idn Instituto da Defesa Nacional

Contributos para uma Estratégia Nacional de Ciberdefesa

fevereiro de 2017

idn Instituto da Defesa Nacional

IDN – PROJETO DE INVESTIGAÇÃO

Contributos para uma Estratégia Nacional de Ciberdefesa

FEVEREIRO 2017

COORDENAÇÃO

Paulo Viegas Nunes

GRUPO DE ESTUDOS

Carlos Pereira Mendes

Jorge Ralo

Lino Santos

Luís Camelo dos Santos

Paulo Moniz

Paulo Viegas Nunes

Sofia de Vasconcelos Casimiro

Prólogo

A evolução tecnológica e o rápido crescimento da Internet, que se assume hoje como uma incontornável ferramenta de comunicação e interação à escala planetária, construíram uma “sociedade em rede” de matriz digital.

O Ciberespaço, enquanto espaço global comum, não é limitado pela esfera pública ou privada, civil ou militar, interna ou externa.

Sem garantir a sua segurança e defesa, que permitem melhorar a estrutura de enquadramento e o desenvolvimento nacional, dificilmente será possível explorar todo o valor que o Ciberespaço oferece às modernas sociedades.

Por essa razão, o Ciberespaço constitui um novo domínio estratégico para Portugal, necessitando de ser pensado como uma área prioritária de defesa de valores e interesses nacionais.

A última revisão do Conceito Estratégico de Defesa Nacional, ocorrida em 2013, integrou já este desígnio na reflexão então realizada, assumindo a “Segurança da Informação e o Ciberespaço” o estatuto de um vetor estratégico central, capaz de condicionar a Segurança e a Defesa Nacional.

Com impacto e influência crescentes no ambiente internacional de segurança, o Ciberespaço é hoje utilizado por atores Estado e não-Estado para, nele e através dele, exercerem poder no domínio social, político/diplomático, económico e até militar.

Reconhecendo este facto, a Aliança Atlântica assumiu formalmente o Ciberespaço como o 4º domínio operacional na Cimeira de Varsóvia, associando este novo espaço de condução de operações militares ao ambiente terrestre, naval e aéreo.

A clarificação dos conceitos de Cibersegurança e Ciberdefesa, promovendo o desenvolvimento de sinergias e uma mais eficiente e eficaz articulação operacional das capacidades que lhes estão associadas, permitirá reduzir e gerir melhor os riscos resultantes da elevada dependência tecnológica da nossa sociedade e do crescente poder (disruptivo e destrutivo) dos ciberataques.

A criação da Estrutura Nacional de Cibersegurança e Ciberdefesa, assumindo-se como imprescindível em Sociedades baseadas/dependentes da Informação, constitui hoje um imperativo tanto no quadro da União Europeia como da OTAN.

A construção de um futuro digital para Portugal exige assim uma Estratégia Nacional de Ciberdefesa, obrigando à revisão do atual quadro legal, à criação de doutrinas, ao levantamento de novas capacidades, estruturas e meios para dar suporte à condução de Operações no Ciberespaço.

Sendo a informação e a segurança no Ciberespaço um dos pilares de qualquer estratégia nacional, o Instituto da Defesa Nacional (IDN), no quadro estrito da sua missão, não poderia deixar de dedicar a este domínio estratégico uma elevada prioridade. Uma prioridade que se repercute nos vários eixos de ação da atividade do IDN - desde a formação, à investigação e sensibilização – e que radica no objetivo de contribuir para a promoção, na sociedade portuguesa, de uma cultura de cibersegurança e de aprofundar o conhecimento, a reflexão e o debate sobre esta matéria.

É nesse contexto, a título de exemplo, que no âmbito da formação o IDN tem vindo a realizar um 'Curso de Cibersegurança e Gestão de Crises no Ciberespaço', em parceria com a Academia Militar, bem como um curso em Bruxelas, no âmbito do Colégio Europeu de Segurança e Defesa da União Europeia - 'Course on the challenges of European cybersecurity' - em parceria com o instituto congénere francês, o *Institut des Hautes Études de Défense Nationale* (IEDHN). E que na mesma perspetiva, no âmbito da investigação, se têm empreendido várias iniciativas, de que se destaca o projeto de investigação conjunto desenvolvido em parceria com o *Centro Superior de Estudios de la Defensa Nacional* (CESEDEN) espanhol, cujos resultados foram publicados em livro sob o título "Estratégia da Informação e Segurança no Ciberespaço". Também a reflexão e o debate têm sido promovidos no contexto das reuniões do Grupo de Estudos dedicado ao tema "Contributos para uma Estratégia Nacional de Informação", criado em 2011, e do qual fazem parte reputados especialistas das várias áreas do conhecimento, privilegiando uma lógica interdisciplinar.

Para estas atividades o Instituto da Defesa Nacional tem contado, como sempre, com a colaboração de conceituados e qualificados peritos, nacionais e internacionais, que assim partilham o seu conhecimento e múltiplas experiências e que constituem uma indispensável mais-valia para a consecução dos objetivos do IDN.

O presente projeto, subordinado ao tema "Contributos para uma Estratégia Nacional de Ciberdefesa", decorre de uma solicitação de Sua Excelência o Ministro da Defesa Nacional, Professor Doutor José Alberto Azeredo Lopes, e beneficiou do imprescindível contributo de um conjunto de colaboradores com um percurso profissional e académico que se destaca em matérias de Cibersegurança e Ciberdefesa. Uma vez mais, só a grande disponibilidade e dedicação empenhada destes colaboradores tornaram possível ao Instituto da Defesa Nacional concretizar um projeto de grande utilidade estratégica. Trata-se, de facto, de um muito valioso e qualificado contributo para a imprescindível definição de uma Estratégia Nacional de Ciberdefesa.

Gostaria, assim, de deixar expresso o profundo agradecimento e reconhecimento do

Instituto da Defesa Nacional pela forma exemplar como os autores deste estudo souberam e quiserem interpretar o desafio que lhes foi lançado, apesar das exigentes responsabilidades profissionais de cada um, demonstrando um elevado sentido de interesse nacional e grande dedicação à causa pública.

Vítor Rodrigues Viana
Diretor do IDN

Índice

Lista de Acrónimos

ANACOM – Autoridade Nacional de Comunicações

APE – Administração Pública do Estado

C2 – Comando e Controlo

CCD – Centro de Ciberdefesa

CD – Ciberdefesa

CDC – *Cyber Defence Committee* (Comité de Ciberdefesa)

CDMB – *Cyber Defence Management Board* (Conselho de Gestão de Ciberdefesa)

CDP – *Capability Development Plan* (Plano de Desenvolvimento de Capacidades)

CEC – Centro de Excelência de Ciberdefesa

CERT – *Computer Emergency Response Team* (Equipa de Resposta a Emergências Computacionais/Informáticas)

CISMIL – Centro de Informações e Segurança Militar

CNCS – Centro Nacional de Cibersegurança

CONOPS – Conceito de Operações (*Concept of Operations)*

CS – Cibersegurança

CSI – Comunicações e Sistemas de Informação

CSIRT – *Computer Security Incidents Response Team* (Equipa de Resposta a Incidentes de Segurança Computacionais/Informáticos)

DDoS – *Distributed Denial of Service*

DNS – *Domain Name System*

DOTMLPF-I – *Doctrine, Organization, Training, Material, Leadership, Personnel, Facilities and Interoperability* (Doutrina, Organização, Treino, Material, Liderança, Pessoal, Infraestruturas e Interoperabilidade)

EC3 – *European Cyber Crime Center* (Centro Europeu de Combate ao Cibercrime)

EDA – *European Defence Agency* (Agência Europeia de Defesa)

EIN – Estratégia da Informação Nacional

ENCD – Estrutura Nacional de Ciberdefesa

ENCDef – Estratégia Nacional de Ciberdefesa

ENCSeg – Estratégia Nacional de Cibersegurança

ENSD – Estratégia Nacional de Segurança e Defesa

ENSI – Estrutura Nacional de Segurança da Informação

EU – *European Union* (União Europeia - UE)

FA – Forças Armadas

G8 – Grupo dos 8 países economicamente mais desenvolvidos

GNS – Gabinete Nacional de Segurança

IA – Inteligência Artificial

ICP Defesa – Infraestrutura de Chaves Públicas da Defesa

ID-I – Investigação, Desenvolvimento e Inovação

IDN – Instituto da Defesa Nacional

IIN – Infraestrutura Nacional de Informação

IoT – *Internet of Things*

ITU – *International Telecomunications Union* (União Internacional das Telecomunicações)

LPDP – Lei de Proteção de Dados Pessoais

MEC – Ministério da Educação e Ciência

MISP – *Malware Information Sharing Project* (Projeto de *Smart Defence NATO*)

MNCD2 – *Multinational Cyber Defence Capability Development* (Projeto de *Smart Defence NATO*)

MNCDE&T – *Multinational Cyber Defence Education and Traning* (Projeto *Smart Defence NATO*)

NATO – *North Atlantic Treaty Organization* (Organização do Tratado do Atlântico Norte - OTAN)

NCIRC – *NATO Computer Incident Response Capability* (Capacidade de Resposta a Incidentes de Computadores da OTAN)

OSCE – *Organization for Security and Co-operation in Europe* (Organização para a Segurança e Cooperação na Europa)

PCM – Presidência do Conselho de Ministros

RAP – *Rapid Action Plan* (Plano de Ação Rápida)

SCN – Sistema de Ciberdefesa Nacional

SIED – Serviço de Informações Estratégicas de Defesa

TIC – Tecnologias de Informação e Computação

TJUE – Tribunal de Justiça da União Europeia

TLP – *Traffic Light Protocol* (Protocolo de sinalização luminosa de tráfego)

Introdução

Devido ao ritmo acelerado da evolução tecnológica e à crescente dependência das modernas sociedades em relação à Internet, o ciberespaço constitui, atualmente, um novo domínio de acesso aberto e global, caracterizando-se pela ausência das tradicionais fronteiras físicas.

A Humanidade desenvolveu-se ao longo das últimas décadas com base na estruturação das suas atividades em rede. Para esse efeito, de forma a promover uma rápida e eficiente partilha da informação, as organizações têm vindo a implementar programas de transformação digital, virtualizando e integrando em rede os seus processos internos e externos, promovendo a inovação e adotando novas práticas capazes de aumentar a sua produtividade. Em linha com este objetivo estratégico estruturante, os Estados têm procurado também melhorar as suas estruturas de governação e de integração social, em prol do bem-estar dos seus cidadãos.

Aproveitando a cobertura global das infraestruturas que suportam a Internet procurou-se, num primeiro momento, ligar o maior número possível de equipamentos e sistemas à Internet, melhorando progressivamente a sua acessibilidade e utilização remota. Posteriormente, uma vez que cada dispositivo passou a ser concebido com base num identificador único e com o pré-requisito de ligação a esta rede global ("a Internet das coisas"), o mundo passou a estar permanentemente *on-line*, aprofundando uma cultura de partilha e conectividade, a que hoje atribuímos, cada vez mais, a designação de "Internet de tudo".

Em linha com esta evolução, afirmando-se como uma sociedade da Era da Informação, caraterizada pela existência de uma Economia cada vez mais centrada em rede, Portugal tornou-se também dependente do funcionamento fiável da Internet e das modernas tecnologias de comunicação e informação, passando a estar cada vez mais exposto e vulnerável a um novo e alargado conjunto de novos riscos de segurança.

A utilização maliciosa do ciberespaço pode ter por alvo indivíduos, organizações ou até Estados, afetando os processos de geração de riqueza e a construção plena de uma cidadania digital, condicionando o exercício dos direitos, liberdades e garantias. A crescente capacidade disruptiva e destrutiva dos ciberataques, demonstra também como esta nova tipologia de ataque pode afetar seriamente as infraestruturas críticas, a segurança e a soberania nacional. A sua natureza transversal, obriga à clarificação do seu enquadramento legal e criminal, ao desenvolvimento de sinergias e a uma colaboração efetiva entre todos os atores envolvidos na segurança e defesa do Estado.

Ambiente Internacional de Segurança – Tendências de Evolução

O ambiente estratégico internacional é cada vez mais marcado pelo ritmo acelerado da transformação digital e pela dependência crescente relativamente à utilização do ciberespaço. Estes fatores, registados à escala mundial, têm vindo a colocar também novos desafios aos Estados, obrigando, nomeadamente, ao levantamento de novas capacidades, à revisão dos seus modelos de governação e à geração de competências, cada vez mais associadas à exploração das Tecnologias de Informação e Comunicação (TIC).

Um número crescente de computadores é todos os dias objeto de ataques e intrusões sendo a sua integridade comprometida por *hackers*. Dados sensíveis são roubados de redes e sistemas informáticos de empresas privadas e do Governo. O ciberespaço é utilizado pelo crime organizado de forma ilícita para realizar fraudes e para extorsão. Vários ciberataques têm também vindo a ser utilizados para espionagem e para o exercício de coação política contra Estados, como componente integrante de campanhas militares ou como ferramentas para desativar infraestruturas industriais. Tais ataques podem afetar a relação entre os Estados, podendo tornar-se uma arma com elevado impacto nas modernas sociedades e na segurança do próprio sistema internacional. Os diversos tipos de ataque e a indisponibilidade do ciberespaço têm assim um importante impacto estratégico.

A necessidade urgente de levantar mecanismos de proteção e defesa, destinados a garantir a livre utilização da Internet e do ciberespaço, têm conduzido os Estados ao aprofundamento de uma cultura de ciberdefesa e à tomada de consciência coletiva, relativamente à importância do desenvolvimento de políticas e estratégias cooperativas de combate a todas as formas de ataque cibernético. Assim, iniciativas recentes de âmbito nacional e internacional (ONU, NATO, UE, OSCE e G8) têm vindo a propor acordos de cooperação e dispositivos legais que definem normas e princípios destinados a garantir uma Internet sustentável e um comportamento aceitável no ciberespaço.

É hoje consensual que o ciberespaço apresenta importantes implicações sociais, políticas, económicas e militares e que ocupará um importante papel em qualquer conflito futuro. Através do ciberespaço e no próprio ciberespaço será possível projetar poder e atacar um adversário. No entanto, com base na análise de conflitos recentes (Estónia-2007, Geórgia-2008, Irão-2009, Ucrânia-2014), constata-se que a exploração do ciberespaço, mesmo que com contornos agressivos, difícilmente se poderá considerar um ato de guerra à luz do Direito Internacional vigente.

Para além das questões associadas à atribuição da autoria de um ciberataque, constata-se que a declaração de um ato de guerra deve ter por base os efeitos de um ciberataque e não os meios ou até os atores responsáveis pelo seu lançamento. A percepção existente, que importa tornar cada vez mais clara, é a de que atualmente os ciberataques aumentaram substantivamente a sua capacidade disruptiva, tornando-se também cada vez mais destrutivos, produzindo efeitos e danos cinéticos/materiais.

A crescente "militarização" da Internet vem assim suscitar uma preocupação redobrada pois não é possível ignorar que os ciberataques lançados ou patrocinados por Estados são aqueles que consubstanciam um maior poder disruptivo. Uma vez que os ciberataques apresentam como vantagem estratégica o facto de terem um impacto menor na opinião pública que as tradicionais formas cinéticas de conflito ou guerra, a sua ocorrência é cada vez mais frequente. Nenhum Estado poderá assim deixar de equacionar e considerar responsavelmente o levantamento de capacidades militares neste dominio, sob pena de não conseguir assegurar a defesa dos seus intereses e o exercício da sua própria soberanía.

Enquadramento, Finalidade e Objetivos do Estudo

Para fazer face ao espectro alargado das novas ameaças, à edificação de capacidades e ao levantamento de estruturas militares no ciberespaço, tanto num plano nacional como internacional, a maior parte dos Países mais desenvolvidos já editou ou está em vias de concluir o processo de publicação da sua Estratégia Nacional de Ciberdefesa.

Num momento em que a Organização do Tratado do Atlântico Norte (OTAN) reconheceu formalmente o ciberespaço como um novo domínio operacional na Cimeira de Varsóvia (7-8 Julho 2016), a União Europeia pretende rever a sua visão estratégica e promover o levantamento de uma capacidade autónoma de Ciberdefesa (Junho de 2016). Portugal tem vindo a liderar diversas iniciativas internacionais e a participar ativamente neste esforço cooperativo, realizando de forma concertada pontes e desenvolvendo as suas capacidades nacionais.

Esta realidade, que se coloca hoje ao nosso País, com especial acuidade e pertinência, constitui simultaneamente um desafio e uma oportunidade de afirmação internacional, impondo uma reflexão destinada a promover o desenvolvimento de uma Estratégia Nacional de Ciberdefesa, capaz de salvaguardar os interesses nacionais, potenciar o desenvolvimento das necessárias capacidades e competências e de garantir, de forma eficaz, a segurança e defesa do País no Ciberespaço.

Este projeto de investigação, tem assim por finalidade caracterizar os principais domínios, desafios e cenários que se colocam atualmente à segurança e defesa do

ciberespaço, contribuindo desta forma para um melhor enquadramento e desenvolvimento de uma Estratégia Nacional de Ciberdefesa.

Dentro deste contexto, contribuindo também para a consolidação de uma Estratégia e de uma Estrutura Nacional de Cibersegurança, capaz de reunir os vários atores nesta matéria, este estudo tem os seguintes objetivos:

- Caracterizar o atual ambiente de segurança internacional e o impacto do ciberespaço na área da Segurança e Defesa Nacional;
- Atendendo ao espectro das ciberameaças e à necessidade de gerir o risco social daí decorrente, analisar os vários domínios e cenários que se colocam à cibersegurança e ciberdefesa do Estado;
- Contribuir para um melhor enquadramento legal do ciberespaço, nomeadamente, no que diz respeito aos diferentes aspetos ligados à cibersegurança e ciberdefesa do Estado;
- Assumindo que o ciberespaço, devido à sua natureza global e transversal, é um domínio de exercício e defesa de soberania, onde a cooperação civil-militar assume uma importância crescente, contribuir para a definição de uma Estratégia Nacional de Ciberdefesa;
- Em articulação com os esforços nacionais e internacionais em curso, promover uma cultura de ciberdefesa e contribuir para o desenvolvimento de capacidades nacionais neste domínio.

Face à finalidade e aos objetivos a atingir, pretende-se articular a investigação a desenvolver de maneira a dar resposta às importantes questões estratégicas formuladas. Neste contexto, após o enquadramento e caracterização dos desafios que se colocam hoje à “Sociedade em Rede”, serão caracterizados os diversos domínios e cenários envolvidos no âmbito da segurança e defesa do ciberespaço, caracterizando-se de forma genérica e específica o seu enquadramento legal.

Procurando promover o desenvolvimento de um conceito de ação estratégica coerente e estruturado, será analisado o enquadramento e proposta uma Estratégia Nacional de Ciberdefesa, capaz de consubstanciar um plano de ação e contribuir para o reforço das capacidades nacionais de cibersegurança e ciberdefesa.

Parte I –
Impacto do Ciberespaço na Sociedade em Rede

Paulo Moniz

A transformação que a sociedade sofreu nas últimas décadas tem sido disruptiva no plano tecnológico, económico e social. Não obstante os graves problemas globais que vivemos nos nossos dias, como o terrorismo e as crises económicas, é inegável que o fenómeno da globalização proporcionou um acelerado desenvolvimento e bem-estar social. Milhões de pessoas viram o seu nível de vida melhorar, passaram a aceder a mais informação e conhecimento e podem agora comunicar, no espaço de um instante, com familiares, amigos ou parceiros de negócios situados num qualquer lugar do mundo.

A globalização a que assistimos no período das nossas vidas, porventura comparável à ocorrida no período dos descobrimentos (Rodrigues e Devezas, 2007), pelo menos no que diz respeito à aproximação dos povos e culturas que proporcionou, assim como à criação de redes de troca e partilha de bens, assenta e depende de um espaço novo, inteiramente criado pelo homem, que desafia o próprio conceito tradicional de espaço. O ciberespaço, concebido sobre um inexorável desenvolvimento científico e tecnológico, permitiu o desenvolvimento da Internet, uma rede global que possibilita a comunicação e troca de informação praticamente instantânea entre quaisquer dois locais remotos do planeta. Assim como os mares permitiram a navegação e a aproximação de culturas e povos, o ciberespaço permitiu uma interação muito mais veloz, global e barata, construindo novas acessibilidades, oportunidades e desafios para os cidadãos e organizações, suportando fluxos de transferência de informação e conhecimento, que se tornaram pedras basilares da nossa sociedade. À semelhança dos mares, o espaço aéreo e o espaço exterior, o ciberespaço surge assim como um novo *Global Common*, ou seja, um espaço essencial ao funcionamento da nossa sociedade, que é partilhado por todos, embora não pertença a nenhum Estado em particular.

A ambição e vontade humana de inovar e evoluir foi-se cimentando, através do ciberespaço, de forma quase descontrolada, onde se assiste ao desenvolvimento de processos e serviços essenciais à nossa sociedade sem que, na maioria das vezes, tenham sido acautelados os riscos deste novo paradigma ainda mal compreendido. Neste sentido, o ciberespaço apresenta-se atualmente como um recurso global, crítico e partilhado da humanidade, que potencia um desenvolvimento sem precedentes, mas que também cria uma dependência perigosa, pois o seu fácil acesso e as assimetrias do exercício de poder que permite, também servem atores mal-intencionados que podem assim perpetrar atos com grande impacto na sociedade.

Torna-se portanto premente entender profundamente este novo paradigma associado ao ciberespaço, não só na compreensão das suas características específicas, mas também no entendimento das potencialidades e riscos que suscita e, com base numa análise de risco social, enquadrada no contexto politico e socioeconómico, delinear estratégias a aplicar a diferentes níveis (organizações internacionais, Estados, empresas e mesmo cidadãos) com o desiderato de garantir um acesso seguro a este novo espaço de interação global, e assim afirmar a marcha de desenvolvimento económico e social sem precedentes que se iniciou neste período da história que temos o privilégio de assistir.

1.1. Ciberespaço – Um Novo "Global Common"

Os *Global Commons* são domínios ou espaços partilhados pelos diversos Estados, mas que não são propriedade de nenhum Estado em particular (Buck,1998). Os mares e o espaço aéreo são *Global Commons* unanimemente aceites e compreendidos há mais tempo, sendo que a evolução tecnológica criou a necessidade de adicionar a esta categoria o espaço exterior, povoado de satélites de comunicações civis e militares à escala global. Mais recentemente, a estes espaços juntou-se também o ciberespaço, onde assenta a Internet, uma rede global de troca de informação e conhecimento.

Os *Global Commons,* devido à sua natureza transversal, funcionam muitas vezes como *hubs* de ligação de diversas redes locais, mas essencialmente são domínios por onde circulam grandes fluxos de informação, pessoas e bens, constituindo-se como recursos vitais para o desenvolvimento social e económico das sociedades modernas. Em nome da clareza de conceitos é importante salientar que existe a noção de recursos comuns de grande utilidade à humanidade, que difere da ideia de *Global Commons* aqui apresentada. Esses recursos, por vezes designados por *Global Public Goods* (GPF, 2017), englobam bens comuns como a água potável do planeta, a disponibilização de energia elétrica ou mesmo o espaço eletromagnético, entre outros. O sentido de *Global Commons* tem pois, na sua definição, implícita a necessidade de assegurar a sua segurança, na medida em que a propriedade relevante é a garantia do acesso a estes domínios por todos, de modo a não colocar em causa o bem-estar económico e social.

A caracterização do ciberespaço como *Global Common,* talvez pelas suas diferenças conceptuais, não é, no entanto, evidente para todos. Convém realçar que existem autores que não reconhecem o ciberespaço como um verdadeiro *Global Common (*Tsagourias e Buchan, 2015), alegando que a infraestrutura base que o suporta é propriedade privada e que, como tal, o princípio da não exclusão de acesso não é assegurado. Reconhecendo a legitimidade da argumentação, importa referir que não será tanto a incerteza da classificação do ciberespaço enquanto *Global Common* que é relevante neste estudo, dado que, efetivamente, num grau de abstração maior, este espaço apresenta-se como um domínio crítico e global de partilha de serviços e informação que não é

propriedade de nenhum Estado em particular, mas antes as características especiais que o definem que importa realçar.

Neste contexto, destaca-se que o ciberespaço surge como o primeiro *Global Common* completamente criado pelo homem. É um domínio que pode, grosso modo, ser dividido em duas camadas distintas, uma física, que corresponde às infraestruturas de servidores, equipamentos de rede e *links* de comunicações que dão corpo à *Internet*, e outra lógica, de aplicações e conteúdos, onde se estabelecem as trocas de informação entre indivíduos e organizações, e em que as fronteiras perdem o sentido e as distâncias deixam de ter significado. É exatamente esta dualidade de visão que complica muito a equação do governo do ciberespaço, dado que por um lado temos a componente física, instalada em território geográfico de Estados soberanos, regidos por leis secularmente estabelecidas e gerida quase na totalidade por empresas privadas e, por outro lado, temos o plano lógico, onde os conceitos de distância e fronteira sofrem uma alteração radical de entendimento.

O ciberespaço, enquanto espaço global, apresenta ainda uma alteração do paradigma relativo às relações de poder (Nye, 2010). Os *Global Commons* têm obedecido a relações de poder estabelecidas pelo devir histórico, normalmente com uma hegemonia de controlo mais ou menos evidente pelas superpotências mundiais, em particular, ao longo dos últimos anos, pelos Estados Unidos. Contudo, neste novo domínio de acesso global, existe uma grande assimetria em relação ao exercício do poder, uma vez que um pequeno ator pode, neste espaço, perpetrar atos com consequências de grande impacto social (ex: Snowden) e mesmo material. Do lado oposto a esta "democratização do poder", temos os Estados e organizações mundiais que foram entretanto confrontados e surpreendidos por esta nova realidade e com a perda do controlo de que usufruíam. Esta situação pode levar, e tem levado, sob a égide da garantia da segurança e do combate aos atores reconhecidamente mal-intencionados, à imposição de medidas de controlo e monitorização do tráfego da *Internet*, provocando inevitáveis retrocessos nos direitos do exercício democrático e nos direitos adquiridos ao longo dos tempos, como a proteção dos dados pessoais e o direito à privacidade.

Assumindo assim este novo domínio, produto da criação humana, como um novo *Global Common*, urge pensá-lo e refletir sobre a sua natureza e as suas especificidades de modo a poder estabelecer princípios de governação que permitam um acesso livre e seguro a este espaço virtual, condição crucial e essencial para o desenvolvimento e bem-estar da nossa sociedade. Neste âmbito, Estados de pequena dimensão geográfica e populacional como Portugal, poderão, nas suas estratégias, tirar partido da assimetria do exercício de poder proporcionada pelo ciberespaço, contudo não poderão também esquecer que, devido às especificidades das suas economias de pequena escala, encontram uma forte dependência no acesso seguro a este *Global Common* e, como tal, deverão desenhar esforços no sentido de encontrar cenários de colaboração e cooperação mundial para alcançar esse desiderato.

1.2. Desenvolvimento Económico e Social

Existe atualmente uma consciência clara e unânime de que o desenvolvimento económico e social sofreu uma transformação radical nas últimas décadas e que a forma de funcionamento do mundo contemporâneo assenta fundamentalmente no valor da informação. O caminho que a humanidade percorreu, acompanhado dos avanços tecnológicos que o cimentaram, dificilmente terá retorno, sendo que as redes, os sistemas e, sobretudo, a Internet, são o substrato necessário para potenciar a circulação transfronteiriça de comunicações, serviços, ideias e conhecimento.

O mundo atual praticamente retirou ao individuo e às organizações a opção de isolamento. O ciberespaço é hoje um campo fértil de estímulo à circulação de ideias, informação e comunicação, sendo que, com facilidade e rapidez, temos acesso a realidades de outros locais do mundo que nunca visitámos, cimentando-se no individuo uma ideia e sentir diferentes em relação às tradicionais noções de distâncias e fronteiras. Este encurtar de intervalos temporais e espaciais, associados à quantidade e facilidade de armazenamento de informação, tem implicações avassaladoras no funcionamento das organizações e indivíduos e, consequentemente, nas suas relações económicas e sociais.

O tecido económico da Era da Informação sofreu uma evolução radical. Com a constituição de um mercado global, assente no ciberespaço, as empresas passam a estar em contacto com novos mercados e oportunidades, mas passam também a estar confrontadas com um ambiente de grande competição que exige delas uma capacidade criativa, de eficiência e diferenciação que não lhes era requerida até então. A construção de uma sociedade em rede cria uma pressão acrescida nas organizações, impondo-lhes uma necessidade de criar valor fundamentalmente dependente da informação, do conhecimento e da forma como gerem esses ativos. Os processos de decisão com base na informação, assim como as competências dos colaboradores das organizações, são fatores cruciais para a sobrevivência das empresas na Era da Informação. A sociedade da informação é, sobretudo, uma sociedade de mercado, conectada e com tendência para que as vantagens competitivas sejam as da manipulação da informação, quer nos processos de adaptação às novas realidades quer nos processos de decisão.

Do ponto de vista social, as implicações da utilização das tecnologias e serviços da Era da Informação são também radicais e resultam, praticamente em todas as vertentes, num desenvolvimento e melhoria de condições de vida dos cidadãos. Neste contexto os benefícios situam-se não só no acesso aos novos serviços oferecidos pelas empresas da Era da Informação, mas também pela possibilidade de comunicarem com outros indivíduos de forma instantânea e barata para qualquer lugar do mundo. Do ponto de vista político, o ciberespaço tem dado uma nova expressão à democracia, facilitando o acesso livre e aberto ao conhecimento e informação, agilizando a criação de movimentos, a partilha de ideologias e mesmo potenciando revoluções (como exemplo a revolução na Tunísia onde a Internet foi a plataforma de convocação para um objetivo politico comum).

De forma a assegurar o desenvolvimento económico e social é necessário garantir a não exclusão dos indivíduos e organizações do ciberespaço, o que passa não apenas pela sua educação para o exercício de uma "cidadania digital", mas, sobretudo, pela garantia de acessos seguros aos meios e sistemas de informação, assim como pela proteção da privacidade.

1.3. Gestão do Risco Social na Sociedade em Rede

À medida que o ciberespaço se vai assumido, cada vez mais, como o substrato no qual se desenvolve a nossa sociedade e em que se materializa a ideia de uma rede única, global, importa reconhecer que são também cada vez mais os utilizadores que passam a estar ligados e com diferentes motivações, que podem ser financeiras, económicas, politicas, criminosas ou terroristas, entre outras. A inclusão destes atores, num domínio de assimetria de poder, coloca a sociedade perante novos riscos que é preciso gerir adequadamente.

O risco é tipicamente formado por uma equação que tem uma tradução em conceitos facilmente entendíveis e bem intuitivos, que considera os recursos a proteger e a sua importância na sociedade, as vulnerabilidades que podem ser exploradas de modo a afetar esses recursos e, por último, o nível de ameaça a que estão expostos, mormente a avaliação das capacidades técnicas e financeiras dos atacantes e as suas motivações. O trabalho a realizar na gestão do risco da sociedade em rede consiste, em primeiro lugar, em identificar corretamente os recursos mais críticos de uma Nação, ou organização, de modo a dirigir os maiores esforços para criar segurança de acordo com essa classificação, otimizando assim o emprego de capacidades técnicas e financeiras dos Estados.

