segurança do ciberespaço. Promover a utilização segura das TIC e do ciberespaço, dando particular importância à capacitação e conhecimento obtidos por adolescentes e pessoas idosas e outros grupos de risco.
Atribuições ISCPSI	Complementaridade Cooperação Sensibilização	Afirmar o ciberespaço como um domínio de desenvolvimento económico e de inovação	Eixo 5 – Investigação e desenvolvimento	Promover a investigação científica e o desenvolvimento nos vários domínios da segurança do ciberespaço.

Figura 6 – Sistematização das atribuições da PSP no quadro da Estratégia Nacional de Segurança do Ciberespaço
Fonte: Autor

O provir institucional induz a consolidação da PSP como polícia integral e proactiva, altamente prestigiada, com elevado grau de profissionalismo, através da simplificação do ciclo produtivo interno, da melhoria da eficácia da ação policial e do incremento da proximidade ao cidadão, sobretudo aos estratos sociais e setores mais vulneráveis à ação criminógena, sem olvidar a dimensão do ciberespaço, a par da valorização dos recursos humanos e da avaliação dos respetivos desempenhos funcionais.[37]

O ambiente interno da PSP é caracterizado por mais de 90% do seu efetivo, cliente interno, pertencer a uma carreira especial, regida por normativo próprio, incluindo o disciplinar, inserido num dispositivo orgânico disperso pelo país, executando uma pluralidade de atividades.

Para um mais eficaz e eficiente cumprimento da sua missão, incumbe também à PSP ministrar formação, ainda que a Segurança do Ciberespaço não tenha dimensão no seu quadro programático académico. A formação específica, inicial e de progressão na carreira, dos elementos policiais, é prestada em estabelecimentos de ensino próprios, a saber, a Escola Prática de Polícia e o Instituto Superior de Ciências Policiais e Segurança Interna (ISCPSI), sendo que este, para além de formar oficiais de polícia, tem por missão, entre outras, promover o seu aperfeiçoamento permanente e realizar, coordenar ou colaborar em projetos de investigação e desenvolvimento no domínio das ciências policiais.[38]

Decorrente do ideário de inovação e modernização, inerente à cultura organizacional da PSP, apesar de não vislumbrarmos um serviço específica e especialmente dedicado à segurança do ciberespaço, existe um crescente reconhecimento das TIC como peça fundamental à eficiência dos serviços públicos, e na sequência das Grandes Opções Estratégicas da PSP para 2013- 2016[39] que a PSP definiu a sua Estratégia para as TIC para o horizonte 2013-2016. Este plano concilia as diretrizes emanadas do Plano Global Estratégico de Racionalização e

[37] Conforme Relatório de Atividades da PSP de 2014, homologado por S.Exa. a MAI em 18/02/2016.
[38] Conforme Estatuto do Instituto Superior de Ciências Policiais e Segurança Interna, aprovado pelo Decreto-Lei n.º 275/2009, de 2 de outubro.
[39] Conforme Grandes Opções Estratégicas da PSP 2013-2016, de 26 de março de 2012.

Redução de Custos com as TIC com a visão específica da PSP para a sua área tecnológica.[40]

O ambiente externo engloba a proteção dos cidadãos e a manutenção da ordem pública na sociedade portuguesa, cada vez mais marcada pela multiculturalidade, comum na Europa comunitária, a par da investigação de um vasto conjunto de ilícitos e do apoio às vítimas de crime. Os fenómenos criminais e os fatores socioculturais potenciadores de violência levam a PSP a desenvolver estratégias que produzam uma resposta eficaz ao controlo da criminalidade. A necessidade de respostas objetivas e consentâneas com a natureza do serviço público de qualidade, levaram ao desenvolvimento de estratégias que incluem o Modelo Integrado de Policiamento de Proximidade[41] que vai ao encontro das exigências de prevenção criminal e de ordem pública atuais, apesar dos domínios da cidadania e segurança digitais e de uma cultura nacional de cibersegurança terem ainda pouca expressividade.[42]

Na ótica do cliente externo, a PSP tem vindo a implementar formas proactivas de atuação, procurando adaptar-se à constante evolução das comunidades locais, sempre na perspetiva da prestação de um serviço público de qualidade que contribua para a satisfação plena dos justos anseios da sociedade portuguesa, direcionando a sua atividade para a resolução dos problemas que afetam a segurança dos cidadãos em geral e, em particular, dos inseridos em grupos de risco. Além do cidadão em geral e de públicos-alvo específicos, que exigem uma maior proximidade policial, a PSP desenvolve toda uma atividade que, direta ou indiretamente, implica a cooperação e interação profissional com diversos organismos públicos, desde os vários operadores judiciários, sobretudo o Ministério Público, a serviços da Administração Pública, central e desconcentrada, às Autarquias Locais e aos estabelecimentos de ensino.

A este propósito, note-se que a literacia e as competências digitais são essenciais para a utilização segura do ciberespaço, principalmente em termos de gestão da

[40] Conforme Visão Global de Operacionalização da Estratégia para as TIC na PSP 2013-2016, de outubro de 2013.
[41] Conforme Diretiva Estratégica n.º 10/2006 de 15 de Maio - Programa Integrado de Policiamento de Proximidade (PIPP) - atualmente designado por Modelo Integrado de Policiamento de Proximidade (MIPP).
[42] Conforme Relatório de Atividades da PSP de 2014, homologado por S.Exa. a MAI em 18/02/2016.

privacidade e identidade e do desenvolvimento e aprofundamento, numa fase precoce, de um comportamento online responsável e ético, onde naturalmente as escolas têm um papel fulcral e determinante, relevando-se a Educação, Sensibilização e Prevenção da Segurança enquanto eixo preludial da Estratégia Nacional e consequentemente, a dimensão estratégica da área de responsabilidade territorial da PSP, através da presença nas principais urbes, onde a utilização de computador e internet é mais frequente.

De acordo com os resultados da edição de 2015 do Inquérito à Utilização de Tecnologias da Informação e da Comunicação pela Famílias do Instituto Nacional de Estatística[43], cerca de 70% das famílias portuguesas têm acesso à internet em casa, sendo que 7 em cada 10 pessoas com idade entre 16 e 74 anos ligam-se à internet e 2 fazem encomendas eletrónicas. Nos últimos 5 anos, a utilização de comércio eletrónico aumentou 13 pontos percentuais, passando de 10% em 2010 para 23% em 2015. A utilização de computador e internet é mais frequente, nas grandes urbes, por pessoas até aos 44 anos, para os homens e para quem completou o ensino secundário ou superior. Em 2015, 70% dos utilizadores de internet em Portugal participam em redes sociais. No ano anterior, a proporção de residentes que utilizou as redes sociais foi superior em 14 pontos percentuais à média da União Europeia a 28 Estados-Membros. Dois terços dos utilizadores de internet acedem à rede em mobilidade, essencialmente através de telemóvel ou smartphone. Contudo, mais de metade (54%) das pessoas que utilizaram a internet referiram ter limitado a sua utilização devido a preocupações com a segurança.

Já o Inquérito às Empresas[44] de 2015 refere que 96% das empresas portuguesas com 10 ou mais pessoas ao serviço acedem à internet em banda larga. Do conjunto de empresas em análise, 70% disponibiliza equipamento portátil com ligação móvel à internet aos seus trabalhadores, o que representa um aumento de 30 pontos percentuais relativamente a 2013. Cerca de 38% das empresas com 10 ou mais pessoas ao serviço utilizam as redes sociais como estratégia de ligação a clientes,

[43] Inquérito anual com base numa amostra representativa dos agregados familiares residentes em Portugal com pelo menos um indivíduo com idade entre 16 e 74 anos. http://www.ine.pt/xportal/xmain?xpid=INE&xpgid=ine_destaques&DESTAQUESdest_boui=211422735&DESTAQUESmodo=2&xlang=pt (acedido em 29/05/2016)

[44] As estimativas apresentadas foram obtidas a partir de uma amostra de 3294 empresas com 10 ou mais pessoas ao serviço, excluindo as atividades de educação e de saúde e as atividades financeiras.http://www.ine.pt/xportal/xmain?xpid=INE&xpgid=ine_destaques&DESTAQUESdest_boui=211421031&DESTAQUESmodo=2&xlang=pt (acedido em 29/05/2016).

fornecedores ou parceiros de negócio A utilização de comércio eletrónico pelas empresas tem vindo a aumentar nos últimos 5 anos, sendo que Portugal foi a principal origem e destino das encomendas eletrónicas recebidas (97%) e efetuadas (90%) pelas empresas que utilizaram comércio eletrónico em 2014. Em 2015, 61% das empresas em análise referiram ter website, mais 6 p.p. do que no ano anterior. 29% das empresas partilham informação de forma eletrónica como estratégia de serviço. Quase metade das empresas com 10 ou mais pessoas ao serviço têm uma política definida e implementada para a prevenção de problemas de segurança informática. Um quinto das empresas portuguesas empregam trabalhadores especializados em TIC ou promovem formação TIC para outro pessoal ao serviço.

Segundo o Relatório Anual de Segurança Interna de 2015[45], Portugal enfrenta ameaças idênticas àquelas que impendem sobre os países do seu espaço geoestratégico e político, designadamente no que se refere ao terrorismo, à criminalidade organizada e ao largo espectro de ciberameaças, atenta a crescente sofisticação quanto a *modus operandi* e capacidade tecnológica. Paralelamente, releva que a ameaça de quebra de segurança dos sistemas informáticos que impende sobre órgãos políticos, estruturas estatais, forças armadas, forças de segurança, universidades, centros de investigação e empresas é hoje significativamente maior que em igual período anterior. Afirma então que elevar os níveis de cibersegurança nacionais continua a ser uma necessidade premente. No que concerne à área da criminalidade informática e praticada com recurso a tecnologia informática, "verifica-se um aumento da generalidade dos crimes referenciados". Frisa ainda que a equipa de resposta a incidentes de cibersegurança do Centro Nacional de Cibersegurança processou cerca de 2 milhões de observáveis por mês, dos quais 400 mil relacionados com o ciberespaço nacional, recebidos de cerca de 60 fontes de informação. Tendo recebido 2646 notificações, dos incidentes analisados e resolvidos, apenas 5% implicaram, direta ou indiretamente, entidades do Estado.

Caracterizado o seu ambiente e clientes, internos e externos, bem como as suas atribuições, competências e organização, importa agora realizar um diagnóstico da situação atual que permita realçar os pontos fortes (vantagens internas) e os pontos

[45] http://www.portugal.gov.pt/media/18859123/20160331-rasi-2015.pdf (acedido em 30/05/2016).

fracos (desvantagens internas), bem como as tendências mais importantes na envolvente externa, sejam as oportunidades (vantagens externas), sejam os riscos (desvantagens externas). Da identificação destes fatores, procedemos adiante à sistematização numa matriz, composta por quatro vetores, designados por pontos fortes (strengths), pontos fracos (weaknesses), oportunidades (opportunities) e riscos (threats), vulgo SWOT, a qual concorre para a compaginação das opções, dos objetivos e, consequentemente, da definição de estratégias de atuação na segurança do ciberespaço.

Figura 7 – Análise SWOT – A PSP e a Segurança do Ciberespaço
Fonte: Autor

CAPÍTULO V

ESTUDO EXPLORATÓRIO

5.1. INTRODUÇÃO

Definimos como âmbito de estudo e campo geral de investigação do trabalho, a segurança do ciberespaço. Tratando-se de um tema abrangente, por motivos de amplitude do trabalho, procedemos à delimitação da nossa investigação à compreensão e definição de uma estratégia institucional da PSP em matéria de segurança do ciberespaço, perspetivando o respetivo enquadramento estratégico, concetual e normativo nacional e internacional. No sentido de alcançar as respostas à pergunta principal e derivadas, procedemos a um estudo exploratório, que incidiu sobre uma amostra não-probabilística ou empírica de tipo intencional, mediante a técnica de recolha de dados, entrevista do tipo semiestruturada, adotando a análise de conteúdo às respostas enquanto técnica de investigação.

5.2. METODOLOGIA

5.2.1. AMOSTRA E PROCEDIMENTO DE RECOLHA DA INFORMAÇÃO

O método configura-se como uma formalização do percurso intencionalmente ajustado ao objeto de estudo, concebido como meio de direcionar a investigação para os seus objetivos e para a investigação das perguntas de o norteiam (Pardal & Correia, 1995). Atendendo a que o presente incide sobre problemáticas novas, poderá permitir renovar perspetivas ou sugerir hipóteses fecundas, visando abrir caminho a futuros estudos, adotamos um estudo exploratório (Quivy & Campenhoudt, 2005). Este, correspondendo a um modelo de análise intensiva e sendo flexível no recurso a técnicas, permite a recolha de informação diversificada de análise e viabiliza o seu conhecimento e caracterização. Ambicionando a solidez, fundamentação e a credibilidade dos dados analisados, recorremos a um guião de entrevista, em apêndice A, desenhado em observância com os objetivos do trabalho e com a pergunta de partida e derivadas, tendo sido aplicado a uma amostra não-probabilística ou empírica de tipo intencional, cujo fundamento de seleção obedeceu, criteriosamente, ao juízo do autor, nos exatos termos dos

objetivos estratégicos, pilares e eixos de intervenção da Estratégia Nacional de Segurança do Ciberespaço e consequentemente da organização departamental da Direção Nacional da PSP e seus cargos dirigentes.

