Universidade Católica Portuguesa

Instituto de Estudos Políticos

O CIBERTERRORISMO COMO TÁTICA DE GUERRA NO SÉC. XXI

O papel das Organizações Internacionais na prevenção e proteção desta ameaça

Dissertação submetida como requerimento parcial para a conclusão do Mestrado em Ciência Política e Relações Internacionais – Segurança e Defesa

Patrícia Ramos de Carvalho Barros Bastos

100520003

Orientadora: Professora Doutora Raquel Duque

dezembro, 2022

Lisboa, Portugal

Agradecimentos

Os meus primeiros agradecimentos são dirigidos à minha orientadora, Professora Doutora Raquel Duque, pela delicadeza e dedicação despendida. Todos os seus conselhos e sugestões, bem como a permanente motivação dada, foram determinantes e essenciais para o resultado final da dissertação.

Não poderia deixar de agradecer também ao Instituto de Estudos Políticos (IEP) por me ter acolhido durante estes cinco anos do meu percurso académico. Um especial agradecimento ao Professor Doutor João Carlos Espada, Diretor do IEP, e à Professora Doutora Ivone Moreira, Coordenadora do Mestrado, por demonstrarem como é possível alcançarmos a excelência através do trabalho árduo e pela sua dedicação aos alunos.

Gostaria de registar a minha enorme gratidão a todas as personalidades entrevistadas, nomeadamente, ao Professor Doutor José Tribolet, Professor Catedrático do Instituto Superior Técnico (IST), à Dra. Dalila Araújo, vice-Presidente do Observatório de Segurança, Criminalidade Organizada e Terrorismo (OSCOT), ao Dr. João Pacheco, Fundador e CEO da empresa Cyberprotech, ao Dr. José Casinha, *Chief Information Security Officer* da empresa OutSystems, ao Dr. Bruno Castro, fundador e CEO da empresa VisionWare, ao Dr. Francisco Nina Rente, cofundador da empresa Art Resilia e da empresa The Rock - Cybsecurity, ao Serviço de Informações de Segurança (SIS) e ao Dr. Pedro Mendonça, coordenador do Observatório de Cibersegurança do Centro Nacional de Cibersegurança (CNCS). Todos os seus contributos revelaram-se fundamentais para esta dissertação, tendo sido uma honra para mim beneficiar da oportunidade das entrevistas concedidas para aprofundar os meus conhecimentos sobre o ciberterrorismo.

Aos meus amigos, agradeço todo o apoio recebido ao longo desta etapa e por terem sido o meu "porto de abrigo" quando mais precisei.

À minha querida Mãe, que sempre me apoiou incondicionalmente, agradeço por todos os conselhos sábios e por todo o amor que me transmitiu. Agradeço também por ter sido a luz que me guiou sempre que me senti perdida.

Ao meu querido Pai, a quem dedico esta dissertação, agradeço pelo amor, pela ternura e por todas as memórias lindas que me deixou. Serás sempre o meu companheiro, estrela da minha vida.

Resumo

Na entrada do milénio, os ataques terroristas de 2001 exigiram às Organizações Internacionais (OI) como a UE (União Europeia) e a NATO (Organização do Tratado do Atlântico Norte) a adaptação a uma ameaça de segurança que criou uma nova realidade nas relações internacionais, o terrorismo de índole fundamentalista islâmico. Com o processo da globalização e a crescente evolução tecnológica, desenhou-se um caminho que fez convergir o terrorismo para o ciberespaço: o ciberterrorismo.

Trata-se de uma extensão natural do terrorismo, mas sem rosto. Um perigo silencioso que está na origem de muitas ameaças à segurança interna de cada Estado e à segurança humana, que depende da tecnologia para o seu bom funcionamento. Considerando a Era em que vivemos, torna-se cada vez mais apelativo causar danos significativos através de mecanismos tecnológicos à distância e, muitas vezes, indetetáveis que o ciberespaço assim permite.

A presente investigação pretende analisar como o ciberterrorismo pode ser considerado como uma tática de guerra no séc. XXI e como tem evoluído ao longo do tempo. Serão analisados marcos históricos como os ciberataques na Estónia em 2007, na Geórgia em 2008 e no Irão em 2010, de forma a ser possível entendermos como estes acontecimentos despertaram a urgência no desenvolvimento de medidas de proteção por parte das OI e dos próprios Estados.