Segundo a ótica dos atores mal-intencionados, quando se perspetiva o ataque, os recursos mais apetecíveis são aqueles que, quando afetados, provocam fortes danos à sociedade, sendo normalmente classificados como infraestruturas críticas nacionais, uma vez que dão suporte a serviços fundamentais nos quais assenta o nosso modo de vida. Surgem neste domínio a disponibilização de energia elétrica e as redes de telecomunicações numa camada hierárquica funcional superior (dado que todos os outros dependem destes dois), mas outros existem como o sector financeiro; transportes; águas ou serviços de emergência. É importante salientar que a análise de impacto destes recursos não se pode situar apenas no plano material, há que considerar também outros aspetos como a confiança que os cidadãos e as organizações depositam no ciberespaço. Assim, ainda que admitindo que um cenário de um acidente de um meio de transporte, provocado por um ciberataque, com vítimas mortais e avultados prejuízos materiais, tenha um impacto muito elevado na nossa sociedade, não podemos esquecer que existem outros cenários, sem consequências físicas diretas, que podem reduzir a confiança das instituições e dos cidadãos nos serviços disponibilizados através do ciberespaço e, desse modo, afetar o desenvolvimento económico e social (a titulo de exemplo a divulgação dos

dados do sistema nacional de saúde teria um impacto devastador na vida dos cidadãos ainda que não lhes cause nenhuma consequência física direta).

Identificados os recursos críticos dos Estados, comunidades de Estados ou organizações, importa conhecer também as vulnerabilidades que afetam estes recursos, sendo certo que as vulnerabilidades no ciberespaço não se situam apenas no plano tecnológico. Nexte contexto, devido ainda à pouca exigência do mercado e à deficiente interiorização de uma cultura de segurança pelos fabricantes de *software,* as vulnerabilidades tecnológicas descobertas e exploradas são inúmeras. Contudo, é também verdade que o comportamento humano menos adequado perante os sistemas e redes de informação tem, também ele, sido alvo de forte exploração por atacantes, com o objetivo de desencadear ações mal-intencionadas e diversificadas como fraudes bancárias ou roubo de informação. É essencial nesta vertente do risco levantar mecanismos de proteção e defesa de modo a garantir uma mitigação das vulnerabilidades e atingir o desiderato do acesso livre e seguro ao ciberespaço. Definir requisitos mínimos de segurança, capazes de salvaguardar a privacidade dos cidadãos, estabelecer capacidades de monitorização, deteção e reação a incidentes de segurança e garantir uma educação para a adoção de um comportamento adequado por parte dos cidadãos no ciberespaço, pode e deve muito bem ser um dos papéis a assumir pelos Estados e por todas as organizações em geral.

Por último, nesta equação que caracteriza o risco da sociedade em rede, temos as ameaças. É necessário compreender o contexto político e socioeconómico onde os Estados e organizações se inserem e perceber quais as ameaças mais prováveis, assim como as motivações dos atacantes. Os ataques podem resultar de ações desenvolvidas por indivíduos isolados, com objetivos pessoais de reconhecimento ou lucro, por grupos de pressão social ou criminosos ou ainda, já na esfera da defesa da soberania dos Estados, resultar de atos de agressão num contexto de ciberguerra. Só com o entendimento profundo dos vetores do risco social podemos delinear estratégias que otimizem o valor gerado e assegurem a segurança do ciberespaço, de modo a defender os Estados e potenciar as assimetrias verificadas ao nível do exercício do poder proporcionadas por este domínio.

1.4. Regulação e Regulamentação

Considerando os riscos de uma sociedade em rede, atendendo a que o desenvolvimento económico e social está cada vez mais suportado no ciberespaço e ao facto do mesmo se encontrar, em grande parte, no controlo de privados, é legítimo acolher a ideia de que os Estados, ou Comunidades de Estados, devem preocupar-se em assegurar o bem-estar da sociedade por via dos instrumentos legais e do poder regulatório que disponham, nomeadamente com o objetivo de garantir um acesso seguro ao ciberespaço a cidadãos e empresas.

Constituíndo um domínio comum, onde organizações e empresas desenvolvem serviços essenciais ao mundo atual, a segurança do ciberespaço, na sua globalidade, mas também em particular em subdomínios à escala da Nação ou organização, é afetada por efeitos colaterais produzidos pelas entidades menos preparadas para funcionarem na rede global, materializando o conceito económico de externalidades (More, 2010). Deste modo, tanto a regulação como a regulamentação devem, no âmbito da sua aplicação e respeitando o principio da proporcionalidade, ter como desiderato assegurar que as capacidades existentes nos diversos atores do ciberespaço são suficientes e niveladas, de forma a garantir um elevado nível de segurança nos serviços desenvolvidos, eliminando assim possíveis desalinhamentos de interesses resultantes do facto deste *Global Common* de interesse publico estar sob controlo de privados.

A regulamentação e o papel regulador a exercer pelo Estado deverá então ter em conta a análise de risco social realizada e deverá materializar, dentro dos limites da sua atuação, uma estratégia de cibersegurança definida, atuando de forma incisiva nos sectores e subsectores mais críticos identificados pelos Estados. A regulamentação deve-se focar no estabelecimento de requisitos mínimos de segurança tecnológica, na exigência do levantamento de capacidades de monitorização, deteção e reação, mas, também, na educação dos cidadãos para a cibersegurança. A colaboração entre organizações civis e militares, dentro e fora do Estados, também merece uma especial atenção, dado que as fronteiras do ciberespaço são difusas. O papel regulador do Estado surge assim como um instrumento fundamental, embora não suficiente por si só, para a garantia de um acesso seguro ao ciberespaço.

1.5. Cibersegurança e Ciberdefesa

A transposição das missões das Forças de Segurança e das Forças Armadas do campo convencional para o ciberespaço não deverá sofrer alterações de entendimento conceptual no que diz respeito às competências e cenários de intervenção. No entanto, devido às características específicas deste novo ambiente de interação, destaca-se que a interdependência entre a ciberdefesa e a cibersegurança é bastante forte e as fronteiras de atuação algo difusas.

De uma forma genérica entende-se a cibersegurança como o conjunto das atividades, que ocorrem no ciberespaço, de prevenção, monitorização e resposta às ameaças que, pela sua natureza disruptiva, coloquem em risco o bem-estar e a salvaguarda dos direitos dos cidadãos ou organizações. Competindo a um conjunto alargado de Entidades assegurar a sua cibersegurança[1] importa referir que, neste novo *Global Common*, também as organizações têm um papel a desempenhar nesta missão. No que diz respeito à ciberdefesa, entende-se que esta inlcui as atividades de prevenção,

[1] A responsabilidade pela cibersegurança nacional encontra-se formalmente distribuída por um conjunto de atores que inclui as Forças e Serviços de Segurança, o Centro Nacional de Cibersegurança e a Autoridade Nacional de Proteção Civil.

monitorização e reação a ameaças que coloquem em risco a soberania nacional, sendo que compete às Forças Armadas assegurar a missão da ciberdefesa.

Para além dos aspetos mais óbvios, relacionados com os meios e recursos disponiveis, as possíveis alterações de perceção, em relação aos cenários convencionais onde atuam forças de segurança e forças armadas, resulta da dificuldade de entendimento claro dos fenómenos no ciberespaço. Compreende-se com clareza que compete ao Ministério da Justiça (através da Polícia Judiciária) e às Forças de Segurança desencadear a resposta do Estado a ações de cibercrime ou *hacktivismo*[2] e que, por sua vez, serão as Forças Armadas a ter um papel idêntico nas ações de ciberguerra. Contudo, na realidade e como exemplo, num hipotético cenário de ataque a uma infraestrutura crítica de energia nacional, devido à natureza do ciberespaço, podemos ficar na incerteza se o mesmo é um ataque direcionado à organização, afetando o serviço aos seus clientes, ou se tem uma intenção de grandes proporções, colocando em causa a soberania de um País. Resulta ainda deste cenário que, em ambas as situações, poderá existir sempre a dificuldade em determinar a autoria do ataque, quer na perspetiva geográfica, quer mesmo na capacidade utilizada, mormente se foi realizado por um simples individuo motivado por interesses próprios (cibercrime) ou se tal corresponde a uma ação planeada e executada numa perspetiva militar (ciberguerra).

Para melhor entendimento das diferenças que resultam do ciberespaço, num cenário convencional de disputa militar entre duas Nações, as Forças Armadas preocupar-se-iam com a defesa das infraestruturas físicas de produção de energia da Nação, focando-se os colaboradores da empresa nas suas atividades operacionais para o fornecimento de energia à sociedade. Num cenário de ciberguerra, a organização tem um papel preponderante na medida que tem no terreno mecanismos de defesa que deve acionar, ao mesmo tempo que deve colaborar na gestão de crise com outras entidades privadas, militares e do Estado. Torna-se assim evidente que, respeitando as atribuições das várias Entidades ligadas à ciberdefesa e cibersegurança e as suas áreas específicas de atuação, deverá existir sempre uma entidade responsável e regulamentação dirigida à coordenação entre os dois domínios, de modo a aproveitar sinergias e concertar uma resposta conjunta em cenários de crise. Pela natureza estruturante da investigação, esta questão será objeto de um tratamento mais detalhado e circunstanciado ao longo deste trabalho.

[2] Tal verifica-se nomeadamente porque se pretende identificar e levar à justiça os criminosos. Adicionalmente, atendo ao impacto disruptivo deste tipo de ataques na atividade das organizações, segundo uma lógica de continuidade de negócio, refere-se também que a resposta a este tipo de fenómenos poderá ter de ser dada pela entidade afetada em coordenação com o CNCS, conforme o seu mandato de CERT Nacional. Por outro lado, o mesmo objetivo de levar à justiça criminosos, também se aplica a terrorismo ou espionagem, envolvendo neste caso os serviços de informações nacionais.

Parte II –
Segurança do Ciberespaço

Lino Santos

Desde o início da década de 2010, o tema da cibersegurança tem preenchido a agenda política associada à segurança nacional de muitos países, refletindo abordagens variadas e complementares, que podem ser sistematizadas e apresentadas considerando o seu objecto ou domínio de aplicação: o Estado, o mercado e os cidadãos.

Os Estados tecnologicamente mais avançados - que, paradoxalmente, são também muitas vezes os mais vulneráveis - ancoram a cibersegurança num contexto de segurança nacional, focando a sua atenção no desenvolvimento de meios técnicos e de capacidades com vista à proteção, mas também à exploração, do ciberespaço. O exemplo mais conhecido - mas longe de ser o único - é o dos Estados Unidos que criaram, recentemente, o *U.S Cyber Command* e identificam, de forma clara, na sua doutrina militar, o ciberespaço como um novo domínio operacional, onde podem vir a ser conduzidas operações defensivas e ofensivas. A cibersegurança de um Estado inclui igualmente a proteção das suas infraestruturas críticas que dependem do ciberespaço para o seu normal funcionamento, elevando a cibersegurança a um patamar de relevo na estratégia de proteção dessas infraestruturas.

Por outro lado, os Estados preocupados com o papel das TIC como fator de inovação e de desenvolvimento da economia, bem como com o facto de esta ser gerida e operada maioritariamente por entidade privadas, colocam o enfoque da cibersegurança nas questões regulatórias e no reforço da resiliência das infraestruturas de comunicação. Esta é a abordagem utilizada pela Comissão Europeia que, possuindo um programa específico para a proteção de infra-estruturas críticas de informação, definiu uma estratégia europeia para a cibersegurança[3] e aprovou recentemente uma diretiva relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União.[4]

[3] Ver JOIN (2013) 1 final, Estratégia da União Europeia para a cibersegurança: Um ciberespaço aberto, seguro e protegido, disponível em http://register.consilium.europa.eu/doc/srv?f=ST+6225+2013+INIT&l=pt, consultado em 1/11/2016.

[4] Ver DIRETIVA (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação na UE, http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L1148&from=EN, disponível em consultado em 1/11/2016.

Com uma perspetiva essencialmente económica, a cibersegurança é vista como fator de geração de confiança no comércio eletrónico e como parte integrante das políticas de desenvolvimento da designada sociedade da informação e do conhecimento.

Por último, a cibersegurança também se refere à segurança dos indivíduos, e em particular à segurança da informação digital circulante ou armazenada destes e sobre estes, à segurança dos seus dados pessoais, à sua privacidade e às suas liberdades e outros direitos individuais, quando inseridos no ciberespaço. Esta perspetiva torna-se particularmente relevante quando grande parte da informação, alguma dela sensível, assume forma digital e se encontra armazenada ou circula em processos no ciberespaço, cabendo ao próprio Estado a promoção das medidas de segurança necessárias para a sua proteção, neste particular assegurando a sua integridade e confidencialidade, assim como a sua operacionalização.

2.1. Domínios e Áreas de Competência

Para lidar com o conjunto de ameaças presente no ciberespaço - da mesma forma que o faz para qualquer ameaça transnacional e assimétrica -, o Estado e a sociedade possuem um conjunto de planos de atuação para lidar com a "ciber (in) segurança". São eles a proteção simples, a prossecução criminal, a guerra e a diplomacia (Santos et al., 2012).

O plano da proteção simples abrange os meios técnicos, processuais e humanos que realizam diariamente as componentes preventiva, reativa e de gestão da qualidade da segurança da informação. É, pois, a primeira linha de proteção das infraestruturas, dos serviços e da informação presentes no ciberespaço. Neste contexto, um ciberataque é entendido como uma sequência de ações destinadas a produzir um resultado não autorizado ou uma perturbação indesejada na confidencialidade, na integridade ou na disponibilidade de um serviço ou produto, ou seja, a proteção do ciberespaço é perspetivada numa lógica de mercado, de continuidade de negócio e, em última instância, do cidadão. Tendo em conta que grande parte das componentes do ciberespaço são propriedade ou são geridas por privados, a sua proteção não é um assunto da exclusiva responsabilidade dos Estados. Em diferentes estágios, são muitos os participantes nesta proteção simples, desde os fabricantes de produtos de *software*, de *hardware* ou de processos, os técnicos que administram os sistemas e as redes, as entidades reguladoras sectoriais, a academia, os *Computer Security Incident Response Team* (CSIRT), até, em última instância, o utilizador de tecnologia - no que se designa de "ciber-higiene." Neste contexto, a *International Telecomunications Union* (ITU) define cibersegurança como o "conjunto de ferramentas, políticas, guias, abordagens de gestão de risco, ações de formação, boas práticas, e tecnologias que podem ser usadas para proteção dos ativos das organizações e dos utilizadores no ambiente virtual. Os ativos das organizações e dos utilizadores

incluem os dispositivos ligados em rede, os utilizadores, as aplicações e serviços, sistemas de telecomunicações e de comunicação multimédia e a informação transmitida e/ou armazenada no mundo virtual."

Num outro plano, o objetivo principal do sistema judicial é o da dissuasão da prática de crimes pela prevenção e, no limite, pela condenação concreta do autor de um crime. No domínio da prossecução criminal, os ciberataques representam atos criminalmente relevantes, passíveis de ação penal, tais como os dirigidos, tendencialmente, contra pessoas (eg. a pornografia de menores e os crimes contra a honra) ou contra interesses patrimoniais (eg. a violação de direitos de autor e direitos conexos e a burla informática) ou, finalmente, contra dados e informação (falsidade informática, dano informático, sabotagem informática, acesso ilegítimo, acesso indevido). Estes últimos configuram, em grande parte, o que se designa por cibercrime. Por outro lado, num mundo cada vez mais digital, é natural que uma grande parte dos elementos de prova, mesmo de crimes tradicionais, assuma essa mesma forma digital. A competência legal para prevenção criminal e a investigação criminal dos crimes informáticos está atribuída por lei à Polícia Judiciária. São participantes neste domínio de atuação, os órgãos de polícia criminal, o Ministério Público e os Magistrados Judiciais.

No plano da guerra e da defesa do Estado são relevantes, por um lado, assegurar a capacidade operacional em missões militares que passa por garantir o correto funcionamento e a proteção das Comunicações e Sistemas de Informação, elementos fundamentais para o exercício do comando e controlo no moderno campo de batalha, hoje em dia muito dependente dasTIC; e, por outro, explorar o ciberespaço para obtenção de vantagem operacional sobre os adversários. Em situações declaradas de estado de sítio ou estado de guerra o comando e a gestão dessas situações, também no ciberespaço, compete à Defesa Nacional.

Finalmente, no domínio da diplomacia, importa prosseguir os interesses políticos nacionais no âmbito das suas relações internacionais, promovendo bilateral ou multilateralmente o desenvolvimento de políticas harmonizadas, como a ratificação da Convenção do Cibercrime, ou, no quadro da ONU, o desenvolvimento do Direito Internacional no ciberespaço.

Este conjunto de planos de "contra-ciberconflitualidade" devem complementar-se e actuar simbioticamente para a eficácia do sistema. O conjunto destes planos representa a capacidade nacional de segurança do ciberespaço. O mesmo cenário de conflito, dependendo da gravidade dos impactos, requer, muito provavelmente, a ação em dois, três ou mesmo nos quatro planos aqui descritos, cada qual com o seu obectivo, com os seus instrumentos e redes transnacionais de cooperação, dentro de um quadro legal próprio.

Num plano de análise distinto, apresenta-se de seguida um conjunto, comummente aceite, de políticas públicas ou linhas de ação que contribuem para a cibersegurança.

2.2. Proteção do Cidadão e das Empresas

Com vista à proteção do cidadão e das empresas, tem especial relevância a componente de formação e consciencialização dos vários agentes da sociedade, nomeadamente o conjunto das atividades de capacitação e de atualização tecnológica dos indivíduos responsáveis pelo manuseamento dos componentes do ciberespaço ou que, de uma forma geral, atuam sobre esses mesmos componentes, bem como as atividades de divulgação e de alerta para os perigos de uma utilização negligente da Internet e das consequências de uma deficiente prevenção e proteção contras as ciberameaças.

Igualmente importantes neste contexto são a normalização e certificação na área dasTIC, concentrando as atividades nacionais e internacionais de produção de referenciais, regras, condições ou requisitos de segurança, bem como a aferição destes com os níveis de conformidade de produtos e serviços na área dasTIC com os mesmos.

Importa aqui referir igualmente o planeamento civil de emergência do ciberespaço, previsto no sistema nacional de planeamento civil de emergência, sob coordenação da Autoridade Nacional de Proteção Civil (ANPC).

2.3. Combate ao Cibercrime

Vários autores (Martins, 2003; Brenner e Schwerha, 2004) definem o cibercrime como todo o acto em que o computador serve de meio para atingir um objetivo criminoso ou em que o computador é o alvo desse acto. Segundo Peter Garbosky, estes crimes podem ser divididos em três grupos: crimes convencionais realizados com recurso a computador; crimes convencionais em que o computador não é o instrumento principal da atividade mas onde o meio de realização de prova assume a forma digital; e crimes em que o alvo são os sistemas informáticos (Grabosky, 2004).

O eixo de combate ao cibercrime compreende o conjunto das iniciativas de atualização e de harmonização legislativa com vista a uma mais eficaz criminalização das condutas referidas, bem como a capacitação dos órgãos de investigação criminal e dos vários agentes judiciários na prossecução dos seus objetivos também no ciberespaço.

2.4 Reação a Ciberincidentes

Numa perspetiva de continuidade de negócio, as CERT ou CSIRT foram criadas para realizar as funções de alerta e de reação a ciberincidentes num contexto aterritorial e distribuído como é a Internet. Um fator bastante importante para o desempenho de uma CERT é o nível de cooperação nacional e internacional.

Por um lado a resposta a um incidente de segurança é normalmente centrada no dano visível, quando o incidente pode ser mais vasto, por outro, grande parte dos incidentes de segurança informática têm carácter transnacional, pelo que requerem a participação de várias entidades e a existência de uma rede de contactos. Sobre este particular, e com o objetivo de reforçar o grau de confiança entre equipas e melhorar a sua eficácia têm sido desenvolvidos vários esforços com vista à homogeneização de políticas de tratamento de informação sensível - protocolo TLP -, à definição de uma taxonomia comum para efeitos de troca de informação, seja de novas vulnerabilidades, seja de incidentes e, ainda, para acordar níveis de qualidade de serviço prestado entre elas.

A recente Diretiva NIS vem reforçar o papel destas CSIRT, promovendo a sua formalização e harmonização de capacidades com vista à criação de uma rede Europeia de reação a ciberincidentes.

2.5. Proteção das Infraestruturas Críticas Nacionais

A proteção de infraestruturas críticas ganhou relevância na sequência do ataque terrorista de 11 de setembro nos Estados Unidos da América.

A União Europeia classifica como infraestrutura crítica o "ativo, ou parte deste, essencial para o funcionamento de funções críticas da sociedade, incluindo a cadeia de fornecimento, a saúde, a proteção, a segurança e o bem-estar económico e social da população, classificando como essencial aquele cuja disrupção ou destruição poderá resultar numa falha para manter essas mesmas funções."[5]

O eixo da proteção de infraestruturas críticas abrange as iniciativas de identificação e de mapeamento das dependências funcionais dentro de um sector ou entre sectores de atividade, a realização de uma análise de risco, bem como a aplicação de medidas de proteção, com vista à mitigação dos riscos identificados nas funções classificadas como críticas.

Em Portugal, os primeiros passos dados no trabalho desenvolvido nesta área resultaram numa "Carta Nacional de Pontos Sensíveis", elaborada pelo antigo Conselho Nacional de Planeamento Civil de Emergência, entretanto integrado na Autoridade Nacional de Proteção Civil. No entanto, o conceito de Proteção de Infraestruturas Críticas tem-se vindo a densificar, apenas e por influência europeia, com a transposição da Diretiva 2008/114/CE relativa a à identificação e designação das infraestruturas críticas europeias e à avaliação da necessidade de melhorar a sua proteção. Esta transposição assigna a competência nesta matéria, através do Decreto-Lei n.º 62/2011, de 9 de maio,

[5] Ver Diretiva 2008/14/EC relativa à identficação e designação das infraestruturas críticas europeias e à avaliação da necessidade de melhorar a sua proteção, disponível em http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345: 0075:0082:EN:PDF, consultado em 1/112016.

ao Sistema de Segurança Interno e à Autoridade Nacional de Proteção Civil, respectivamente nas componentes de *Security* e de *Safety*.

2.6. Gestão de Crises e Operações Militares no Ciberespaço

O possível impacto disruptivo decorrente de ciberataques para as nossas infra-estruturas críticas e serviços vitais de informação podem elevar um simples incidente, até então tratado nos planos da proteção simples e da prossecuação criminal, a um estado de sítio ou de emergência, ou ainda, com o devido enquadramento na Carta das Nações Unidas quanto ao uso da força, à necessidade de desenvolver ações ofensivas também no ciberespaço. Esta tem sido, bem ou mal, uma abordagem seguida por muitos países tendente à criação de comandos integrados das operações a desenvolver no ciberespaço (O´Connell, 2012).

De facto, temos vindo a assistir, por um lado, a uma crescente "militarização" do ciberespaço a que corresponde uma "corrida às ciberarmas" e, por outro, a uma diluição da fronteira entre o cibercrime organizado, movimentos hacktivistas e as capacidades militares nesta área, patente desde o desenvolvimento de armas até à condução de operações no ciberespaço, tornando o processo de atribuição, e consequentemente o enquadramento legal, particularmente difícil (Guedes, 2010).

Neste quadro, quer a NATO, quer a EU, promovem esforços para que as Forças Armadas dos seus Estados membros possuam uma capacidade para intervir no domínio cibernético de forma a assegurar, em situações de excepção, o regular funcionamento das instituições democráticas e o exercício das funções de soberania do Estado, nomeadamente, mediante a condução de operações no ciberespaço.

Este esforço deve, no entanto, ser articulado com os restantes planos de "contra-ciberconflitualidade". Mesmo nas situações de excepção descritas, os canais operacionais de cooperação nacional e internacional devem ser realizados pelos pontos de contacto existentes, reservando para a ação militar o comando e controlo e a condução de ações ofensivas (Santos et al., 2012).

2.7. Orientação Política para a Cibersegurança

A orientação política para a Cibersegurança, através da Estratégia Nacional para a Segurança do Ciberespaço, prevê, por um lado, o levantamento de capacidades para as atividades de proteção simples, de prossecução criminal e de guerra, e, por outro, uma coordenação político-estratégica destas mesmas atividades. Neste sentido, a Estratégia Nacional de Segurança do Ciberespaço[6]

[6] Ver RCM n.º 36/2015, de 12 de junho, disponível em https://dre.pt/application/file/67443061, consultado em 1/11/2016.

configura o instrumento político inter-ministerial com a visão estratégica para a cibersegurança para um espaço temporal de três anos.

Esta estratégia assenta num conjunto de 5 pilares, a saber: (1) a subsidiariedade da cibersegurança à segurança nacional; (2) a complementaridade e a partilha de responsabilidade entre os atores; (3) a proporcionalidade das medidas decorrentes de uma avaliação de risco; (4) a cooperação e colaboração entre aliados e parceiros, nacionais e internacionais; e (5) a sensibilização como medida necessária para previnir os riscos.

A Estratégia estende-se por seis eixos de atuação que incluem um conjunto de medidas com vista à: criação de uma coordenação político-estratégica para a segurança do ciberespaço, na dependência direta do Primeiro-Ministro e contando com representantes de todas as partes interessadas; a consolidação do papel de coordenação operacional do Centro Nacional de Cibersegurança; a criação de condições para a identificação de um nível de alerta nacional em matéria de segurança do ciberespaço, partilhado entre todas as entidades envolvidas; o desenvolvimento da capacidade de ciberdefesa; o reforço do combate ao cibercrime; medidas para a proteção do ciberespaço e das infraestruturas; bem como as ações de promoção de uma cultura de cibresegurança e educação para o uso seguro das tecnologias e a cooperação nacional e internacional.

2.8. Sinergias Nacionais

Como referido, Portugal precisa de criar uma estrutura de coordenação político-estratégica para a cibersegurança que reúna o conjunto de atores relevantes de cada um dos quatro planos de contra-ciberconflitualidade, tornando coerente a ação política neste domínio.

No plano tático e operacional, a prevenção e a reação a ciberataques é feita concorrentemente nestes quatro planos. Na grande maioria das situações esta resposta pressupõe uma intervenção no plano da protecção simples, visando a continuidade do “negócio” e uma investigação criminal com vista à identificação e apresentação em tribunal dos reponsáveis. Em situações extremas, onde possam ocorrer impactos no espaço físico que configurem situações de crise ou de emergência, previstas na lei, também os planos da guerra e da diplomacia podem ser chamados a intervir.

Ora, é nestas situações de pretensa escalada da ameaça ou aumento da gravidade da situação que é primeiramente percebida a necessidade de uma constante articulação entre os principais atores de cada um dos planos descritos. Por outro lado, não sendo propriamente necessária, é por demais evidente que a proximidade cultural, a partilha de informação, a criação de referênciais comuns, bem como a cooperação na investigação e

desenvolvimento científico, são fatores que potenciam a eficácia global e indivídual dos vários planos de atuação.

Para esta permanente articulação, muito contribuirá a produção de um quadro situacional da cibersegruança nacional previsto nas alíneas e), f) e g) do Eixo 1 da Estratégia Nacional de Segurança do Ciberespaço, uma ferramenta que permitirá aos diferentes atores agir de forma simbiótica quer em situações de baixa ou de alta intensidade.

2.9. Cooperação Internacional

A arquitetura e as características deste mundo virtual limitam a capacidade de qualquer Estado, *per si*, assegurar a integridade do seu ciberespaço e a proteção dos seus cidadãos no mesmo. Neste contexto, merecem especial relevância as redes transnacionais de cooperação nos diferentes planos e eixos de intervenção (Keohane e Nye, 1970; Slaughter, 2004).[7] Este mesmo desiderato configura um dos cinco pilares da Estratégia Nacional de Segurança do Ciberespaço.

No plano da proteção simples destacam-se as redes, mais ou menos formais, de equipas de resposta a ciberincidentes, tais como a *Taskforce of Computer Security Incident Response Teams* (TF-CSIRT), a Rede Europeia de CSIRT prevista na directiva SRI ou o *Forum of Incident Response and Security Teams*– FIRST. No plano da prossecução criminal destacam-se o *grupo de Lyon* para o combate ao cibercrime, a criação do *European Cybercrime Center* (EC3) dentro da Europol e os trabalhos do Conselho da Europa nesta mesma área. Já no plano da guerra, a formação de doutrina e criação de capacidades de defesa coletiva tem como força motriz a NATO e os seus aliados mais avançados e como centro de gravidade o Centro de Excelência desta organização em Talim. Finalmente, no plano da diplomacia, destacam-se os grupos de trabalho *Friends of Presidency* para a ciberegurança e os trabalhos da OSCE no plano das *Confidence Building Measures on Cybersecurity,* bem como o *Global Forum for Cyber Expertise.*

Em cada um dos planos de "contra-ciberconflitualidade", estas redes transnacionais, mais ou menos formais, têm um papel decisivo na proteção do ciberespaço.

[7] Neste particular ganham particular relevância conceitos das Relações Internacionais como o transnacionalismo de Joseph Nye e Robert Keohane ou a soberania desagregada de Anne-Marie Slaughter.

Parte III –
Defesa do Ciberespaço

Luís Camelo dos Santos, Paulo Viegas Nunes,
Jorge Ralo, Carlos Pereira Mendes

A moderna conflitualidade assume cada vez mais contornos pouco definidos, adoptando simultaneamente diversos vetores de ataque. Explorando assimetrias e vários vetores de projeção de poder (ex: diplomático, informação, militar e económico), assistimos hoje, de forma praticamente ininterrupta, a uma conflitualidade de baixa intensidade, mas de natureza permanente, transversal e híbrida.

3.1. A Componente Cibernética das Ameaças Híbridas

A guerra híbrida, apesar de não ser um fenómeno novo, encontrou na componente cibernética um instrumento de ação de elevado potencial em função do custo reduzido, rapidez de atuação, sensação de anonimato e leque crescente de possíveis alvos com potencial impacto no domínio cibernético. Enquanto fusão de diferentes capacidades e táticas num conflito, eliminando ou atenuando as fronteiras estabelecidas entre os diferentes domínios operacionais, neste tipo de conflitos constata-se o emprego de diferentes tipos de recursos, métodos e técnicas, em diferentes combinações, com o objetivo de atingir o maior efeito possível. Esta nova vertente da moderna conflitualidade, tornou-se particularmente evidente nas guerras híbridas mais recentes (ex: Georgia e Ucrânia), caracterizadas não só por uma utilização extensiva do ciberespaço para a condução de ciberataques, mas também como vetor privilegiado para ações de propaganda e recrutamento.

A utilização do ciberespaço num contexto de ameaça híbrida poderá ser perspetivada de duas formas: a primeira, tirando partido das oportunidades nele criadas, enquanto domínio mediático de comunicação, que permite transformá-lo numa ferramenta de propaganda, manipulação e distorção da informação; uma segunda, através da sua utilização enquanto domínio operacional utilizado para o combate, de modo a complementar ou amplificar os efeitos das operações militares convencionais. Atendendo a este último enquadramento, importa ajustar as capacidades militares a esta nova realidade operacional, nomeadamente, dotando as Forças Armadas de mecanismos de adaptação à guerra híbrida nas suas diversas variantes, dando prioridade à melhoria do conhecimento situacional e privilegiando as áreas da prevenção e dissuasão.