Assim, a amostra do presente estudo é composta pelos seguintes respondentes, com as respetivas funções, à data da recolha da informação:

- Coordenador do Centro Nacional de Cibersegurança, Dr. José Carlos Martins;
- Diretor do Departamento de Operações, Superintendente Luís Filipe Cardoso de Sousa Simões;
- Diretor do Departamento de Informações Policiais, Superintendente Luís Miguel Fiães Fernandes;
- Diretor do Departamento de Investigação Criminal, Superintendente José Carlos Bastos Leitão;
- Diretor do Departamento de Formação, Superintendente João Manuel Alves Amado;
- Diretor do Departamento de Sistemas de Informação e Comunicações, Superintendente João Carlos Jesus Filipe Ribeiro;
- Diretora do Gabinete de Sistemas de Informação, Dra. Lurdes Rosa.

5.2.2. ESTRATÉGIA DE ANÁLISE DA INFORMAÇÃO

Adotamos a análise de conteúdo às respostas das entrevistas, enquanto técnica de investigação que viabiliza, de modo sistemático e quantitativo, a descrição do conteúdo da comunicação, incidindo sobre a captação de ideias e de significações da comunicação às perguntas do guião de entrevista, relevando a frequência do aparecimento de certas características de conteúdo ou de correlação entre elas. Assumindo assim, “a escolha dos termos utilizados pelo entrevistado, a sua frequência e o seu modo de exposição são fontes de informações a partir dos quais o investigador tenta construir conhecimento” (Quivy & Campenhoudt, 2005, p. 226), e que “apenas a utilização de métodos construídos e estáveis permite ao investigador elaborar uma interpretação que não tome como referência os seus próprios valores e representações” (p.227).

5.2.3. APRESENTAÇÃO DOS RESULTADOS

As entrevistas recebidas, depois de analisadas e processadas em termos de conteúdos, permitiram a compilação e sistematização de resultados, a seguir apresentados.

No que respeita à questão 1 (Na sua opinião, qual a importância estratégica da segurança do ciberespaço para o País e em particular para a PSP?), os resultados alcançados foram os seguintes:

Matriz cromática das unidades de contexto e de registo da questão 1.		
Entrevistado	**Unidade de Contexto**	**Unidade de Registo**
1	• Prioritário e estratégico para o Estado e sociedade. • Prioritário e estratégico para a PSP.	1.1 1.2
2	• Prioritário e estratégico para o Estado e sociedade • Prioritário e estratégico para a PSP. • Estratégico para o mercado digital.	1.1 1.2 1.3
3	• Não respondeu.	1.4
4	• Não respondeu.	1.4
5	• Não respondeu.	1.4
6	• Prioritário e estratégico para o Estado e sociedade. • Prioritário e estratégico para a PSP	1.1 1.2
7	• Prioritário e estratégico para o Estado e sociedade. • Prioritário e estratégico para a PSP. • Estratégico para o mercado digital.	1.1 1.2 1.3

Matriz de análise de conteúdo da questão 1 da entrevista.										
Categorias	**Unidades de registo**	**Entrevistados**							**Unidades de Enumeração**	**Resultados**
		1	**2**	**3**	**4**	**5**	**6**	**7**		
Importância estratégica para o país	1.1 - Prioritário e estratégico para o Estado e sociedade.	x	x				x	x	4	57%
	1.3 - Estratégico para o mercado digital.		x					x	2	28,6%
	1.4-Não respondeu			x	x	x			3	43%
Importância estratégica para a PSP	1.2 - Prioritário e estratégico para a PSP	x	x				x	x	4	57%
	1.4 - Não respondeu			x	x	x			3	43%

Os resultados indicam que 57% dos entrevistados consideram que a segurança do ciberespaço é prioritária e estratégica para o Estado, sociedade e para a PSP, sendo que 28,6% entendem-na como igualmente estratégica para a confiança dos

cidadãos no mercado digital, relevando-se que 43% não respondeu à questão formulada.

No que concerne à questão 2 (Como caracteriza os riscos e ameaças do ciberespaço relativamente à Segurança Interna?), resulta:

Matriz cromática das unidades de contexto e de registo da questão 2		
Entrevistado	**Unidade de Contexto**	**Unidade de Registo**
1	• Os riscos e ameaças são latentes e elevadas. • As ameaças e riscos do ciberespaço afetam de forma transversal cidadãos, empresas e Estado.	1.1 1.2
2	• Os riscos e ameaças são latentes e elevadas. • As ameaças e riscos do ciberespaço afetam de forma transversal cidadãos, empresas e Estado.	1.1 1.2
3	• Não respondeu.	1.3
4	• Não respondeu.	1.3
5	• Não respondeu.	1.3
6	• Os riscos e ameaças são latentes e elevadas. • As ameaças e riscos do ciberespaço afetam de forma transversal cidadãos, empresas e Estado.	1.1 1.2
7	• Os riscos e ameaças são latentes e elevadas. • As ameaças e riscos do ciberespaço afetam de forma transversal cidadãos, empresas e Estado.	1.1 1.2

Matriz de análise de conteúdo da questão 2 da entrevista.										
Categorias	**Unidades de registo**	**Entrevistados**							**Unidades de Enumeração**	**Resultados**
		1	2	3	4	5	6	7		
Riscos e ameaças do ciberespaço relativamente à Segurança Interna	1.1 - Os riscos e ameaças são latentes e elevadas.	x	x				x	x	4	57%
	1.2 - As ameaças e riscos do ciberespaço afetam de forma transversal cidadãos, empresas e Estado.	x	x				x	x	4	57%
	1.3 - Não respondeu.			x	x	x			3	43%

Os entrevistados que responderam à pergunta, 57%, concordam que os riscos e ameaças do ciberespaço à Segurança Interna são latentes e elevadas e que afetam

de forma transversal cidadãos, empresas e Estado. Vincamos que 43% não responderam à pergunta formulada.

Relativamente à questão 3 (O enquadramento legal nacional e internacional aplicável à segurança do ciberespaço é suficiente para a definição de uma estratégia institucional da PSP? Porquê?), apurámos:

Matriz cromática das unidades de contexto e de registo da questão 3.		
Entrevistado	**Unidade de Contexto**	**Unidade de Registo**
1	• Desconhece, em pormenor, o enquadramento jurídico. • Sim, atendendo aos pilares de Cooperação e Sensibilização que alicerçam a Estratégia Nacional de Segurança do Ciberespaço.	1.1 1.2
2	• Sim, atendendo aos pilares de Cooperação e Sensibilização que alicerçam a Estratégia Nacional de Segurança do Ciberespaço.	1.2
3	• Desconhece, em pormenor, o enquadramento jurídico.	1.1
4	• Não respondeu.	1.3
5	• Não respondeu.	1.3
6	• Desconhece, em pormenor, o enquadramento jurídico. • Sim, atendendo aos pilares de Cooperação e Sensibilização que alicerçam a Estratégia Nacional de Segurança do Ciberespaço	1.1 1.2
7	• Sim, atendendo aos pilares de Cooperação e Sensibilização que alicerçam a Estratégia Nacional de Segurança do Ciberespaço.	1.2

Matriz de análise de conteúdo da questão 3 da entrevista.										
Categorias	**Unidades de registo**	**Entrevistados**							**Unidades de Enumeração**	**Resultados**
		1	**2**	**3**	**4**	**5**	**6**	**7**		
Adequação do enquadramento legal nacional e internacional aplicável à segurança do ciberespaço à definição de uma estratégia institucional da PSP	1.1 - Desconhece, em pormenor, o enquadramento jurídico.	x		x			x		3	43%
	1.2 - Sim, atendendo aos pilares de Cooperação e Sensibilização que alicerçam a Estratégia Nacional de Segurança do Ciberespaço.	x	x				x	x	4	57%
	1.3 - Não respondeu.				x	x			2	28.6%

Em relação a esta questão, 43% dos entrevistados reconhece desconhecer, em pormenor, o enquadramento jurídico nacional e internacional aplicável à segurança

do ciberespaço, sendo que 28,6% não respondeu à pergunta formulada. Já 57% entende que o ordenamento legal é suficiente para a definição de uma estratégia institucional da PSP atendendo aos pilares de cooperação e sensibilização que alicerçam a Estratégia Nacional de Segurança do Ciberespaço.

Relativamente à questão 4 (O quadro de atuação e de cooperação da PSP no domínio da Segurança do Ciberespaço impele à definição de uma estratégia institucional respetiva? Porquê?), temos:

Matriz cromática das unidades de contexto e de registo da questão 4.		
Entrevistado	**Unidade de Contexto**	**Unidade de Registo**
1	Sim. No quadro das relações institucionais e de cooperação que estabelece com outros parceiros em matéria de segurança do ciberespaço.	1.1
2	A PSP não tem ainda necessidade de definir uma estratégia institucional formal.	1.2
3	Não respondeu.	1.3
4	Não respondeu.	1.3
5	Não respondeu.	1.3
6	A PSP não tem ainda necessidade de definir uma estratégia institucional formal.	1.2
7	Sim. No quadro das relações institucionais e de cooperação que estabelece com outros parceiros em matéria de segurança do ciberespaço.	1.1

Matriz de análise de conteúdo da questão 4 da entrevista.										
Categorias	**Unidades de registo**	**Entrevistados**							**Unidades de Enumeração**	**Resultados**
		1	**2**	**3**	**4**	**5**	**6**	**7**		
Definição de uma estratégia institucional face ao quadro de atuação e de cooperação da PSP no domínio da Segurança do Ciberespaço	1.1 - Sim. No quadro das relações institucionais e de cooperação que estabelece com outros parceiros em matéria de segurança do ciberespaço.	x						x	2	28%
	1.2 - A PSP não tem ainda necessidade de definir uma estratégia institucional formal.		x				x		2	28,6%
	1.3 - Não respondeu.			x	x	x			3	43%

Verificamos que 28% dos entrevistados consideram que o quadro de atuação e de cooperação da PSP no domínio da Segurança do Ciberespaço impele à definição de uma estratégia institucional em razão das relações institucionais e de

cooperações que estabelece com outros parceiros. No entanto, 28,6% entende que a PSP não tem ainda necessidade de definir uma estratégia institucional formal atendendo ao estado embrionário da Estratégia Nacional de Segurança do Ciberespaço e da sua operacionalização. Evidenciamos ainda que 43% não respondeu à questão formulada.

No que concerne à questão 5 (Na eventual definição de uma estratégia institucional da PSP em matéria de segurança do ciberespaço, que competências conceberia para o Departamento que dirige?), apurámos os seguintes resultados:

Matriz cromática das unidades de contexto e de registo da questão 5.		
Entrevistado	**Unidade de Contexto**	**Unidade de Registo**
1	Formação.	1.1
2	Investigação Criminal.	1.2
3	Não respondeu.	1.3
4	Não respondeu.	1.3
5	Não respondeu.	1.3
6	Segurança dos Sistemas de Informação.	1.4
7	Não aplicável.	1.5

Matriz de análise de conteúdo da questão 5 da entrevista.										
Categorias	**Unidades de registo**	**Entrevistados**							**Unidades de Enumeração**	**Resultados**
		1	2	3	4	5	6	7		
Conceção de competências do Departamento que dirige na estratégia institucional	1.1 - Formação	x							1	14,2%
	1.2 – Investigação Criminal		x						1	14,2%
	1.3 – Não respondeu			x	x	x			3	43%
	1.4 – Segurança dos Sistemas de Informação						x		1	14,2%
	1.4 – Não aplicável							x	1	14,2%

43% dos entrevistados não respondeu à questão formulada e que a mesma não era aplicável a outro, sendo que os restantes identificam competências próprias de

Formação, Investigação Criminal e Segurança dos Sistemas de Informação enquanto primordiais para os departamentos que dirigem.

Por fim, relativamente à questão 6 (Considera adequada a criação na estrutura da PSP de um órgão especifico e especializado em matérias de Segurança do Ciberespaço? Porquê?)