Será examinada a evolução cronológica das estratégias de cibersegurança e ciberdefesa da UE e da NATO com vista a identificar como os casos de estudo serviram de impulso para o desenvolvimento de um quadro político de defesa que fosse capaz de proteger os Estados das ameaças cibernéticas atuais. Nesta sequência, pretende-se verificar a relevância do trabalho desempenhado por estas organizações na prevenção e proteção contra o ciberterrorismo. Este trabalho pretende ainda proporcionar recomendações para ações que podem ser tomadas, quer a nível internacional, quer a nível nacional para o reforço e melhoria da segurança cibernética.

Palavras-Chave: Ciberespaço; Ciberterrorismo; Cibersegurança; Ciberdefesa; União Europeia; NATO.

Abstract

At the beginning of the millennium, the terrorist attacks of 2001 required International Organizations such as the EU (European Union) and NATO (North Atlantic Treaty Organization) to adapt to a security threat that created a new reality in international relations, the terrorism of an Islamic fundamentalist nature. With the process of globalization and the growing technological evolution, a path was traced that made terrorism convert to cyberspace: cyberterrorism.

It is a natural extension of terrorism, but it has no face. A silent danger that is at the origin of many threats to the internal security of each State and to human security, which depends on technology for its proper functioning. Considering the era we live in, it becomes increasingly appealing to cause damage through remote and often undetectable technological control that cyberspace allows.

In this investigation, it is intended to analyze how cyberterrorism can be considered as a war tactic in the 21st century and how it has evolved over time. Historical milestones such as the cyberattacks in Estonia in 2007, in Georgia in 2008 and in Iran in 2010 will be analyzed in order to understand how these events aroused the urgency to develop protection measures by the International Organizations and also by the States.

The chronological evolution of the EU and NATO cybersecurity and cyberdefense strategies will be examined in order to identify how the case studies served as an impetus for the development of a defense policy framework capable of protection States from current cyber threats. In this sequence, it is intended to verify the importance of the work performed by these organizations in the prevention and protection against cyberterrorism. This work also intends to provide recommendations that reflect the actions that must be taken, both internationally and nationally, to reinforce and improve cybersecurity.

Keywords: Cyberspace; Cyberterrorism; Cybersecurity; Cyberdefense; European Union; NATO.

“There are only two types of organizations: those that have been hacked and those who don’t yet know they have been hacked.”

John Chambers, antigo CEO da empresa CISCO Systems

Lista de Figuras

Índice

Introdução

Segundo Susan Buck (1998), o ciberespaço apresenta-se como um dos *Global Commons,* isto é, como um dos domínios partilhados pelos diversos Estados, mas que não são propriedade de nenhum Estado em particular. É, também, o primeiro domínio de operações completamente criado pelo Homem que apresenta uma camada física e uma camada lógica. Na primeira, encontram-se as infraestruturas de serviços, de redes, de comunicações, ou seja, o "corpo" por detrás da Internet; a segunda, é entendida como as trocas de informações entre os atores, sejam estes indivíduos singulares ou organizações.

A introdução do ciberespaço na esfera das Relações Internacionais veio, segundo Nye (2010), ampliar o "jogo de xadrez" entre os atores contribuindo para uma maior assimetria no exercício de poder dado que um ator isolado e sem grandes recursos pode levar a cabo uma operação com grandes impactos sociais e materiais sobre um determinado alvo. O facto de os Estados e OI não terem um controlo eficaz sobre o ciberespaço proporciona a ocorrência de variados e numerosos atos hostis, transformando este domínio numa "arma cibernética" usada quer pelos Estados, para afirmar o seu ciberpoder, quer pelas organizações terroristas que procuram causar danos e perturbar a ordem internacional.

Ao longo dos anos, assistimos ao desenvolvimento das potencialidades e das vulnerabilidades do ciberespaço. Se, por um lado, é um meio facilitador de comunicação e partilha de informação entre diferentes atores, por outro lado veio permitir um aumento da cibercriminalidade dadas as suas características globais e abertas, não havendo barreiras nem fronteiras físicas a conquistar para perpetuar ataques. O surgimento de atores hostis não-estatais no ciberespaço proporcionou, assim, uma nova dimensão no fenómeno do terrorismo, acarretando riscos acrescidos para a segurança mundial.