Neste contexto, importa referir que Portugal defendeu desde o início a estratégia proposta pela NATO para o combate à guerra híbrida, tendo por base uma lista de princípios gerais que visam responder a estas ameaças de uma forma coerente e integrada, abordando os diversos modelos de guerra híbrida, independentemente da sua origem, defendendo a segurança e estabilidade da Aliança. De igual modo, assinala-se também a existência de um forte apoio nacional ao desenvolvimento do plano para a implementação desta estratégia, elaborado em cooperação com outras organizações, em particular com a União Europeia. Esta cooperação assume particular importância, uma vez que nenhuma nação ou organização internacional tem todos os meios necessários para combater esta nova tipologia da ameaça, sendo que a coordenação final das ações a desenvolver recairá sobre o Estado ou Estados afetados, responsáveis em primeira instância pela resposta à ameaça híbrida.

À semelhança da posição que tem sido defendida por Portugal para a implementação do Plano de Ação Rápida (RAP) da NATO, o combate à guerra híbrida deverá ser conduzido considerando as três missões da Aliança (Defesa Coletiva, Gestão de Crises e Segurança Cooperativa), assentando no princípio da indivisibilidade da segurança, espelhado na fórmula "28/28 – 360º". Esta visão estratégica, reforçando a coesão e solidariedade da NATO, significa também que todos os Aliados deverão ser capazes de responder homogeneamente a ataques dirigidos contra qualquer ponto situado na área de responsabilidade da NATO, nomeadadamente, aqueles que explorem a vertente cibernética.

3.2. Ciberespaço: o 4º Domínio Operacional

O ciberespaço apresenta um impacto transversal e uma natureza transnacional que o tornam um espaço de interação social de características únicas. Caracterizado por desafios próprios, que combinam a existência de ameaças provenientes de atores estatais e não estatais, o ciberespaço expõe vulnerabilidades civis e militares, requerendo por essa razão respostas multidimensionais nos domínios civil-militar e nacional-internacional.

A crescente ocorrência de ciberataques contra Estados Soberanos[8], fez com que muitas das maiores potencias mundiais (ex: EUA, China e Russia), detentores de uma capacidade militar convencional à escala global, tenham vindo a criar, essencialmente ao longo dos últimos anos, não só os mecanismos necessários para evitarem ser atacadas mas também a capacidade para projetar poder neste novo dominio operacional. Neste contexto, importa referir que, com

[8] Os ciberataques conduzidos contra a Estónia (Abril/Maio de 2007) e contra a Geórgia (Agosto de 2008), constituem bons exemplos do que aqui se refere.

a criação do *U.S. Cyber Command* em 2010[9], os EUA passaram a encarar e a assumir doutrinariamente o ciberespaço como um novo domínio operacional. Ao nível europeu, esta decisão foi também entretanto seguida por outros Estados (ex: Alemanha, Reino Unido, Espanha e França) que anunciaram mais recentemente o levantamento de Comandos responsáveis pela condução de operações militares no ciberespaço. Demonstrando grande preocupação com o impacto crescente do ciberespaço no ambiente de segurança internacional, a própria Aliança Atlântica acabou por igualmente reconher, na Cimeira de Varsóvia (07-09 Julho de 2016), o ciberespaço como um 4º dominio operacional, a par da terra, mar e ar.

Neste quadro, verifica-se que o ambiente do moderno campo de batalha se apresenta cada vez mais descontínuo e multidimensional, constatando-se que as operações militares têm vindo progressivamente a incluir o desenvolvimento de operações em redes de computadores (defensivas, de exploração e ofensivas), juntando aos tradicionais espaços de atuação o ciberespaço. O reconhecimento formal do ciberespaço como domínio operacional por parte de um Estado, traduzindo o empenhamento nacional na proteção e salvaguarda da sua liberdade de ação no espaço cibernético, exige simultaneamente uma mudança da tradicional abordagem militar (defensiva), centrada na garantia da informação (defesa das comunicações e sistemas de informação), para uma postura centrada no impacto dos ciberincidentes e ciberataques no cumprimento das missões das Forças Armadas (mais dinâmica) [10].

Portugal, bem como as organizações internacionais que o País integra, enfrentam atualmente desafios de segurança semelhantes, onde pontuam adversários que utilizam a Internet como domínio previligiado para a condução de ciberataques, com o objetivo de negar o acesso ou degradar a informação e/ou sistemas de informação essenciais ao exercício da soberania dos Estados. Neste contexto, considera-se determinante assumir, também no plano nacional, o ciberespaço como um novo domínio operacional.

Esta assunção, por ora apenas equacionada ao nível conceptual e doutrinário, deverá agora consubstanciar-se, ao nível da Defesa Nacional, através da delineação de uma estratégia de ciberdefesa consequente, capaz de materializar o levantamento das necessárias capacidades militares, definir procedimentos normalizados e estabelecer mecanismos de cooperação eficazes com todos os parceiros relevantes (no plano nacional e internacional). Esta constitui uma condição necessária ao cumprimento das missões das Forças Armadas neste novo domínio de atuação.

---

[9] Tendo em Junho de 2009 sido anunciada pelo Secretário da Defesa a criação do *U.S. Cyber Command*, este novo Comando Militar declarou ter adquirido a sua plena capacidade operacional em 3 de Novembro de 2010.

[10] O paradigma operacional alterou-se assim da garantía da informação (*Information Assurance*) para a garantía da própria missão (*Mission Assurance*), refletindo o papel central que o ciberrespaço e o próprio ambiente de informação assumem hoje no moderno campo de batalha.

3.3. Exercício da Soberania e Defesa dos Interesses Nacionais

O Estado Português tem como tarefa fundamental garantir a independência nacional e criar as condições económicas, sociais e culturais que a promovam. A par de todos os restantes sectores do Estado, é para o cumprimento desta tarefa que concorre a missão da Defesa Nacional, protegendo o País contra qualquer agressão ou ameaça externa. No âmbito da Defesa Nacional cabe às Forças Armadas a defesa militar da República, em obediência aos órgãos de soberania competentes. A Política de Defesa Nacional integra os Princípios, Objetivos, Orientações e Prioridades definidos na Constituição, na Lei de Defesa Nacional, no Programa do Governo e no Conceito Estratégico de Defesa Nacional. Inclui ainda as políticas sectoriais do Estado necessárias para o cumprimento dos objetivos da Defesa Nacional.

No contexto do combate às ameaças no ciberespaço, as Forças Armadas deverão também concorrer para a prossecução da segurança e proteção do ciberespaço de interesse nacional nas suas várias vertentes, nomeadamente, atendendo ao impacto dos ciberataques e ao consequente aumento do risco social. Neste âmbito, para além da cibersegurança sectorial da Defesa Nacional, que será da sua exclusiva responsabilidade, as Forças Armadas poderão vir também a ser chamadas a intervir, nomeadamente, no quadro da defesa da soberania nacional. Neste âmbito, o seu quadro de atuação dependerá de uma colaboração ativa com os restantes órgãos do Estado, Forças e Serviços de Segurança.

Impõe-se assim à maior parte dos Países a necessidade de equacionar a edificação de novas estruturas e a implementação de novos procedimentos operacionais, táticos e técnicos que capacitem as suas Forças Armadas para desempenhar um espectro alargado de missões no ciberespaço, nomeadamente, através do exercício de uma presença permanente e vigilante e da capacidade para executarem todo o espectro de operações militares no espaço cibernético. Neste quadro, deverá ser atribuída especial importância à articulação das capacidades já desenvolvidas e a desenvolver neste domínio com as restantes capacidades militares (existentes noutros domínios), estabelecendo desta forma uma atuação sinérgica e articulada em todo o espectro das operações executadas pelas Forças Armadas.

Uma capacidade operacional de ciberdefesa deverá envolver também o conhecimento e os recursos necessários para prever, influenciar ou bloquear as ações que potenciais adversários venham a desenvolver no ciberespaço, antes, durante e após as operações militares. Neste contexto, a avaliação do espectro da ameaça e a consequente identificação dos potenciais agressores ou atacantes, bem como as suas intenções subjacentes, exigem umas Forças

Armadas com capacidade de recolha e análise de informações no ciberespaço, capazes de permitir assegurar, em tempo, uma resposta eficaz e dissuasora. Concorrentemente, no quadro da salvaguarda da soberania e defesa dos interesses nacionais, deverão ainda ser desenvolvidos esforços no sentido de garantir a adaptação e harmonização do ordenamento jurídico nacional à necessidade de as Forças Armadas poderem dispor das competências indispensáveis à condução de operações militares no ciberespaço.

3.4. Orientação Política para a Ciberdefesa

Assumindo um papel de crescente importância para o exercício da soberania e para a defesa dos interesses nacionais, o ciberespaço carece de uma visão política clara e coerente, capaz de permitir definir objetivos e traçar os caminhos conducentes à edificação de capacidades nacionais neste domínio. Neste âmbito, apesar de não existir uma política nacional formalmente definida, foi elaborada, em Junho de 2015, a "Estratégia Nacional para a Segurança do Ciberespaço"[11].

No âmbito específico da formulação de uma visão política para a ciberdefesa, também sem caracter formal, salienta-se a elaboração de um despacho orientador por parte de Sua Exa o Ministro da Defesa Nacional, em 28 de outubro de 2013[12].

A política para a ciberdefesa, constituindo o suporte para a definição de uma estratégia específica neste domínio, estabelece assim as linhas orientadoras para todo o esforço que a jusante deverá ser feito, nomeadamente na definição do quadro conceptual, doutrinário e normativo da ciberdefesa, bem como na elaboração de um plano de ação conducente à implementação desta capacidade.

A "Orientação Política para a Ciberdefesa" (2013) estabelece os seguintes objetivos: (1) garantir a proteção, a resiliência e a segurança das redes de Comunicações e Sistemas de Informação e (CSI) da Defesa Nacional contra ciberataques; (2) assegurar a liberdade de ação do País no ciberespaço e, quando necessário e determinado, a exploração proativa do ciberespaço para impedir ou dificultar o seu uso hostil contra o interesse nacional; (3) contribuir de forma cooperativa para a cibersegurança nacional.

Para a consecução destes objetivos foram também definidas sete linhas de ação orientadoras: (1) estabelecimento da estrutura de ciberdefesa nacional; (2) integração das operações no ciberespaço no âmbito das capacidades militares;

[11] Ver RCM n.º 36/2015, de 12 de junho, disponível em https://dre.pt/application/file/67443061, consultado em 1/11/2016. Esta estratégia, prevendo o levantamento de capacidades nos vários domínios envolvidos (incluindo a ciberdefesa), define também a necessidade de estabelecimento de uma coordenação político-estratégica das diversas àreas envolvidas.

[12] Despacho Nº 13692/MDN. *Orientação Política para a Ciberdefesa*. Diário da Republica II Série, 208, 28 de outubro de 2013, pp. 31977-31979.

(3) conduzir todo o espectro de operações militares no ciberespaço; (4) reforçar a capacidade de informações no ciberespaço; (5) desenvolver um sistema de alerta imediato e partilha de informação aos vários níveis e patamares de decisão; (6) promover uma cultura de gestão do risco através da incorporação de requisitos de gestão de risco nas aquisições a realizar e na cadeia de abastecimento; e, por último, (7) centralizar a formação e o treino em ciberdefesa e adequar a gestão dos recursos humanos de modo a garantir a sua permanência nestas atividades.

A forma como a orientação política para a ciberdefesa foi formulada em 2013, incluiu no mesmo documento uma visão político-estratégica e, na sua essência, acabou por ser assumida pelas Forças Armadas como uma diretiva iniciadora para a elaboração de um plano de edificação da capacidade nacional de ciberdefesa. Este plano, elaborado no início de 2014, teve como corolário a criação do Centro de Ciberdefesa das Forças Armadas.

Não tendo em conta a existência da "Estratégia Nacional para a Segurança do Ciberespaço" (que só viria a ser aprovada em junho de 2015) nem a recente assumpção do ciberespaço como 4º domínio operacional pela NATO (aprovada na Cimeira de Varsóvia em julho de 2016), a "Orientação Política para a Ciberdefesa" necessita agora de ser revista e atualizada, permitindo um melhor enquadramento político das atividades de defesa do ciberespaço e a definição de uma Estratégia Nacional de Ciberdefesa.

3.5. Cenários de Empenhamento e Resposta Nacional

O ciberespaço, enquanto espaço de defesa de valores e interesses, materializa uma área de responsabilidade coletiva, tornando necessário identificar o papel a desempenhar pelos diversos órgãos, públicos e privados, na garantia da sua proteção e utilização segura. Neste contexto, importa analisar o risco social e o impacto dos diversos tipos de ataque cibernético, separando os de motivação criminosa daqueles que, por apresentarem um maior poder disruptivo, possam colocar em risco a Segurança e Defesa do Estado. Este último tipo de ataques, enquadra-se no domínio da ciberdefesa, exigindo uma participação ativa das Forças Armadas[13].

Face à natureza assimétrica e transversal das ciberameaças, onde se torna difícil clarificar a origem (interna ou externa) e o impacto dos ciberataques, as Forças Armadas deverão também assim assegurar o desenvolvimento de capacidades e assumir competências no domínio da defesa cibernética do País,

[13] Conforme já antes referido, à luz da Constituição da República Portuguesa, as Forças Armadas constituem o corpo social responsável pela Defesa do Estado contra ameaças externas e devem assegurar, em situações de excepção (ex: estado de sítio ou de emergência), o regular funcionamento das instituições democráticas e o exercício das funções de soberania do Estado.

nomeadamente, as que permitem contribuir para proteger as infraestruturas de informação críticas e o governo electrónico do Estado.

Neste contexto, segundo uma perspetiva de duplo-uso, as Forças Armadas deverão trabalhar em conjunto com outros atores relevantes neste domínio, contribuindo desta forma para, colaborativamente, melhorar a proteção e coordenar a defesa dessas infraestruturas. 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.

Atendendo à tipologia da ameaça, ao impacto previsto e ao processo nacional de gestão de crises, a natureza da resposta a adoptar pelo País será também necessariamente diferente, ajustando-se a atuação das Forças Armadas aos diversos cenários de empenhamento daí decorrentes. De uma forma não prescritiva, a tabela apresentada no Anexo I, procura caracterizar as diversas possibilidades de variação dos elementos que caracterizam os múltiplos cenários possíveis, ligando-os ao processo de gestão de crises que lhes está associado. Este tipo de análise, permitirá assim perspectivar o impacto no "espaço-solução" da imposição de um determinado pressuposto, facilitando uma avaliação das diferentes opções estratégicas disponíveis.

Após testar o impacto dos diversos tipos de ataque à luz do racional apresentado, foram objeto de uma análise mais específica e de uma discussão mais detalhada os cenários que apresentavam respetivamente "maior probabilidade" de ocorrência e "maior perigo" para o Estado. A situação identificada como "mais perigosa" a equacionar, foi a materializada pela ocorrência de um ciberataque lançado por parte de atores Estado uma vez que, pelas suas capacidades, este tipo de atores é o que pode realizar um ataque com maior impacto/severidade social. Para fazer face a este tipo de cenários, teríamos de desenvolver uma capacidade de ciberdefesa que fosse capaz de proteger todas as infraestruturas críticas nacionais, uma vez que todas elas poderão potencialmente vir a ser atacadas. Por outro lado, quando se perspetivou o cenário de maior probabilidade de ocorrência, verificou-se que este se consubstanciava, invariavelmente, através de um ciberataque lançado por um ator (não tipificado), sobre as redes de telecomunicações e os sistemas de informação a ela ligados.

Assumindo que o risco social é determinado não só com base na severidade (nível de impacto) mas também pela probabilidade de ocorrência de um ataque, constatamos que a sobreposição/interligação destes dois cenários aponta para que a capacidade de ciberdefesa nacional aposte, de forma cada vez mais consistente e eficaz, na protecção das infraestruturas de informação do Estado, onde se incluem naturalmente também as afetas à Defesa Nacional.

A partir desta constatação, tendo por base a tabela disponibilizada no Anexo I, será agora possível identificar alguns dos diversos parâmetros (colunas da tabela) que caracterizam a análise do risco social e a gestão de crises no ciberespaço. Ainda que de forma sumária, avaliando a variação de cada um dos parâmetros

(linhas associadas a cada coluna) será possível ainda levar um pouco mais longe este esforço de cenarização e avaliar o impacto individual e agregado da aplicação de diversos pressupostos adicionais aos cenários genéricos antes identificados.

3.6. Enquadramento da Atuação das Forças Armadas

O quadro de atuação das Forças Armadas, sendo definido ao nível político-estratégico, terá de ser naturalmente equacionado ao nível de todos os possíveis cenários, sem deixar de ter em atenção o atual estado de edificação da capacidade nacional de ciberdefesa e as atribuições decorrentes das missões atribuídas ao Centro de Ciberdefesa das Forças Armadas.

No plano nacional, essencialmente devido à natureza difusa do ciberespaço antes referida, à sempre difícil dicotomia da segurança nacional (vertente interna vs externa) e, ainda, à ausência de um quadro legal totalmente claro de delimitação de responsabilidades, a definição dos cenários de empenhamento das Forças Armadas em estados de não-guerra ou exceção exige uma clarificação adicional. Só assim será possível potenciar uma atuação sinérgica de todos os atores que participam na gestão de crises no ciberespaço, rentabilizando os recursos nacionais e evitando a sua desnecessária duplicação.

No que diz respeito a cenários de crise, a legislação aplicável é a Lei de Segurança Interna (Lei Nº 53/2008[14]). No âmbito das suas competências de coordenação, o Secretário-Geral do Sistema de Segurança Interna (SGSSI) estabelece mecanismos de articulação entre as diversas Forças e Serviços de Segurança (FSS), com os organismos congéneres internacionais e estrangeiros e com todos os sistemas periféricos, públicos e privados, relevantes na área da segurança. No plano das suas competências de controlo, tem poderes de direcção e articulação das FSS, através dos respectivos dirigentes máximos, em eventos de elevado risco ou incidentes tático-policiais específicos, que impliquem uma atuação conjugada. Finalmente, em situações excepcionais, determinadas pelo Primeiro-Ministro, como ataques terroristas ou catástrofes naturais que requeiram a intervenção articulada de diferentes forças e serviços, estes são colocados sob o comando operacional do Secretário-Geral, através dos seus dirigentes máximos.

A participação das Forças Armadas no SSI, encontra-se tipificada no artigo 35º, onde é referido que estas colaboram em matéria de Segurança Interna nos termos da Constituição e da Lei, competindo ao Secretário-Geral e ao CEMGFA assegurarem entre si a sua articulação operacional. No entanto, não estão ainda criados os mecanismos de articulação necessários[15], sendo que o atual modelo não especifica uma resposta conjunta das FSS e das Forças Armadas numa

[14] Ver: http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1012&tabela=leis.
[15] Pelo apurado, estão em elaboração praticamente desde que a Lei foi aprovada.

situação de crise. Neste âmbito, importa ainda destacar que, através da última alteração que foi feita à Lei de Segurança Interna, em 2015, foi acrescentado ao Conselho Superior de Segurança Interna, onde já tem assento o CEMGFA e o coordenador do Centro Nacional de Cibersegurança. Tal como acontece já em diversos Países, tendo por fundamento a necessidade de enquadrar as questões associadas à proteção e à defesa do ciberespaço, num contexto mais alargado, parece fazer cada vez mais sentido que a gestão de crises neste domínio passe a incluir também o responsável pela coordenação da ciberdefesa nacional, nomeadamente, para garantir ao General CEMGFA a disponibilidade de uma assessoria especializada.

A NATO reconhece desde 2014 a aplicabilidade do Direito Internacional no ciberespaço. As operações militares no ciberespaço são reguladas pelo Direito Internacional, incluindo o Direito Internacional Humanitário, que se aplica às operações conduzidas neste domínio da mesma forma que se aplica num conflito armado. Reconhece-se ainda que, dependendo das circunstâncias, um ciberataque pode ser considerado um ataque armado e, de acordo com a Carta das Nações Unidas (artigo 51º), um Estado afetado pode, nestes casos, agir em legítima defesa. Se o Estado atacado for membro da NATO, esta ação pode levar à invocação do Artigo 5.º do Tratado de Washington.

No contexto da preparação dos seus cenários de empenhamento para fazer face a um conflito no Ciberespaço, a NATO optou por acordar que cada situação de crise ou de potencial agressão no ciberespaço, deverá ser sempre analisada caso a caso, mantendo assim alguma flexibilidade na análise e preparação das modalidades de ação a adoptar na sua resposta. No contexto nacional, a "Orientação Política para a Ciberdefesa" atribui ao EMGFA dois papéis fundamentais no que diz respeito à ciberdefesa: a condução de operações militares no ciberespaço e a proteção das redes e sistemas de informação da Defesa Nacional. Nesse sentido, e considerando o reconhecimento do ciberespaço como um novo domínio operacional, a ciberdefesa deverá incluir o desenvolvimento de capacidades de condução de operações defensivas, de exploração (obtenção de informações em prol da geração de uma consciência da situação operacional – *situational awareness*) e ofensivas, numa perspetiva de integração com a componente operacional das Forças Armadas nos outros domínios, através da sua integração no Comando Conjunto de Operações Militares. Para o efeito concorre também o desenvolvimento da capacidade de recolha e produção de informações no ciberespaço, nas suas várias vertentes.

A materialização das missões da ciberdefesa exige, como ponto de partida, a distinção clara entre estes dois domínios de atuação. A componente associada à proteção das redes e sistemas de informação, de âmbito interno, requer uma atuação centrada essencialmente nas atividades associadas à segurança da informação. No caso da componente ligada à condução de operações militares no ciberespaço, o foco centra-se no quadro mais alargado das missões atribuídas às Forças Armadas, envolvendo operações militares conduzidas num contexto de guerra ou de gestão de crises. Com base nesta clarificação, importa desenvolver

doutrina e procedimentos operacionais que permitam a utilização das capacidades cibernéticas como capacidades operacionais autónomas ou conjugadas, no quadro de uma operação militar ou da gestão de uma crise no ciberespaço.

3.7. Sinergias Nacionais

A proteção do ciberespaço, constituindo uma tarefa extremamente exigente, não conseguirá ser garantida de forma isolada por qualquer instituição ou Estado. A construção de uma sociedade em rede e o exercício de uma cidadania digital responsável, obrigam a que os indivíduos, a administração pública, o sector privado, as Empresas e os Governos passem a partilhar um espaço comum e, consequentemente, a ter de assumir ativamente responsabilidades complementares na segurança do ciberespaço nacional. Atendendo aos diferentes papéis a desempenhar por cada um e sem nunca perder de vista as questões relacionadas com a autonomia necessária à prossecução dos objetivos específicos de cada organização, importa assegurar uma atuação sinérgica de todos os atores, explorando para esse efeito a unidade de esforço e a implementação de soluções que aproveitem possíveis economias de escala, promovendo assim uma maior racionalização dos recursos disponíveis.

Uma vez que a maioria das redes e infraestruturas de prestação de serviços que utilizamos diariamente são detidas e operadas pelo sector privado, as inovações tecnológicas incorporadas e o conhecimento detido por estas organizações revela-se crucial para a defesa do ciberespaço. A cooperação destas entidades com as organizações responsáveis pela cibersegurança e ciberdefea do Estado, em particular no que diz respeito à partilha de informação relativa a ameaças, poderá reforçar a resiliência das redes e ajudar a prevenir, responder e recuperar após a ocorrência de ciberataques. As parcerias com o sector privado deverão por isso constituir um vetor relevante na prossecução das atividades da ciberdefesa e, como tal, concorrerem para a proteção dos sistemas de informação e de comunicações no universo da Defesa Nacional.

A acelerada evolução tecnológica e a sua capacidade transformadora dos processos de comunicação que caracterizam o ciberespaço, obrigam igualmente a uma colaboração próxima com a Indústria nacional. A sofisticação crescente dos equipamentos (*hardware* e *software*) e a existência de um ciclo de vida cada vez mais reduzido, colocam um enfase especial na capacidade de inovação e no capital intelectual, criando assimetrias ao nível do desenvolvimento tecnológico dos vários Países. Face ao número crescente de ferramentas de ataque e de código malicioso que exploram as fragilidades existentes no *firmware dos* equipamentos, muitas vezes intencionalmente criadas, e ao comprometimento da cadeia logística dos sistemas tecnológicos das organizações nacionais, os Estados são hoje confrontados com a necessidade de assegurarem um nível mínimo de soberania tecnológica. Tanto no âmbito da ciberdefesa como da cibersegurança nacional, a colaboração próxima com a Indústria e com a comunidade nacional ligada ao sistema nacional de Investigação,

Desenvolvimento e Inovação (ID-I), revela-se fundamental para permitir acompanhar o estado da arte, descobrir novas vulnerabilidades e corrigir com a maior rapidez possível as que forem entretanto identificadas. Sem o acompanhamento próximo da dinâmica da evolução tecnológica e sem a criação de uma base industrial mínima no domínio da cibersegurança e ciberdefesa, dificilmente será possível assegurar a desejável soberania tecnológica.

Para além da sua matriz tecnológica, o ciberespaço requer também, num curto prazo e aos mais variados níveis, o desenvolvimento de competências e qualificações específicas.Tratando-se de uma área de capital intelectual intensivo, onde os recursos humanos qualificados são relativamente reduzidos, o sistema educativo em geral e o papel da Academia em particular assumem um papel central no desenvolvimento das capacidades nacionais. Neste contexto, em particular, tendo por base a liderança Nacional do Projeto NATO de *Smart Defence,* designado por *Multinational Cyber Defence on Education and Training (MNCDE&T)*, as Forças Armadas lançaram em 2015 uma extensão nacional deste Projeto.Tendo por objetivo o desenvolvimento de um currículo comum e preenchimento das lacunas de formação, educação e treino existentes, tanto no âmbito da ciberdefesa como da cibersegurança nacional, esta iniciativa conta já com 106 organizações participantes congregando, em torno deste objetivo comum, 16 organizações públicas (incluindo o CCD e o CNCS), 28 Instituições Universitárias, 6 centros de investigação, 6 associações, 48 Empresas e 3 bancos.

Tendo por base as várias áreas e domínios onde se torna necessário explorar sinergias, na sua máxima extensão possível, importa reconhecer que a ENSC, constitui já um primeiro elemento enformador do modelo de cooperação a implementar. Neste quadro, a ENSC procura garantir a proteção e defesa das infraestruturas críticas e dos serviços vitais de informação nacionais, visando assegurar a utilização livre, segura e eficiente do ciberespaço por parte de todos os cidadãos, empresas e entidades públicas e privadas. Atribuindo especial enfase à cooperação, a ENSC procura concorrer também para a definição das áreas de atuação dos diversos atores intervenientes na cibersegurança do Estado. No entanto, a ENSC apresenta algumas lacunas que importa serem corrigidas em próxima revisão, nomeadamente, a que decorre da ausência de atribuições à ciberdefesa (capacidade intrínseca das Forças Armadas) no quadro da coordenação político-estratégica para a segurança e defesa do ciberespaço.

Com o objetivo de dotar as entidades do Estado e os operadores de infraestruturas críticas nacionais com as valências mínimas para análise, mitigação e resolução de incidentes de segurança no ciberespaço, o CNCS definiu também entretanto um modelo de maturidade e um calendário de implementação visando a criação de capacidades mínimas de reação a incidentes de cibersegurança. Com base neste enquadramento, foi prontamente confirmado o alinhamento procedimental e técnico com o Centro de Ciberdefesa (CCD) das Forças Armadas, especificamente na vertente da capacidade de cibersegurança sectorial da Defesa Nacional. Pese embora o estabelecimento dos processos de troca de informação entre o CCD e o CNCS, o facto é que

ainda não se materializou o necessário esforço cooperativo entre os vários órgãos com responsabilidades na segurança do ciberespaço nacional, conforme preconiza a ENSC. Neste contexto, urge iniciar rapidamente este processo, que deverá ocorrer sob a direção do CNCS, devendo os esforços iniciais serem canalizados para a caraterização das eventuais ameaças e partilha de informação técnica.

Conclui-se assim que a eficácia das ações de defesa do ciberespaço depende, fundamentalmente, da atuação sinérgica e colaborativa da sociedade portuguesa, envolvendo não apenas os órgãos do Ministério da Defesa Nacional (MDN), do Estado-Maior-General das Forças Armadas (EMGFA) e dos Ramos das Forças Armadas (Marinha, Exército e Força Aérea), mas também as entidades responsáveis pela cibersegurança do País, a comunidade académica, os sectores público e privado e a base industrial de defesa.

3.8. Cooperação Internacional

No contexto de alianças e de compromisos internacionais, os Estados têm hoje que articular as suas políticas e estratégias nacionais, de forma a reforçar a defesa de intereses comuns e a salvaguardar valores coletivos. Com o intuito de identificar possíveis áreas de cooperação futuras, desta feita no plano internacional, importa caracterizar as principais iniciativas e esforços cooperativos no âmbito da segurança e defesa do ciberespaço.

As caraterísticas difusas de que se reveste o ciberespaço, nomeadamente, as que se referem à dificuldade ou mesmo impossibilidade de se estabelecerem os seus limites e esferas de responsabilidade, exigem que as respostas, nomeadamente às ações hostis que nele se desenvolvem, só possam ser encontradas num ambiente de franca cooperação e colaboração. Este princípio, consubstanciado no facto de dificilmente ser possível encontrar localmente resposta para problemas de natureza global, aplica-se tanto à necessidade de desenvolver sinergias nacionais (domínio público/privado) como ao nível da cooperação internacional, sendo neste último domínio atribuído especial destaque à cooperação internacional com as principais organizações internacionais que Portugal integra.

O crescente número de incidentes cibernéticos, que têm recentemente vindo a afectar transversalmente vários Estados, evidencia a necessidade de desenvolver, implementar e coordenar políticas cooperativas. Estas políticas, orientadas para a melhoria da capacidade de resposta conjunta dos Estados à ocorrência de ciberataques, devem ser capazes de abordar de forma agregada as questões relacionadas com a cibersegurança e ciberdefesa do ciberespaço, estabelecendo mecanismos de cooperação efetiva entre Estados, dentro e fora da Aliança Atlântica e da UE.

Com esta finalidade, a NATO aprovou a sua "*Enhanced Policy on Cyber Defence*", subscrita pelos chefes de estado e de governo dos Países Aliados na Cimeira de Gales, onde reconheceu o aumento das ameaças cibernéticas contra as redes e sistemas dos Aliados e da NATO, prevendo a adoção de uma resposta conjunta para fazer face a essas ameaças, independentemente de se tratar de ataques puramente cibernéticos ou correlacionados com operações militares convencionais. Na sequência desta decisão, Portugal e a NATO assinaram em 2016 um memorando de entendimento na área da ciberdefesa que permitirá implementar mecanismos de cooperação e assistência ao nível da partilha de informação relativa a ameaças e incidentes, assim como à condução de atividades bilaterais, tendo em vista a proteção das respetivas comunicações e sistemas de informação. Na resposta a incidentes de ciberdefesa, este documento inclui também os mecanismos que regulam o eventual pedido nacional de assistência à NATO.