Matriz cromática das unidades de contexto e de registo da questão 6.		
Entrevistado	**Unidade de Contexto**	**Unidade de Registo**
1	Imprescindível atendendo aos riscos e ameaças à integridade, disponibilidade e confidencialidade das informações, dados e sistemas informáticos da PSP.	1.1
2	Imprescindível atendendo aos riscos e ameaças à integridade, disponibilidade e confidencialidade das informações, dados e sistemas informáticos da PSP.	1.1
3	Sim, atendendo à tecnicidade e especificidade da segurança do ciberespaço.	1.2
4	Não respondeu.	1.4
5	Não respondeu.	
6	Imprescindível atendendo aos riscos e ameaças à integridade, disponibilidade e confidencialidade das informações, dados e sistemas informáticos da PSP.	1.1
7	Imprescindível atendendo aos riscos e ameaças à integridade, disponibilidade e confidencialidade das informações, dados e sistemas informáticos da PSP. Sim, composto por uma equipa técnica e operacional interna com capacidade de resolução de incidentes de cibersegurança e uma equipa de planeamento e estratégia que se responsabilizaria por formar, educar, treinar e sensibilizar a estrutura da PSP para as questões de segurança do ciberespaço.	1.1 1.3

Matriz de análise de conteúdo da questão 6 da entrevista.										
Categorias	**Unidades de registo**	**Entrevistados**							**Unidades de Enumeração**	**Resultados**
		1	2	3	4	5	6	7		
Criação na estrutura da PSP de um órgão especifico e especializado em matérias de Segurança do Ciberespaço	1.1 - Imprescindível atendendo aos riscos e ameaças à integridade, disponibilidade e confidencialidade das informações, dados e sistemas informáticos da PSP	x	x				x	x	4	57%
	1.2 - Sim, atendendo à tecnicidade e especificidade da segurança do ciberespaço.			x					1	14,2%
	1.3 - Sim, composto por uma equipa técnica e operacional interna com capacidade de resolução de incidentes de cibersegurança e uma equipa de planeamento e estratégia que se responsabilizaria por formar, educar, treinar e sensibilizar a estrutura da PSP para as questões de segurança do ciberespaço.							x	1	14,2%
	1.4 - Não respondeu.				x	x			2	28,6%

57% dos entrevistados considera imprescindível a criação na estrutura da PSP de um órgão especifico e especializado em matérias de Segurança do Ciberespaço, considerados os riscos e ameaças à integridade, disponibilidade e confidencialidade das informações, dados e sistemas informáticos da instituição. Já 14,2% concorda justificando-o com a tecnicidade e especificidade da segurança do ciberespaço, aditando que o mesmo deveria ser composto por uma equipa técnica e operacional interna com capacidade de resolução de incidentes de cibersegurança e uma equipa de planeamento e estratégia que se responsabilizaria por formar, educar, treinar e sensibilizar o dispositivo da PSP para as questões de segurança do ciberespaço. Registamos, por fim, que 28,6% não respondeu à questão formulada.

CONCLUSÕES

O trabalho seguiu um procedimento de escrita e de organização contemplando o procedimento metodológico, alinhando objetivos e perguntas na exploração do percurso tendente ao ensejo motivador do estudo.

Dedicámos o primeiro capítulo à ancoragem concetual da segurança do ciberespaço, abordando e definindo os conceitos estruturantes que sustentam o trabalho, a saber, ciberespaço; segurança do ciberespaço; ameaça; cibercriminalidade; capacidade de ciberdefesa; infraestrutura crítica; e prevenção da segurança do ciberespaço. Fizemo-lo, alicerçando-o na neutralidade epistemológica, sem prejuízo da complexidade de processos que são fenomenológicos e na completude, unidade e coerência face ordenamento jurídico. Compreende-se, pois, a preferência por definições dadas por conceitos normativos ou legais, sempre que tipificados nacional ou internacionalmente ou aclarados por organizações internacionais de que Portugal é parte, ao invés de conceitos ontológicos, tendencialmente proteiformes ou que sirvam interesses corporativos ou ideológicos, superando-se assim visões atomísticas que tomem como referência valores e representações próprias que concorram para um nevoeiro terminológico denso e aparentemente insuperável, que marca o panorama nacional.

Abordámos, no segundo capítulo, a caracterização estratégica da segurança do ciberespaço, sobrelevando-se a Era da Informação, que se consubstancia no domínio sobre a informação, encarada enquanto matéria-prima e fator de produção, e consequentemente sobre o conhecimento. A Sociedade em Rede, cujo motor de desenvolvimento assentou na internet e que tem origem na coincidência histórica de três processos independentes, a revolução da tecnologia da informação, a crise económica do capitalismo e do estatismo e a consequente reestruturação de ambos, que fizeram surgir uma nova estrutura social dominante. E a Sociedade de Risco, em que o desenvolvimento da ciência e da tecnologia já não permitem prever e controlar efetivamente os riscos e ameaças que contribuíram para criar. Resulta igualmente que o ciberespaço aduz características particulares à sua governação e regulação, que colocam em equação o entendimento de dois conceitos estruturantes e nucleares da ordem internacional e na conceção de Estado, a soberania e a segurança, num mundo crescentemente dependente, interligado e em rede, comprovado por dados da *Internet World Stats*. Assim, é igualmente

consensual que a garantia da segurança das infraestruturas tecnológicas, das redes e dos sistemas de informação depende da capacidade de os utilizadores finais saberem tomar medidas que previnam os riscos a que se encontram expostos, atento o vulgar, gradativo e inexorável predomínio da tecnologia digital, relevando-se então, estrategicamente, a educação, sensibilização e prevenção da segurança do ciberespaço e uma cultura global de cibersegurança.

Apresentámos no terceiro capítulo o enquadramento normativo da segurança do ciberespaço, patenteando, no âmbito do quadro comunitário, as principais organizações e normas e subsequentemente no quadro nacional, expusemos os normativos jurídicos mais relevantes e orientações estratégicas neste domínio. Concluímos que o quadro europeu aborda o ciberespaço como uma área de justiça onde os direitos humanos, incluindo o acesso às novas tecnologias, a liberdade de expressão, o direito à privacidade e a proteção dos dados pessoais devem ser preservados e onde a criminalidade concernente, através de um esforço cooperativo de todos os Estados membros, é prevenida, investigada em sede criminal e objeto de ulterior prossecução penal. Para tal concorre um acervo estratégico, doutrinário e normativo que densifica a sua definição de segurança do ciberespaço, traduzida nas precauções e ações que podem ser utilizadas para proteger o ciberespaço, tanto nos domínios civil como militar, contra as ameaças decorrentes da interdependência das suas redes e infraestruturas informáticas, procurando manter a sua integridade e disponibilidade e a confidencialidade das informações nelas contidas, ou que as possam danificar. As iniciativas comunitárias neste âmbito têm-se vindo a focar essencialmente na harmonização da legislação em matéria de cibercrime, através de disposições comuns relativamente a ataques contra os sistemas de informação e no desenvolvimento de políticas de proteção das infraestruturas críticas de informação, estabelecendo regras mínimas relativas à definição de infrações penais e de sanções aplicáveis, procurando igualmente maximizar a cooperação entre as autoridades competentes, nomeadamente as forças e serviços de segurança e outros serviços especializados dos Estados-Membros, bem como as agências e organismos especializados competentes da União Europeia, tais como a EUROJUST, a EUROPOL e designadamente o Centro Europeu de Cibercriminalidade e a Agência Europeia para a Segurança das Redes e da Informação. O desenvolvimento da sociedade

da informação, dominado pela globalização da troca de informação e pelo uso de tecnologias cada vez mais intrusivas na vida privada, tem igualmente acarretado desafios constantes no domínio da proteção da privacidade. Associada, está a necessidade de incrementar a utilização da Sociedade de Informação e a consequente Economia de Conhecimento, como instrumentos de crescimento económico, luta contra a infoexclusão e iliteracia digital, sendo que o objetivo geral é extrair benefícios económicos e sociais sustentáveis de um Mercado Único Digital, com base na internet e em aplicações interoperáveis.

No quadrante nacional, concluímos que a segurança do ciberespaço é concebida pela respetiva estratégia nacional como parte integrante da segurança nacional, referindo-a como essencial para o funcionamento do Estado, para o desenvolvimento económico e a inovação, bem como para a confiança dos cidadãos no mercado digital e no ciberespaço. Do seu escopo, resultam objetivos estratégicos e linhas de ação, consubstanciados em eixos de intervenção, com vista a uma eficaz gestão de crises, a uma coordenação da resposta operacional a ciberataques, a um desenvolvimento das sinergias nacionais e a uma intensificação da cooperação nacional, europeia e internacional neste domínio, assentando em princípios de subsidiariedade, complementaridade, proporcionalidade, sensibilização e cooperação entre públicos e privados. Concluímos que, intervindo-se de forma global no âmbito da segurança do ciberespaço e assentando a estratégia precisamente nos princípios indicados, seria pertinente dotá-lo de um quadro jurídico completo e estável da reserva de lei, porquanto a positivação da opção política numa mera Resolução do Conselho de Ministros assume-se manifestamente insuficiente e inconsequente no plano das garantias jurídico-constitucionais (Castro, Raquel, 2016). Admitindo também a estratégia que a responsabilidade pela segurança do ciberespaço nacional encontra-se distribuída por diferentes atores com missões e objetivos diversos, não existindo um fio condutor nem a coerência necessária nas políticas e iniciativas desenvolvidas por cada um deles, cabe também definir claramente a execução e articulação da capacidade de ciberdefesa, evitando-se sobreposições e duplicações que ponham em causa a agilidade dos processos e o pleno respeito do Estado de Direito Democrático e dos princípios enformadores das diferentes funções do Estado. Concomitantemente, concluímos, por um lado, que a ordem jurídica portuguesa é

marcada por uma indefinição legal de conceitos neste domínio, agravado pela urgência da clarificação do conceito de cibersegurança ou de segurança do ciberespaço e pela identificação rigorosa do seu objeto e do âmbito de aplicação do respetivo regime jurídico (Castro, Raquel, 2016). Por outro, resulta que, não tendo sido definidos os poderes de autoridade nacional competente em matéria de cibersegurança do Centro Nacional de Cibersegurança, relativamente ao Estado e aos operadores de infraestruturas críticas nacionais, tal competência é juridicamente inconsequente, porquanto é na qualidade de autoridade pública que um organismo atua quando está no âmbito do regime jurídico que lhe é próprio, não sendo o objeto ou o fim da atividade que importa, mas o regime jurídico a que está submetida[46].

Sistematizámos, no quarto capítulo, o âmbito de atuação e de cooperação da PSP no campo de ação da segurança do ciberespaço, atentas as suas atribuições e competências e os exatos termos da Estratégia Nacional de Segurança do Ciberespaço. A sua correlação, plasmada na figura 6 do presente, resulta num quadro harmonioso de inevitável, indelével e imprescindível repercussão, direta ou indiretamente, atentos os objetivos estratégicos, princípios e eixos enformadores da Estratégia Nacional. Concomitantemente, da caracterização do ambiente e clientes, internos e externos, das atribuições, competências e organização, sustentada igualmente em resultados da edição de 2015 do inquérito à utilização de TIC pela famílias e empresas do Instituto Nacional de Estatística e do Relatório Anual de Segurança Interna de 2015 no que ao ciberespaço diz respeito, decorre um diagnóstico da situação atual da PSP que concorre para a compaginação das opções, dos objetivos e, consequentemente, da definição de estratégias de atuação na segurança do ciberespaço.

Consagrámos no quinto capítulo a apresentação e discussão dos resultados do estudo de caso do tipo de exploração que incidiu sobre uma amostra não-probabilística ou empírica de tipo intencional, cujo fundamento de seleção obedeceu, criteriosamente, ao juízo do autor, nos exatos termos dos objetivos estratégicos, pilares e eixos de intervenção da Estratégia Nacional de Segurança

[46] Conforme Acórdão do Supremo Tribunal Administrativo, 2ª Secção, de 12-03-2014, N.º de Processo: 01060/13.

do Ciberespaço e na consequente relação com a organização departamental da Direção Nacional da PSP e respetivos cargos dirigentes.

Embora tenhamos procurado elaborar o guião de entrevista de forma ajustada às características culturais da população alvo e que o seu número de questões, seis, atendesse à sua disponibilidade de tempo, sublinhando-se a sua validação e envio atempado, conforme comprovado no Apêndice A, os resultados traduzem uma frequência significativa de respostas "não sei" ou "não respondo", que merecem ser cuidadas rigorosamente por poderem aduzir conclusões. De facto, este tipo de resposta pode ter interpretações diversas, pelo que não é correto dar-lhe uma interpretação unívoca de desconhecimento da matéria, podendo significar receio de emitir opinião, ou revelar uma atitude, ou estar associado à não compreensão das perguntas, ou traduzir falta de tempo para responder ao guião de entrevista (Quivy & Campenhoudt, 2005).