Cada vez mais a atividade do dia-a-dia da sociedade e das organizações ocorre e depende das atividades no ciberespaço. Este é uma extensão do mundo físico, e todos os eventos que ocorrem neste último irão repercutir-se no ciberespaço e vice-versa, pois ambos estão ligados e sincronizados um com o outro.

O aparecimento de atores não-estatais no ciberespaço combinado com a popularidade do radicalismo proporcionaram uma nova dimensão para o terrorismo atuar. Serve de ferramenta na construção de uma nova face de conflito, pondo assim a segurança e a paz mundiais em risco. A evolução tecnológica bem como a evolução da Internet, fizeram

aumentar a possibilidade de ocorrerem ciberataques terroristas pois, através do veículo virtual que é o ciberespaço, a informação viaja a ritmos alucinantes e pode ser intercetada, produzida e manipulada por criminosos.

Os Estados e as OI foram confrontados com uma nova realidade para a qual não estavam preparados para lidar, tendo sido obrigados a mudar drasticamente as suas políticas de segurança e de defesa, passando a incluir termos como "ciberterrorismo", "cibersegurança" e "ciberdefesa", que não tinham grande enfoque antes do início do milénio.

Nesta dissertação, adotou-se o conceito de ciberterrorismo como "o uso politicamente motivado de computadores e tecnologias de informação para causar perturbações severas ou medo generalizado na sociedade"[1], pois apesar de haver várias interpretações no que consiste um ato ciberterrorista, esta mostra-se a mais adequada para tratar toda a informação recolhida. Neste sentido, pretende-se responder à seguinte pergunta de investigação: *Pode o ciberterrorismo ser utilizado como uma tática de guerra no século XXI?*.

Esta dissertação encontra-se organizada em quatro capítulos, sendo o primeiro denominado "Ciberterrorismo" onde se realiza um estudo sobre a história deste fenómeno, explicitando o seu aparecimento, bem como as dinâmicas dos atores do ciberespaço, alicerçando a investigação na obra "Cyber Power" de Joseph Nye. Como terceiro ponto, dá-se o reconhecimento dos diferentes tipos de ciberataques e como estes podem ser a nova e moderna forma de criar hostilidades entre os atores.

No segundo capítulo, "Ciberterrorismo como tática de guerra", apresenta-se a evolução do fenómeno da guerra até ao século XXI, desenvolvendo-se uma linha de pensamento desde os tempos de Clausewitz até ao início do milénio com a designada Guerra ao Terror. Por forma a refletir como novas táticas de guerra, selecionaram-se três casos de estudo – os ciberataques à Estónia (2007), à Geórgia (2008) e ao Irão (2010).

[1]Definição adotada pelo Centro de Excelência da NATO para a Ciberdefesa Cooperativa (CCDCOE). Disponível em: https://ccdcoe.org/library/publications/cyber-terrorism-in-theory-or-in-practice/

No capítulo seguinte, foi feita a contextualização das OI, nomeadamente, da União Europeia e da NATO sobre o seu papel na prevenção e proteção da ameaça cibernética. Apresenta-se, por ordem cronológica, os trabalhos desenvolvidos por estas duas organizações no âmbito da cibersegurança/ciberdefesa, como bem como as políticas da defesa e segurança adotadas para os Estados-Membros (UE) e Aliados (NATO).

Por fim, o último capítulo, as "Recomendações", reproduzem-se e analisam-se as entrevistas efetuadas a especialistas em cibersegurança, a entidades públicas com competências na área da cibersegurança e ciberdefesa e ainda a empresas que desenvolvem atividades neste domínio. Através desta análise, pretende-se transmitir as preocupações e sugestões que cada um proporcionou com base na sua experiência laboral.

Metodologia

A presente dissertação foi elaborada através de uma abordagem qualitativa. Pretendeu-se analisar e interpretar a prevenção e a proteção face ao ciberterrorismo no século XXI, investigando assim a evolução dos apoios aos Estados-Membros da UE e da NATO. A análise das medidas implementadas por estas duas OI revelou-se pertinente devido à convergência de países que as constituem e por ambas terem vindo a desenvolver a área do ciberterrorismo.

Neste raciocínio, tornou-se incontornável adotar a teoria do Institucionalismo Liberal, dado que esta "formula um projeto de segurança coletiva assente num esforço partilhado de pacificação de conflitos através de processos de negociação e conciliação alcançados por leis e instituições"[2]. A influência nos ordenamentos jurídicos dos EM é um elemento de estudo desta corrente teórica, e, por conseguinte, tanto a UE como a NATO, que têm como um dos princípios basilares a cooperação em prol da garantia da paz e segurança, adquirem especial relevância para a presente dissertação.