No âmbito específico da ciberdefesa, Portugal assumiu também com a NATO diversos compromissos cronologicamente distribuídos, nomeadamente, o desenvolvimento de doutrina, normas e procedimentos operacionais que possibilitem a integração da ciberdefesa nas operações e no planeamento operacional, o reconhecimento da aplicação de legislação internacional ao ciberespaço e o estabelecimento de medidas de gestão de risco e partilha de informação.

No âmbito da partilha de informação entre a NATO e as nações aliadas, Portugal participa no projeto de Smart Defence "*Malware Information Sharing Platform (MISP)*" estando a avaliar a possibilidade de integrar o projeto "*Multinational Cyber Defence Capability Development* (MNCD2)" que, apesar das mais valias existentes, tem a sua adesão condicionada ao pagamento dos respetivos custos de participação. Também na área da educação, treino e exercícios, presentemente uma das mais prementes e onde a cooperação internacional se equaciona com maior acuidade, importa registar e salientar a natureza da participação nacional. Neste contexto, Portugal assume um papel de particular destaque, nomeadamente, por assegurar a liderança do projeto de Smart Defence "*Multinational Cyber Defence Education & Training*" e por estar prevista a edificação da futura *NATO Communications, Information & Cyber Academy* em Oeiras, trazendo desta forma uma acrescida visibilidade nacional perante a NATO e a comunidade internacional.

Tendo em vista o desenvolvimento de capacidades militares, agregando diversas iniciativas emergentes dos Estados Membros sobre a forma de uma cooperação multilateral sinérgica, a UE definiu também o conceito de "agregar e partilhar" ("*pooling & sharing*"), evitando desta forma duplicações desnecessárias e salvaguardando os interesses da UE. Neste contexto, o Comité Director das Capacidades (*Capabilities Steering Board)* da UE de 11 de outubro de 2012, manifestou um forte apoio às linhas de orientação estratégica propostas pela *European Defence Agency (EDA)* na área da ciberdefesa. Ao nível da UE, a cooperação na àrea da ciberdefesa tem como face mais visível a iniciativa "*EU*

Cyber Defence Centre/Capability", tendo sido cometida à EDA, no âmbito do *Capability Development Plan (CDP)*, a tarefa de analisar o conceito e a viabilidade da criação de um Centro/Capacidade de Ciberdefesa da UE. Esta tarefa deu origem ao lançamento do projeto "*frameCyberCAP*" por parte da EDA, que culminou com o levantamento de um leque alargado de opções possíveis, situadas entre os extremos de não desenvolver qualquer capacidade (manter a situação atual) até à edificação plena de um centro de ciberdefesa de natureza operacional[16].

Também no âmbito da Educação e Treino na área da Ciberdefesa, Portugal tem vindo a assumir um papel de especial relevo nos esforços cooperativos da EU. Neste âmbito, assumiu em 2015, conjuntamente com a França, a liderança da Cyber Defence Discipline do EU Military Training Group (EUMTG), responsável pela definição dos requisitos de treino em ciberdefesa. Ainda neste domínio, na sequência de um processo aquisitivo lançado pela EDA, foi também atribuída a Portugal a gestão da futura Cyber Defence Training and Exercises Platform (CDTEXP). Esta plataforma, que se prevê venha a incluir diferentes domínios de utilização (nacional, EU e multinacional), constituirá certamente, a partir do final de 2017, uma efetiva ferramenta de cooperação e partilha de recursos na área da Educação, Treino e Exercícios, assegurando assim uma estreita cooperação com a NATO.

O nosso país tem reiteradamente defendido o reforço político do relacionamento NATO-UE e o aprofundamento da cooperação em "novas" áreas como a ciberdefesa ou o combate às ameaças híbridas. Enquanto Estado membro das duas organizações internacionais, Portugal tem vindo assim a defender o alinhamento estratégico das atividades de segurança e defesa já em curso ou a desenvolver no âmbito destas duas organizações. Para além da área da Educação e Treino em ciberdefesa, onde tem vindo a ter uma intervenção direta, Portugal tem ainda defendido a participação da UE em exercícios NATO de gestão de crises, onde se inclui a ciberdefesa, bem como a retoma de exercícios conjuntos (NATO-UE), que permitam testar procedimentos acordados entre as duas organizações.

No seio destas duas organizações internacionais, Portugal apoiou a declaração conjunta NATO-EU, assinada em julho de 2016, na Cimeira de Varsóvia, considerando que faz sentido político uma declaração alargada que vá ao encontro da partilha de valores comuns e à união das duas organizações para fazer face aos desafios de segurança atuais. Em matéria de desenvolvimento de capacidades, o nosso País tem sublinhado a necessidade da exploração de

[16] Para além destas opções, foram também ainda identificados como modelos possíveis para a implementação deste Centro: (1) o estabelecimento de uma solução híbrida que consiste num "Virtual/Networked Cyber Defence Centre", com apoio por parte de diferentes *clusters* de peritos[16]; (2) o modelo anterior em versão reduzida abrangendo somente a educação, treino e exercícios; (3) uma solução híbrida somente para as áreas da educação, treino e exercícios, com uma "Executive Academic Board" sob a égide do *European Security and Defence College* (ESDC), responsável pelos aspetos da educação e treino no domínio da ciberdefesa.

sinergias e da complementaridade das iniciativas a desenvolver, evitando assim a duplicação de esforços. No âmbito da ciberdefesa, em linha com esta orientação estratégica, Portugal tem procurado aproximar a NATO e a UE especialmente na vertente da formação e treino, tendo em vista disponibilizar à EU a oferta curricular da futura escola de Oeiras, com óbvios ganhos mútuos, sobretudo tendo em consideração que a academia funcionará no regime de financiamento pelo cliente (por contraposição ao regime de financiamento comum da NATO).

Com impacto nacional no domínio da ciberdefesa, importa referir ainda a cooperação NATO - UE no quadro da "Política Reforçada de Ciberdefesa da NATO", aprovada em Gales. O acordo técnico entre os centros de resposta a incidentes cibernéticos da NATO e da UE constituiu o primeiro passo concreto dessa cooperação, que poderá facilitar a extensão a outras áreas, como a formação, treino e exercícios, e a partilha de doutrina sobre a integração da ciberdefesa no planeamento e condução das operações militares. A 2ª Conferência internacional dos Projetos de *Smart Defence* NATO na área da ciberdefesa, realizada em 28 de abril de 2016 em Lisboa, que contou com a participação de altos representantes da NATO e da UE, teve como foco principal a exploração de potenciais sinergias entre as duas organizações, tendo ficado patente o papel fulcral que a futura Academia NATO de Oeiras poderá desempenhar neste âmbito. Concorrentemente, Portugal vem desenvolvendo esforços no âmbito da ciberdefesa com países ibero-americanos, no domínio da CPLP e da iniciativa 5+5, com o objetivo de, a partir de afinidades organizacionais, culturais e linguísticas, se poderem vir a potenciar o desenvolvimento de iniciativas cooperativas ao nível da formação (competências em ciberdefesa, criação de conteúdos curriculares e intercâmbio académico), treino operacional, análise de informações de ciberdefesa e da investigação e desenvolvimento.

Atendendo ao conjunto de iniciativas internacionais, já em curso ou a lançar num futuro próximo por organizações a que Portugal pertence, constata-se existir uma visão doutrinária cada vez mais convergente, capaz de vir a favorecer uma estratégia comum. De forma sintética, a tabela apresentada no Anexo II identifica as áreas comuns de cooperação estratégica internacional no Ciberespaço, estruturando-as de acordo com os objetivos a atingir e com os elementos associados ao desenvolvimento de capacidades cooperativas na área da cibersegurança e da ciberdefesa. Para cada uma das possíveis linhas de desenvolvimento destas áreas e no âmbito das principais organizações internacionais a que Portugal pertence (NATO, EU, ONU/ITU e OCDE) procurou-se identificar também as iniciativas em curso e avaliar a sua relevância no domínio estratégico, operacional e económico/industrial.

A tabela apresentada permite assim identificar áreas comuns de cooperação internacional e de potencial convergência estratégica do nosso País, facto que poderá potenciar futuramente o desenvolvimento de sinergias e esforços cooperativos de natureza multilateral.

Conclui-se assim que, para Portugal, a Cibersegurança e a Ciberdefesa surgem como áreas de natural cooperação civil-militar e como áreas prioritárias de desenvolvimento de capacidades cooperativas, nomeadamente, segundo o conceito de "*Smart Defence*" no âmbito da NATO e de "*Polling & Sharing*" no contexto da UE.

Parte IV –
Quadro Legal para a Cibersegurança e a Ciberdefesa

Sofia de Vasconcelos Casimiro

Num Estado de Direito, a segurança e a defesa têm de atuar num quadro legal bem definido. Após a sedimentação secular de um quadro legal estável e relativamente eficaz nestas áreas, é chegado o momento de o adaptar ao contexto do ciberespaço. O crescente protagonismo deste novo domínio e o seu impacto nas diversas áreas da sociedade determinam a inevitabilidade da ponderação do seu posicionamento face ao Direito.

Para além de os atos praticados em rede poderem ser contrários a normas jurídicas e, assim, poderem desencadear uma responsabilidade civil, criminal, contraordenacional ou outra, esses atos podem colocar em risco a soberania, a independência nacional e a integridade do território, bem como a liberdade e a segurança das populações. O processo de indagação e de identificação daquelas que devem ser a principais preocupações na construção de um quadro legal para o ciberespaço leva-nos, assim, inevitavelmente a abordar as áreas da segurança e da defesa. O estudo de um quadro legal para a cibersegurança e a ciberdefesa apresenta-se, pois, como um capítulo necessário para a cabal compreensão destes fenómenos.

Este capítulo inicia-se com um enquadramento geral do Direito e dos conceitos de cibersegurança e de ciberdefesa, dando lugar, seguidamente, ao recorte dos principais grupos de questões jurídicas sobre cibersegurança e ciberdefesa, para, num terceiro momento, e em relação a cada grupo assim recortado, identificar as necessidades legislativas mais prementes. Este capítulo termina com conclusões preliminares, respeitantes ao tópico que o ocupa. De forma a auxiliar no acompanhamento deste capítulo, o esquema apresentado no Anexo III sintetiza as principais temáticas a abranger na construção de um quadro legal para a cibersegurança e a ciberdefesa.

4.1. Direito, Cibersegurança e Ciberdefesa

O Direito consiste num conjunto de normas de conduta social, que determinam como a sociedade se organiza e como os vários elementos que a compõem, humanos e institucionais, devem atuar. Muito embora haja sempre um espaço de liberdade, sobre o qual o Direito não se imiscui, a maior parte da vida em sociedade

está abrangida pelo Direito, com vista a conformar a atuação dos sujeitos aos desígnios em cada momento fixados pelos detentores do poder legislativo.

O ciberespaço tem assumido uma centralidade crescente no quotidiano dos Estados, das organizações e dos cidadãos, não podendo ser ignorado pelo Direito, que deverá, através das suas normas, contribuir para a sua otimização, prevenir conflitos e oferecer vias de resolução dos que venham a ter lugar. As questões jurídicas suscitados pelo ciberespaço são inúmeras e tendem a crescer à medida que as potencialidades das novas tecnologias de informação e comunicação se expandem. Nenhuma enumeração das questões jurídicas suscitadas pelo ciberespaço pode ser fechada, sendo que a cada avanço das tecnologias, ou a cada avanço na imaginação dos que a utilizam, novos desafios se colocam e, quase invariavelmente, com reflexos no mundo do Direito.

A crescente dependência da sociedade relativamente às tecnologias de informação e comunicação tem vindo a permitir destacar um grupo de questões jurídicas ligadas à segurança e defesa em rede, que podem identificar-se como questões jurídicas de cibersegurança e ciberdefesa.

A distinção entre a cibersegurança e a ciberdefesa não se apresenta ainda devidamente clarificada, mormente no campo do Direito, estando atualmente a delinear-se uma tendência, no campo internacional e nacional, para distinguir estas figuras, a montante, pelos diversos graus de segurança envolvida, intervenientes e ou valores em risco, bem como, a jusante, pelas suas consequências, potencialmente diversas, e formas de resposta. Não se insere no escopo deste capítulo dirimir esta questão. Contudo, para maior facilidade de compreensão destes conceitos no seio deste capítulo, será utilizada a expressão “ciberdefesa” para referir questões de segurança no contexto da utilização de meios eletrónicos que envolvam a segurança do próprio Estado (abrangendo a segurança das várias dimensões que o compõem: povo, território e poder político), reservando-se a expressão “cibersegurança” para todas as demais questões de segurança no contexto da utilização de meios eletrónicos.

4.2. Transversalidade do Tema e Principais Questões Jurídicas

Uma grande parte das questões jurídicas que hoje se suscitam no contexto do ciberespaço reconduz-se a questões jurídicas de cibersegurança ou ciberdefesa. O universo de temas relevantes para este trabalho, do ponto de vista jurídico, é assim alargado, aconselhando que se desenvolva um trabalho prévio de agrupamento desses vários temas em grandes temáticas aglutinadoras dos seus principais traços comuns. Este trabalho de agrupamento terá de assentar em critérios que se apresentem relevantes do ponto de vista jurídico.

A principal distinção, ou *summa divisio*, transversal a todos os demais grupos temáticos que se possam recortar, pode ser estabelecida entre as matérias enquadradas por normas jurídicas materiais ou substantivas (que designaremos "matérias substantivas") e as matérias enquadradas por normas jurídicas adjetivas ou processuais (que designaremos "matérias adjetivas"). Esta classificação pretende distinguir entre os temas essencialmente materiais, que respeitam diretamente às relações sociais, nomeadamente aos direitos atribuídos e deveres impostos; e os processuais, que se prendem com a efetivação das normas jurídicas substantivas pelos órgãos do Estado, quer sob o impulso dos interessados, quer oficiosamente.

Aplicando esta primeira classificação, podem autonomizar-se as matérias que, por exemplo, criminalizam certas atuações em rede ou que, por outra forma, regulam diretamente essas atuações ou atuações que tenham impacto na segurança das redes ou dos dados que nestas circulam, assim as separando das matérias relativas aos meios processuais necessários para a efetivação da responsabilidade por atuações em rede, incluindo nomeadamente os meios de recolha e de preservação da prova digital e as formas de cooperação internacional para fins de investigação.

Dentro de cada uma das ramificações resultante da aplicação da referida *summa divisio*, podem operar-se posteriores subdivisões. Assim, dentro das matérias substantivas, atendendo ao critério da imputação dos atos praticados em rede, impõe-se uma primeira bifurcação entre, por um lado, o enquadramento jurídico dos atos praticados em rede que sejam imputáveis a um Estado diverso daquele onde o incidente de segurança se verifica, e, por outro lado, o enquadramento jurídico dos demais atos praticados em rede. Consoante estejamos perante um ou outro contexto, o conjunto de normas jurídicas aplicáveis é distinto. Para facilitar a diferenciação, passaremos a designar o primeiro grupo de "atos imputáveis a um ou mais Estados" e o segundo grupo de "atos não imputáveis a um ou mais Estados".

Identificamos assim, desde já, pelo menos três grandes grupos temáticos: dentro das matérias substantivas, (i) o grupo dos atos imputáveis a um ou mais Estados; e (ii) o grupo dos atos não imputáveis a um ou mais Estados; autonomizando-se ainda, já fora das matérias substantivas, o (iii) grupo das matérias adjetivas. As próximas linhas seguem esta sequência, finalizando com uma súmula das principais conclusões resultantes deste excurso aos três grandes grupos temáticos identificados[17].

É necessário adiantar que a repartição entre os três referidos grupos, sendo embora útil para, de forma mais sumária – como se pretende num trabalho desta natureza – recortar os principais temas com relevância para o enquadramento jurídico nas áreas da cibersegurança e ciberdefesa, não esgota o universo dos que devem compõem este enquadramento. Várias outras repartições, assentes

[17] Veja-se o esquema constante do Anexo III.

em diversos critérios, podem ser feitas dentro de cada grupo. O presente trabalho não se compadece, porém, com a densificação da exposição que resultaria da adoção de um número superior de categorias. Por esta razão, far-se-á apenas uma referência ao facto de as matérias adjetivas, tal como as substantivas, carecerem sempre, necessariamente, de entidades que deem suporte às respetivas atividades. A criação destas entidades, ou a criação de novas atribuições e competências que possam ir ao encontro daquelas matérias adjetivas e substantivas, é um passo essencial para a completude de um quadro legal em cibersegurança e ciberdefesa. Esta referência não irá merecer autonomização, sendo antes incluída nas conclusões preliminares.

4.3. Matérias Substantivas

4.3.1. Atos imputáveis a um ou mais Estados

Nos casos em que um incidente – seja ou não qualificável como uso da força ou mesmo ataque armado – é imputável a um ou mais Estados[18], são aplicáveis as normas internacionais que regulam a relação entre os Estados, incluindo as normas respeitantes a conflitos, quer na vertente do *jus ad bellum*, quer na vertente do *jus in bellum*. Isto significa que as normas internacionais determinarão em que circunstâncias se deverão iniciar e desenrolar os conflitos. Em particular, quando se verifique um incidente através de meios informáticos que seja imputável a um ou mais Estados, e dependendo da natureza e da gravidade desse incidente, poderão ser aplicáveis a Carta das Nações Unidas e o Tratado do Atlântico Norte para determinar a possível reação do Estado que sofreu o incidente.

Cabe destacar, a este respeito, alguns dos resultados das mais recentes cimeiras da NATO, nomeadamente a Cimeira de Lisboa de 2010, a Cimeira de Gales, nos dias 4 e 5 de setembro de 2014, e a Cimeira de Varsóvia, nos dias 8 e 9 de julho de 2016. Estas duas cimeiras debruçaram-se sobre o enquadramento de ataques a Estados perpetrados por meios eletrónicos. Aquando da Cimeira de Lisboa de 2010, foi já tomado o compromisso de atender à dimensão ciber dos conflitos e de, nomeadamente, aumentar as capacidades de ciberdefesa[19].

Uma das conclusões resultantes da Cimeira de Gales, de 2014, foi a de considerar que o Direito Internacional, incluindo o Direito Internacional

[18] A imputação de atos aos Estados é aqui referida em termos muito amplos, abrangendo os casos em que eventuais atos lesivos estão a ser praticados através de um terceiro Estado que não é parte no conflito (por exemplo, através da instrumentalização dos seus servidores para realizar um ataque a outro Estado).

[19] Veja-se o número 2 e, sobretudo, o número 40 da Declaração da Cimeira de Lisboa, de 2010. A vertente do ciberespaço foi igualmente referida no novo Conceito Estratégico adoptado nessa Cimeira.

Humanitário e a Carta das Nações Unidas, é aplicável ao ciberespaço[20]. Especificou-se ainda que um ciberataque pode constituir um "ataque armado" suscetível de desencadear a aplicação do artigo 5.º do Tratado do Atlântico Norte, devendo a invocação deste artigo ser apreciada caso a caso pelo Conselho do Atlântico Norte[21].

Na Cimeira de Varsóvia de 2016, foi aprovado pelos Chefes de Estado o Compromisso de Ciberdefesa (*Cyber Defence Pledge*), que enquadra a dimensão ciber como uma nova dimensão operacional, ao lado do ar, terra e mar[22]. Esta mesma mensagem foi adotada nos documentos oficiais aprovados no seio da NATO, em que se reitera "o mandato defensivo da NATO e reconhece o ciberespaço como um domínio de operações no qual a NATO deve defender-se de forma tão eficaz como no ar, terra e mar"[23].

No plano internacional, o enquadramento legal dos atos imputáveis a um ou mais Estados, praticados através de meios eletrónicos, tende, assim, a ser equiparado aos atos praticados através de outros meios. Esta questão tem vindo a ser sucessivamente clarificada a nível internacional, devendo Portugal adotar todas as medidas que lhe permitam assumir um papel participativo nesta clarificação, não apenas para fazer ouvir a sua voz, como também para se assumir como um parceiro incontornável nesta matéria[24]. Tende-se, aliás, para uma clarificação crescente dos temas relacionados com a utilização dos meios eletrónicos através do trabalho doutrinário que tem vindo a ser desenvolvido sobre o texto dos principais tratados internacionais com relevância para esses temas, vertido no *Manual de Tallinn*[25]. Através deste trabalho doutrinário, procuram-se interpretar as referidas normas internacionais no contexto específico do ciberespaço, de maneira a que se clarifique se, e em que termos, são aplicáveis no ciberespaço. Uma vez que as normas internacionais que compõem o Direito Internacional dos Conflitos e o Direito Internacional

[20] Veja-se, em particular, o número 72 da Declaração da Cimeira de Gales, de 2014.

[21] *Ibis, ibidem*.

[22] Este documento encontra-se disponível em http://www.nato.int/cps/en/natohq/official_texts_133177.htm.

[23] Vejam-se, em particular, os pontos 70 e 71 do Comunicado da Cimeira de Varsóvia.

[24] Não há qualquer razão para que Portugal não participe ativamente neste momento definidor do novo domínio operacional e na respetiva configuração, nomeadamente, estando presente e intervindo nas reuniões sobre o tema e enviando especialistas nacionais para os principais *fora* onde este é discutido. Os trabalhos que foram desenvolvidos com vista a atualizar a primeira edição do *Manual de Tallinn* (veja-se a nota seguinte), são um exemplo de trabalhos onde teria sido importante assegurar a participação de especialistas portugueses.

[25] O título completo desta obra, que tem vindo a ser abreviadamente conhecida como *Manual de Tallinn*, consiste, na sua primeira edição, de 2013, em *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press, 2013), e, na sua recente segunda edição, de fevereiro de 2017, em *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017). Este manual consiste num trabalho doutrinário de especialistas em Direito Internacional dos Conflitos e em Direito Internacional Humanitário que visa analisar a aplicação, no contexto do ciberespaço, de um amplo leque de princípios e regras internacionais. É importante salientar que, como trabalho doutrinário que é, este manual não é vinculativo, muito embora seja invocado em diversas sedes e esteja a ocupar um papel orientador para os especialistas da área e para os próprios Estados.

Humanitário resultam de um longo e demorado processo, assente essencialmente no costume, este trabalho doutrinário procura acelerar esse processo, apontando respostas para questões jurídicas que, num contexto como o do ciberespaço, não se compadecem com demoras.

O trabalho doutrinário, por esta ou outras formas – salientando-se que Portugal pode ter a iniciativa de apresentar e organizar outras formas de contribuição para este trabalho – apresenta-se imprescindível para auxiliar na clarificação das muitas questões que ainda permanecem por responder.

O incidente que, em 2016, consistiu no acesso indevido e posterior divulgação não autorizada de um número muito elevado de mensagens de correio eletrónico que se encontravam armazenadas num servidor de correio eletrónico do Comité Nacional do Partido Democrata dos Estados Unidos da América, ocorrido em plenas eleições presidenciais norte-americanas, é bem ilustrativo das dificuldades de subsunção das novas realidades ao quadro legal vigente. Muito embora os Estados membros da NATO já tenham esclarecido que um ciberataque pode constituir um ataque armado, suscetível de desencadear a aplicação do artigo 5.º do Tratado do Atlântico Norte, as fronteiras do que pode constituir um ciberataque, enquadrável nesse regime, não estão ainda bem definidas. Uma corrente tem sustentado que um ciberataque só se verifica quando das atuações em rede resultem danos sobre bens materiais, mortos ou feridos. Outra corrente faz depender a qualificação não da natureza das consequências mas antes da dimensão dessas consequências[26]. Neste contexto, o enquadramento legal dos referidos eventos dividiu os especialistas, uma vez que não resultaram quaisquer danos sobre bens materiais, nem mortos ou feridos. Enquanto alguns identificaram apenas uma violação de leis nacionais, relacionadas com o acesso a infraestruturas civis, outros entenderam poder tratar-se de uma interferência inadmissível nos assuntos internos dos Estados Unidos da América, podendo mesmo representar uma violação da soberania deste Estado e, assim, do Direito Internacional[27].

Há, pois, que desenvolver esforços acrescidos para que o quadro legal aplicável a este e outros eventos em rede seja mais facilmente definido, permitindo determinar até onde poderão os Estados atuar, quer da parte dos que pretendam desenvolver certas atuações em rede, quer dos que pretendam reagir a estas atuações. Interessa, nomeadamente, fixar critérios para determinar quando o uso de meios eletrónicos poderá representar o uso da força e quando este uso da força se traduz já num ataque armado.

Com exceção de trabalhos como o de elaboração e desenvolvimento do *Manual de Tallinn*, que terão um grande peso nas soluções a acolher pelos vários Estados – e em cujo seio seria muito importante assegurar a participação de

[26] Veja-se o *Manual de Tallinn*, *op. cit.*, p. 56, número 9 da Regra 13 *et passim*.

[27] Jill Dougherty, *NATO cyberwar challenge: establish rules of engagement*, CNN, 2016, disponível em http://edition.cnn.com/2016/11/07/politics/nato-cyber-centre-international-law/index.html.

Portugal –, as normas internacionais específicas para o contexto do ciberespaço que vierem a ser criadas dependerão da concertação dos Estados, pelo que não merecerão maior atenção neste trabalho. Resta acrescentar que muito se ganharia, mormente em termos de segurança jurídica, se fosse criado um Direito Internacional sobre este e outros temas relacionados com a atuação no ciberespaço, para além da já existente Convenção sobre o Cibercrime ou Convenção de Budapeste, de 23 de novembro de 2001. Uma vez que o ciberespaço não conhece fronteiras – exceto aquelas que artificialmente se procuram implementar através de sistemas de filtragem ou por outras formas de bloqueio de acessos[28] – é um domínio que carece particularmente de uma abordagem concertada no plano internacional[29].

A nível nacional, contudo, são várias as medidas que podem ser adotadas por cada Estado com vista a contribuir para uma redução dos riscos inerentes a incidentes que sejam originados por meios eletrónicos e ou para uma maior agilidade na resposta a esses incidentes. Estas medidas são, contudo, medidas comuns aos atos que sejam imputáveis a outras entidades, uma vez que fazem sentido independentemente da autoria dos atos praticados por meios eletrónicos, pelo que se antecipa aqui um tema igualmente aplicável ao ponto seguinte.

Neste âmbito, interessa a cada Estado aprovar um quadro legal que imponha a implementação de medidas técnicas e organizativas adequadas à prevenção, gestão e redução dos riscos para a segurança das redes e dos equipamentos eletrónicos, bem como da informação e dos demais bens jurídicos que naqueles se suportam. A obrigação de implementação destas medidas deve ser transversal a todos os que interagem com meios eletrónicos, embora a sua aplicação deva atender ao papel que cada um ocupa, variando desde a imposição dos mais elementares deveres de cautela aos utilizadores comuns[30],

---

[28] O caso da *firewall* da China, que tem vindo a merecer a designação de *Great Firewall of China*, é bem ilustrativo da tentativa de implementar fronteiras no ciberespaço (veja-se, entre muitas outras possíveis referências, Simon Denyer, "China's scary lesson to the world: Censoring the Internet works", *The Washington Post*, 23 de maio de 2016, disponível em https://www.washingtonpost.com).

[29] O presidente da Microsoft apelou recentemente à criação de um Direito Internacional que fixasse normas respeitantes a ciberataques, naquilo que designou uma Convenção de Genebra Digital (veja-se Brad Smith, *The need for a Digital Geneva Convention*, disponível em https://blogs.microsoft.com). Entendemos igualmente que deveríamos procurar seguir este caminho, se para isso houver vontade e convergência de posições.

[30] Aos utilizadores comuns pode, por exemplo, impor-se o dever de assegurarem que têm instalado um antivírus atualizado e que têm uma formação para poder utilizar, com o mínimo de segurança, um equipamento eletrónico, mormente quando o mesmo se conecte a redes informáticas onde assentem bens jurídicos de terceiros, como equipamentos ou dados. Note-se que a grande maioria dos incidentes de segurança em rede, quando estes tenham origem maliciosa, resulta exatamente da falta de observância de regras básicas de segurança por parte dos utilizadores dos meios eletrónicos e prospera devido a esta mesma falta. O ataque de DDoS ao operador de DNS Dynamic Network Services, Inc., conhecido pelo logótipo Dyn, em 21 de outubro de 2016, é bem demonstrativo desta afirmação, sendo embora apenas um dos muitos casos que poderiam ser aqui referenciados para o efeito. Neste ataque, explorou-se a falta de proteção de vários dispositivos da IoT ligados à rede, desde impressoras a câmaras Web, pertencentes a milhões de

até à imposição de deveres de garantir a segurança e a integridade dos meios e, por essa forma, a continuidade dos serviços ou a proteção dos bens que se suportam nos referidos meios electrónicos, a todos os que detenham controlo sobre esses meios.

De igual forma, os Estados devem estruturar um quadro legal que, verificados determinados requisitos, imponha a notificação dos incidentes de segurança com determinada relevância e, sobretudo, com possível impacto para terceiros, seja pela dimensão do incidente, seja pela sua capacidade difusora, seja ainda pela probabilidade de se repetir noutro contexto. Para além de se poder prever a obrigação de a referida notificação ser efetuada a outras entidades, deve, antes de mais, ser imposta a obrigação de ser efetuada a uma entidade que centralize as várias informações relativas a incidentes por meios eletrónicos e que possa emitir orientações quanto aos próximos passos a seguir pela entidade visada, bem como, quando necessário, reencaminhar a informação para outras entidades.

Em Portugal, ambas as referidas obrigações, quer de implementação de medidas de segurança, quer de notificação, encontram-se previstas, nesta data, apenas para o sector das comunicações eletrónicas[31]. As empresas que oferecem redes de comunicações públicas ou serviços de comunicações eletrónicas acessíveis ao público têm a obrigação de implementar as medidas técnicas e organizativas adequadas à prevenção, gestão e redução dos riscos para a segurança das redes e serviços, com vista a impedir ou minimizar o impacto dos incidentes de segurança nas redes interligadas, a nível nacional e internacional, e nos utilizadores. Quando se verifiquem violações de segurança ou perdas de integridade com impacto significativo no funcionamento das redes e serviços, as empresas que oferecem redes de comunicações públicas ou

---

utilizadores dispersos por todo o mundo (vejam-se, por exemplo, as declarações emitidas pela Dynamic Network Services, Inc., a propósito destes ataques, intituladas *Dyn Statement on 10/21/2016 DDoS Attack, de 22 de outubro de 2016,* e *Dyn Analysis Summary of Friday October 21 Attack*, de 26 de outubro de 2016, disponíveis no endereço http://dyn.com/blog, bem como artigo da BBC intitulado *'Smart' Home Devices Used as Weapons in Website Attack*, de 22 de outubro de 2016, disponível em http://www.bbc.com/news/technology-37738823).