Apesar desta evidente limitação investigatória, do estudo exploratório é exequível consolidar conclusões à questão de investigação e às perguntas derivadas.

Assim, sem prejuízo da superficialidade revelada relativamente ao conhecimento do enquadramento jurídico nacional e internacional da segurança do ciberespaço, concluímos que o mesmo é suficiente e impele à definição de uma estratégia institucional da PSP, no quadro das relações institucionais que estabelece com outros organismos e em razão dos pilares de cooperação e de sensibilização que alicerçam a Estratégia Nacional de Segurança do Ciberespaço.

Contudo, concluímos, no que concerne à pergunta de partida, que não é evidente uma necessidade atual e premente de definição de uma estratégia institucional formal, atendendo ao estado embrionário do quadro legal e situacional da segurança do ciberespaço nacional, por não existir um fio condutor nem a coerência necessária nas políticas e iniciativas desenvolvidas neste domínio, apesar de terem sido identificados os eixos de Investigação Criminal, Formação e Segurança do Sistemas de Informação enquanto nucleares na sua equação.

Paradoxalmente, concluímos, pela ampla consonância revelada, que os riscos e ameaças à Segurança Interna são latentes e elevadas, afetando de forma transversal cidadãos, empresas e Estado, sendo que a segurança do ciberespaço é entendida como prioritária e estratégica para todos eles e, em particular, para a

PSP, o que entronca claramente na sua missão: assegurar a legalidade democrática, garantir a segurança interna e o livre exercício dos direitos fundamentais dos cidadãos, bem como o normal funcionamento das instituições democráticas.

Resulta, por fim, uma manifesta concordância da imprescindibilidade de criação na estrutura da PSP de um órgão específico e especializado em matéria de segurança do ciberespaço, considerados os riscos e ameaças à integridade, disponibilidade e confidencialidade das informações, dados e sistemas informáticos da instituição.

Os resultados obtidos, à luz da ancoragem conceptual, do enquadramento estratégico e normativo não nos permitem apresentar como resultado do presente trabalho qualquer proposta de estratégia institucional de Segurança do Ciberespaço. No entanto, os mesmos construtos abordados teoricamente e que suportaram o presente trabalho, permitem deixar uma hipótese para futuros trabalhos, a qual constitui o apêndice B, C e D, sem qualquer vínculo ou definição *ex ante* de enquadramento.

BIBLIOGRAFIA

Ascensão, O. (2001). *Criminalidade Informática*. In: Estudos sobre Direito da Internet e da Sociedade da Informação. Coimbra: Editora Almedina.

Benedikt, M. (1991). *Introduction to Cyberspace: first steps*, MIT Press. Retirado de http://services.exeter.ac.uk/cmit/media/texts/benedikt1991/introduction.pdf.

Beck, U. (1992), *Risk Society: Towards a New Modernity*, Londres, Sage Publications.

Beck, U. (2002), *La Sociedad del Riesgo Global*, trad. esp., Madrid, Siglo xxi.

Bendiek, A. (2012) *European cyber security policy*. Retirado do site de German Institute for International and Security Affairs. Retirado de http://www.swp-berlin.org/fileadmin/contents/ products/research_papers/2012_RP13_bdk.pdf

Cardoso, G. (2014). *Os Media na Sociedade em Rede* (2ª ed.). Lisboa: Fundação Calouste Gulbenkian.

Carvalho, Jorge Silva (2006). *Segurança Nacional e Informações*. Segurança e Defesa, n.º 1, 2006.

Castells, M. (1999), *A Era da Informação: Economia, Sociedade e Cultura*, vol. iii, São Paulo, Paz e Terra.

Castells, M. (2003). *O fim do milénio – A era da informação: Economia, sociedade e cultura* (Vol. 3). (A. Figueiredo, & R. Espanha, Trads.). Lisboa: Fundação Calouste Gulbenkian.

Castells, M. (2007). *A galáxia internet: Reflexões sobre internet, negócios e sociedade* (2ª ed.). (R. Espanha, Trad.). Lisboa: Fundação Calouste Gulbenkian.

Castells, M. (2011). *A Sociedade em rede* - A era da informação: Economia, sociedade e cultura (4ª ed., Vol. 1). (A. Lemos, C. Lorga, & T. Soares, Trads.). Lisboa: Fundação Calouste Gulbenkian.

Castro, Nuno Teixeira (2015) *Reflexões Quanto ao Impacto das Novas Tecnologias sobre a Legalidade Penal*, Relatório de Mestrado da disciplina de Cibercrime

(inédito), do Mestrado em Segurança da Informação e Direito do Ciberespaço, numa organização conjunta entre o IST, FDUL e Escola Naval.

Castro, Raquel Alexandra Brízida (2016). *Constituição e Ciberespaço: Argumentos para um "Direito Constitucional do Inimigo"?*. Cyberlaw by CIJIC, n.º 1, 204-243.

CCDCOE (2013). *Confidence Building Measures for Cyberspace – Legal Implications*. NATO Cooperative Cyber Defence Centre of Excelence, Tallinn.

Couto, Abel Cabral, General - (1988a) - *Elementos de Estratégia*; Vol I. Lisboa: IAEM.

Dias, P. (2014). *Viver na sociedade digital: Tecnologias digitais, novas práticas e mudanças sociais*. Cascais: Princípia Editora, Lda.

Denning, Dorothy E., (1999). *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*, Washington D.C. Retirado de http://www.nautilus.org/info-policy/workshop/papers/denning.htm.

Demchak, Chris e Dombrowski, Peter (2011). *Rise of Cybered Westephalian Age*. Strategic Studies Quarterly, vol 5, n.º 1, p. 32 - 61.

ENISA (2015). *CSIRT- Related capacity building activities*. ENISA. 2015 update.

Freire, F. V., & Caldas, A. (2013). *O Ciberespaço: Desafios à Segurança e à Estratégia*. Atena, 30, 90–168.

Freire, F. V., Nunes, V., Acosta, O., & Rojas, E. (2013). *Estratégia da informação e segurança no ciberespaço*. Cadernos do IDN, 12.

Fernandes, J. (2012). *Utopia, liberdade e soberania no ciberespaço. Nação e defesa*, 133, 11–31.

Fernandes, J. (2014). *Os desafios da segurança contemporânea: Estado, identidade e multiculturalismo*. Lisboa: Pedro Ferreira-Artes Gráficas, Lda.

FCCN. (2012). *Taxonomia comum para a rede Nacional de CSIRTs*. Retirado de http://www.cncs.gov.pt/cert-pt/documentos.

Gibson, William (1988). *Neuromante*, Lisboa, Gradiva, Col. «Contacto», n.º 4.

Klimburg, Alexander (2011). *Mobilising Cyber Power. Survival: Global Politics and Strategy*, vol. 53, nº 1, pp. 41-60.

Lévy, Pierre (2000). *O Ciberespaço, a Cidade e a Democracia Eletrónica*. Cibercultura, Lisboa, Instituto Piaget.

Marques, Garcia & Martins, Lourenço (2000). *Direito da Informática, Lições de Direito da Comunicação*, Almedina.

McLuhan, Marshall (1962). *The Gutenberg Galaxy: The Making of Typographic Man*. University of Toronto. Canada. Press - Social Science.

Pardal, Luís e Correia, Engénia (1995). *Métodos e Técnicas de Investigação Social***,** Porto, Areal Editores.

Quivy, R. & Campenhoudt, L. V. (2005). *Manual de Investigação em Ciências Sociais*, Lisboa, Gradiva.

Rodrigues, Benjamim Silva (2009). *Direito Penal – Parte Especial, Tomo I – Direito Penal Informático-Digital*, Coimbra Editora.

Schäfer, Wolf (2003). *The New Global History Toward a Narrative for Pangaea Two*. State University of New York at Stony Brook, Department of History. EUA.

Toffler, Alvin (2003). *A Terceira Vaga*, Livros do Brasil, Lisboa.

Valente, M. M. (2013). *Segurança: um tópico jurídico em construção*. Lisboa: Âncora Editora.

Wegener, Alfred (1929). *The Origin of Continents and Oceans*. (4th edition). Translated from the Fourth Revised German Edition by John Biram with an Introduction by B. C. King. London. Methuen and Co.

Wiener, Norbert (1948). *Cybernetics or Control and Communication in the Animal and the Machine*. Tradução espanhola, Barcelona, Tusquets Editores, Col. Metatemas, nº 8, 2.ª ed., 1998.

Documentos oficiais dos órgãos da União Europeia

Tratado de Lisboa que altera o Tratado da União Europeia e o Tratado que institui a Comunidade Europeia, assinado em Lisboa em 13 de dezembro de 2007 JO C 306 de 17.12.2007, p. 1).

Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao

tratamento de dados pessoais e à livre circulação desses dados (JO L 281 de 23.11.1995, p. 31).

Diretiva 2000/31/CE do Parlamento Europeu e do Conselho, de 8 de junho de 2000, relativa a certos aspetos legais dos serviços da sociedade de informação, em especial do comércio eletrónico, no mercado interno (JO L 178, 17.7.2000, p. 1).

Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (JO L 201 de 31.7.2002, p. 37).

Diretiva 2007/64/CE do Parlamento Europeu e do Conselho, de 13 de novembro de 2007, relativa aos serviços de pagamento no mercado interno (JO L 319 de 5.12.2007, p.1).

Diretiva 2008/114/CE do Conselho, de 8 de dezembro de 2008, relativa à identificação e designação das infraestruturas críticas europeias e à avaliação da necessidade de melhorar a sua proteção (JO L 345 de 23.12.2008, p. 75—82).

Diretiva 2013/40/UE do Parlamento Europeu e do Conselho, de 12 de agosto de 2013, relativa a ataques contra os sistemas de informação e que substitui a Decisão-Quadro 2005/222/JAI do Conselho (JO L 218 de 14.8.2013, p. 8—14).

Comissão Europeia, Proposta de Diretiva do Parlamento Europeu e do Conselho relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União» COM (2013) 48 final.

Decisão-Quadro 2008/977/JAI do Conselho, de 27 de novembro de 2008, relativa à proteção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal (JO L 350 de 30.12.2008, p. 60).

Decisão - Quadro 2005/222/JAI, relativa a ataques contra os sistemas de informação (JO L 69 de 16.3.2005, p. 67).

Decisão 2014/415/UE do Conselho, de 24 de junho de 2014, relativa às regras de execução da cláusula de solidariedade pela União (JO L 192 de 1.7.2014, p. 53).

Regulamento (CE) 45/2001/CE do Parlamento Europeu e do Conselho, de 18 de dezembro de 2000, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados, JO L 8 de 12.1.2001, pp. 1-22.

Regulamento (CE) n.º 460/2004 que cria a Agência Europeia para a Segurança das Redes e da Informação, (JO L 77 de 13.3.2004, p. 1).

Resolução do Parlamento Europeu, de 25 de novembro de 2009, relativa à Comunicação da Comissão ao Parlamento Europeu e ao Conselho – Um espaço de liberdade, segurança e justiça ao serviço dos cidadãos – Programa de Estocolmo.

Quadro Estratégico da UE para a Ciberdefesa (Consilium 15585/14].

Comunicação da Comissão ao Parlamento Europeu, ao Conselho e ao Comité das Regiões: Rumo a uma política geral de luta contra o cibercrime [COM (2007) 267 final de 22 de maio de 2007]

Comunicação Conjunta intitulada “Estratégia da União Europeia para a cibersegurança: Um ciberespaço aberto, seguro e protegido”, fevereiro de 2013 [JOIN (2013) 1].

Parecer do CESE sobre a Sociedade da Informação Segura (JO C 97 de 28.4.2007, p. 21).

Parecer do Comité sobre o Novo regulamento relativo à ENISA (JO C 107 de 6.4.2011, p. 58).

Parecer do CESE sobre fazer progredir a Internet (JO C 175 de 28.7.2009, p. 92).

Parecer do CESE sobre Proteção das infraestruturas críticas da informação (JO C 255 de 22.9.2010, p. 98).

Parecer do CESE sobre Uma Agenda Digital para a Europa, (JO C 54 de 19.2.2011, p. 58).

COM (2001) 298 final (Segurança das redes e da informação: Proposta de abordagem de uma política europeia).

COM (2004) 702 final (Proteção das infraestruturas críticas no âmbito da luta contra o terrorismo).

COM (2006) 251 final (Estratégia para uma sociedade da informação segura).

COM (2006) 786 final (Programa Europeu de Proteção das Infraestruturas Críticas).

COM (2009) 149 final (Proteger a Europa contra os ciberataques e as perturbações em grande escala: melhorar a preparação, a segurança e a resiliência).