Para responder à pergunta de investigação "pode o ciberterrorismo ser considerado como uma tática de guerra no séc. XXI?", foram analisados casos de ciberataques marcantes na história como a Estónia (2007), Geórgia (2008) e Irão (2010), pois cada um destes contribuiu para fortalecer as políticas de cibersegurança das OI e dos Estados como também serviram para mudar a perspetiva destes em relação ao novo *modus operandis* de uma possível guerra no futuro.

No primeiro capítulo pretendeu-se responder às perguntas derivadas "o que é o ciberterrorismo?" e "como funcionam as operações no ciberespaço?" o que implicou a consulta das definições dadas pelos organismos das OI como o Centro de Excelência NATO para a Ciberdefesa Cooperativa (CCDCOE), a Agência da União Europeia para a Formação Policial (CEPOL), Agência da União Europeia para a Cibersegurança (ENISA) e também pelo Centro Nacional de Cibersegurança (CNCS). Para a compreensão sobre as dinâmicas desta ameaça e como se correlaciona o poder e o ciberespaço encontram-se autores fundamentais como Joseph Nye (2010), Gabriel Weimann (2004), Lino Santos e Armando Marques Guedes (2015), Luís Brito (2010), Paulo Moniz (2019), António Tomé

[2] Dias, Mónica e Orlando Samões. "Liberalismo e Institucionalismo liberal". *Segurança Contemporânea.* Editado por Raquel Duque, Diogo Noivo e Teresa de Almeida e Silva. Lisboa, 2016.

(2015) e os cadernos do Instituto de Defesa Nacional (IDN), números 12 (2013) e 133 (2012).

No segundo capítulo procedeu-se a uma análise dos casos de estudo escolhidos para os quais foram consultados relatórios oficiais e artigos de sites oficiais, como também se revelaram imprescindíveis as obras de Singer e Friedmann (2014), Clarke e Knake (2012), James Farwell (2011), Paulo Shakarian (2011), de David Sanger (2012) e (2018), David Hollis (2011) para uma melhor perceção do que são as capacidades de um ciberataque. Numa outra nota, para entendermos a evolução das técnicas de guerra ao longo dos séculos foram consultados trabalhos de Carl Von Clausewitz (1997), Mary Kaldor (2012), Teresa Almeida Cravo (2014), João Paulo Pereira (2021) e Vítor Viana (2010).

No terceiro capítulo foi formulada a pergunta derivada "que meios é que a UE e a NATO dispõem para proteger e prevenir dos seus Estados-Membros da ameaça do ciberterrorismo?" tendo-se procedido à análise individual de cada organização através da consulta de várias declarações oficiais e relatórios dos respetivos organismos para ser possível entender a evolução dos trabalhos relativos ao combate ao ciberterrorismo.

Finalmente, o quarto e último capítulo desenvolveu-se através da realização de entrevistas a especialistas, entidades nacionais e empresas no âmbito da cibersegurança. Para a análise das entrevistas foi escolhida uma estratégia de investigação qualitativa, nomeadamente a análise de conteúdo, que é descrita por Bardin (1977) como "um conjunto de técnicas de interpretação de comunicação visando obter, por procedimentos sistemáticos e objetivos de descrição do conteúdo das mensagens, indicadores (quantitativos ou não) que permitam a inferência de conhecimentos relativos às condições de produção/reação destas mensagens".

Desta forma, procedeu-se à divisão categorial a qual teve como objetivo refletir cada um dos temas (Ciberespaço, Ciberterrorismo, Organizações Internacionais, Cibersegurança e Estado de arte em Portugal) os quais funcionaram como o "espelho" das perguntas do guião. Obtiveram-se, respetivamente, as categorias "potencialidades e vulnerabilidades", "evolução da tipologia de ameaças", "proteção e prevenção", "revisão de prioridades" e "nível de desenvolvimento".