[31] Veja-se a Lei das Comunicações Eletrónicas, aprovada pela Lei n.º 5/2004, de 10 de fevereiro, e, em particular, os seus artigos 54.º-A a 54.º–G, introduzidos pela Lei n.º 51/2011, de 13 de Setembro. Note-se, contudo, que estas obrigações legais, que atualmente se verificam apenas no sector das comunicações eletrónicas, não afastam a possibilidade de as entidades, voluntariamente, as implementarem, quer individualmente, quer através da adesão a códigos de conduta ou a outros instrumentos que agrupem determinados atores – normalmente por sectores de atividade, como sucede no sector da banca. Neste sentido, destaca-se o facto de várias entidades optarem por implementar medidas técnicas e organizativas para proteger as suas redes e dados e por notificarem os incidentes de segurança que eventualmente ocorram. Esta notificação é normalmente efetuada a parceiros estratégicos, entidades encarregadas dessas funções no sector em questão, ou a outras entidades que entendam relevantes para cada contexto, bem como à entidade que, em cada momento, centralize informações sobre incidentes de cibersegurança, como sucede com o CERT nacional.

serviços de comunicações eletrónicas acessíveis ao público devem notificar a Autoridade Nacional de Comunicações (ANACOM)[32].

Quando haja violação da segurança que provoque, de modo acidental ou ilícito, a destruição, perda, a alteração, a divulgação ou o acesso não autorizado a dados pessoais transmitidos, armazenados ou de outro modo tratados no contexto da prestação de serviços de comunicações eletrónicas acessíveis ao público, as empresas que oferecem serviços de comunicações eletrónicas acessíveis ao público devem ainda notificar a Comissão Nacional de Proteção de Dados e, se estiver em causa a violação de dados pessoais que possam afetar negativamente os assinantes ou utilizadores dos serviços, notificar estes assinantes ou utilizadores afetados para que estes possam tomar as precauções necessárias[33].

Fora do sector específico das comunicações eletrónicas, apenas encontramos, no Direito português, obrigações gerais impostas aos responsáveis pelo tratamento de dados pessoais, que devem implementar medidas técnicas e organizativas adequadas para proteger os dados pessoais contra qualquer forma de tratamento ilícito dos dados[34].

O Direito da União Europeia determinará, contudo, que o cenário legal atual se altere a muito curto trecho. Com efeito, a aprovação da Diretiva de segurança das redes e da informação[35] determina que o Estado português integre no seu ordenamento jurídico, até ao dia 9 de maio de 2018, normas jurídicas que imponham a todos os operadores de serviços essenciais, bem como aos prestadores de serviços digitais, obrigações de implementação de medidas técnicas e organizativas adequadas e proporcionadas para gerir os riscos que se colocam à segurança das redes e dos sistemas de informação que utilizam no contexto da sua atividade. Deve igualmente ser imposta, a estas entidades, a obrigação de tomar as medidas adequadas para evitar os incidentes e para reduzir ao mínimo o seu impacto, a fim de assegurar a continuidade dos seus serviços.

---

[32] Esta notificação deve ter lugar nas circunstâncias, no formato e de acordo com os procedimentos descritos no Anexo A da Decisão da ANACOM de 22 de dezembro de 2011. Verificadas determinadas circunstâncias, descritas na Lei das Comunicações Eletrónicas, pode ser ainda obrigatória a divulgação ao público dos incidentes verificados, caso em que se deverão seguir os procedimentos descritos no Anexo B desta mesma Decisão. A ANACOM aprovou, por decisão de 29 de dezembro de 2016, um projeto de regulamento relativo à segurança e à integridade das redes e serviços de comunicações eletrónicas que irá substituir a referida Decisão de 22 de dezembro de 2011. Nos termos legais, este projecto foi submetido a um procedimento de consulta pública, que terminou o seu prazo no dia 14 de março de 2017. A ANACOM encontra-se a analisar os contributos que recebeu no âmbito da consulta pública, com vista a aprovar o texto final do regulamento.

[33] Estas obrigações de notificação em caso de violação de segurança que afete os dados pessoais encontram-se reguladas na Lei n.º 41/2004, de 18 de agosto (alterada e republicada pela Lei n.º 46/2012, de 29 de agosto) e no Regulamento (UE) n.º 611/2013, que estabelecem as circunstâncias, prazos e o tipo de informações que devem ser prestadas.

[34] Vejam-se os artigos 14.º e 15.º da Lei da Proteção de Dados Pessoais (LPDP), aprovada pela Lei n.º 67/98, de 26 de outubro.

[35] Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho de 6 de julho de 2016 relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União.

Dentro do mesmo período temporal, o Estado português deve ainda impor a estas mesmas entidades a obrigação de notificação, sem demora injustificada, dos incidentes com um impacto importante na continuidade dos serviços por si prestados.

Com a transposição da referida Diretiva, estender-se-ão a outros sujeitos as obrigações que, atualmente, estão só previstas – e com contornos diferentes – para o sector das comunicações eletrónicas.

De igual forma, a aprovação do Regulamento Geral sobre a Proteção de Dados[36] determinará o alargamento dos deveres de notificação em caso de violação de dados pessoais, atualmente previstos apenas para o sector das comunicações eletrónicas. Com a aplicação deste Regulamento – que, apesar de já ter entrado em vigor no dia 24 de maio de 2016, só será plenamente aplicável a partir de 25 de maio de 2018 – estes deveres de notificação serão aplicáveis a todas as entidades que tratem dados pessoais.

Estas obrigações, respeitantes à implementação de medidas de segurança e a notificações em caso de verificação de incidentes de segurança, serão aplicáveis transversalmente, quer os atos perpetrados em rede sejam da autoria de Estados ou de qualquer outra entidade, contribuindo, num e noutro contexto, para reforçar a segurança dos Estados, das organizações e dos cidadãos.

Estas matérias, sendo embora essenciais para a construção de um quadro legal de cibersegurança e ciberdefesa, não são ainda suficientes para dotar o Estado de todos os instrumentos necessários para fazer face a estas realidades. Cabe ainda questionar se Portugal está dotado de instrumentos jurídicos que lhe permitam (i) reunir informação suscetível de prevenir ou de diminuir os riscos decorrentes de atos ilícitos praticados em rede que possam colocar em risco a segurança do Estado; e (ii) realizar operações em rede para garantir esta mesma segurança do Estado. Em determinados contextos, não bastará assumir uma postura preventiva ou mesmo reunir todas as informações relativas à autoria dos ataques e ao modo de atuação, sendo necessário adotar uma postura ativa com vista à cessação dos ataques, à neutralização das ameaças e, em suma, à defesa dos interesses fundamentais do Estado.

Ora, este quadro legal não existe. Atualmente, perante as normas jurídicas vigentes em Portugal, num contexto em que se verifiquem atos ilícitos praticados em rede que exijam a atribuição de competências que não estão atribuídas e a adoção de medidas que não estão previstas, dificilmente se conseguirá reagir sem que se apele aos regimes do estado de sítio e do estado de emergência[37] Estes regimes foram delineados num momento histórico em que o ciberespaço

[36] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE.

[37] Este regime encontra-se previsto essencialmente na Constituição da República Portuguesa, mormente nos artigos 19.º e 138.º, e na Lei n.º 44/86, de 30 de setembro, com as alterações introduzidas pela Lei Orgânica n.º 1/2011, de 30 de novembro, e pela Lei Orgânica n.º 1/2012, de 11 de Maio.

não existia, não atendendo assim a qualquer especificidade que possa decorrer dos meios eletrónicos. Contudo, e sem prejuízo de os referidos regimes poderem ser acionados também em caso de ciberataques, entende-se essencial e urgente a criação de um quadro legal que enquadre, independentemente de qualquer declaração de estado de sítio ou de emergência, operações em rede e, em geral, operações realizadas por meios eletrónicos, que sejam adequados para a defesa de interesses fundamentais do Estado e, em geral, para a defesa do Estado. Este quadro legal, a implementar na área da defesa nacional, deverá abranger a previsão de um corpo de entidades e órgãos a quem caberá a sua implementação, bem como a realização das operações propostas, encabeçadas por um órgão de tomada de decisão superior e, com mais ou menos intercalações de níveis diversos de poder de tomada de decisão, terminar, na base, com um órgão operacional, de execução das decisões tomadas.

Esta é uma importante lacuna do ordenamento jurídico português, que urge colmatar com a maior celeridade.

4.3.2. Atos não imputáveis a um ou mais Estados

No contexto dos atos não imputáveis a Estados[38], afastam-se as normas jurídicas internacionais destinadas a regular os conflitos entre Estados, entrando em cena todo um enquadramento jurídico distinto em matéria de responsabilização pelos atos praticados por meios eletrónicos.

Paralelamente às normas jurídicas aplicáveis em qualquer dos contextos, nomeadamente as que impõem deveres de implementação de medidas de segurança e de notificação, bem como as que definem o quadro legal para as operações em rede, já abordadas no ponto anterior, justifica-se um quadro legal específico para a responsabilização por atos ilícitos praticados por meios eletrónicos.

Pode optar-se por vários tipos de responsabilização, tendo sentido abranger quer a responsabilidade criminal, quer a responsabilidade civil, quer ainda, em determinados contextos, uma responsabilidade contraordenacional.

A responsabilidade criminal por atos que possam atentar contra a segurança dos meios eletrónicos, bem como contra os vários bens jurídicos que nestes se suportam, encontra-se já prevista no Direito Penal português. São disso exemplo o acesso indevido a dados pessoais[39] e outros atos previstos na LPDP, bem como, sobretudo, os que se encontram tipificados nos artigos 3.º a 8.º da Lei do Cibercrime[40]. Nesta matéria, praticamente todos os atos que possam atentar contra a cibersegurança e a ciberdefesa encontram-se abrangidos, sendo, assim, suscetíveis de desencadear responsabilidade criminal (muito embora, num ou

[38] Recordem-se os termos amplos em que esta expressão é utilizada, conforme indicado na nota (18).
[39] Veja-se o artigo 44.º da LPDP.
[40] A Lei do Cibercrime foi aprovada pela Lei n.º 109/2009, de 15 de Setembro.

noutro ponto, se justificasse uma intervenção do legislador para dirimir dificuldades de interpretação ou mesmo para suprimir disposições legais que se tornaram obsoletas, como sucede respetivamente nos casos dos artigos 221.º e 193.º do Código Penal; ou ainda para cominar a atuação com penas mais graves, quando, por exemplo, as mesmas se inserem num processo de engenharia social).

O ordenamento jurídico português já não se encontra tão bem apetrechado em matéria de disposições legais que limitem determinadas atuações, no contexto dos meios eletrónicos, quando as mesmas não se revistam de uma gravidade tal que mereçam um enquadramento criminal. Na verdade, pode justificar-se que certas normas que têm vindo a ser incluídas na chamada ética de atuação em rede venham a ser acolhidas pelo Direito positivo, quando se verifique que a sua observância tem um impacto demasiado relevante na cibersegurança e ciberdefesa para serem ignoradas. Estas normas podem ser acolhidas com vista a diminuir os danos decorrentes de atos ilícitos praticados em rede e a facilitar a investigação posterior desses atos. A definição concreta de quais sejam estas normas deve estar sujeita a um apertado juízo de proporcionalidade, com vista a evitar uma limitação injustificada e desnecessária da liberdade dos sujeitos. Exemplos de algumas destas normas podem ser encontrados na imposição, dentro de determinadas circunstâncias, de especiais deveres aos utilizadores, quando utilizem meios eletrónicos disponibilizados ao público, como sejam deveres de manter nos próprios equipamentos eletrónicos programas informáticos que assegurem, dentro de determinados níveis de probabilidade, que não estão infetados com programas maliciosos[41]; ou a imposição de deveres a quem disponibilize a terceiros o acesso a meios eletrónicos, de forma a assegurarem que controlam a identificação de quem acede a esses meios[42]. A

[41] As normas jurídicas devem refletir a consciência social. Contudo, em determinadas matérias, deve ser o poder legislativo a conformar essa consciência social, alertando para necessidades e desenvolvendo, paulatinamente, a convicção da sua essencialidade. Muito embora os referidos deveres de conduta possam ser inicialmente entendidos como uma inadmissível intervenção no espaço de liberdade de cada um, os efeitos perniciosos da sua inobservância podem assumir proporções demasiado gravosas para continuar a ignorar-se a sua indispensabilidade. Estes deveres, repita-se, devem ser criados com a mínima extensão possível, no que for estritamente necessário para cumprirem os fins a que se destinam.

[42] Uma eventual via de evolução futura, nesta sede, poderá ser a da eliminação ou redução, em grande medida, do anonimato em rede. Sendo embora muito polémica neste momento histórico em que nos encontramos, uma vez que não merece a adesão por parte da opinião pública a nível mundial, e contraria mesmo o crescente reforço da privacidade em várias partes do globo – de que é exemplo último o Regulamento Geral sobre a Proteção de Dados, no espaço da União Europeia –, esta via de evolução pode vir a encontrar um maior acolhimento por parte da opinião pública à medida que os efeitos devastadores dos incidentes em rede aumentem e sejam mais visíveis para o utilizador comum, podendo, ademais, ser devidamente conciliada com as preocupações de privacidade, atendendo sempre aos princípios da necessidade, adequação e proporcionalidade. A procura da eliminação de um total anonimato em rede poderia passar pela imposição de novos deveres aos prestadores de serviços de comunicações eletrónicos e a todas as demais entidades que, noutros contextos, dessem acesso a redes de comunicações eletrónicas, de maneira a que estivessem sempre em condições de fornecer a identificação dos concretos utilizadores da rede, em cada momento, caso essa identificação fosse necessária no contexto da investigação de determinado tipo de crimes. Note-se que este cenário significaria

violação de tais normas desencadearia a responsabilidade civil pelos danos criados – o que já poderá verificar-se atualmente, em determinadas circunstâncias, embora haja vantagem em clarificar muitas destas situações – e, em certos casos, poderia determinar uma responsabilidade contraordenacional.

Adicionalmente, quando as referidas atuações em rede sejam suscetíveis de colocar em risco a defesa do Estado, deve criar-se um quadro legal específico, na área da defesa nacional, que permita identificar claramente a quem cabe a competência para tomar decisões quanto aos próximos passos e que atribua capacidades operacionais para reagir, nos termos do que já foi referido no ponto anterior.

4.4. Matérias Adjetivas

As matérias adjetivas assumem uma importância central na cibersegurança e ciberdefesa. Sem um Direito adjetivo devidamente estruturado e eficaz, o Direito substantivo fica esvaziado, sem meios de se impor coercivamente. Uma vez apurada a prática de um ato ilícito em rede, importa atuar celeremente com vista à sua cessação e repressão. Destacamos, de entre as matérias que se enquadram nas normas adjetivas, as relacionadas com a coordenação e a cooperação entre as entidades nacionais com competências nas áreas da cibersegurança e ciberdefesa; as relacionadas com a cooperação internacional; e as relacionadas com a prova digital.

Num contexto como o dos meios informáticos e das redes informáticas, é essencial assegurar a coordenação e a cooperação entre entidades com competências nas áreas da cibersegurança e ciberdefesa. Neste momento, não

levar mais longe a já existente Lei n.º 32/2008, de 17 de julho. A este propósito, deve referir-se uma recente decisão proferida pelo Tribunal de Justiça da União Europeia (TJUE), no âmbito do processo C-484/14, que se destinava a apurar a responsabilidade de uma empresa que, dedicando-se a uma atividade que em nada está relacionada com a prestação de serviços de comunicações eletrónicas – uma vez que a empresa vende ou aluga material de iluminação e de som –, disponibiliza, nas suas instalações, acesso gratuito e anónimo à Internet, através dos serviços de acesso que contrata a um prestador de serviços de comunicações eletrónicas. Pela disponibilização de acesso gratuito e anónimo à Internet, esta empresa procurava atrair mais clientes, tal como sucede atualmente com várias outras empresas, em vários sectores de atividade. Sucede, porém, que através do acesso assim concedido, foram disponibilizados em rede determinados conteúdos protegidos por direitos de autor e direitos conexos, sem que tivesse sido dada a devida autorização por parte dos respetivos titulares dos direitos. Neste processo procurava-se assim apurar até que ponto deveria a empresa ser responsabilizada pelos atos ilícitos praticados por terceiros através do acesso que disponibilizava à rede Internet. Na sua decisão, proferida em 15 de Setembro de 2016, o TJUE rejeitou a responsabilidade da empresa pelos atos ilícitos praticados – à luz da Diretiva 2000/31/CE, que consiste na Diretiva sobre o Comércio Eletrónico, transposta na nossa ordem jurídica pela Lei n.º 7/2004, de 7 de janeiro. Contudo, o TJUE abriu a possibilidade de o tribunal nacional impor à empresa a obrigação de garantir a segurança do acesso à rede pela implementação de um procedimento que consistisse em dar a palavra-passe de acesso à rede apenas a quem previamente se identificasse perante a empresa, assim impedindo o acesso anónimo à Internet.

se identificam normas jurídicas que imponham esta coordenação e cooperação a todas as entidades com relevância nestas áreas, verificando-se ainda que as raras normas que referem esta cooperação são excessivamente vagas e não esclarecem quanto aos canais de comunicação a estabelecer ou às formas de interação a desenvolver. É necessário fixar um quadro legal que imponha, de forma clara, os procedimentos de coordenação e de cooperação entre as referidas entidades. A necessidade de estabelecer mecanismos claros de coordenação e de cooperação entre o Centro Nacional de Cibersegurança e o Centro de Ciberdefesa das Forças Armadas representa um exemplo manifesto da lacuna identificada no atual ordenamento jurídico português quanto à coordenação e cooperação nas áreas versadas, muito embora as lacunas de regulamentação sejam mais abrangentes e se estendam muito para além do seu núcleo mais evidente. Uma vez que muitos sectores estratégicos do Estado português se encontram na mão de entidades privadas, este dever deve abarcar, indistintamente, o sector público e o sector privado, devendo ainda abranger muitas áreas de atividade. A colmatação desta lacuna pode passar pela criação de um órgão superior de coordenação, que seja exterior às entidades que vise coordenar, mas que consiga trabalhar em estreita ligação com as mesmas.

O Direito português não integra ainda um regime jurídico suficientemente desenvolvido a este respeito. Muito embora haja disposições legais esparsas sobre deveres de colaboração e de obediência[43], que determinam uma necessária interação entre certas entidades, estas disposições não se encontram devidamente harmonizadas, não se ligam sistematicamente entre si nem formam, por isso, um corpo coerente e completo de normas sobre o tema.

[43] A título de exemplo, note-se que, por força do n.º 1 do artigo 6.º da Lei de Bases da Proteção Civil, aprovada pela Lei n.º 27/2006, de 3 de julho, todos os cidadãos têm o dever de colaborar na prossecução dos fins de segurança interna, cumprindo as disposições preventivas estabelecidas na lei, acatando ordens e mandados legítimos das autoridades e não obstruindo o normal exercício das competências dos funcionários e agentes das forças e dos serviços de segurança. Os funcionários (na aceção do artigo 386.º do Código Penal), e os militares têm o dever especial de colaboração com as forças e os serviços de segurança, nos termos da lei. Tal significa que, se no decorrer dos ciberincidentes, e em resposta aos ciberincidentes, as forças e os serviços de segurança solicitarem colaboração, esta colaboração deve ser prestada (podendo mesmo, caso não se colabore, incorrer na prática de um crime de desobediência, p.p. no artigo 348.º do Código Penal).
Acresce ainda que os funcionários e agentes do Estado e das pessoas coletivas de direito público, os membros dos órgãos de gestão das empresas públicas, bem como os responsáveis pela administração, direção ou chefia de empresas privadas cuja laboração, pela natureza da sua atividade, esteja sujeita a qualquer forma específica de licenciamento, têm o dever especial de colaboração com os órgãos e agentes de proteção civil (n.ºs 2 e 3 do artigo 6.º da Lei de Bases da Proteção Civil). A violação deste dever especial de colaboração implica, consoante os casos, responsabilidade criminal (pela prática do crime de desobediência) e disciplinar, nos termos do n.º 5 do artigo 6.º da Lei de Bases da Proteção Civil.
Para além deste dever especial, qualquer desobediência e a resistência às ordens legítimas das entidades competentes de proteção civil, quando praticadas em situação de alerta, contingência ou calamidade, são sancionadas nos termos da lei penal e as respetivas penas são sempre agravadas em um terço, nos seus limites mínimo e máximo (n.º 4 do artigo 6.º e artigo 11.º da Lei de Bases da Proteção Civil). Quaisquer falhas na implementação das medidas de proteção civil poderão desencadear responsabilidade civil, nos termos gerais, e, eventualmente, responsabilidade disciplinar.

De igual forma, no atual panorama de globalização, impulsionado exatamente pelos meios informáticos, a cooperação internacional é um vetor central para o sucesso de grande parte das diligências destinadas a identificar o autor do ato ilícito e a responsabilizá-lo por esse ato.

No campo específico dos "crimes relacionados com sistemas ou dados informáticos, bem como para efeitos de recolha de prova, em suporte electrónico, de um crime", esta cooperação internacional já se encontra prevista no Direito português[44], como resultado sobretudo da ratificação da Convenção sobre o Cibercrime. Contudo, a falta de uniformização dos procedimentos adotados pelos vários Estados, da configuração concreta dos vários tipos de crimes, das permissões existentes em cada Estado para dar acesso a elementos de identificação ou outros que sejam úteis para fins de investigação, bem como a falta de uniformização da terminologia acolhida em cada legislação, em sede de Direito Penal e Direito Processual Penal, entre outros fatores, têm representado um grande entrave ao estabelecimento de uma eficaz cooperação internacional nestas áreas, mesmo dentro do espaço da União Europeia. Adicionalmente, várias situações ficam de fora da matéria relacionada com os referidos crimes relacionados com sistemas ou dados informáticos, nomeadamente, quando se pretende uma cooperação para fins de defesa do Estado, independentemente da prática de algum crime. A cooperação internacional é, assim, uma matéria que carece de uma intervenção do legislador, embora, uma vez mais, dependa de uma concertação entre Estados, não dependendo apenas do legislador português. Por esta razão, tal como se verificou a propósito das normas jurídicas que respeitam ao enquadramento dos atos imputáveis a um ou mais Estados, não será incluída entre as matérias identificadas enquanto prioritárias na atuação do legislador português. O facto de este critério conduzir ao afastamento da qualificação das normas de cooperação internacional, bem como das normas de enquadramento dos atos imputáveis a um ou mais Estados, como prioritárias não deve levar ao esmorecimento dos esforços de concertação, a nível internacional, nestas matérias. Deve antes perceber-se que, no contexto de globalização atual, estas normas são de importância central para que as demais não fiquem esvaziadas de todo o seu efeito útil.

O terceiro ponto referido, respeitante à prova digital, carece também de uma intervenção do legislador português. Muito embora haja avanços muito significativos nos anos recentes no sentido de clarificar os meios de prova admissíveis e a forma como poderão ser recolhidos, preservados ou acedidos[45],

[44] Vejam-se os artigos 20.º e seguintes da Lei do Cibercrime, aprovada pela Lei n.º 109/2009, de 15 de setembro.

[45] Veja-se, de novo, a Lei do Cibercrime (artigos 11.º e seguintes), bem como a Lei n.º 32/2008, de 17 de julho, e os artigos 187.º a 189.º do Código de Processo Penal, com a alteração operada pela lei n.º 48/2007, de 29 de agosto. Refira-se aqui, até a título de exemplo dos múltiplos avanços e recuos na área, que a Diretiva da União Europeia que determinou a aprovação da Lei n.º 32/2008, de 17 de julho (Directiva n.º 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de Março, relativa à conservação de dados gerados ou tratados no contexto da oferta de

ainda há um grande trabalho a realizar para que se alcance um regime jurídico completo e eficaz nesta matéria. Este tema tem sido marcado por sucessivos avanços e recuos, mesmo ao nível da interpretação das normas jurídicas aplicáveis, que não têm contribuído para uma simplificação e consolidação das práticas adotadas pelos que, diariamente, têm que lidar com estas realidades. A definição de um quadro legal claro que permita harmonizar práticas de tratamento da prova digital, incluindo nesta expressão todas as operações sobre a mesma – como a preservação, recolha, acesso, entre muitas outras – é central para que se otimizem os meios disponíveis, se simplifiquem operações, se alcance uma maior taxa de sucesso no aproveitamento das provas e se reforce a cooperação internacional – pela adoção de práticas aceites a um nível geograficamente mais alargado[46].

Adicionalmente aos pontos atrás identificados, devem ainda ser aprovadas as normas adjetivas que sirvam de suporte às normas substantivas que vierem a ser criadas.

4.5. Conclusões Preliminares

Do atrás exposto, no que ao enquadramento legal respeita, resulta a identificação de várias insuficiências do ordenamento jurídico português em matéria de cibersegurança e ciberdefesa[47]. Atendendo às características e circunstancialismos do presente trabalho, elaborado num curto período temporal e destinado a captar os traços mais impressivos dentro destes temas, sem pretensões de exaustividade e de profundidade, destaca-se, em particular, a

serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações), foi considerada inválida pelo Tribunal de Justiça da União Europeia com base no entendimento de que a retenção de dados pessoais nela prevista restringia em demasia a privacidade dos cidadãos, sem que os fins de investigação criminal visados justificassem essa restrição, de acordo com um juízo de proporcionalidade (Acórdão do Tribunal de Justiça da União Europeia proferido no dia 8 Abril 2014, no âmbito dos processos C-293/12 e C-594/12).

[46] As normas ISO nesta matéria são um bom exemplo a seguir no sentido da harmonização das práticas adotadas, assim contribuindo igualmente para uma melhor cooperação internacional e para o maior sucesso no aproveitamento das provas. Estas normas devem, porém, ser acolhidas pela legislação para que tenham carácter vinculativo.

[47] Salienta-se que o facto de certas temáticas não serem incluídas entre as que são identificadas no capítulo como merecedoras de uma intervenção legislativa mais urgente e detalhada não significa que o respetivo regime seja isento de falhas e não necessite de vários aperfeiçoamentos. A temática da cooperação internacional no contexto das matérias adjectivas, como já referido, é disso bem ilustrativa, uma vez que ainda terá de se desenvolver muito trabalho para que, sobretudo fora do espaço da União Europeia – mas também dentro deste espaço –, essa cooperação seja eficaz. Tiveram de se tomar opções e fixar prioridades, assentes quer na premência das medidas legislativas em questão, quer na viabilidade da sua aprovação, atendendo a que muitas das normas necessárias carecem de um ponto comum de entendimento entre Estados.

necessidade de aprovação de disposições legais que contenham as seguintes normas jurídicas[48]:

(i) Normas jurídicas que imponham a implementação das medidas necessárias para garantir a segurança das redes e ou dos bens que nestas se suportam (cobertas, em parte, pela Diretiva de segurança das redes e da informação e pelo Regulamento Geral sobre a Proteção de Dados);

(ii) Normas jurídicas que imponham deveres de notificação em caso de incidente (cobertas, em parte, pela Diretiva de segurança das redes e da informação e pelo Regulamento Geral sobre a Proteção de Dados);

(iii) Normas jurídicas que permitam o tratamento de informação relevante para a segurança do Estado e a realização dos diversos tipos de operações em rede para esse mesmo fim;

(iv) Normas jurídicas que imponham especiais deveres de conduta no contexto dos meios eletrónicos, com vista a diminuir os danos decorrentes de atos ilícitos praticados em rede e a facilitar a investigação posterior desses atos;

(v) Normas jurídicas relativas à prova digital;

(vi) Normas jurídicas relativas à interação entre as várias entidades nacionais com competências nas áreas da cibersegurança e ciberdefesa;

(vii) Normas jurídicas que criem as entidades necessárias e ou que estabeleçam as atribuições e competências necessárias para implementar o quadro legal descrito nas alíneas anteriores.

A aprovação de um quadro legal mais completo na área da cibersegurança e da ciberdefesa permitirá dotar o Estado português das ferramentas necessárias para melhor fazer face aos desafios do ciberespaço. Este quadro legal permitirá igualmente que o Estado português se posicione na linha da frente nesta matéria.

[48] Como já foi referido, no esquema constante do Anexo III pode visualizar-se uma apresentação gráfica das conclusões preliminares deste capítulo.

Parte V –
Estratégia Nacional de Ciberdefesa

Paulo Viegas Nunes

Face aos desafios e ameaças que a Internet e o próprio ciberespaço colocam hoje a todas as sociedades desenvolvidas, Portugal tem vindo, essencialmente ao longo dos últimos anos, a desenvolver um conjunto de iniciativas destinadas a garantir uma utilização mais livre, fiável e segura deste espaço de interação global. Atendendo à necessidade de desenvolver uma estratégia concertada, integradora e mobilizadora de sinergias nacionais, capaz de reduzir o risco social e potenciar a utilização do ciberespaço, pretende-se neste capítulo desenvolver um quadro de análise a partir do qual se procura edificar e propor o levantamento de uma Estratégia Nacional de Ciberdefesa.

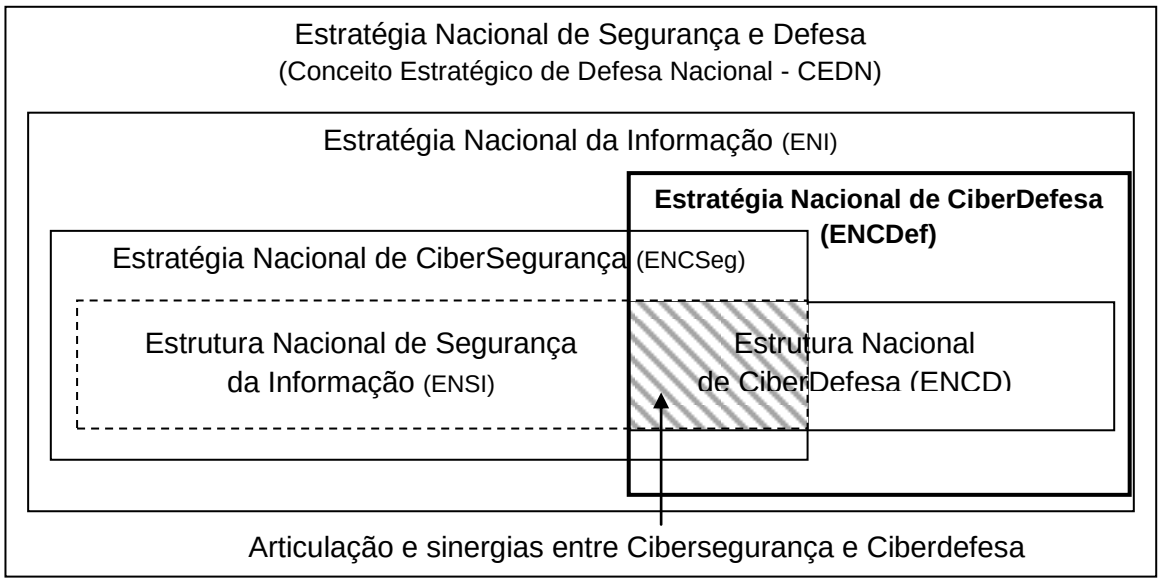
O levantamento desta Estratégia é equacionado no quadro das iniciativas atualmente em curso no País, nomeadamente, as decorrentes da revisão do Conceito Estratégico de Defesa Nacional (2013), da definição de uma "Orientação Política para a Ciberdefesa" (2013) e da consequente criação de um Centro de Ciberdefesa das Forças Armadas (2014), do levantamento de um Centro Nacional de Cibersegurança (2014), da criação de uma Estratégia Nacional de Cibersegurança (2015) e da necessidade de edificação de uma efetiva capacidade nacional de Ciberdefesa. Neste âmbito, são também tidos em atenção os esforços cooperativos já lançados por outros Países e pelas Organizações Internacionais de que Portugal faz parte integrante (NATO e UE), uma vez que estes constituem elementos de referência para o desenvolvimento de um conceito de ação estratégica neste domínio.