COM (2010) 2020 (Sobre uma estratégia para um crescimento inteligente, sustentável e inclusivo).

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

Comissão Europeia. (2014). *Compreender as políticas da União Europeia: Agenda Digital para a Europa.*

Conselho da Europa. (2001). Convenção sobre o cibercrime.

Legislação

Constituição da República Portuguesa.

Código Penal

Código de Processo Penal

Lei n.º 67/98, de 26 de outubro. *Diário da República*, 1.ª Série, n.º 247, 5536-5546. Assembleia da República. (Lei da Proteção de Dados Pessoais. Transpõe para a ordem jurídica interna a Diretiva n.º 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de outubro de 1995).

Lei n.º 9/2007, de 19 de fevereiro. *Diário da República*, 1.ª Série, n.º 35, 1238-1252. Assembleia da República. (Estabelece a orgânica do Secretário-Geral do Sistema de Informações da República Portuguesa, do Serviço de Informações Estratégicas de Defesa e do Serviço de Informações de Segurança).

Lei n.º 49/2008, de 27 de agosto. *Diário da República*, 1.ª Série, n. º165, 6038-6042. Assembleia da República. (Aprova a Lei da Organização de Investigação Criminal).

Lei n.º 53/2007, de 31 de agosto. *Diário da República*. 1ª Série, n.º 168, Assembleia da República. (Aprova a orgânica da Polícia de Segurança Pública).

Lei n.º 53/2008, de 29 de agosto. *Diário da República*, 1.ª Série, n.º 167, 6135-6141. Assembleia da República. (Aprova a Lei de Segurança Interna).

Lei n.º 109/2009, de 15 de setembro. *Diário da República*, 1.ª Série, n.º 179, 6319-6325. Assembleia da República. (Aprova a Lei do Cibercrime, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de fevereiro).

Decreto-Lei, n.º 275/2009, de 02 de outubro. Diário da República, 1.ª série — n.º 192, Ministério da Administração Interna. (Aprova o Estatuto do Instituto Superior de Ciências Policiais e Segurança Interna).

Lei n.º 34/2013, de 16 de maio. *Diário da República,* 1.ª Série, n.º 94, 2921-2942. Assembleia da República. (Estabelece o regime do exercício da atividade de segurança privada e procede à primeira alteração à Lei n.º 49/2008, de 27 de agosto, no concernente às competências da Polícia Judiciária em matéria de investigação criminal).

Decreto-Lei n.º 62/2011 de 9 de maio. *Diário da República*, 1.ª Série, n.º 89, 2624-2627. Ministério da Defesa Nacional. (Estabelece os procedimentos de identificação e de proteção das infraestruturas essenciais para a saúde, a segurança e o bem-estar económico e social da sociedade nos setores da energia e transportes e transpõe a Diretiva n.º 2008/114/CE, de 8 de dezembro).

Decreto-Lei n.º 69/2014, de 9 de maio. *Diário da República*, 1.ª Série, n.º 89, 2712-2719. Presidência do conselho de Ministros. (Aprova a orgânica do Gabinete Nacional de Segurança, estabelecendo os termos do funcionamento do Centro Nacional de Cibersegurança).

Resolução do Conselho de Ministros n.º 12/2012, de 7 de fevereiro. *Diário da República*, 1.ª série, n.º 27, 596-605. (Aprova as linhas gerais do plano global estratégico de racionalização e redução de custos com as TIC na Administração Pública).

Resolução do Conselho de Ministros n.º 19/2013, de 21 de março. *Diário da República*, 1.ª Série, n.º 67, 1981-1995. Presidência do Conselho de Ministros. (Aprova o Conceito Estratégico de Defesa Nacional).

Resolução do Conselho de Ministros n.º 26/2013, de 19 de abril. *Diário da República*, 1.ª Série, n.º 77, 2285-2289. Presidência do Conselho de Ministros. (Aprova as linhas de orientação para a Reforma «Defesa 2020»).

Resolução do Conselho de Ministros n.º 42/2012, de 13 de abril. *Diário da República*, 1.ª Série, n.º 74, 1925-1926. Presidência do Conselho de Ministros. (Cria a Comissão Instaladora do Centro Nacional de Cibersegurança).

Despacho n.º 13692/2013 de 28 de outubro. *Diário da República*, 2.ª Série, n.º 208, 31976-31979. Ministério da Defesa Nacional. (Determina a publicação da diretiva iniciadora com a orientação política para a ciberdefesa).

Documentos institucionais

Diretiva Estratégica n.º 10/2006, de 15 de maio, que cria o Programa Integrado de Policiamento de Proximidade - atualmente designado por Modelo Integrado de Policiamento de Proximidade – Direção Nacional da PSP.

Grandes Opções Estratégicas da PSP 2013-2016, de 26 de março de 2012. Direção Nacional da PSP.

Relatório de Atividades da PSP de 2014. Direção Nacional da PSP. Homologado por S.Exa. a Ministra da Administração Interna em 18 de fevereiro de 2016.

Visão Global de Operacionalização da Estratégia para as TIC na PSP 2013-2016, de outubro de 2013. Direção Nacional da PSP.

APÊNDICE A

GUIÃO DE ENTREVISTA

POLÍCIA SEGURANÇA PÚBLICA
INSTITUTO SUPERIOR DE CIÊNCIAS POLICIAIS E SEGURANÇA INTERNA
DIREÇÃO DE ENSINO
SECRETARIA ESCOLAR

Exmo. Senhor
Diretor Nacional Adjunto/Unidade Orgânica de
Recursos Humanos
(Departamento de Formação)
DN/PSP - Largo da Penha de França, 1

Sua Referência:
Sua Comunicação:
Nossa Referência: 195/SECDE/2016
Classificador: M/148121
Processo: SECDE201600001CCD
Data: 2016-05-04
Assunto: PEDIDO DE COLABORAÇÃO PARA A REALIZAÇÃO DO RELATÓRIO FINAL DO CCDP

Diretor Nacional Adjunto/UORH
José Ferreira de Oliveira
Superintendente-Chefe

1. O Curso de Comando e Direção Policial (CCDP), no seu plano de estudos, aprovado pela Portaria n.º 199/2014, de 3 de outubro, compreende a elaboração de um relatório final, conforme o art.º 4.º, n.ºs 2 e 4, da referida portaria, que deverá, obrigatoriamente, incidir sobre um dos temas aprovados por despacho de SEXA o Diretor Nacional da PSP, de 29 de outubro de 2014.

2. Neste sentido, o Comissário M/148121, Nuno Miguel Alves e Silva, irá realizar o seu relatório final subordinado ao tema "Enquadramento estratégico, concetual e normativo da Segurança do Ciberespaço: subsídios para a definição de uma estratégia institucional da Polícia de Segurança Pública", do qual é Orientador o Intendente Rui Filipe Resende Coelho de Moura.

3. Deste modo, solicita-se a V.ª Ex.ª autorização para a aplicação de uma entrevista, da qual se envia o guião, aos Exmos. Srs. Oficiais:

a) Diretor do Departamento de Operações - Superintendente Luís Filipe Cardoso de Sousa Simões;

b) Diretor do Departamento de Informações Policiais - Superintendente Luís Miguel Fiães Fernandes;

c) Diretor do Departamento de Investigação Criminal - Superintendente José Carlos Bastos Leitão;

R. 1º de Maio, nº3 1349-040 Lisboa Tel.: 213613900 Fax: 213610535 www.iscpsi.pt | iscpsi@psp.pt

DIREÇÃO NACIONAL PSP/ DAG — Entrada Nº 14527
SECÇÃO CORRESPONDÊNCIA — Data 09 MAIO 2016
PO 3FOS
10/5/16

135573
Pagina1/2

d) Diretor do Departamento de Formação - Superintendente João Manuel Alves Amado;

e) Diretor do Departamento de Sistemas de Informação e Comunicações - Superintendente João Carlos Jesus Filipe Ribeiro; e

f) Diretora do Gabinete de Sistemas de Informação - Dr.ª Lurdes Rosa.

4. Os dados a obter tornam-se imprescindíveis para o desenvolvimento do Relatório Final.

5. Mais se informa V.ª Ex.ª que o Comissário Nuno Silva se compromete ao dever de confidencialidade e anonimato, relativamente aos dados recolhidos, fora do âmbito do seu trabalho.

O Diretor

Pedro José Lopes Clemente
Superintendente-Chefe

R. 1º de Maio, nº3 1349-040 Lisboa Tel.: 213613900 Fax: 213610535 www.iscpsi.pt | iscpsi@psp.pt

GUIÃO DE ENTREVISTA

O Curso de Comando e Direção Policial integra uma componente letiva e compreende a realização de um relatório final sobre uma temática relevante para a segurança interna de entre as previamente definidas por Despacho exarado por S.Exa. o Diretor Nacional da PSP.

Neste sentido, Nuno Miguel Alves e Silva, Comissário, N/M148121, subordinará o seu estudo sobre o macro tema n.º 12 – Dimensões da Segurança Interna, tendo como objeto: *Enquadramento estratégico, concetual e normativo da segurança do ciberespaço: Subsídios para a definição de uma estratégia institucional da PSP*, do qual é orientador o Sr. Intendente Rui Filipe Resende Coelho de Moura, Diretor do Gabinete de Estudos e Planeamento da Direção Nacional da PSP.

Ambicionando a solidez, fundamentação e a credibilidade dos dados analisados, deseja recorrer a entrevistas semi-estruturadas, validadas e aplicadas a cargos dirigentes da PSP.

Assim, presente entrevista insere-se no âmbito do Relatório Final do Curso de Comando e Direção Policial, ministrado pelo Instituto Superior de Ciências Policiais e Segurança Interna, habilitante de promoção à categoria de subintendente na carreira de oficial de polícia e não conferente de grau académico.

Centrando-se numa investigação qualitativa e tendo como âmbito de estudo e campo geral de investigação, a segurança do ciberespaço, o Relatório Final que sustenta a presente entrevista tem como objetivo equacionar a definição de uma estratégia institucional da Polícia de Segurança Pública em matéria de segurança do ciberespaço, perspetivando, nacional e internacionalmente, o respetivo enquadramento estratégico, concetual e normativo.

(1) Na sua opinião, qual a importância estratégica da segurança do ciberespaço para o País e em particular para a PSP?

(2) Como caracteriza os riscos e ameaças do ciberespaço relativamente à Segurança Interna?

(3) O enquadramento legal nacional e internacional aplicável à segurança do ciberespaço é suficiente para a definição de uma estratégia institucional da PSP? Porquê?

(4) O quadro de atuação e de cooperação da PSP no domínio da Segurança do Ciberespaço impele à definição de uma estratégia institucional respetiva? Porquê?

(5) Na eventual definição de uma estratégia institucional da PSP em matéria de segurança do ciberespaço, que competências conceberia para o Departamento que dirige?

(6) Considera adequada a criação na estrutura da PSP de um órgão especifico e especializado em matérias de Segurança do Ciberespaço? Porquê?

APÊNDICE B

Modelo concetual de edificação de uma capacidade de prevenção e resposta a incidentes de segurança no ciberespaço

Procurando dotar as entidades do Estado e os operadores de infraestruturas críticas nacionais com as valências mínimas para a análise, a mitigação e a resolução de incidentes de segurança no ciberespaço, o Centro Nacional de Cibersegurança, através de um modelo de maturidade[47], definiu um conjunto de capacidades – técnicas, humanas e processuais – que constituem uma base harmonizada e desejável nesta matéria, visando igualmente integrar as entidades no ecossistema nacional de segurança do ciberespaço e criar condições para uma melhoria sustentada das mesmas.

Com efeito, é esperado que as entidades de maior dimensão ou que executam funções críticas, como pode ser entendida a PSP, possuam as seguintes capacidade e funcionalidades:

- Tenha definido um ponto de contato e articule com o CNCS a reação a incidentes de cibersegurança.
- Tenha identificadas as áreas de atividade e serviços considerados críticos ou vitais e realize gestão de ativos para as mesmas.
- Colete e armazene metadados de comunicações eletrónicas e outros registos de serviços informáticos necessários para a análise de incidentes.
- Detenha um conjunto de instrumentos técnicos e serviços, autónomos ou contratados, para mitigação dos tipos de ciberataques mais comuns.
- Possua os recursos humanos com as competências necessárias para realizar grande parte das investigações forenses necessárias e articule com eficácia com o CNCS.
- Tenha aprovados e implementados procedimentos internos de resposta a incidentes de cibersegurança;

[47] Vide http://www.cncs.gov.pt/media/2015/06/Roadmap-Capacidades-Minimas.pdf

- Tenha definida a estrutura e a cadeia de responsabilidade nesta matéria e realize, periodicamente, simulacros de cibersegurança;
- Possua uma equipa dedicada à reação a incidentes de cibersegurança – CSIRT;
- Colabore em projetos de desenvolvimento e partilhe informação de cibersegurança de uma forma regular dentro da comunidade nacional de CSIRT; e
- Participe em exercícios nacionais e internacionais de cibersegurança.