5.1. Enquadramento

Dentro da lógica da defesa dos seus interesses, é de esperar que atores mal-intencionados procurem manipular e controlar os fluxos de informação que circulam nas redes de comunicações dos diversos países, afetando a disponibilidade e a utilização segura do ciberespaço. Quando estão em risco a segurança e o bem-estar social, o Estado terá que desenvolver uma "Política para o domínio da Informação" que permita garantir, não só a convergência estrutural para os parâmetros tecnológicos da Sociedade de Informação e do Conhecimento, como também a Segurança e a Defesa da sua Infraestrutura de Informação.

Atendendo ao princípio de que a cada forma de coação corresponde uma estratégia distinta (Couto, 1988: 227), a utilização da informação e do ciberespaço como forma de coação faz surgir uma nova estratégia, a Estratégia da Informação Nacional (EIN). Assim, como uma das componentes desta Estratégia e subordinada à Estratégia de Segurança e Defesa do Estado (ENSD), surgem as Estratégias Nacionais de Cibersegurança (ENCSeg) e de Ciberdefesa (ENCDef).

Constituindo o ciberespaço uma das componentes do ambiente da informação, a Estrutura Nacional de Segurança da Informação[49] (ENSI), deve ser perspetivada no âmbito da ENCSeg[50] (ver Figura 1). Por outro lado, importa também referir que, assim como existe uma estreita ligação entre a Segurança e a Defesa Nacional, também a cibersegurança se revela indissociável da ciberdefesa do Estado. Na prática, isto significa que não será possível garantir a cibersegurança sem o levantamento de uma capacidade de ciberdefesa. A edificação desta capacidade, por seu turno, deverá ser orientada pela ENCDef, consubstanciando-se através da criação de uma Estrutura Nacional de Ciberdefesa (ENCD).



Adaptado de Nunes (2015, p.216)

Figura 1 – Enquadramento da Estratégia Nacional de Ciberdefesa

Neste contexto, face ao enquadramento apresentado e atendendo à sua natureza complementar e supletiva relativamente à ENCSeg, a Estratégia Nacional de Ciberdefesa (ENCDef), pode ser definida como o:

Conjunto integrado de iniciativas (de natureza orgânica, operacional e genética) que, face à ocorrência de ciberataques, que podem por em risco a salvaguarda dos interesses nacionais e a governação do Estado, pretendem essencialmente

[49] Atualmente em revisão, no âmbito da medida 4 da Resolução do Conselho de Ministros Nº 12/2012.

[50] Entendida como um "conjunto integrado de iniciativas (de natureza orgânica, operacional e genética), destinadas a potenciar a livre utilização do ciberespaço e garantir a sua segurança, promovendo a proteção da Infraestrutura de Informação Crítica Nacional contra eventuais ciberataques, de âmbito nacional ou internacional que, pelo seu carácter disruptivo, afetem a Sociedade Portuguesa e a defesa dos Interesses Nacionais" (Nunes, 2012).

defender a Soberania Nacional, garantir a liberdade de ação das Forças Armadas nos vários domínios de emprego operacional (incluindo terra, mar, ar e ciberespaço) e contribuir, de forma sinérgica e cooperativa, para a cibersegurança do País.

Devido ao enquadramento apresentado, constata-se que a ENCDef deverá contribuir tanto para o desenvolvimento da capacidade de ciberdefesa nacional (edificação da ENCD) como, de forma articulada e sinérgica, para a implementação dos processos de Segurança da Informação associados ao ciberespaço (zona sombreada da Figura 3) que são necessários mobilizar para garantir a própria Ciberdefesa do País e a salvaguarda dos interesses nacionais. A ENCDef encontra-se assim alinhada não só com a ENCSeg mas também com a ENI e com a própria Estratégia Nacional de Segurança e Defesa (refletida no CEDN).

Neste contexto, parece claro que os benefícios decorrentes da livre utilização do ciberespaço, condição fundamental para gerar valor e fomentar a riqueza nacional, só serão atingidos se formos capazes de proteger e defender as infraestruturas de informação nacionais, garantindo um nível aceitável e sustentável de segurança, fiabilidade e disponibilidade na sua exploração. Tal desiderato só será garantido com a existência de uma ENCDef, assente num nível de ambição coerente, e capaz de conduzir ao levantamento de uma capacidade de ciberdefesa credível.

5.2. Finalidade – Nível de Ambição

O enquadramento e a definição da ENCDef constituem os fundamentos da visão estratégica que se pretende estruturar neste domínio. No entanto, a clarificação da sua finalidade revela-se também um elemento fundamental para podermos deduzir os objetivos a atingir e, a partir daí, perspetivar as linhas de ação estratégica que vão orientar a sua implementação.

A finalidade a atingir pela ENCDef, conforme foi possível constatar (Figura 1), decorre do nível de ambição e da finalidade que for definida para a ENI e, de forma subsidiaria para a ENCD. Com base neste pressuposto, procuraremos estabelecer o âmbito e os princípios que caracterizam a ENI, de forma a permitir posteriormente determinar a finalidade a atingir pela ENCDef.

A Estratégia da Informação tem como âmbito a “info-conflitualidade resultante das relações de competição e conflito geradas entre a “info-esfera” do País, definida com base nos interesses nacionais, e a “info-esfera” de outros atores (Estado ou não-Estado)” (Nunes, 2010). Atendendo ao âmbito da EIN, considera-se que esta pode apresentar três finalidades principais: Garantia da Informação (*Information Assurance*)[51], Superioridade da Informação (*Information Superiority*)[52] e Domínio

[51] Neste âmbito, o principal desafio que os Estados e a generalidade das organizações têm que enfrentar é a proteção da sua infraestrutura de informação. Este desiderato requer tanto a implementação de mecanismos de Segurança como de Defesa da IIN.

da Informação (*Information Dominance*)[53].Tendo por base as capacidades nacionais (Nunes, 2012), consideramos que Portugal deve orientar a sua Estratégia da Informação de acordo com a prioridade de satisfação da primeira finalidade apresentada (curto prazo) e perspetivar a segunda (médio/longo prazo). Não se considera como objetivo realista o levantamento das capacidades necessárias à consecução da terceira finalidade (Domínio da Informação).

A Estratégia da Informação torna-se assim indispensável em todos os domínios da conflitualidade refletindo-se, ao nível da globalização da economia e das transações digitais (Estratégia Económica), nas redes de influência social e diplomática criadas com base na Internet (Estratégia Política), na influência dos média e do ciberespaço na gestão das perceções (Estratégia Psicológica) e na utilização dos sistemas de armas (Estratégia Militar).

Assumindo-se a Garantia da Informação como a finalidade primária da EIN, considera-se que a Estratégia Nacional de Ciberdefesa, face à necessidade de articulação e integração permanente que tem de existir entre a cibersegurança e a ciberdefesa, deverá apresentar a mesma finalidade. Neste contexto, importa também referir que a NATO, na definição da sua Política de Ciberdefesa (CM, 2011), também elegeu a Garantia da Informação (*Information Assurance*) como objetivo final a atingir[54].

Tendo sido definida a finalidade da ENCDef, importa agora clarificar os objetivos a atingir e as linhas de orientação geral e específica que a estes se encontram associadas, de forma a traduzir a visão numa ação estratégia coerente e eficaz.

5.3. Objetivos a atingir

O Ciberespaço não é limitado pela esfera pública ou privada, civil ou militar, interna ou externa, constituindo um domínio estratégico prioritário de defesa de valores e interesses nacionais (não alienável). Neste domínio, onde se geram novas oportunidades, mas também surgem novos riscos, Portugal deverá procurar atingir, no âmbito da sua ciberdefesa, os seguintes três objetivos principais:

- Garantir a proteção, a resiliência e a segurança das redes e dos Sistemas de Informação e Comunicações da Defesa Nacional contra ciberataques;

[52] Uma vez garantida a disponibilidade e a integridade dos sistemas de informação de um Estado, uma opção futura que se coloca é a expansão da sua info-esfera de influência em direcção a outros ambientes mais alargados, dentro dos quais a organização ou o Estado pretende intervir.

[53] Após estabelecido um certo grau de superioridade no ambiente de informação, um ator estará em posição para lançar uma campanha orientada para a obtenção de uma vantagem operacional, se assim o desejar. A condução com sucesso desta campanha requer o domínio do ambiente de informação adversário por aqueles que necessitem dessa informação.

[54] De acordo com a Política de Ciberdefesa NATO (CM, 2011), a cibersegurança só poderá ser conseguida com base na implementação de mecanismos de Segurança da Informação (INFOSEC) e da sua integração e articulação sinérgica com uma capacidade de Ciberdefesa.

- Assegurar a liberdade de ação do País no ciberespaço, de forma a permitir salvaguardar a defesa dos interesses nacionais e afirmar a Soberania Nacional neste domínio;
- Contribuir de forma cooperativa para a Cibersegurança Nacional.

Relativamente ao primeiro objetivo, considera-se que a proteção, resiliência e segurança da Informação que circula nas redes de comunicações da Defesa Nacional e das Forças Armadas constitui um pré-requisito para a livre utilização do ambiente da informação e que esta só pode ser garantida através de um conceito alargado de proteção das infraestruturas de informação, onde a articulação e a exploração de sinergias entre a cibersegurança e a ciberdefesa é decisiva para garantir essa proteção.

Considera-se que a filosofia a seguir, se deverá articular de acordo com uma perspectiva de gestão do risco: proteção, deteção e reação. Reconhecendo-se que se trata de garantir o funcionamento ininterrupto e a recuperação das infraestruturas de informação face à ocorrência de ciberataques, importa também perceber que as Forças Armadas só serão capazes de atingir este objetivo se tiverem capacidade para defender o País contra este tipo de ataques, nomeadamente, detendo e neutralizando aqueles que coloquem em risco a Soberania Nacional. A proteção, deteção e reação têm a ver essencialmente com a área da cibersegurança ao passo que o defender e o deter se encontram mais ligadas à Ciberdefesa.

A exploração eficaz do ciberespaço, enunciada no segundo objetivo, pressupõe uma clara definição dos objetivos operacionais a atingir e a capacidade das Forças Armadas para moldarem o ambiente de informação, de acordo com os interesses nacionais a defender. Tal desiderato só se consegue através do desenvolvimento de Operações no Ciberespaço (incluindo Operações em Redes de Computadores), potenciando os “pontos fortes” na exploração de oportunidades e reduzindo ao máximo o impacto de eventuais ataques que pretendam explorar os “pontos fracos” e as vulnerabilidades nacionais neste domínio.

O terceiro objetivo, decorrendo da necessidade de asegurar uma permanente articulação operacional entre as estruturas de ciberdefesa e de cibersegurança, pretende garantir uma complementaridade de esforços e a existência de sinergias destinadas a melhorar a proteção e a defesa do País contra a ocorrência de ciberataques cada vez mais disruptivos e destrutivos.

Para além destes três objetivos genéricos que, na sua essência, definem os fins (*ends*) a atingir, importa também identificar os objetivos específicos ou caminhos a seguir (*ways*) que lhes estão asociados, caracterizando assim, de uma forma mais concreta, o que se pretende atingir. Neste ámbito, foram identificados os seguinters objetivos específicos:

- Assegurar, de forma conjunta, a liberdade de ação e a utilização eficaz do ciberespaço pelas Forças Armadas (FA), impedindo ou dificultando assim a sua utilização contra os interesses da Defesa Nacional;

- Desenvolver competências e gerir os recursos humanos necessários à condução das atividades de defesa no Ciberespaço;
- Contribuir para a produção de conhecimento situacional do ciberespaço e para a recolha de informações de interesse para a Defesa Nacional;
- Desenvolver e manter atualizada a doutrina de emprego das capacidades associadas à Ciberdefesa;
- Adotar medidas que contribuam para reforçar a Segurança das Comunicações e Sistemas de Informação (CSI) das FA e da Defesa Nacional;
- Adequar as estruturas de Investigação, Desenvolvimento e Inovação (I&D-I) das FA e implementar linhas de investigação conjuntas, especialmente orientadas para o desenvolvimento da capacidade nacional de Ciberdefesa;
- Definir os princípios básicos que norteiem a criação de legislação e normas específicas para as atividades de Defesa no Ciberespaço;
- Contribuir para a cibersegurança dos ativos de informação necessários à Defesa do Estado, situados dentro e fora do âmbito do MDN;
- Melhorar a capacidade de defesa colectiva e de ciberdefesa cooperativa do País, através da exploração de Sinergias Nacionais e da Cooperação Internacional.

A visão clara das implicações/necessidades associadas a cada um dos objetivos enunciados, conforme se ilustra na tabela em Anexo V, permitirá traçar o caminho a seguir, perspectivando uma orientação geral e específica para os atingir.

5.4. Linhas de Ação

No âmbito da ENCDef, para além de objetivos genéricos e concretos a atingir e das orientações (gerais e específicas) a seguir para a sua implementação, importa também definir linhas de ação concretas (*means*), destinadas a reforçar o potencial estratégico nacional neste sector. Cada uma destas linhas de ação interliga-se necessariamente com as restantes, reforçando a capacidade do País para garantir não só uma exploração mais livre e eficiente, mas também uma utilização mais protegida, segura e soberana do ciberespaço. Neste contexto, associadas a cada um dos objetivos específicos, elencou-se um conjunto de 52 linhas de ação estratégica, que se apresentam no Anexo V.

De forma transversal, as atividades desenvolvidas no âmbito da implementação da Estratégia Nacional de Ciberdefesa, contribuirão para a consolidação do vector estratégico “Informação e Segurança do Ciberespaço”, influenciando também todos os outros vectores que contribuem para a Estratégia Nacional de Segurança e Defesa do País.

5.5. Visão Operacional, Organizacional e Genética

As operações no ciberespaço e os procesos e mecanismos de Segurança da Informação que determinam a Proteção da IIN constituem os “pilares” da condução operacional da Estratégia Nacional de Ciberdefesa. A compreensão da sinergia e interdependência destes elementos, permite deduzir a resposta estrutural e genética associada à sua implementação. O objetivo a atingir é o de promover uma adequada visão da utilização do ciberespaço, integrando as atividades a desenvolver pelos diversos atores, nomeadamente, em situações de crise ou conflito.

5.5.1. Desafios Operacionais da Ciberdefesa

A dimensão cibernética dos “conflitos híbridos”, cujos atores envolvidos e vetores de ataque são pouco visíveis, vem reforçar a necessidade de existir uma visão alargada dos mesmos para enfrentar o novo espectro da ameaça, aumentando a necessidade de reforçar a cooperação civil-militar aos vários patamares de decisão, desde o nível político-estratégico até ao nivel operacional e tático/técnico. Fundamentalmente pela natureza da rede de interdependências gerada pela sociedade e pelas póprias Forças Armadas, a proteção das infraestruturas críticas nacionais constitui certamente uma grande preocupação, materializando uma área prioritária de cooperação. Neste contexto, importa recordar os efeitos disruptivos e multidimensionais associados à “campanha híbrida” lançada contra a Ucrânia.

Portugal deve assim estar preparado para, proativamente, antecipar, prevenir e defender-se contra ciberataques, dissuadindo potenciais atores hostis, tornando ineficientes os seus ataques e limitando o seu impacto. Para esse efeito, de forma a conduzir uma ciberdefesa eficaz, Portugal deve desenvolver, com base numa aproximação multi-nível, um conjunto integrado e coordenado de módulos de capacidade associados à ciberdefesa.

Estes módulos de capacidade, devem ser integradas de forma transversal tanto ao nível das Forças Armadas como do próprio nível político, uma vez que exigem uma estreita coordenação entre o sector público e privado, explorando para esse efeito, na máxima extensão possível, sinergias nacionais e a cooperação internacional, de acordo com o quadro de alianças e cooperação definido.

5.5.2. Impacto Organizacional

A definição de uma Estratégia Nacional de Ciberdefesa, naturalmente pensada para fazer face não só aos desafíos operacionais que se enfrentam hoje, mas também aos que se perspectivam no futuro, deverá assentar numa organização

coerente, capaz de definir uma resposta sinérgica, pensada ao nível nacional, mas também necessariamente articulada no plano internacional, explorando para esse efeito o quadro de Alianças e cooperação em que Portugal se insere.

No entanto, no plano nacional, face ao estado ainda relativamente pouco maduro do quadro doutrinário e do proceso de levantamento de capacidades, um dos principais problemas a enfrentar é a possível fragmentação de esforços, decorrente, nomeadamente, da não existência de uma Estratégia enformadora. Neste contexto, estes esforços traduzem-se por vezes no desenvolvimento de atividades pouco eficientes, produzindo uma resultante pouco expressiva ou ineficaz.

Tendo como linha orientadora a dedução de uma resposta estrutural, ajustada aos desafíos organizacionais que a ciberdefesa nacional encerra, considera-se importante a caracterização da atual situação Portuguesa, procurando clarificar o papel das diversas Entidades/Órgãos na condução operacional da Cibersegurança e Ciberdefesa do País.

Ao nível da Cibersegurança, importa referir que os dados recolhidos reflectem que a segurança dos sistemas de informação nacionais se encontra por vezes muito associada à tradicional proteção perimétrica, sendo gerida de forma heterogénea, dirigida à proteção hermética e institucional das diversas infraestruturas de informação. Uma vez que não existe ainda um quadro legislativo específico, capaz de contrariar este tipo de situações, existem diversas instituições e organizações que implementam autonomamente, e de forma por vezes desenquadrada, as suas políticas de segurança, sem que seja possível identificar uma estrutura integradora e normalizadora de âmbito nacional. O maior problema que se coloca, a este nível, reside na dificuldade em implementar uma política integrada e uma Estrutura Nacional de Segurança da Informação (ENSI) que, passando pela atribuição das necessárias responsabilidades de coordenação institucional, permita minimizar o risco social, maximizar a utilização dos recursos disponíveis e garantir uma efetiva operacionalização da Proteção da Infraestrutura de Informação Nacional (IIN).

Ainda que o Centro Nacional de Cibersegurança (CNCS)[55] assuma já as funções normalmente atribuídas a um CERT Nacional[56], articulando-se como as Entidades competentes[57] para a gestão de endereços IP (associados ao domínio.pt), promovendo a implementação de Políticas de Segurança e o

[55] Após a extinção da Fundação para a Computação Científica Nacional (FCCN) e a sua posterior integração na FCT, a marca CERT.PT transitou para o CNCS, passando este Centro a integra-lo na sua estrutura.

[56] O CNCS assugura na sua plenitude as funções de CERT Nacional, encontrando-se em fase de adaptação aos requisitos definidos pela Diretiva NIS e em fase de certificação pelo Trusted Introducer for CSIRTs in Europe.

[57] A gestão de endereços IP na Europa é da responsabilidade do RIPE. Os nomes DNS são responsabilidade da Associação DNS Portugal. Ambas as funções não fazem parte de um portfolio de serviços de um CERT Nacional.

desenvolvimento de ações de sensibilização[58] para a necessidade de garantir a proteção das redes e sistemas de informação nacionais, enquanto CERT Nacional possui ainda uma capacidade limitada para articular uma reação ajustada a todo o espectro de ameaças e, assim, para se poder também afirmar como um fator dissuasor de potenciais ciberataques de larga escala à IIN. Constituindo o CNCS um órgão de natureza iminentemente operacional, atualmente integrado na estrutura do Gabinete Nacional de Segurança (GNS), importa referir que não existe atualmente nenhum Órgão/Entidade com responsabilidades de coordenação Estratégica e Política sendo, na sua ausência, a mesma garantida pelo GNS, pela Presidência do Conselho de Ministros (PCM) ou mesmo pelo próprio CNCS, nomeadamente, ao nível da participação em grupos de trabalho internacionais. Neste contexto, salienta-se o facto de, já em 2012, no âmbito dos trabalhos da Comissão Instaladora do Centro Nacional de Cibersegurança, ter sido identificada a necessidade de se proceder ao levantamento de um Conselho Nacional de Cibersegurança, a quem seriam atribuidas estas responsabiliadades.

No que se refere ao domínio da Ciberdefesa, na sequência do Despacho n.º 13692/2013, do Ministro da Defesa Nacional (28 de Outubro), que determinou a criação do Centro de Ciberdefesa (CCD) das Forças Armadas, importa registar o início do funcionamento deste Centro (final de 2014) e destacar a sua importância central, nomeadamente, como ponto de coordenação operacional da segurança das redes e dos sistemas de informação das Forças Armadas e da Defesa Nacional. No entanto, o número reduzido dos efetivos existentes e a sua capacidade mitigada para conduzir operações militares no ciberespaço, decorrente essencialmente do atual posicionamento orgânico do CCD, recomenda uma revisão das estruturas existentes, nomeadamente à luz do reconhecimento doutrinário do ciberespaço como 4º domínio operacional da guerra, a par da terra, mar e ar. Face à necessidade de assegurar uma resposta operacional credível e uma atuação sinérgica e cooperativa, tanto no plano nacional como internacional, também na área da Ciberdefesa deverá existir uma Entidade responsável pela coordenação política e estratégica ao nível nacional.

Salvo melhor opinião, nomeadamente para fazer face a situações de gestão de crises no ciberespaço que envolvam a participação direta das Forças Armadas, onde os patamares mais elevados de decisão política e militar assumem particular importância, parece fazer sentido a criação de um órgão de coordenação político-estratégica, sob a forma de um Conselho Nacional de Ciberdefesa. Em linha com o racional seguido para o caso da Cibersegurança, a este Conselho competirá promover a necessária articulação de esforços aos níveis e patamares de decisão político-estratégica com os Órgãos e Entidades

[58] Quer a promoção de políticas de segurança, quer a sensibilização não são core dos CERT nacionais. São no entanto coordenadas/conduzidas pela autoridade nacional de cibersegurança. No nosso caso a autoridade também tem no seu *portfolio* o CERT. O contexto da definição e promoção de políticas de segurança para as entidades do estado e operadores de infraestruturas é atribuição do CNCS e enquadrável na directiva NIS.

que intervêm na área da Cibersegurança Nacional, facilitando também a cooperação internacional na área específica da Ciberdefesa, tanto no âmbito NATO como da UE.

Tendo por base a gestão de crises no ciberespaço, procurando visualizar os vários patamares de decisão e o correspondente alinhamento dos processos que decorrem aos diferentes níveis de gestão (tático, operacional, estratégico e político), adoptou-se o modelo das "4 pirâmides" (Cibersegurança, Ciberdefesa, UE e NATO). A partir da observação deste modelo, apresentado na figura 2, é possível constatar que o nível tático agrega os utilizadores dos vários domínios analisados.

No plano nacional, interagindo através da Rede Nacional de *Computer Security Incident Response Teams (CSIRTs)*, os órgãos responsáveis por garantir a resposta operacional são o Centro Nacional de Cibersegurança e o Centro de Ciberdefesa das Forças Armadas. Ao nível da cooperação internacional, o CNCS e o CCD articulam também a sua atividade respetivamente com o *European Cyber Crime Center (EC3),* com a Rede Europeia de *Computer Emergency Response Teams (CERTs)* e com a *NATO Computer Incident Response Capability (NCIRC)*.

Analisadas as várias estruturas existentes ao nível político-estratégico, tanto no âmbito nacional como internacional (NATO e UE), constata-se existirem situações muito diferenciadas. Assim, verificou-se que estas estruturas ainda não se encontram definidas nem foram ainda criadas no âmbito nacional, no âmbito da UE existem várias Instituições e Agências com responsabilidades sobrepostas (e pouco claras) e que, apenas no contexto NATO, se encontram institucionalmente definidas estruturas orgânicas ao nível estratégico (*NCIRC Coordination Center e Task Force Cyber*) e Político (*Cyber Defence Committee – CDC* e *Cyber Defence Management Board – CDMB*).

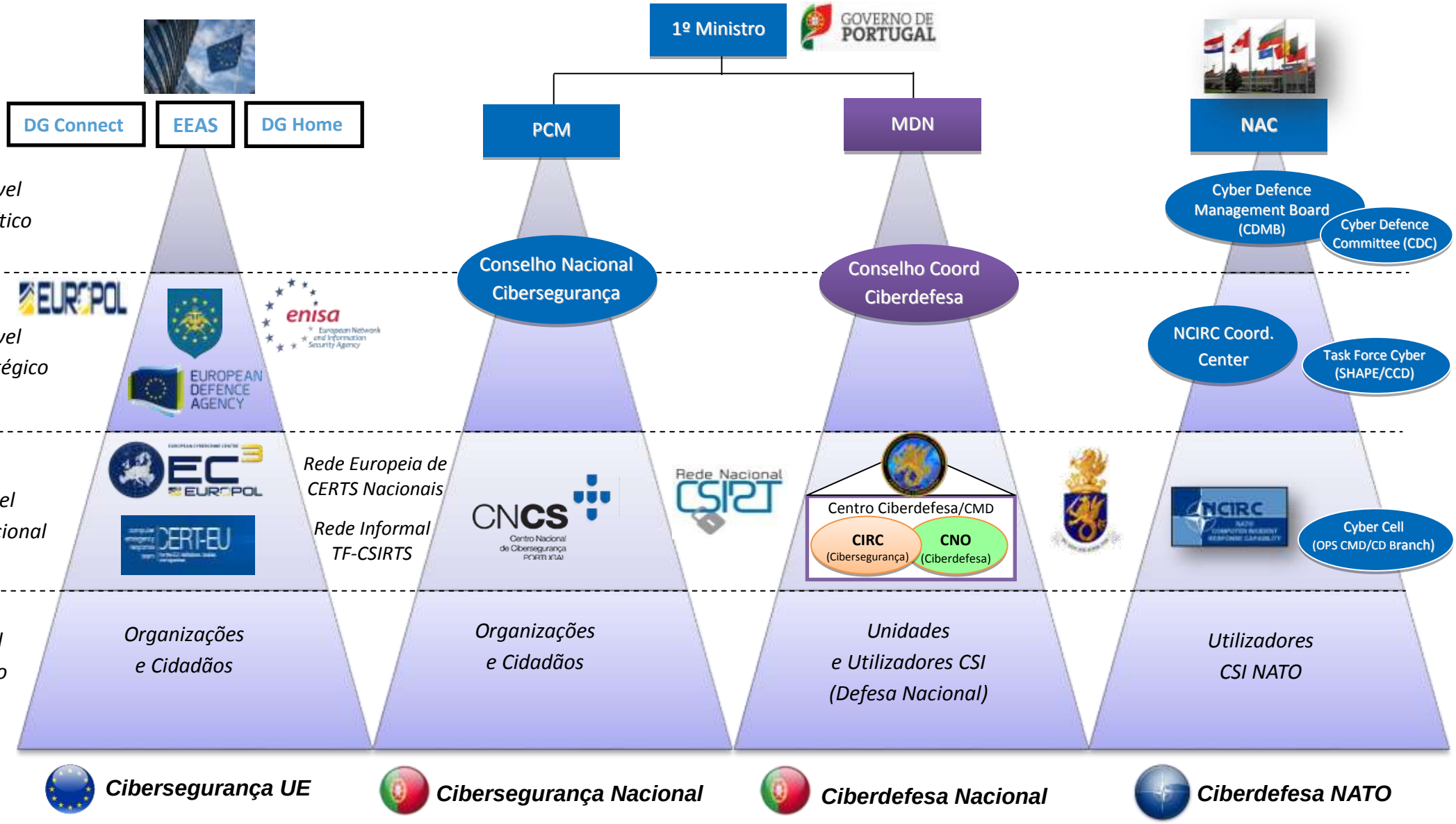
A partir da análise sumária realizada, tanto no âmbito da Cibersegurança como da Ciberdefesa, conclui-se que, para fazer face aos novos desafios operacionais que se colocam atualmente a Portugal e às implicações doutrinárias daí decorrentes (nacionais, NATO e UE), importa promover, com a maior brevidade possível, um ajustastamento das estruturas orgânicas existentes.

Em linha com o modelo de referência adoptado (figura 4), assume também especial importância a definição de doutrinas e processos que permitam assegurar o alinhamento de procesos e a efetiva coordenação das ações envolvidas. Podem evitar-se assim conflitos e estimular a cooperação intra e inter institucional, quer no âmbito nacional quer internacional, delimitando os problemas de natureza criminal/policial dos que afectam a Segurança e Defesa do Estado.

A resposta estrutural apresentada também exige a criação de legislação específica que, garantindo o difícil equilíbrio entre direitos individuais e responsabilidades institucionais, permita clarificar o objetivo, as atribuições e as competências dos diversos órgãos que materilizam a componente estrutural da Estratégia Nacional de Ciberdefesa. A adoção do modelo proposto, permitirá

assim, de uma forma necessariamente genérica e respeitando os vários níveis de tomada de decisão, definir uma articulação orgânica eficaz, tanto no contexto nacional como internacional.

Figura 2 – Visão Orgânica para a Cibersegurança e Ciberdefesa – Articulação Nacional e Internacional



5.4.3. Visão Genética: O Desenvolvimento de Capacidades

No domínio militar existe a necessidade de proteção permanente das Comunicações e Sistemas de Informação (CSI) que suportam o Comando e Controlo (C2) das Forças militares, garantindo assim a segurança dos fluxos de informação associados ao seu emprego operacional. Neste âmbito, a Defesa Nacional deverá encarar como prioritária a redução da vulnerabilidade dos sistemas CSI e dos sistemas de armas das Forças Armadas, nomeadamente, através de uma adequada gestão dos riscos cibernéticos existentes e de uma efetiva mitigação dos mesmos.

De forma a manterem a sua relevância e eficácia operacional, as Forças Armadas têm também, de forma dinâmica, que ajustar as suas capacidades à rápida evolução do moderno campo de batalha, procurando assim, tão rápido quanto possível, preencher as lacunas de capacidades existentes de forma a reduzir o risco operacional a que as suas Forças estão sujeitas. Tal como acontece com qualquer outra capacidade, atendendo às lacunas e vulnerabilidades existentes, será necessário definir, de forma ajustada e corerente, um plano de desenvolvimento da Capacidade Nacional de Ciberdefesa.

Tanto ao nível NATO como da União Europeia, a ciberdefesa tem vindo, desde 2010, a ser identificada como uma área prioritária ao nível do desenvolvimento de capacidades. Com base na evolução do ambiente de segurança internacional e do próprio espectro da ameaça, podemos antecipar que a ciberdefesa permanecerá no topo da agenda destas organizações internacionais ao longo da próxima década, constituindo também, pelo menos durante o mesmo período, igualmente uma prioridade nacional. De acordo com o processo de desenvolvimento de capacidades adoptado tanto no contexto NATO como da EU, torna-se assim necessário avaliar todas as linhas de desenvolvimento relevantes para a construção ou edificação desta capacidade.