Para tal, pela sua densidade, recorremos rigorosamente ao Modelo concetual de edificação de capacidades de prevenção e resposta a incidentes de segurança do ciberespaço da ENISA (ENISA, 2015), o qual teoriza-se numa lógica de prestação de serviços, entendidos enquanto instrumentos plurais concatenados e não como fim em si mesmos. Assim, podem ser agrupados em três categorias fundamentais, a saber, Serviços reativos; Serviços proativos e Serviços de gestão da qualidade de segurança, nomeadamente:

Serviços Reativos	Serviços Proativos	Serviços de Gestão da Qualidade da Segurança
✓Alertas e avisos; ✓Gestão de incidentes; • Análise de incidentes; ➢ Recolha de provas forenses ➢ Rastreio ou localização • Apoio na resposta a incidentes • Coordenação da resposta a incidentes • Resposta a incidentes no local ✓Gestão de vulnerabilidades; • Análise de vulnerabilidades • Resposta a vulnerabilidades • Coordenação da resposta a vulnerabilidades ✓Gestão de artefactos; • Análise de artefactos; • Resposta a artefactos; • Coordenação da resposta a artefactos.	✓Recomendações; ✓Observatório Social e de Tecnologia; ✓Auditorias ou avaliações de segurança; • Verificação de infraestrutura • Verificação de melhores práticas • Exame • Testes de penetração ✓Configuração e manutenção de ferramentas, aplicações e infraestruturas; ✓Desenvolvimento de ferramentas de segurança; ✓Serviços de deteção de intrusões; ✓Difusão de informações relacionadas com a segurança.	✓ Análise dos riscos; ✓ Continuidade da atividade e planificação da recuperação de emergência ✓ Consultoria de segurança; ✓ Prevenção e sensibilização; ✓ Formação; ✓ Avaliação ou certificação de produtos.

1. **Serviços reativos -** Os serviços reativos são concebidos para responder a pedidos de assistência, a notificações de incidentes e a quaisquer ameaças ou ataques contra sistemas. Estes podem ser desencadeados por notificação de terceiros, por monitorização e ou por registos e alertas dos sistemas de deteção de intrusões. Conceptualmente, incluem-se nos serviços recativos os Alertas e avisos; a Gestão de Incidentes; a Gestão de Vulnerabilidades e a Gestão de artefactos.

   1.1. **Alertas e avisos -** Envolve a divulgação de informações que descrevam ataques, vulnerabilidades de segurança, alertas de intrusão, vírus informáticos ou falsos alarmes e a rápida divulgação de recomendações para enfrentar os problemas. O alerta, aviso ou recomendação é enviado como reação ao problema em causa, a fim de informar os utilizadores da atividade e de os ajudar a proteger os seus sistemas ou a recuperar os sistemas eventualmente afetados.

   1.2. **Gestão de incidentes -** A gestão de incidentes inclui a receção, triagem e resposta a solicitações e notificações, bem como a análise de incidentes e ocorrências. Casuisticamente, as atividades de resposta podem incluir a (i) Tomada de medidas tendentes a proteger sistemas e redes afetados ou ameaçados pela atividade de intrusos; (ii) Apresentação de soluções e de estratégias de atenuação a partir das recomendações ou alertas pertinentes; (iii) Busca de atividade de intrusos noutras partes da rede; (iv) Filtragem do tráfego da rede; (v) Reconstrução de sistemas; (vi) Correção ou reparação de sistemas; e (vii) Desenvolvimento de alternativas ou de estratégias de solução provisória. Atendendo a que as atividades de gestão de incidentes poderão ser executadas de diversas formas, importará subcategoriza-las em função do seu tipo e da assistência prestada, nomeadamente a Análise de incidentes; Resposta a incidentes no local; o Apoio na resposta a incidentes; e a Coordenação da resposta a incidentes:

      1.2.1. **Análise de incidentes** - Essencialmente, a análise de um incidente consiste no exame de todas as informações disponíveis e das provas ou artefactos de apoio relacionados com um incidente ou ocorrência. A análise tem por objetivo identificar (i) o âmbito do incidente, (ii) a extensão dos danos causados pelo incidente, (iii) a natureza do

incidente e (iv) as estratégias de resposta ou soluções provisórias. Dois subserviços podem ser prestados no âmbito da análise de incidentes, em função da missão, dos objetivos e dos processos, designadamente a Recolha de provas forenses e o Rastreio ou localização.

1.2.1.1. Recolha de provas forenses - Abarca a recolha, preservação, documentação e análise de provas num sistema informático comprometido, a fim de determinar alterações ao sistema e apoiar a reconstrução das ocorrências conducentes a essa situação. As tarefas inerentes à recolha de provas forenses incluem, embora não se limitem (i) à realização de cópias de imagens digitais do disco rígido do sistema afetado; (ii) à verificação de mudanças no sistema, como novos programas, ficheiros, serviços e utilizadores; (iii) à observação de processos em curso; e (iv) à procura de programas e ferramentas intrusivas.

1.2.1.2. Rastreio ou localização - Compreende a localização da origem de um intruso ou a identificação de sistemas a que o intruso teve acesso. Esta atividade pode incluir (i) a tentativa de identificação do intruso; (ii) o rastreio ou a localização da forma como o intruso invadiu os sistemas afetados e as redes conexas, (iii) quais os sistemas utilizados para conseguir esse acesso, (iv) qual o ponto de origem do ataque e (v) que outros sistemas e redes foram utilizados no quadro do ataque.

1.2.1.3. Resposta a incidentes no local - Envolve apoio direto, no local, colaborando na recuperação de um determinado incidente. Neste caso, analisa fisicamente os sistemas afetados e dirige a reparação e a recuperação dos sistemas, não se limitando a assegurar um apoio de resposta ao incidente por telefone ou por correio eletrónico. Este serviço inclui as medidas de nível local necessárias em caso de suspeita ou de ocorrência de incidente.

1.2.1.4. Apoio na resposta a incidentes - Assiste e orienta a vítima do ataque na recuperação de um incidente, por telefone, e-mail, fax ou documentação diversa. Pode igualmente implicar a prestação

de assistência técnica na interpretação dos dados recolhidos; o fornecimento de contactos ou a emissão de orientações sobre estratégias de atenuação e de recuperação. Contudo, não implica ações diretas de resposta a incidentes, limitando-se o serviço à prestação de orientação à distância visando a recuperação.

1.2.1.5. Coordenação da resposta a incidentes - Coordena o esforço de resposta das partes envolvidas no incidente, que são, em princípio, a vítima do ataque, outros sítios envolvidos no ataque e quaisquer sítios que requeiram assistência na análise do ataque. Pode incluir igualmente as partes que prestam apoio em TI à vítima, como prestadores de serviços, outras equipas de resposta a incidentes e os administradores de sistema e de rede locais. O trabalho de coordenação pode ainda implicar a recolha de contactos, a notificação de sítios sobre o seu potencial envolvimento (enquanto vítima ou fonte de um ataque), a recolha de dados estatísticos sobre o número de sítios envolvidos e a facilitação do intercâmbio e da análise de informações. Parte do trabalho de coordenação pode também acarretar a notificação e a colaboração com consultores jurídicos, departamentos de recursos humanos e de relações públicas de determinada organização, bem como a coordenação com as autoridades judiciárias e/ou forças e serviços de segurança.

1.2.2. Gestão das vulnerabilidades - A gestão das vulnerabilidades contempla a (i) receção de informações sobre vulnerabilidades de hardware e software, (ii) a análise da natureza, mecânica e efeitos das vulnerabilidades e (iii) o desenvolvimento de estratégias de resposta para deteção e reparação de vulnerabilidades. Atendendo a que as atividades de gestão das vulnerabilidades poderão ser executadas variadamente, importará subclassificá-las em função do tipo e da assistência prestada, nomeadamente em Análise das vulnerabilidades; Resposta às vulnerabilidades e Coordenação da resposta às vulnerabilidades.

1.2.2.1. Análise das vulnerabilidades - Procede a análises técnicas e a exames de vulnerabilidades de hardware ou de software que incluem a verificação de suspeitas de vulnerabilidades e o exame técnico da vulnerabilidade do hardware ou do software, com vista a determinar onde se situa e de que modo pode ser explorada. A análise pode incluir a verificação do código-fonte, com recurso a um programa de correção, a fim de determinar onde ocorre a vulnerabilidade, ou a tentativa de reproduzir o problema num sistema de teste.

1.2.2.2. Resposta às vulnerabilidades - Consiste em determinar a resposta adequada para atenuar ou reparar a vulnerabilidade. Esta atividade pode incluir o desenvolvimento ou a pesquisa de correções, reparações e soluções provisórias. Pode ainda acarretar a notificação da estratégia de atenuação a terceiros, nomeadamente através da formulação e difusão de recomendações e/ou alertas.

1.2.2.3. Coordenação da resposta às vulnerabilidades - Inclui a facilitação da análise de uma vulnerabilidade ou do relatório de vulnerabilidade, a coordenação dos calendários de lançamento dos documentos e das correções ou soluções provisórias correspondentes, e a síntese da análise técnica realizada por diferentes partes. Este serviço pode ainda incluir a manutenção de um arquivo ou base de conhecimentos, pública ou privada, de informações sobre as vulnerabilidades e as estratégias de resposta correspondentes.

1.3. Gestão de artefactos - Um artefacto é qualquer ficheiro ou objeto encontrado num sistema suscetível de estar relacionado com a exploração ou o ataque de sistemas e redes, ou que esteja a ser utilizado para contornar medidas de segurança. A gestão dos artefactos implica a receção de informações sobre os artefactos utilizados em ataques de intrusão, reconhecimento e noutras atividades não autorizadas ou perturbadoras, e de cópias dos mesmos. Depois de recebidos, os artefactos são analisados. Essa análise incide na natureza, mecânica, versão e utilização do artefacto

em causa, sendo em seguida desenvolvidas (ou sugeridas) estratégias de resposta para a deteção, remoção ou defesa contra o artefacto. Atendendo a que a atividade de gestão de artefactos poderá ser executada de diversas formas, este serviço é subclassificado em função do tipo de atividade executada e do tipo de assistência prestada, designadamente a Análise de artefactos; a Resposta aos artefactos; e a Coordenação da resposta aos artefactos.

1.3.1. Análise de artefactos - Serviço que procede ao exame e análise técnicos de todos os artefactos encontrados num sistema. A análise efetuada pode incluir a identificação do tipo de ficheiro e da estrutura do artefacto, a comparação de um novo artefacto com artefactos existentes ou com outras versões do mesmo artefacto, a fim de detetar a semelhanças e as diferenças, ou ainda a engenharia inversa ou a desmontagem do código, para determinar a finalidade e a função do artefacto.

1.3.2. Resposta aos artefactos - Inclui a determinação das medidas adequadas para detetar e remover artefactos de um sistema, bem como medidas para impedir a instalação de artefactos, o que pode implicar a criação de assinaturas adicionáveis ao software antivírus ou ao sistema de deteção de intrusão.

1.3.3. Coordenação da resposta aos artefactos - Implica partilhar e sintetizar os resultados das análises e as estratégias de resposta adequadas a um artefacto com outros investigadores, equipas de resposta a incidentes informáticos, fornecedores e outros peritos em segurança. As atividades incluem a notificação de terceiros e a síntese de análises técnicas de diversas fontes. Podem ainda incluir a manutenção de um arquivo, público ou reservado aos utilizadores, de artefactos conhecidos, do seu impacto e das estratégias de resposta correspondentes.

2. **Serviços proativos -** Os serviços proativos são concebidos para melhorar a infraestrutura e os processos de segurança da comunidade de utilizadores antes de se registar ou de ser detetado qualquer incidente ou ocorrência. Os seus

principais objetivos consistem em evitar incidentes e reduzir o seu impacto e extensão quando se registam. Incluem-se nos serviços proactivos as Recomendações; o Observatório de tecnologia; as Auditorias ou avaliações de segurança; a Configuração e manutenção de ferramentas de segurança, aplicações, infraestruturas e serviços; o Desenvolvimento de ferramentas de segurança; os Serviços de deteção de intrusão; e a Difusão de informações relacionadas com a segurança.

2.1. **Recomendações -** Incluem alertas de intrusão, avisos de vulnerabilidade e recomendações de segurança, com o intuito de informar os utilizadores sobre novas evoluções com impacto de médio-longo prazo, como vulnerabilidades recém-detetadas ou novas ferramentas de intrusão.

2.2. **Observatório Social e de Tecnologia -** Acompanha e observa novos progressos técnicos, atividades de intrusão e tendências conexas, a fim de contribuir para a identificação de ameaças futuras. Os tópicos analisados devem ter em conta medidas legais e legislativas, ameaças sociais ou políticas e tecnologias emergentes. Desenvolve e otimiza modelos de análise e avaliação do risco, de forma a garantir a produção de produtos informacionais adequados ao apoio e fundamentação da decisão, diminuindo os índices de incerteza das mesmas pelos vários níveis resolutivos. Apoia a tomada de decisão estratégica através da produção de avaliações de risco e acompanha os fenómenos geradores de insegurança no ciberespaço, com vista a prevenir, conter e neutralizar situações que representem riscos para os Direitos Fundamentais dos cidadãos. Realiza estudos e relatórios analíticos, de carácter estratégico, sobre tendências Ilícitas no quadro da Segurança do Ciberespaço. Incrementa a recolha específica e completa dos dados estatísticos necessários à avaliação e análise científica da sua atividade. Efetua o acompanhamento permanente do fenómeno da violência e radicalismo no ciberespaço. Este serviço implica o acompanhamento de listas de endereços securizadas, sítios Web dedicados à segurança, bem como notícias e artigos de imprensa nos domínios da ciência, tecnologia, política e governação, a fim de extrair informações pertinentes para a segurança dos sistemas e redes dos utilizadores.

2.3. Auditorias ou avaliações de segurança - Assegura a verificação e a análise aprofundadas da infraestrutura de segurança, com base nos requisitos definidos pela mesma ou por outras normas setoriais aplicáveis. Pode ainda incluir uma avaliação das práticas de segurança das organizações. Podem ser executados diferentes de auditorias ou avaliações, incluindo a Verificação da infraestrutura; o Exame e Testes de penetração.

2.3.1. Verificação da infra-estrutura - Verificação manual das configurações de hardware e software, routers, firewalls, servidores e dispositivos de desktop, no intuito de garantir que estes correspondem às melhores práticas das políticas de segurança da organização ou do setor e às configurações-tipo.

2.3.2. Exame - Atividade desenvolvida com recurso a scanners de vulnerabilidade ou de vírus, a fim de identificar sistemas e redes vulneráveis.

2.3.3. Testes de penetração - Desenvolvimento de um conjunto comum de práticas contra as quais os testes ou avaliações são conduzidos, a par do desenvolvimento de um conjunto de aptidões requeridas ou de requisitos de certificação para quem executa os testes, avaliações, auditorias ou análises.

2.4. Configuração e manutenção de ferramentas, aplicações, infraestruturas e serviços - Identifica e fornece orientações sobre a forma de configurar e manter em segurança ferramentas, aplicações e a infraestrutura informática geral utilizada pela comunidade de utilizadores. Para além de fornecer orientações, poderá proceder a atualizações das configurações e à manutenção das ferramentas e serviços de segurança, como sistemas de deteção de intrusões (IDS), exploração da rede ou sistemas de acompanhamento, filtros, wrappers, firewalls, redes virtuais privadas ou mecanismos de autentificação.

2.5. Desenvolvimento de ferramentas de segurança - Inclui o desenvolvimento de ferramentas novas e destinadas exclusivamente aos utilizadores que sejam solicitadas ou desejadas pela comunidade de

utilizadores. Paralelamente, abarca o desenvolvimento de correções de segurança para software adaptado utilizado pela comunidade de utilizadores ou distribuições securizadas de software para reconstrução de sistemas centrais comprometidos. Poderá igualmente envolver o desenvolvimento de ferramentas ou roteiros que aumentem o número de funcionalidades dos instrumentos de segurança existentes, como uma nova ligação a um scanner de vulnerabilidades ou da rede a roteiros que facilitem a utilização de tecnologia de cifragem ou a mecanismos automatizados de distribuição de correções.

2.6. **Serviços de deteção de intrusão -** Revê os registos IDS existentes, analisa e inicia respostas para todas as ocorrências que correspondam ao limiar que definiu, ou reencaminha os alertas nos termos de um acordo de nível de serviços predefinido ou com uma estratégia em escalada.

2.7. **Difusão de informações relacionadas com a segurança -** Fornece aos utilizadores uma recolha exaustiva e de fácil consulta de informações úteis para os ajudar a melhorar a segurança. Essas informações podem incluir: (i) diretrizes de notificação e contactos de emergência; (ii) arquivos de alerta, avisos e outras comunicações; (iii) documentação sobre as melhores práticas atuais; (iv) orientações gerais de segurança informática; (v) políticas, procedimentos e listas de verificação; (vi) desenvolvimento de proteções e informações de distribuição; (vii) ligações a fornecedores; estatísticas e tendências atuais em matéria de notificação de incidentes; (viii) outras informações suscetíveis de melhorar as práticas de segurança geral.

3. **Serviços de gestão da qualidade da segurança -** Estes serviços visam a tomada em consideração do feedback e dos ensinamentos adquiridos das boas práticas nacionais. As descrições que se seguem explicam de que forma a proficiência pode beneficiar cada um destes serviços de gestão da qualidade, nomeadamente a Análise dos riscos; a Planificação da continuidade da atividade e da recuperação de emergência; a Consultoria de segurança; a Sensibilização; a Educação/Formação; e a Avaliação ou certificação dos produtos.

3.1. **Análise dos riscos -** Recolhe informações adequadas a fim de analisar os riscos atuais e emergentes e os que possam interferir com a solidez e a disponibilidade das redes de comunicações eletrónicas e com a autenticidade, integridade e confidencialidade das informações acessíveis e transmitidas através delas, bem como fornecer os resultados das análises ao seu universo de utilizadores. Promove, igualmente, por forma sistemática, a pesquisa, a análise e o processamento de notícias e a difusão e arquivo das informações operacionais produzidas em matéria de Segurança do Ciberespaço.

3.2. **Planificação da continuidade da atividade e da recuperação de emergência -** Tendo em conta as ocorrências do passado e as previsões de incidentes emergentes ou as tendências de segurança, a planificação dos esforços deve ter em conta a experiência e as suas recomendações na determinação da resposta a incidentes tendo em vista a continuidade de qualquer atividade.

3.3. **Consultoria de segurança -** Serviço que pode ser utilizado para prestar aconselhamento e orientação quanto às melhores práticas de segurança a observar pelos utilizadores nas suas atividades. Formula igualmente recomendações ou identifica requisitos a observar na aquisição, instalação ou securização de novos sistemas, dispositivos de rede, aplicações de software ou processos organizativos que afetem a sua atividade. Inclui igualmente a prestação de orientação e assistência no desenvolvimento de políticas de segurança à escala da comunidade de utilizadores.

3.4. **Prevenção e Sensibilização -** A concretização da Cibersegurança não se esgota na aplicação de tecnologia. Por um lado, é sobretudo uma questão comportamental e uma responsabilidade partilhada entre pessoas envolvidas. Por outro, não é um assunto da exclusiva responsabilidade do Estado mas antes uma responsabilidade partilhada com o setor privado e os cidadãos. Afigura-se então que a prevenção e sensibilização para a Segurança do Ciberespaço é a consequência lógica destas premissas e o denominador comum. Este serviço procura afirmar a absoluta necessidade de cooperação estratégica e operacional em projetos e consórcios da mesma natureza, constituindo um instrumento de atuação sistémico,

preditivo e proactivo, visando garantir a segurança, prevenir e reduzir a violência, comportamentos de risco e incivilidades, bem como melhorar o sentimento de segurança no ciberespaço, envolvente e decorrente.

3.5. Formação - A literacia e as competências digitais são essenciais para a utilização segura do ciberespaço, principalmente em termos de gestão da segurança, privacidade e identidade e do desenvolvimento e aprofundamento de um comportamento responsável e ético. Este serviço consiste no fornecimento aos utilizadores de informações sobre questões relacionadas com a segurança informática no âmbito de seminários, workshops, cursos e outras ações de formação. Os tópicos podem incluir, principalmente, diretrizes de notificação de incidentes, métodos de reposta adequados, ferramentas de resposta a incidentes, métodos de prevenção de incidentes e outras informações necessárias para proteger, detetar, notificar e responder a incidentes de segurança informática.

3.6. Avaliação ou certificação dos produtos - Avaliações de produto relativamente a ferramentas, aplicações ou outros serviços, a fim de se certificar da segurança dos produtos e da sua conformidade com práticas de segurança hodiernas ou com práticas organizacionais aceitáveis. As ferramentas e aplicações avaliadas podem ser de fonte aberta ou produtos comerciais. Este serviço pode ser prestado como avaliação ou no quadro de um programa de certificação, consoante as normas aplicadas nacional ou internacionalmente.

APÊNDICE C

MODELO DE PROTOCOLO DE COOPERAÇÃO ENTRE A POLÍCIA DE SEGURANÇA PÚBLICA E O CENTRO NACIONAL DE CIBERSEGURANÇA

Considerando que a Estratégia Nacional de Segurança do Ciberespaço, aprovada pela Resolução do Conselho de Ministros n.º 36/2015, estabelece objetivos e linhas de ação com vista a um desenvolvimento das sinergias nacionais e a uma intensificação da cooperação nacional, europeia e internacional neste domínio, fundando-se no compromisso de aprofundar a segurança das redes e da informação e de potenciar uma utilização livre, segura e eficiente do ciberespaço;

Considerando que é atribuição do Gabinete Nacional de Segurança – Centro Nacional de Cibersegurança, adiante CNCS, contribuir para que o país use o ciberespaço de uma forma livre, confiável e segura, através da promoção da melhoria contínua da Cibersegurança nacional e da cooperação internacional, em articulação com todas as autoridades competentes, bem como da implementação das medidas e instrumentos necessários à antecipação, à deteção, reação e recuperação de situações que, face à iminência ou ocorrência de incidentes ou ciberataques, ponham em causa o funcionamento das infraestruturas críticas e os interesses nacionais;

Considerando que na prossecução das suas atribuições, o CNCS possui, entre outras, as seguintes competências legais:

- Desenvolver capacidades nacionais de prevenção, monitorização, deteção, reação, análise e correção destinadas a fazer face a incidentes de cibersegurança e ciberataques;

- Promover a formação e a qualificação de recursos humanos na área da cibersegurança, com vista à formação de uma comunidade de conhecimento e de uma cultura nacional de cibersegurança;
- Exercer os poderes de autoridade nacional competente em matéria de cibersegurança, relativamente ao Estado e aos operadores de infraestruturas críticas nacionais;
- Contribuir para assegurar a segurança dos sistemas de informação e comunicação do Estado e das infraestruturas críticas nacionais;
- Promover e assegurar a articulação e a cooperação entre os vários intervenientes e responsáveis nacionais na área da cibersegurança;
- Assegurar a produção de referenciais normativos em matéria de cibersegurança;
- Apoiar o desenvolvimento das capacidades técnicas, científicas e industriais, promovendo projetos de inovação e desenvolvimento na área da Cibersegurança.

Considerando que a Polícia de Segurança de Segurança Pública, doravante PSP, é uma força de segurança, com natureza de serviço público, tendo por missão assegurar a legalidade democrática, garantir a segurança interna e os direitos dos cidadãos, nos termos da Constituição e da lei;

Considerando que constituem atribuições da PSP, entre outras:

- Garantir as condições de segurança que permitam o exercício dos direitos e liberdades e o respeito pelas garantias dos cidadãos, bem como o pleno funcionamento das instituições democráticas, no respeito pela legalidade e pelos princípios do Estado de direito;
- Garantir a ordem e a tranquilidade públicas e a segurança e a proteção das pessoas e dos bens;
- Prevenir a criminalidade em geral, em coordenação com as demais forças e serviços de segurança;

- Desenvolver as ações de investigação criminal e contraordenacional que lhe sejam atribuídas por lei, delegadas pelas autoridades judiciárias ou solicitadas pelas autoridades administrativas;
- Manter a vigilância e a proteção de pontos sensíveis, nomeadamente infraestruturas rodoviárias, ferroviárias, aeroportuárias e portuárias, edifícios públicos e outras instalações críticas;
- Participar, nos termos da lei e dos compromissos decorrentes de acordos, tratados e convenções internacionais, na execução da política externa, designadamente em operações internacionais de gestão civil de crises, de paz, e humanitárias, no âmbito policial, bem como em missões de cooperação policial internacional e no âmbito da União Europeia e na representação do País em organismos e instituições internacionais;
- Contribuir para a formação e informação em matéria de segurança dos cidadãos;
- Licenciar, controlar e fiscalizar o fabrico, armazenamento, comercialização, uso e transporte de armas, munições e substâncias explosivas e equiparadas que não pertençam ou se destinem às Forças Armadas e demais forças e serviços de segurança, sem prejuízo das competências de fiscalização legalmente cometidas a outras entidades;
- Licenciar, controlar e fiscalizar as atividades de segurança privada e respetiva formação, em cooperação com as demais forças e serviços de segurança e com a Inspeção-Geral da Administração Interna;
- Garantir a segurança pessoal dos membros dos órgãos de soberania e de altas entidades nacionais ou estrangeiras, bem como de outros cidadãos, quando sujeitos a situação de ameaça relevante;
- Assegurar o ponto de contacto permanente para intercâmbio internacional de informações relativas aos fenómenos de violência associada ao desporto.