De forma a garantir o necessário alinhamento dos esforços, em curso nos vários domínios em que decorre a edificação de capacidades de ciberdefesa, a decisão de aplicar a metodologia DOTMLPF-I[59] à análise da componente genética da Estratégia Nacional de Ciberdefesa parece-nos a mais ajustada. O sucesso de qualquer iniciativa, que passe pela construção de uma capacidade de ciberdefesa nacional dependerá assim da combinação lógica e coerente das seguintes linhas de desenvolvimento dessa mesma capacidade:

[59] Tendo como origem uma designação anglo-saxónica, esta definição de capacidade refere-se a *Doctrine, Organization, Training, Material, Leadership, Personnel, Facilities and Interoperability* (Doutrina, Organização, Treino, Material, Liderança, Pessoal, Infraestruturas e Interoperabilidade).

- **Doutrina**: na sequência da aprovação da orientação política para a ciberdefesa que, na prática, constituiu uma diretiva iniciadora para o levantamento da capacidade nacional de ciberdefesa, torna-se agora necessário desenvolver um conceito de emprego que oriente e dirija a sua vertente operacional. Este conceito constitui um elemento fundamental para a aplicação da Ciberdefesa tanto no contexto da condução de operações militares como das operações de gestão de crises, definindo uma base doutrinária comum e os procedimentos necessários para a criação de uma verdadeira consciência da situação operacional (*cyber situational awareness*), partilhada entre todos os atores intervenientes desde o nível estratégico até ao nível tático. Neste contexto, importa salientar que a cooperação e a colaboração constituem um fator crítico para uma ciberdefesa eficiente e proativa. Devido às suas implicações, nomeadamente, na forma como os processos que lhe estão associados devem passar a ser conduzidos, será de esperar que a visão doutrinária adoptada venha a influênciar também as estruturas e as organizações atualmente existentes.

- **Organização**: neste momento, no contexto nacional, as estruturas organizacionais associadas tanto à área da cibersegurança como à ciberdefesa, são ainda relativamente embrionárias, apresentando um efetivo muito limitado de recursos humanos. Neste âmbito, importa assinalar o facto de a evolução orgânica registada na grande maioria dos países da Aliança Atlântica ir no sentido da criação de uma organização específica para a ciberdefesa, consistente com o facto de o ciberespaço passar a constituir um novo domínio operacional. Decorrente desta visão, será de esperar que no curto/médio prazo venha a ser levantada uma cadeia de Comando e Controlo (C2) própria da ciberdefesa, capaz de assegurar que todas as tarefas relacionadas com a defesa cibernética do Estado, tanto num contexto de gestão de crises como de guerra, são suficientemente cobertas. A prazo, no âmbito da estrutura das Forças Armadas, tal poderá implicar a criação de um novo Comando ao nível conjunto e uma adaptação/reformulação das estruturas existentes, tanto ao nível dos vários Ramos das Forças Armadas como ao nível do próprio Ministério da Defesa Nacional.

- **Treino**: assumindo-se que o desenvolvimento de competências envolve várias áreas complementares, é hoje assumido que a área do Treino, inclui também a Formação, a Educação, a Avaliação e a realização de Exercícios. Constituindo a área da ciberdefesa um domínio de conhecimento intensivo, não será de estranhar que tanto a NATO como a UE tenham elegido este domínio como prioritário para a edificação das suas capacidades de ciberdefesa. De facto, a situação atual, caracterizada por uma elevada carência de recursos humanos qualificados (civis e militares), parece indicar que a criação de um número suficiente de

quadros, dotados das necessárias competências, constituirá, no decurso da próxima década, uma das áreas de maior preocupação tanto para as Forças Armadas e para a Defesa Nacional, como para o País em geral. Assim, a realização de exercícios e de atividades de treino especializado, desempenhará um papel muito relevante não só na descoberta dos talentos existentes no domínio militar como também para atrair jovens que, sendo dotados das necessárias qualificações técnicas, pretendam servir nas Forças Armadas. Portugal, através da liderança nacional do Projeto NATO *Multinational Cyber Defence Education and Training (MNCDE&T)*, já realizou uma análise das necessidades de treino existentes, identificando as audiências de treino e as competências de que estas necessitam para realizar as várias tarefas associadas à ciberdefesa. No âmbito dos trabalhos em curso, foi também reunido um conjunto alargado de informação relativa aos cursos, atividades de treino e exercícios existentes, permitindo identificar as lacunas existentes neste domínio. De forma a preencher estas lacunas, estão também a ser desenvolvidas novas iniciativas tanto no âmbito nacional como internacional. De modo a evitar uma eventual fragmentação desta importante linha de desenvolvimento da capacidade de ciberdefesa e a promover o desenvolvimento de sinergias, Portugal propôs, tanto no contexto NATO como da UE, a criação de um currículo comum para a ciberdefesa, assente numa gestão e organização centralizada, mas também numa execução descentralizada. Só desta forma será possível aproveitar os benefícios decorrentes de uma "economia de escala" ou da reutilização de módulos de formação e exercícios entre o domínio nacional, NATO e da UE. O facto de ter sido atribuída a Portugal a gestão da Plataforma Centralizada de Educação e Treino da UE, que permitirá integrar estes três domínios (Nacional, EU e Internacional/NATO), e a transferência da futura N*ATO Communication, Information and Cyber School* para Oeiras (a realizar até ao final de 2018) reforça o papel central do nosso País neste domínio.

- **Material**: as soluções tecnológicas tradicionais (*hardware* e *software*) não são suficientes para proteger as redes de dados não estruturados, distribuídas ao longo de uma multitude de dispositivos e sistemas estáticos/fixos e projetáveis. Os sistemas de encriptação de dados, apesar de fornecerem uma camada adicional de segurança, no que se refere à confidencialidade e à autenticidade, são hoje manifestamente insuficientes para garantir a segurança da informação, nomeadamente, a partir do momento em que o atacante ou o código malicioso utilizado tenha tido sucesso na penetração do sistema. Uma questão adicional, que se coloca hoje com especial acuidade, tem também a ver com o modo como será possível garantir a proteção (proativa ou reativa) contra a existência de ataques cada vez mais sofisticados. A existência de sistemas fiáveis de gestão de identidades e acessos, a par da utilização de ferramentas de correlação de eventos (SIEM), de deteção de padrões de anomalias (*machine learning*) e de *Cyber Intelligence,* constitui também um objetivo

importante a atingir, uma vez que as redes que apoiam a missão das Forças Armadas têm vindo a evoluir no sentido de um ambiente federado e orientado à prestação de serviços. Neste contexto, a validação da identidade dos utilizadores terá que atravessar várias redes e aplicações associadas à forma como os mesmos podem aceder à informação e serviços pretendidos. Assegurar a identidade e a autenticação dos utilizadores assume ainda maior relevância quando se utilizam dispositivos móveis. Novos conceitos emergentes e inovadores como a "Internet das coisas" (*Internet of Things* - IoT), *Cloud Computing*, Inteligência Artificial (IA), *Web 2.0*, *Big Data*, sistemas automatizados, arquitecturas federadas e orientadas para a prestação de serviços, computação móvel, ou mesmo a utilização crescente da virtualização e de sistemas de computação embebida, são aspectos que vão certamente influenciar o desenvolvimento de capacidades de ciberdefesa, tornando necessário um acompanhamento próximo e uma avaliação permanente das implicações militares destes desenvolvimentos tecnológicos, tanto segundo uma perspectiva dos atacantes como dos defensores.

- **Pessoal**: o ser humano constitui um elemento estruturante da cadeia de valor associada tanto à cibersegurança como à ciberdefesa. Neste contexto, reconhecendo a importância das competências individuais dos especialistas, deverá ser atribuída uma especial importância ao recrutamento e retenção de talentos. Face à existência de um elevado défice de pessoal qualificado, registado aos diversos níveis, desde o nível estratégico ao nível tático e técnico, muitos países têm vindo a explorar um modelo de reservistas de forma a aproveitar ao máximo o número limitado de profissionais existentes no âmbito nacional. A reduzida quantidade de especialistas em ciberdefesa, dotados das necessárias competências, constitui hoje e constituirá certamente nos próximos anos, a maior lacuna existente nas Forças Armadas ao nível de pessoal especializado. Por esta razão, os esforços liderados por Portugal, tanto no âmbito internacional (NATO, UE) como nacional, assumem uma importância acrescida, constituindo uma "janela de oportunidade" para acelerar a criação de um conjunto alargado de quadros qualificados nesta área.

- **Liderança**: alinhado com a estratégia adoptada, com os conceitos e visões operacionais, tanto no âmbito internacional (NATO e UE) como nacional, será de esperar que venham a ser definidos, com maior clareza, os princípios e as próprias estruturas que asseguram a governação nacional, tanto da área da cibersegurança como da ciberdefesa. Também no contexto do planeamento e da condução de operações militares, se perspectiva o desenvolvimento de um conceito operacional de ciberdefesa. Este conceito, deverá ser capaz de clarificar a responsabilidade dos vários níveis de comando das Forças Armadas, permitir a definição de Regras de Empenhamento (RoE) ajustadas à situação operacional e promover a inclusão dos aspetos ligados à

ciberdefesa, tanto ao nível do planeamento como da condução de todo o tipo de operações militares. Este alinhamento, permitirá às Forças Armadas definir perfis de liderança consistentes com a estrutura e a cadeia de comando que se torna necessária levantar para fazer face à condução de todo o espectro das operações no ciberespaço.

- **Infraestruturas**: a implementação da capacidade nacional de ciberdefesa deve, sempre que possível, aproveitar as infraestruturas existentes. No entanto, uma vez que se trata de uma nova capacidade, cuja edificação se iniciou recentemente, será de esperar que venham a ser criadas novas organizações e, eventualmente, também novas infraestruturas especializadas. Muitas destas infraestruturas poderão vir a ser necessárias para instalar as diversas componentes/módulos que materializam a capacidade de ciberdefesa, nomeadamente, as associadas à área dos Security Operations Centers (SOC) e dos CIRC/CERT, *Cyber Ranges* (simuladores) e de laboratórios de análise forense digital (*off-line* e *on-line*).

- **Interoperabilidade**: os sistemas e serviços, os procedimentos e a doutrina utilizada no âmbito das missões e operações militares deve ser interoperável, respeitando inclusivamente todos os níveis de segurança. Neste contexto, deverá ser garantida a compatibilidade com os sistemas tecnologicamente mais avançados (estado da arte) mas também com equipamentos e sistemas menos sofisticados. A interoperabilidade poderá ser atingida com base não só na adoção de procedimentos comuns mas também através da utilização de regras de compatibilidade mínima, capazes de permitir garantir a normalização dos sistemas, serviços e redes. A utilização de normas comuns permitirá, entre outros aspectos, assegurar a intermutabilidade de *hardware* e *software* entre sistemas afins e, adicionalmente, também a capacidade para comunicar e trocar informação entre os diversos Comandos e Unidades, com sistemas de vários Ramos das Forças Armadas e, quando necessário, nomeadamente em situações de gestão de crises, com as estruturas ligadas à área da cibersegurança. Nos casos em que não for possível assegurar a interoperabilidade dos sistemas, podem surgir vulnerabilidades adicionais, susceptíveis de comprometer a segurança das infraestruturas de informação, criando eventuais "pontos de entrada" passíveis de vir a ser explorados pelos ciberataques. Este tipo de riscos necessita assim de ser identificado, quantificado e convenientemente gerido.

Atendendo a que as decisões de investimento dos Estados traduzem normalmente escolhas formuladas entre diversas opções e que, quando os recursos são limitados, estas se tornam por vezes mutuamente exclusivas, a metodologia agora apresentada (DOTMPLF-I) constitui certamente uma boa base para o estabelecimento criterioso de prioridades, facilitando a edificação da capacidade nacional de ciberdefesa.

5.5. Plano de Ação para a Ciberdefesa

O desenvolvimento de um quadro estratégico consistente, assente numa articulação coerente e sinérgica das três componentes (operacional, orgânica e genética), estruturantes da Estratégia Nacional de Ciberdefesa, assume particular importância mas torna-se essencial ir um pouco mais longe, passando da visão à ação. Neste âmbito, a formulação de um conceito de ação estratégica consistente, permitirá fazer face aos desafios suscitados pela edificação de uma capacidade nacional de ciberdefesa, definindo um plano de ação estratégica coerente com o nível de ambição definido.

O plano de ação para a ciberdefesa deverá, sequencialmente e por ordem decrescente de importancia, assentar num conjunto de 5 eixos prioritários:

- **Levantamento da Estrutura de Governação e Gestão Integrada**

  Encontrando-se o levantamento da estrutura de governação da cibersegurança já em curso, mas ainda não completo, assume-se como prioritária a edificação da estrutura de governação associada à ciberdefesa. Sem esta estrutura, não será possível garantir a gestão integrada e equilibrada das capacidades nacionais, identificando com clareza as áreas de responsabilidade e as competências associadas às várias Entidades que intervêm na cibersegurança e ciberdefesa do País. Neste âmbito, assume especial relevância a criação de um Conselho Nacional de Ciberdefesa e de um Conselho Nacional de Cibersegurança que, promovendo uma aproximação coerente e lógica das capacidades existentes ao nível político-estratégico, permita facilitar a articulação operacional entre a área da Cibersegurança e da Ciberdefesa.

- **Sensibilização, Educação e Treino**

  A sensibilização para a cibersegurança constitui um elemento fundamental para criar em todos os cidadãos uma noção correcta dos desafios e riscos emergentes no ciberespaço (ao nível individual, organizacional e nacional). Neste âmbito, importa igualmente reforçar a formação e a educação (graduada e pós-graduada) investindo nas Pessoas, apostando no desenvolvimento do capital intelectual nacional. Face ao número reduzido de especialistas disponíveis na área e à necessidade de garantir a colocação da “pessoa certa no lugar certo” importa desenvolver um programa atrativo de captação e retenção de talentos. De forma a validar as competências existentes, ou a adquirir, torna-se necessário também implementar um programa integrado de treino (ao nível individual, de equipa e coletivo) e um conjunto consistente de exercícios periódicos. Mesmo que sejam adquiridos equipamentos da última geração e sejam levantadas infraestruturas ao nível do estado da arte, sem recursos humanos qualificados, dificilmente se poderá equacionar a existência de uma capacidade de cibersegurança ou ciberdefesa.

- **Informação e Conhecimento Situacional**

  Só identificando precocemente a existência de alterações anómalas aos padrões de trafego e a correspondente identificação de um possível ataque, será possível garantir uma proteção efetiva. O conhecimento da atividade (maliciosa e não maliciosa) e a atualização permanente da evolução da ameaça, revelam-se elementos fundamentais para assegurar a defesa dos sistemas de informação e das redes. Sem conhecermos o ambiente operacional e sem sabermos reconhecer se estamos sob ataque, dificilmente poderemos equacionar a possibilidade de condução de operações no ciberespaço e, consequentemente, também assegurar a ciberdefesa.

- **Aquisição de Equipamentos e Criação de Infraestruturas Adequadas**

  Ainda que seja importante reconhecer a necessidade de podermos dispor de equipamentos considerados de "última geração", nomeadamente, para fazer face ao ritmo acelerado da evolução tecnológica e à sofisticação crescente das ciberameaças, a capacitação tecnológica plena só deverá ocorrer quando for possível dispor de quadros suficientemente qualificados para assegurar a sua operação. Num momento inicial de levantamento da capacidade de ciberdefesa, nomeadamente, em situações em que ainda não existem os equipamentos e as infraestruturas consideradas mínimas para atingir um nível de maturidade residual deverá, em algumas áreas, ser equacionado, de forma equilibrada, um plano de aquisições destinado à capacitação tecnológica mínima exigida.

- **Sinergias Nacionais e Cooperação Internacional**

  Tanto o desenvolvimento de sinergias nacionais como a colaboração internacional constituem elementos estruturantes do levantamento da Estratégia Nacional de Ciberdefesa, tanto no domínio operacional como estrutural. Uma vez que o ciberespaço não reconhece quaisquer fronteiras físicas, nenhum Estado, organização ou individuo poderá isoladamente fazer face a ciberataques de grandes dimensões e proteger-se de forma eficaz. Infelizmente, neste contexto, face ao espectro alargado da ameaça, não será possível equacionar a existência de "soluções locais para problemas globais". O estabelecimento de parcerias de natureza civil-militar, onde a Academia e a Indústria podem vir a assumir um papel de grande importância, permitirá certamente acelerar e melhorar a Formação e Educação de especialistas assim como o processo de capacitação tecnológica. Neste contexto, assume igualmente grande relevância o investimento em I&D e em áreas tecnológicas de ponta, componentes essências para a criação de um nível mínimo de "soberania tecnológica". Ao nível do desenvolvimento de capacidades, a adoção de uma aproximação cooperativa, permitirá reduzir custos e evitar a desnecessária duplicação de esforços.

À luz da hierarquia de prioridades agora definida, será possível, de forma lógica e coerente, revisitar a tabela do Anexo IV e diferenciar entre si as diversas linhas de ação antes identificadas. Após esta prioritização, tendo também em mente os objetivos a atingir, caberá às Forças Armadas a formulação de um conceito de emprego operacional (CONOPS) e subsequentemente a elaboração de um plano de implementação da capacidade de ciberdefesa.

A existência de um plano de ação, concretizando a visão estratégica formulada ao nível político, permitirá assim realizar a ponte entre o conceito e a ação, contribuindo decisivamente para conferir uma maior solidez à execução da Estratégia Nacional de Ciberdefesa.

Conclusões

O ciberespaço, não reconhecendo as tradicionais fronteiras físicas, impõe novas formas de interação e de relacionamento à escala global, colocando o País na vanguarda da revolução digital. A recente definição de uma agenda digital permitirá disponibilizar benefícios económicos e sociais sustentáveis, estimular a criação de empregos, a sustentabilidade e inclusão social, extrair o máximo benefício das novas tecnologias digitais e melhorar a estrutura de enquadramento nacional.

A dependência crescente relativamente ao ciberespaço, de todos os domínios da vida das modernas sociedades, conduz no entanto ao surgimento de novas vulnerabilidades e riscos que têm de ser analisados e, se possível, cuidadosamente geridos de forma a poderem ser mitigados. O inegável valor associado à livre utilização da Internet pode desta forma ser seriamente comprometido por uma vaga crescente de ciberataques, minando a confiança na segurança global do ciberespaço, colocando novos e importantes desafíos à Segurança e Defesa Nacional.

Numa sociedade em rede, as ameaças podem surgir de qualquer local e ter efeitos assimétricos e fortemente disruptivos, aumentando os riscos sociais existentes. Métodos de ataque semelhantes podem ser utilizados para atingir indivíduos, empresas ou Estados. Assistindo-se ao desenvolvimento de capacidades defensivas e ofensivas e à condução de operações militares por parte de vários Países e Organizações, o ciberespaço adquiriu o estatuto de novo dominio operacional. Tal como a terra, o mar e o ar, a Aliança Atlântica reconheceu recentemente a identidade deste novo campo de batalha e a necessidade de criar novas estruturas especializadas, incorporando a ciberdefesa no planeamento de todas as suas atividades e operações militares. Esta decisão, com fortes implicações no conceito de defesa coletiva da NATO, obrigará as várias Nações Aliadas a asumirem um compromisso acrescido ao nível do desenvolvimento das suas capacidades nacionais, nomeadamente, de forma a assegurarem a proteção das suas Forças Armadas e a viabilizarem a sua participação em operações militares conjuntas e combinadas no ámbito NATO.

Existe assim hoje um consenso generalizado, tanto no plano nacional como internacional, que a sobrevivência das modernas sociedades depende cada vez mais de uma capacidade de ciberdefesa credível, capaz de contribuir para a defesa dos Estados, para a proteção das infraestruturas críticas, para proteger o valor gerado, garantir a liberdade de ação e promover a afirmação nacional no ciberespaço.

Neste contexto, não será possível ignorar a necessidade de criação de uma Estratégia Nacional de Ciberdefesa, enquadrada no Conceito Estratégico de Defesa Nacional e articulada, de forma coerente e lógica, através da sua componente operacional, estrutural e genética. Respeitando as atribuições e áreas de competências das várias Entidades e Organizações envolvidas na sua conceção, a implementação desta Estratégia passará certamente pelo reajustamento do atual quadro legal, pela adaptação das doutrinas existentes, pela revisão das estruturas e meios necessários para a sua operacionalização.

De forma a maximizar a sua resultante operacional, a Estratégia Nacional de Ciberdefesa deverá também assentar no desenvolvimento de sinergias nacionais e na cooperação internacional, evitando a desnecessária duplicação de recursos, promovendo uma articulação dos esforços já em curso no nosso País, tanto no âmbito da cibersegurança, como ao nível do combate ao cibercrime, à ciberespionagem e ao ciberterrorismo.

Para Portugal, um ciberespaço disponível, fiável e confiável constitui um domínio estratégico prioritário, não alienável, de defesa de valores e interesses nacionais. Face à natureza deste novo ambiente operacional e ao impacto crescente das ciberameaças, a construção de um futuro digital para Portugal exige o desenvolvimento de uma Estratégia Nacional de Ciberdefesa.

Referências

BBC (2016). *'Smart' Home Devices Used as Weapons in Website Attack*, disponível em http://www.bbc.com/news/technology-37738823

Brenner, S. W. e J. J. Schwerha, IV (2004). Introduction-Cybercrime: A Note on International Issues. International Systems Frontiers 6 (2), pp. 111-114

Buck, Susan J. (1998). *The Global Commons An Introduction*. Island Press, Washington DC.

CEDN (2013). *Conceito Estratégico de Defesa Nacional,* aprovado em 05 de Abril de 2013, através da Resolução do Conselho de Ministros n.º 19/2013, Diário da República.

Couto, Cabral (1988). *Elementos de Estratégia,* Volume I, IAEM.

Denyer, Simon (2016). *China's scary lesson to the world: Censoring the Internet works*, The Washington Post, disponível em https://www.washingtonpost.com

Dougherty, Jill (2016). *NATO cyberwar challenge: establish rules of engagement*, CNN, disponível em http://edition.cnn.com/2016/11/07/politics/nato-cyber-centre-international-law/index.html

Dynamic Network Services, Inc. (2016). *Dyn Analysis Summary of Friday October 21 Attack*, disponível em http://dyn.com/blog

Dynamic Network Services, Inc. (2016). *Dyn Statement on 10/21/2016 DDoS Attack*, disponível em http://dyn.com/blog

ENC (2012). Proposta de Estratégia Nacional de Cibersegurança, disponível em http://www.gns.gov.pt/NR/rdonlyres/ED57762F-3556-4C05-9644-888E35C790BB/0/PropostaEstratégiaNacionaldeCibersegurançaPortuguesa.pdf, consultada em 23Nov12, 17H45.

ENSC (2015). *Estratégia Nacional de Segurança do Ciberespaço*. RCM N.º 36/2015, de 12 de junho, disponível em https://dre.pt/application/file/67443061, consultado em 1/11/2016.

EU (2009). EU Concept for Computer Network Operations in EU-led Military Operations (CNO) [13537/09. dated 22 September 2009]

EU (2012). EU Concept for Cyber Defence for EU-led Military Operations [EEAS 01729/12. dated 08 October 2012]

GPF (2017). Global Policy Forum. Disponível em https://www.globalpolicy.org/social-and-economic-policy/global-public-goods-1-101.html, consultada em 01Fev17, 18H00.

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

Guedes M. A. (2010). The new geopolitical coordinates of cyberspace. Revista Militar, (2503/2504), 823-847.

IDN-CESEDEN (2013). Estratégia da Informação e Segurança no Ciberespaço. Caderno IDN Nº12. Lisboa, Imprensa Nacional – Casa da Moeda.

IETF (2007). Internet Engineering Task Force (IETF), «RFC 4949 - Internet Security Glossary, Version 2», Agosto.

ISO (2004). International Organization for Standardization, «ISO/IEC 13335-1:2004 - Information technology -- Security techniques -- Management of information and communications technology security -- Part 1: Concepts and models for information and communications technology security management».

Keohane, Robert O. e Joseph S. Nye, eds. (1972) Transnational relations and world politics, Cambridge, Massachusetts, USA, Harvard University Press

Martins, L. (2003). Direito da Sociedade da Informação, Vol. IV, Chapter Criminalidade Informática. Coimbra: Coimbra Editores.

MDN (2013). *Orientação Política para a Ciberdefesa*, Despacho Nº 13692/MDN. Diário da Republica II Série, de 28 de outubro, pp. 31977-31979.

MD-NL (2012). The Defence Cyber Strategy. Dutch Ministry of Defense, September.

More, Tyler (2010). *The Economics of Cybersecurity: Principles and policy options*. International Journal of Critical Infrastructure Protection. Vol3.

NATO (2011). NATO Public Diplomacy Division, «Defending the networks - The NATO Policy on Cyber Defence». 2011.

NATO (2012). «NATO and cyber defence», 02-ago-2012. [Online]. Disponível em: http://www.nato.int/cps/en/natolive/topics_78170.htm, consultada em 24Ago12.

Nunes, Paulo (2010). "Mundos Virtuais, Riscos Reais: Fundamentos para a definição da Estratégia da Informação Nacional", Actas I Congresso Nacional Segurança e Defesa, Dezembro.

Nunes, Paulo (2012). "A Definição de uma Estratégia Nacional de Cibersegurança", artigo publicado na Revista "Nação e Defesa", Nº 133, número especial dedicado à "Cibersegurança", Imprensa Nacional – Casa da Moeda.

Nunes, Paulo (2015). Sociedade em Rede, Ciberespaço e Guerra de Informação. Instituto da Defesa Nacional. Coleção Atena Nº34, Imprensa Nacional – Casa da Moeda.

Nye, Joseph S. (2010). Cyber Power. Harvard Kennedy School.

O'Connell, M. E. (2012). Cyber security without cyber war. Journal of Conflict and Security Law, 17(2), 187-209.

PDC (2012). *Política Cibernética de Defesa do Brasil* – documento MD31-P-02 (1ª Edição/2012), Anexo à Portaria Normativa Nº 3.389/MD, de 21 de Dezembro de 2012**,** publicada no dia 27 de Dezembro, no Diário Oficial da União.

RCM 12/12, (2012). *Criação do GPTIC*. Resolução do Conselho de Ministros Nº12 de 2012, DR, 1.ªSérie -N.27, 07Fev.

Rodrigues, Jorge e Devezas, Tessaleno (2007). *Pioneers of Globalization*, Centro Atlântico, Lisboa.

Santos, Lino, Bravo, Rogério, Nunes, Paulo V. (2012), Proteção do Ciberespaço: Uma visão analítica, in Soares, C. G. , Teixeira A. P., Jacinto C.(Eds), Riscos, Segurança e Sustentabilidade, Salamandra, Lisboa, 2012, pp.163-176

Schmitt, Michael N., *et al.* (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press.

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

Slaughter, A. (2004). A New World Order. Princeton University Press.

Smith, Brad (2017). *The need for a Digital Geneva Convention*, disponível em https://blogs.microsoft.com.

Suleyman, Anil (2004). «NCIRC (NATO Computer Incident Response Capability)», in *11th TF-CSIRT Meeting*, Madrid, 2004.

TJUE, Acórdão proferido em 15 de Setembro de 2016, no âmbito do processo C-484/14.

Tsagourias, Nicholas e Buchan, Russel (2015). *Research Handbook on International Law and Cyberspace*. Edward Edgar Publishing.

US Army (2010). «Cyberspace Operations Concept Capability Plan 2016-2028». U.S. Army Capabilities Integration Center, 22-feb-2010.

WBG (2016). World Development Report 2016, World Bank Group - Digital Dividends.

WIKI (2012). Wikipedia contributors, «ISO/IEC 27001», Wikipedia, la *enciclopedia libre*. Wikimedia Foundation, Inc., 07-ago-2012.

ANEXOS

Parâmetros Associados ao Problema

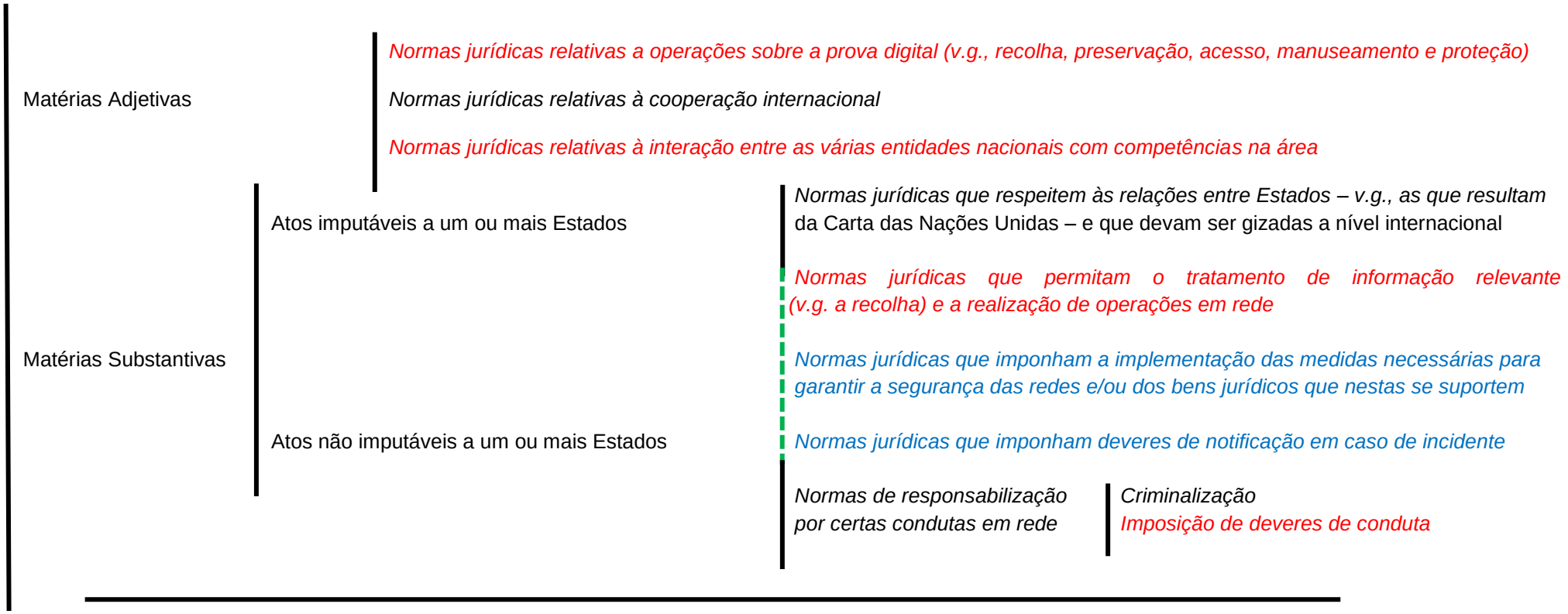
Gama de variação de cada Parâmetro

Tipologia da Ameaça			Impacto e Análise das vulnerabilidades				Gestão de Crises no Ciberespaço						
Finalidade do Ataque	Ator Responsável	Tipo de Ataque (Efeitos)	Escala do Ataque (Geográfica)	Nível de Impacto	Infraestruturas e Sistemas Críticos	Vetores e Linhas de Ação Estratégica Afetadas (CEDN de 2013)	Possível Quadro legal	Entidade 1ª Responsável (EPR) pela Gestão da Crise	Constituição do Gabinete de Gestão de Crise (Ministério – EPR)	Nível da Crise (Situação/ Estado de Exceção)	Estruturas nacionais envolvidas em cada Fase/passo	Estruturas internacionais envolvidas em cada Fase/passo	Problemas/ insuficiências existentes
Hacking	Amadores	Físico	Individuo	Residual	Energia	Exercer Soberania, neutralizar ameaças e riscos à Segurança Nacional	Entre outros diplomas legais, Lei n.º 109/2009, de 15 de setembro, e, no caso de crimes graves, Lei n.º 32/2008, de 17 de julho. Caso envolva dados pessoais, Lei n.º 67/98, de 26 de outubro. Se incitação ao ódio ou violência, artigo 240.º do Código Penal.	Centro Nacional de Cibersegurança	Presidência do Conselho de Ministros	Situação de Normalidade	SOC/CIRC da Organização	Bilateral	Sistema Nacional de Gestão de Crises
Cracking	Hackers	Sintaxe	Local/ Organização	Baixo	Comunicações e Serviços Digitais	Responder às vulnerabilidades nacionais		Gabinete Coordenador de Segurança	Ministro da Defesa	Estado de Emergência ou Crise	CERT Sectorial e Entidades Reguladoras	Multilateral	Doutrina / Procedimentos
Agitação Social	Crackers	Semântico	Regional	Médio	Transportes	Valorizar os recursos e as oportunidades nacionais		Proteção Civil	Ministério da Administração Interna	Estado de Sítio	Centro Nacional de Cibersegurança	CPLP	Regras de Empenhamento (ROE)
Crime Económico	Grupos de Pressão		Nacional	Alto	Sector Bancário			Forças de Segurança	Ministério da Justiça	Estado de Guerra	Gabinete Coordenador de Segurança	UE	Falta de Estratégia Nacional de Ciberdefesa
Espionagem	Criminosos		Internacional	Total	Mercado Financeiro		Artigo 317.º do Código Penal ou artigo 34.º do Código de Justiça Militar	Serviços de Informações	Ministério da Economia (Energia, Transportes e Comunicações)		Centro de Ciberdefesa das Forças Armadas	NATO	Falta de Política Nac para a Segurança e Defesa do Ciberespaço
Terrorista	Terroristas		Global		Sector da Saúde		Lei n.º 52/2003, de 22 de Agosto	Forças Armadas	Ministério dos Negócios Estrangeiros				
Militar	Estados				Fornecimente e Distribuição de Água Potável		Carta das Nações Unidas (v.g., artigos 42.º e 51.º); Tratado do Atlântico Norte (v.g., artigo 5.º); e regras de Direito Internacional Humanitário		Ministério da Saúde				

ANEXO II - Áreas de Cooperação Internacional no Ciberespaço – Visão Nacional

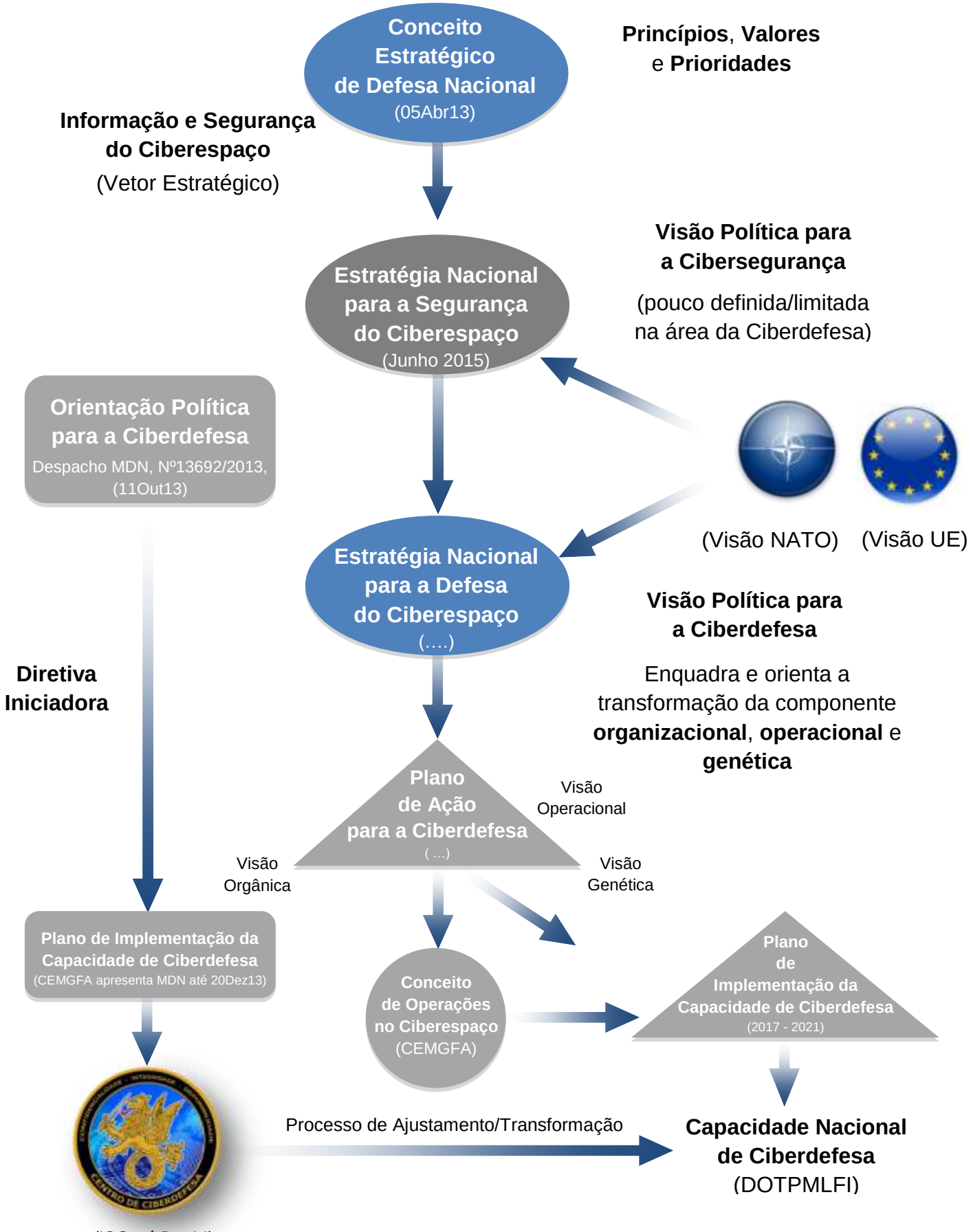
Áreas Comuns de Cooperação Estratégica Internacional no Ciberespaço	Linhas de Desenvolvimento	NATO	UE	ONU	OCDE	Relevância Estratégica	Relevância Operacional	Relevância Económica/ Industrial	Área Nova?
Documentos Estratégicos (de Referência)		• Conceito Estratégico (2010) • Política de Ciberdefesa (2014) • Conclusões da Cimeira de Wales (2014) • Conclusões da Cimeira de Varsóvia (2016) • Declaração Conjunta NATO-EU (06Dez2016)	• Estratégia de Segurança Global (2016) • Agenda Digital para a Europa (2010-20) • Conceito Estratégico de Cibersegurança (2014) • Diretiva NIS (2016) • Declaração Conjunta NATO-EU (06Dez2016)	• Carta das Nações Unidas • Tratado Internacional das Telecomunicações (2012)	• Guidelines Seg SI e Redes (2002) • Recomendação Coop Internacional na Lei Proteção Privacidade (2007)	**E- Elevada; M –** Média; **B** - Baixa			**S**-Sim; **N**-Não
Defesa Coletiva	**Cibersegurança/ Ciberdefesa**	• Ciberdefesa (área prioritária) e 4º Domínio Operacional da Guerra	• Cibersegurança (área prioritária)	• Cibersegurança/e-Governance (área prioritária)	• Cibersegurança (área estruturante economia global)	**E**	**E**	**E**	**S**
	Combate ao Terrorismo	• Combate ao Terrorismo (área prioritária)	• Combate ao Cibercrime em geral (área prioritária)	• Regulação do Ciberespaço (área prioritária)	• Combate ao Cibercrime e Privacidade (área prioritária)	**E**	**E**	**B**	N
	Proteção Infraestruturas Críticas	• Segurança Energética (área prioritária)	• Proteção das Infraestruturas Críticas de Informação (área prioritária)	• Contenção de Ataques de larga escala (área prioritária)	• Proteção SI e Redes (área prioritária)	**E**	**E**	**M**	**S**
	Impacto das novas Tecnologias	• Análise das Tecnologias Emergentes (área prioritária)	• Análise das Tecnologias Emergentes (área prioritária)	• e-Governance e Normalização (área prioritária)	• Monitorização impacto económico das TIC (área prioritária)	**E**	**E**	**E**	N
Gestão de Crises	**Cooperação Civil-Militar**	• Aproximação Civil-Militar (*Comprehensive Approach*)	• Aproximação Civil-Militar (Comprehensive Approach)	• Cooperação Política	• Cooperação Político-Económica	**E**	**E**	**M**	**S**
	Compreensão do Ambiente Internacional	• Monitorização/Análise do Ambiente Internacional e Ameaça Híbrida	• Monitorização/Análise do Ambiente Internacional	• Monitorização do Ambiente Internacional	• Monitorização de Mercados e Economia Global	**E**	**E**	**M**	N
	Partilha de Informações (*Intelligence Sharing*)	• Melhoria da partilha de Informações	• Melhoria da partilha de Informações	• Troca de informação em fora especializados	• Troca de informação em fora especializados	**E**	**E**	**M**	N
Segurança Cooperativa	**Segurança e Defesa**	• EU e Rússia	• NATO	• Cooperação Internacional	• Cooperação Internacional e Desenvolvimento	**E**	**E**	**M**	N
	Cibersegurança/ Ciberdefesa	• UE	• NATO, USA, China e Índia	• Cooperação Internacional	• Cooperação Internacional e Desenvolvimento	**E**	**E**	**M**	**S**
Desenvolvimento de Capacidades Cooperativas área da Cibersegurança/ Ciberdefesa		• Iniciativas de Smart Defence *MNCDE&T-Portugal Lead Nation* *POC:Information Assurance and Cyber Defence Capability Panel (CaP4 IACD)*	• Iniciativas de Polling&Sharing *Cyber Defence Training and Exercises Platform (CDTEXP) – Portugal Lead Nation* *POC: ENISA e Project Team Cy Defence (PT CD) - EDA.*	• Tratados Internacionais POC: POC: Global Cybersecurity Agenda (GCA), da ITU.	• Recomendações e Guidelines *POC: Working Party On Information Security And Privacy, da OCDE.*	**E**	**E**	**E**	**S**
	Doutrina e Organização	• Política, Plano de Ação e Conceito de Ciberdefesa NATO, como refª. • Partilha de informação e melhores práticas; • Cyber Pledge (Cimeira de Varsóvia, 2016)	• Cyber Defence Discipline (Lead Nations PT e FR) • Conceito de Computer Network Operations e Conceito de Ciberdefesa da UE, como refª. • Partilha de informação e melhores práticas;	• Princípios de regulação e cooperação no ciberespaço. • Partilha de informação e melhores práticas	• Recomendações e orientações. • Partilha de informação e melhores práticas	**E**	**E**	**M**	**S**
	Interoperabilidade	• Sinergias civis/militares e cooperação com a comunidade de cibersegurança civil. Ex: *NATO Crypto Interoperability Strategy* (cooperação NATO-EU); *NATO PKI; NATO Common Criteria CaT*. • Declaração Conjunta NATO-EU (06Dez2016)	• Desenvolvimento, na área da cibersegurança, de uma rede europeia de CERTs (Ex:ENISA). • Na área da ciberdefesa, exploração de sinergias civis/militares e cooperação com a comunidade de cibersegurança civil. • Declaração Conjunta NATO-EU (06Dez2016)	• Adoção de políticas, princípios de normalização e requisitos técnicos	• Adoção de políticas, princípios de normalização e requisitos técnicos.	**E**	**E**	**E**	N
	Instalações	• Desenvolvimento partilhado de novas áreas para treino e exercícios de ciberdefesa; • Cyber Range (Estónia); • Cyber Lab na NCI &Cyber Academy (Oeiras)	• Desenvolvimento partilhado de novas áreas para treino e exercícios de ciberdefesa;	• Desenvolvimento de centros especializados para cooperação internacional	• Desenvolvimento de centros especializados para cooperação internacional	**E**	**E**	**B**	N
	Liderança e Pessoal	• Campanhas coordenadas de sensibilização e formação na área da ciberdefesa;	• Campanhas coordenadas de sensibilização e formação na área da Cibersegurança;	• Campanhas coordenadas de sensibilização e formação na área da Cibersegurança;	• Campanhas de sensibilização na área da cibersegurança;	**E**	**E**	**B**	N
	Material e Tecnologia	• Partilha de resultados e esforços de I&D conjuntos em áreas de interesse comum. Ex: *Multinational Cyber Defence Capability Development (MNCD2); NATO Information Assurance Product Catalogue (NIAPC);* • Pool de capacidades de ciberdefesa para apoio às operações NATO.	• Partilha de resultados e esforços de I&D conjuntos em áreas de interesse comum. • Pool de capacidades de ciberdefesa para Quartéis-Generais de nível Operacional e Tático (OHQ/FHQ)	• Partilha de resultados e esforços de I&D conjuntos em áreas de interesse comum.	• Partilha de resultados e esforços de I&D conjuntos em áreas de interesse comum.	**E**	**E**	**E**	**S**
	Treino e Exercícios	• Pooling de recursos de treino/educação; • Partilha de informação sobre ameaças e incidentes em contexto operacional de ciberdefesa para apoio de missões NATO (POC: NCIRC). • Declaração Conjunta NATO-EU (06Dez2016) • Exercício *NATO Cyber Coalition (POC ACT)*.	• Pooling de recursos de treino/educação; • Partilha de informação sobre ameaças e incidentes em contexto operacional de cibersegurança (POC ENISA) e ciberdefesa (POC EUMS) para apoio de missões de segurança e defesa da UE (missões CSDP). • Declaração Conjunta NATO-EU (06Dez2016) • Exercício *Cyber Europe*.	• Pooling de recursos de treino/educação existentes;	Nada a referir.	**E**	**E**	**B**	**S**

Adaptado de IDN-CESEDEN (2013)



Normas jurídicas que criem as entidades necessárias e/ou que estabeleçam as atribuições e competências necessárias para implementar o referido quadro legal

- Normas jurídicas inexistentes ou insuficientes
- Normas jurídicas em vias de aprovação, por efeito da vigência de Diretiva da União Europeia
- Normas jurídicas que são simultaneamente relevantes em contexto de atos imputáveis a Estados e em contexto de atos não imputáveis a Estados


Conceito Estratégico de Defesa Nacional
(05Abr13)
Princípios, Valores e Prioridades
Informação e Segurança do Ciberespaço
(Vetor Estratégico)
Estratégia Nacional para a Segurança do Ciberespaço
(Junho 2015)
Visão Política para a Cibersegurança
(pouco definida/limitada na área da Ciberdefesa)
Orientação Política para a Ciberdefesa
Despacho MDN, Nº13692/2013, (11Out13)
(Visão NATO)
(Visão UE)
Estratégia Nacional para a Defesa do Ciberespaço
(….)
Visão Política para a Ciberdefesa
Enquadra e orienta a transformação da componente organizacional, operacional e genética
Diretiva Iniciadora
Plano de Ação para a Ciberdefesa
(…)
Visão Operacional
Visão Orgânica
Visão Genética
Plano de Implementação da Capacidade de Ciberdefesa
(CEMGFA apresenta MDN até 20Dez13)
Conceito de Operações no Ciberespaço
(CEMGFA)
Plano de Implementação da Capacidade de Ciberdefesa
(2017 - 2021)
Processo de Ajustamento/Transformação
Capacidade Nacional de Ciberdefesa
(DOTPMLFI)
(IOC até Dez14)

ANEXO V - Estratégia Nacional de Ciberdefesa – Finalidade, Objetivos e Linhas de Ação

Adaptado de: MDN (2013), Nunes (2012), PDC (2012) e MD-NL (2012).

Finalidade O que se pretende atingir (*What*)	**Objetivos Genéricos** (*Ends*)	**Objetivos Específicos** *(Ways)*	**Linhas de Ação** Atividades a desenvolver para se atingirem os objetivos (*Means*)	**Prioridade Relativa**
Face à ocorrência de ciberataques, que podem por em risco a salvaguarda dos interesses e a governação do Estado, a capacidade de ciberdefesa pretende essencialmente defender a Soberania Nacional, garantir a liberdade de ação das Forças Armadas nos vários domínios de emprego operacional (incluindo o ciberespaço) e contribuir, de forma sinérgica e cooperativa, para a cibersegurança do País.	Garantir a proteção, a resiliência e a segurança das redes de Comunicações e Sistemas de Informação (CSI) da Defesa Nacional contra ciberataques Assegurar a liberdade de ação do País no ciberespaço	1. Garantir a liberdade de ação e a utilização eficaz do ciberespaço pelas Forças Armadas (FA) e impedir ou dificultar a sua utilização contra os interesses da Defesa Nacional;	a) Levantar o Sistema de Ciberdefesa Nacional (SCN), tendo por base a criação e operacionalização de um Centro de Ciberdefesa das Forças Armadas;	1
			b) Criar um Conselho de Ciberdefesa para realizar a coordenação nacional com a estrutura de Cibersegurança, a levantar, e promover a integração da Ciberdefesa no âmbito do processo de gestão de crises nacional;	1
			c) Estabelecer critérios de análise do risco e realizar a sua gestão de forma a reduzir para níveis aceitáveis os riscos das infraestruturas críticas de informação de interesse para o desenvolvimento das atividades ligadas à Defesa Nacional;	3
			d) Criar uma Política de Segurança da Informação e processos de cibersegurança comuns a todas as estruturas das FA, de forma a normalizar procedimentos e reforçar a proteção dos ativos de informação da Defesa Nacional; e	1
			e) Assegurar a capacidade conjunta das FA operarem e conduzirem operações em rede, com liberdade de ação e segurança, fortalecendo, desta forma, a sua capacidade de Comando e Controle (C2).	1
	Garantir a proteção, a resiliência e a segurança das redes de CSI da Defesa Nacional contra ciberataques Contribuir de forma cooperativa para a Cibersegurança Nacional	2. Desenvolver competências e gerir os recursos humanos necessários à condução das atividades de Defesa no Ciberespaço	a) Definir perfis e criar cargos/funções específicos para atender às necessidades da Ciberdefesa;	1
			b) Identificar, selecionar e recrutar o pessoal dotado das competências ou aptidões específicas ligadas à ciberdefesa, existente no ambiente interno e externo das FA;	2
			c) Criar instrumentos para atrair, recrutar e reter o pessoal especializado nas estruturas de Ciberdefesa, motivando a sua permanência e permitindo assim garantir a continuidade da sua atividade.	2
			d) Propor a criação de uma Reserva Nacional capaz de, em caso de crise ou conflito, permitir apoiar as atividades de Defesa no Ciberespaço;	1
			e) Estabelecer critérios de inamobilidade e controlar a mobilização e desmobilização do pessoal que participa nas atividades de Defesa no Ciberespaço;	1
			f) Formar e qualificar, de forma contínua, pessoal para atuar nas atividades de Ciberdefesa, aproveitando para esse efeito, sempre que possível, as estruturas de formação existentes;	2

Finalidade O que se pretende atingir (*What*)	**Objetivos Genéricos** (*Ends*)	**Objetivos Específicos** *(Ways)*	**Linhas de Ação** Atividades a desenvolver para se atingirem os objetivos (*Means*)	**Prioridade Relativa**
			g) Estimular e viabilizar a participação do pessoal afeto à área da Ciberdefesa em cursos, estágios, seminários e outras atividades afins, realizadas em Portugal e no estrangeiro;	2
			h) Realizar eventos periódicos, de âmbito nacional e internacional, que possibilitem a apresentação e discussão pública de temas relevantes para a Ciberdefesa.	2
			i) Realizar parcerias estratégicas e intercâmbios, na área da formação, do treino e dos exercícios de Cibersegurança e Ciberdefesa, entre as FA e instituições nacionais e internacionais de interesse;	2
			j) Incluir conteúdos relacionados com a Segurança de Informação, Cibersegurança e Ciberdefesa nos currículos dos cursos ministrados, aos diversos níveis, em todos os estabelecimentos de ensino e centros de formação das FA; e	2
			k) Propor, em coordenação com o Ministério da Educação (ME), a realização de uma campanha nacional de educação e sensibilização Nacional para a Cibersegurança e Ciberdefesa, visando aumentar assim o nível de consciencialização da sociedade portuguesa para este problema.	2
	Garantir a proteção, a resiliência e a segurança das redes de CSI da Defesa Nacional contra ciberataques	3. Contribuir para a produção de conhecimento situacional do ciberespaço e para a recolha de informações de interesse para a Defesa Nacional	a) Adequar a doutrina associada à área das informações de modo a incluir o ciberespaço como fonte importante de recolha de dados;	3
			b) Criar estruturas especializadas de informações no Ciberespaço (*Cyber Intelligence*), conforme as necessidades dos órgãos de informações das FA e do SCN;	1
			c) Estabelecer um canal técnico entre o Centro de Ciberdefesa, o Centro de Informações e Segurança Militar (CISMIL) e o Serviço de Informações Estratégicas de Defesa (SIED), no tocante à área do Ciberespaço; e	1
			d) Levantar mecanismos de recolha de informação associada às ameaças internas e externas, reais ou potenciais, para contribuir para a formação da consciência situacional necessária às atividades das FA no ciberespaço e nos restantes domínios operacionais.	3
	Garantir a proteção, a resiliência e a segurança das redes de CSI da Defesa Nacional contra ciberataques	4. Criar, desenvolver e manter atualizada a doutrina de emprego das capacidades associadas à Ciberdefesa	a) Criar e desenvolver a doutrina nacional de Ciberdefesa;	1
			b) Apoiar o desenvolvimento de trabalhos académicos ligados à segurança e defesa do ciberespaço, nomeadamente de natureza doutrinária, em instituições de ensino superior (civis e militares), de interesse para as atividades da Defesa Nacional;	5
			c) Promover o intercâmbio doutrinário, incluindo os aspetos normativos e técnicos, com instituições civis e militares, nacionais e de nações amigas, nomeadamente, no quadro da NATO e UE;	5

Finalidade O que se pretende atingir (*What*)	**Objetivos Genéricos** (*Ends*)	**Objetivos Específicos** *(Ways)*	**Linhas de Ação** Atividades a desenvolver para se atingirem os objetivos (*Means*)	**Prioridade Relativa**
	Assegurar a liberdade de ação do País no ciberespaço		d) Inserir a área da Ciberdefesa em todos os exercícios conjuntos, atividades de treino operacional, exercícios de simulação de combate e nas operações conjuntas;	2
			e) Organizar exercícios nacionais periódicos de ciberdefesa (como o Exercício "Ciber Perseu") que, de forma conjunta, permitam testar e avaliar as capacidades residentes nas FA.	2
			f) Criar um sistema de gestão do conhecimento e de lições aprendidas, nomeadamente, para apoiar a criação e atualização da doutrina de Ciberdefesa; e	2
			g) Atribuir ao Centro de Ciberdefesa a responsabilidade por propor as inovações e atualizações da doutrina nacional para a área da defesa do Ciberespaço.	1
	Garantir a proteção, a resiliência e a segurança das redes de CSI da Defesa Nacional contra ciberataques	5. Adotar medidas que contribuam para reforçar a Segurança dos sistemas CSI das FA e da Defesa Nacional;	a) Implementar uma Politica de Segurança da Informação conjunta capaz de, face à ocorrência de ciberataques, garantir a continuidade de operação e a recuperação dos sistemas CSI das FA e da Defesa Nacional,	1
			b) Implementar processos normalizados de gestão de incidentes, tendo em conta a legislação e normas vigentes, as melhores práticas, os padrões internacionais mais relevantes, a doutrina de emprego e os requisitos operacionais específicos de cada Ramo das FA;	1
			c) Implementar uma Infraestrutura de Chaves Públicas da Defesa (ICP Defesa);	4
			d) Determinar padrões interoperáveis de criptografia da Defesa em complemento aos da Administração Central do Estado; e	4
			e) Implementar a realização sistemática de auditorias de Segurança aos sistemas CSI das FA e da Defesa.	4
	Garantir a proteção, a resiliência e a segurança das redes de CSI da Defesa Nacional contra ciberataques Assegurar a liberdade de ação do País no ciberespaço	6. Potenciar a Investigação, Desenvolvimento e Inovação (I&D-I) das FA e implementar linhas de investigação conjuntas, orientadas para o desenvolvimento da capacidade de Ciberdefesa;	a) Definir, no âmbito da Defesa, uma estratégia de Ciência e Tecnologia e as linhas de investigação a desenvolver para o levantamento da capacidade de Ciberdefesa nacional.	5
			b) Planear e lançar projetos de I&D-I, de forma a potenciar as capacidades nacionais existentes e integrar os esforços conjuntos das FA, para atender às necessidades inerentes ao desenvolvimento da capacidade de Ciberdefesa;	4
			c) Identificar competências específicas em I&D-I (individuais e organizacionais), de interesse para a área da Ciberdefesa, no âmbito do MDN e dos centros de I&D civis (públicos e privados), estabelecendo parcerias entre centros de excelência nacionais e internacionais, para potenciar sinergias, explorar esforços cooperativos e evitar a dispersão de recursos;	5

Finalidade O que se pretende atingir (*What*)	**Objetivos Genéricos** (*Ends*)	**Objetivos Específicos** *(Ways)*	**Linhas de Ação** Atividades a desenvolver para se atingirem os objetivos (*Means*)	**Prioridade Relativa**
	Contribuir de forma cooperativa para a Cibersegurança Nacional		d) Criar parcerias e mecanismos de cooperação entre as estruturas de I&D-I militares e os centros de I&D civis (públicos e privados), de modo a estimular a integração das iniciativas de interesse para a defesa do ciberespaço;	5
			e) Criar programas, no âmbito do MDN, em parceria com o Ministério da Ciência, Tecnologia e Ensino Superior (MCTES), que contemplem o emprego dual (civil e militar) das tecnologias e ferramentas utilizadas no ciberespaço, para fortalecer o envolvimento do sector industrial nas fases de desenvolvimento dos projetos de interesse para a Ciberdefesa.	5
	Garantir a proteção, a resiliência e a segurança das redes de CSI da Defesa Nacional contra ciberataques Assegurar a liberdade de ação do País no ciberespaço Contribuir de forma cooperativa para a Cibersegurança Nacional	7. Rever e desenvolver o quadro legal existente, adaptando o ordenamento jurídico nacional de forma a permitir apoiar as actividades de Defesa no Ciberespaço;	a) Colaborar com a Presidência do Conselho de Ministros (PCM), com o Gabinete Nacional de Segurança (GNS) e/ou com o Órgão a quem for atribuída a responsabilidade de elaboração da Política Nacional de Cibersegurança;	5
			b) Manter atualizada a Política de Ciberdefesa em consonância com a Política Nacional de Cibersegurança, quando a mesma existir;	1
			c) Definir as atribuições e responsabilidades das várias entidades envolvidas nas atividades de Defesa Cibernética, no respeito do quadro legal em vigor;	1
			d) Elaborar propostas de criação, desenvolvimento e adequação de legislação nacional, com a finalidade de apoiar as atividades de Defesa no Ciberespaço;	1
			e) Propor a criação de um programa orçamental específico, destinado a financiar e a viabilizar as ações e atividades relacionadas com o desenvolvimento da capacidade nacional de Ciberdefesa;	5
			f) Rever os pressupostos de planeamento estratégico militar e as possibilidades de emprego operacional para considerar as ações no ciberespaço; e	1
			g) Propor a adequação da Lei do Recrutamento, da Lei de Mobilização Nacional e do Sistema Nacional de Mobilização para torná-los compatíveis com as necessidades da Ciberdefesa;	1
	Contribuir de forma cooperativa para a Cibersegurança Nacional	8. Contribuir cooperativamente para a cibersegurança dos ativos de informação do Estado, situados dentro e fora do âmbito do MDN	a) Colaborar, dentro dos limites da legislação em vigor, com os demais órgãos da Administração Pública do Estado (APE), em estreita coordenação com o Centro Nacional de Cibersegurança (CNCS), para o restabelecimento da sua Cibersegurança;	5
			b) Manter uma base de dados de conhecimento e estabelecer um canal técnico, para partilha de informação relativa a incidentes de rede, entre o Centro de Ciberdefesa, o CNCS e os restantes órgãos do Estado responsáveis pelo combate ao Cibercrime, ao Ciberterrorismo e à Ciberespionagem; e	3

Finalidade O que se pretende atingir (*What*)	**Objetivos Genéricos** (*Ends*)	**Objetivos Específicos** *(Ways)*	**Linhas de Ação** Atividades a desenvolver para se atingirem os objetivos (*Means*)	**Prioridade Relativa**
			c) Atuar no reconhecimento de artefactos e desenvolvimento de ferramentas cibernéticas, em conjunto com o CNCS, contribuindo assim para a proteção dos ativos de informação do APE.	3
	Assegurar a liberdade de ação do País no ciberespaço Contribuir de forma cooperativa para a Cibersegurança Nacional	9. Melhorar a capacidade de Ciberdefesa Cooperativa do País, através da exploração de Sinergias Nacionais e da Cooperação Internacional	a) Promover a realização de Exercícios nacionais e internacionais na área da ciberdefesa, abertos à participação de entidades civis, nomeadamente, as que são responsáveis pela cibersegurança do país e as que são responsáveis pela operação das infraestruturas críticas nacionais.	
			b) Criar, em articulação com o Sistema de Ciberdefesa Nacional, um Centro de Excelência de Ciberdefesa (CEC), constituído por especialistas (militares e civis), para melhorar a capacidade de ciberdefesa cooperativa nacional, através da cooperação e da partilha de informação no âmbito nacional e internacional, desenvolvendo para esse efeito atividades de educação, I&D, análise de lições aprendidas e assessoria;	5
			c) Desenvolver a atividade do CEC de forma a que este Centro se venha a constituir como a principal fonte de conhecimento nacional nas seguintes áreas estratégicas da Ciberdefesa: Enquadramento legal e desenvolvimento de políticas; desenvolvimento de Conceitos e pensamento Estratégico; Estudo do ambiente tático e das Operações Centradas em Rede; Proteção de Infraestruturas de Informação Críticas.	5
			d) Apoiar, na área da Cibersegurança e Ciberdefesa, a instalação e o funcionamento da futura *NATO Communications, Information and Cyber Academy* da NATO em Oeiras, com base nas competências residentes no CEC.	4
			e) Potenciar e valorizar o Projeto de *Smart Defence MNCDE&T* (vertente NATO e Nacional) e explorar as oportunidades decorrentes do exercício das funções de *Discipline Leader* para E&T em Ciberdefesa, na área CSDP da EU.	2
			f) Assumir e potenciar a gestão da plataforma centralizada de E&T em Ciberdefesa da UE, de forma a potenciar o papel de Portugal como integrador das iniciativas NATO-EU nesta área.	2
			g) Promover intercâmbios e estabelecer processos de troca de conhecimentos com Centros de Excelência nacionais e internacionais, nomeadamente, no âmbito da NATO e da EU.	5