É celebrado entre a PSP, neste ato representado por _____, e o CNCS, neste ato representado por _____, o presente protocolo que se regerá pelas cláusulas seguintes:

CLÁUSULA PRIMEIRA

(Objeto)

O presente Protocolo regula as formas de cooperação entre o CNCS e a PSP, em matéria de cibersegurança, definindo o seu âmbito, tipo de ações de cooperação, assim como a forma de gestão e a sua duração.

CLÁUSULA SEGUNDA

(Cooperação)

1. O CNCS e a PSP comprometem-se a cooperar no âmbito da formação, sensibilização e consciencialização com o objetivo de promoção de uma cultura nacional de cibersegurança que abarque a sociedade civil em geral, com especial enfoque nas crianças, jovens e idosos, bem como nos profissionais da PSP.
2. O CNCS e a PSP comprometem-se a cooperar no desenvolvimento de capacidades de prevenção, monitorização, deteção, reação, análise e correção destinadas a fazer face a incidentes de cibersegurança e a ciberataques, sem prejuízo dos poderes de autoridade nacional competente em matéria de Cibersegurança do CNCS, relativamente ao Estado e aos operadores de infraestruturas críticas nacionais.
3. O CNCS e a PSP comprometem-se a partilhar entre si informação relevante em matéria de cibersegurança.
4. Sempre que necessário as medidas indicadas serão acordadas e reduzidas a escrito, através da elaboração de planos de trabalho ou de cartas de acordo.
5. Os planos de trabalho a que se refere no número anterior deverão obedecer ao regime definido, dentro dos princípios gerais comuns a este tipo de cooperação a desenvolver por cada uma das partes e respetivos sistemas de financiamento.

CLÁUSULA TERCEIRA

(Capacidades de análise, mitigação e resolução de incidentes de segurança no ciberespaço)

Procurando dotar a PSP com as valências adequadas para a análise, a mitigação e a resolução de incidentes de segurança no ciberespaço, o CNCS e a PSP cooperam no sentido de edificar as seguintes capacidades e funcionalidades da PSP:

a) Definição de um ponto de contato que articule com o CNCS a reação a incidentes de cibersegurança.

b) Identificação das áreas de atividade e serviços considerados críticos ou vitais para a PSP e realização gestão de ativos para as mesmas.

c) Coleção e armazenamento de metadados de comunicações eletrónicas e outros registos de serviços informáticos necessários para a análise de incidentes.

d) Definição de um conjunto de instrumentos técnicos e serviços, autónomos ou contratados, para mitigação dos tipos de ciberataques mais comuns.

e) Aprovação e implementação de procedimentos internos de resposta a incidentes de cibersegurança.

f) Definição da estrutura e cadeia de responsabilidade de resposta a incidentes de cibersegurança e realização periódica de simulacros de cibersegurança.

g) Edificação de uma equipa dedicada à reação a incidentes de cibersegurança – CSIRT.

h) Colaboração em projetos de desenvolvimento e partilhe informação de cibersegurança de uma forma regular dentro da comunidade nacional de CSIRT.

i) Participação em exercícios nacionais e internacionais de cibersegurança.

CLÁUSULA QUARTA

(Projetos de Investigação e Financiamento)

O CNCS e a PSP colaborarão no desenvolvimento de capacidades técnicas e científicas promovendo ou participando em projetos de inovação e desenvolvimento na área da cibersegurança.

CLÁUSULA QUINTA

(Encargos)

1. Os encargos decorrentes do desenvolvimento das atividades previstas no presente protocolo, bem como outras que venham a ser acordadas em aplicação do presente protocolo, são da exclusiva responsabilidade de cada uma das partes, salvo situações particulares que deverão ser objeto de acordo escrito.
2. Da execução do presente Protocolo não pode resultar para a PSP o dever de pagamento de qualquer encargo ao CNCS ou a terceiros nem, através dele, vincular a PSP a, no futuro, adquirir qualquer sistema ou produto relacionado com o projeto a que o mesmo se refere

CLÁUSULA SEXTA

(Divulgação)

Ambas as partes podem fazer referência à celebração deste protocolo nas suas ações e materiais de comunicação e promoção.

CLÁUSULA SÉTIMA

(Alterações ao Protocolo)

Qualquer alteração ao presente Protocolo deverá revestir a forma de documento escrito assinado pelas partes, devendo ser objeto de proposta a apresentar à outra parte.

CLÁUSULA OITAVA

(Vigência e Denúncia)

1. O presente Protocolo produz efeitos a partir da data da sua assinatura e vigorará pelo período de um ano, renovando-se automaticamente por iguais períodos caso não seja resolvido por comum acordo das partes outorgantes ou unilateralmente rescindido com fundamento no incumprimento das obrigações de uma das partes.
2. O presente Protocolo pode ser denunciado a qualquer momento, sendo tornado eficaz no final do semestre em que é denunciado ou em data acordada entre as partes.
3. A cessação do presente Protocolo não prejudica a integral conclusão dos projetos em curso à data em que aquela ocorra, exceto quando ocorram circunstâncias de força maior que inviabilizem a sua conclusão.

O presente Protocolo é redigido em dois exemplares idênticos, constituído por (n) páginas, o qual é assinado pelas partes, sendo entregue um original aos seus representantes.

Lisboa, junho de 2016.

APÊNDICE D

MODELO DE PROTOCOLO DE COOPERAÇÃO ENTRE O INSTITUTO SUPERIOR DE CIÊNCIAS POLICIAIS E SEGURANÇA INTERNA E O CENTRO NACIONAL DE CIBERSEGURANÇA

Considerando que a Estratégia Nacional de Segurança do Ciberespaço, aprovada pela Resolução do Conselho de Ministros n.º 36/2015, estabelece objetivos e linhas de ação com vista a um desenvolvimento das sinergias nacionais e a uma intensificação da cooperação nacional, europeia e internacional neste domínio, fundando-se no compromisso de aprofundar a segurança das redes e da informação e de potenciar uma utilização livre, segura e eficiente do ciberespaço, afigurando como crucial fomentar e apoiar atividades e iniciativas de investigação cientifica envolvendo entidades de investigação e a academia;

Considerando que é atribuição do Centro Nacional de Cibersegurança, funcionando no âmbito do Gabinete Nacional de Segurança, doravante designado de CNCS, contribuir para que o país use o ciberespaço de uma forma livre, confiável e segura, através da promoção da melhoria contínua da Cibersegurança nacional e da cooperação internacional, em articulação com todas as autoridades competentes, bem como da implementação das medidas e instrumentos necessários à antecipação, à deteção, reação e recuperação de situações que, face à iminência ou ocorrência de incidentes ou ciberataques, ponham em causa o funcionamento das infraestruturas críticas e os interesses nacionais;

Considerando que é competência do CNCS promover a formação e a qualificação de recursos humanos na área da Cibersegurança, com vista à formação de uma comunidade de conhecimento e de uma cultura nacional de Cibersegurança, bem

como apoiar o desenvolvimento das capacidades técnicas, científicas e industriais, promovendo projetos de inovação e desenvolvimento na área da Cibersegurança;

Considerando que o Instituto Superior de Ciências Policiais e Segurança Interna, adiante designado de ISCPSI, é uma instituição de ensino superior público universitário policial integrada na Polícia de Segurança e que tem por missão ministrar formação inicial e ao longo da vida aos oficiais de polícia da Polícia de Segurança Pública, através de ciclos de estudos conducentes à obtenção de graus académicos em ciências policiais e de ciclos de estudos não conferentes de grau académico, nos termos da legislação aplicável;

Considerando que o ISCPSI pode ainda ministrar formação académica e técnico-profissional destinada aos técnicos superiores e dirigentes das forças, serviços e organismos de segurança, das polícias municipais e de outras entidades com atribuições e competências no âmbito da Segurança Interna;

É celebrado, entre o ISCSPI, neste ato representado por _____, e o CNCS, neste ato representado por _____, o presente protocolo que se regerá pelas cláusulas seguintes:

Cláusula Primeira

(Objeto)

O presente Protocolo regula, de forma geral, as relações institucionais entre o ISCPSI e o CNCS, definindo o seu âmbito, tipo de ações de cooperação, assim como a forma de gestão e a sua duração.

Cláusula Segunda

(Cooperação)

1. O ISCPSI e o CNCS comprometem-se, na medida das suas possibilidades, a promover, incentivar e desenvolver ações de colaboração, formação, publicação e divulgação no quadro do ensino superior, da investigação

científica e da prevenção na área da Cibersegurança e no âmbito da Segurança Interna.

2. A cooperação entre as duas Instituições signatárias desenvolve-se, concretamente, dentro do quadro e domínios que sejam considerados de interesse comum, designadamente nas seguintes áreas:
    a. Desenvolvimento de projetos nacionais ou internacionais de investigação científica e desenvolvimento, integrados em objetivos de interesse nacional, nomeadamente no âmbito da Segurança Interna e em particular da Cibersegurança;
    b. Intercâmbio de informação, documentação, publicações, doutrinas e boas práticas;
    c. Utilização das tecnologias de informação e de comunicação no desenvolvimento de sinergias tecnológicas e pedagógicas, no âmbito da investigação científica;
    d. Apoio à realização de estágios curriculares;
    e. Realização de colóquios, conferências, encontros, jornadas e seminários.
3. As partes comprometem-se ainda a estabelecer relações de cooperação ou associação, no âmbito das suas atribuições e competências, com outras entidades públicas ou privadas, nacionais ou estrangeiras, no âmbito da cooperação multilateral, em iniciativas que procurem promover uma comunidade de conhecimento e uma cultura nacional de Cibersegurança.
4. A concretização das medidas específicas de cooperação entre as partes são acordadas, sempre que necessário, e reduzidas a escrito, através da elaboração de planos de trabalho ou de adendas.
5. Os planos de trabalho a que se refere no número anterior, obedecem ao regime definido, dentro dos princípios gerais comuns a este tipo de cooperação a desenvolver por cada uma das partes e respetivos sistemas de financiamento.

Cláusula Terceira

(Projetos de Investigação Científica)

O ISCPSI e o CNCS colaboram na realização e apoio à realização de projetos de investigação científica que versem sobre matérias de interesse comum.

Cláusula Quarta

(Intercâmbio de Informação e Documentação)

As Instituições signatárias procedem à permuta de publicações e de literatura científica, nos domínios de interesse comum, em repositório institucional ou através de outro meio documental acordado pelas partes.

Cláusula Quinta

(Realização de Formação)

As partes signatárias asseguram a execução de atividade e programas de formação, com participação de docentes universitários, investigadores, alunos e outro público não académico, de forma a criar intercâmbio científico e cultural.

Cláusula Sexta

(Instalações)

Para os efeitos previstos na cláusula 2.ª do presente Protocolo, as Instituições signatárias definem os termos em que é efetuada a cedência de instalações.

Cláusula Sétima

(Pagamentos)

Os encargos financeiros decorrentes da execução do presente Protocolo são definidos pelas partes para cada ação a desenvolver, tomando como base o princípio da reciprocidade.

Cláusula Oitava

(Alterações ao Protocolo)

Qualquer alteração ao presente Protocolo reveste a forma de documento escrito assinado pelas partes, devendo ser objeto de proposta a apresentar à outra parte.

Cláusula Nona

(Vigência e Denúncia)

1. O presente Protocolo produz efeitos a partir da data da sua assinatura e vigorará pelo período de um ano, renovando-se automaticamente por iguais períodos, caso não seja resolvido por comum acordo das partes outorgantes ou unilateralmente rescindido com fundamento no incumprimento das obrigações de uma das partes.
2. O presente Protocolo pode ser denunciado a qualquer momento, sendo tornado eficaz no final do semestre em que é denunciado ou em data acordada entre as partes.
3. A cessação do presente Protocolo não prejudica a integral conclusão dos projetos em curso à data em que aquela ocorra, exceto quando ocorram circunstâncias de força maior que inviabilizem a sua conclusão.

O presente Protocolo é redigido em dois exemplares idênticos, constituído por (n) páginas, o qual é assinado pelas partes, sendo entregue um original aos seus representantes.

Lisboa, Junho de 2016.