Por conseguinte, as subcategorias apresentaram-se como uma combinação das categorias escolhidas com os discursos de cada entrevistado. Neste raciocínio, foi possível observar que muitos dos entrevistados coincidiram no conteúdo das respostas a cada questão

proposta, o que permitiu identificar denominadores comuns nos discursos que contribuíram para a elaboração das subcategorias. Enumeraram-se, então, as seguintes subcategorias – "dependência tecnológica", "rapidez e acesso", "plataforma para o futuro", "sofisticação das ameaças", "11 de setembro no ciberespaço", "melhoria das políticas", "cooperação", "evolução das estruturas organizacionais", "proteção da informação", "educação/formação dos cidadãos", "proteção das infraestruturas físicas", "ordenamento jurídico" e "entidades dedicadas à cibersegurança". Importa mencionar que estas subcategorias foram determinantes para a construção do capítulo "Recomendações" pois permitiram realçar os aspetos mais relevantes para eventuais medidas e políticas futuras.

O tipo de entrevistas escolhido para esta dissertação consiste numa entrevista semiestruturada, que, segundo Pardal e Correia (1995), situa-se num meio termo entre as entrevistas estruturadas e não-estruturadas, ou seja, não é inteiramente livre e aberta, mas também não é totalmente rigorosa e inflexível. Foi elaborado um guião matriz de entrevistas com cinco perguntas previamente estabelecidas, mas foi possível a inclusão de novos dados focados no assunto questionado.

O critério para a seleção da amostra entrevistada baseou-se na vasta experiência e conhecimento que todas as entidades têm na área da cibersegurança e nas áreas conexas a esta. Desta forma, foram entrevistados o Professor Doutor José Tribolet, Professor Catedrático do Instituto Superior Técnico (IST), a Dra. Dalila Araújo, vice-Presidente do Observatório de Segurança, Criminalidade Organizada e Terrorismo (OSCOT), o Dr. João Pacheco, Fundador e CEO da empresa Cyberprotech, o Dr. José Casinha, *Chief Information Security Officer* da empresa OutSystems, o Dr. Bruno Castro, fundador e CEO da empresa VisionWare, o Dr. Francisco Nina Rente, cofundador da empresa Art Resilia e da empresa The Rock - Cybsecurity, o Serviço de Informações de Segurança (SIS) e o Dr. Pedro Mendonça, coordenador do Observatório de Cibersegurança do Centro Nacional de Cibersegurança (CNCS).

1. Ciberterrorismo

1.1. Conceito de Ciberterrorismo

No mundo globalizado em que vivemos, a evolução das Tecnologias de Informação e Comunicação (TIC) converteu o ciberespaço num dos elementos essenciais para a nossa sociedade, pois veio proporcionar uma facilidade nas relações entre os cidadãos e as empresas, e também entre o Estado e os cidadãos através da prestação de serviços à comunidade por parte da administração pública.

Sendo o ciberespaço o "conjunto de redes de computadores nas quais todo o tipo de informação é circulado" (Gibson, 1984), também apresenta as suas vulnerabilidades, pois houve um aumento da sua utilização, mas de maneira maliciosa, que causou incidentes de segurança a muitos Estados. Exemplos disto serão os ciberataques ocorridos na Estónia, em 2007, e na Geórgia, em 2008, que vieram demonstrar como um Estado pode ficar frágil e exposto a riscos no ciberespaço e que terá de "garantir não só a sua utilização segura aos seus cidadãos como também a salvaguarda da própria soberania" (IDN, 2013). Podemos, assim, afirmar que o ciberespaço é um lugar de muitas oportunidades, mas, ao mesmo tempo, de muitos perigos que se têm vindo a intensificar ao longo do tempo.

Na esfera das relações internacionais, a União Europeia considerou o ciberespaço como o quarto elemento operacional, um novo meio que detém a capacidade de mudar o equilíbrio de poder existente. Surge como uma oportunidade para os Estados reduzirem assimetrias entre si e permite que outros atores não-Estatais também se possam mobilizar neste espaço virtual e reforçar o seu poder[3].

Dispor de informação é dispor de poder e aquela assume cada vez mais valor pois as novas tecnologias permitem que circule a uma escala global e de forma instantânea, o que, previsivelmente, suscita interesse da parte dos atores internacionais que pretendem reter informação de forma a geri-la para ganharem vantagem sobre os seus concorrentes ou adversários. Note-se que os Estados "sempre foram ciosos de controlo da informação, pelo que um dos grandes desafios que se lhes apresenta na atualidade prende-se com a

[3] Santos, Lino e Armando Guedes. "Breves reflexões sobre Poder e Ciberespaço". *Revista de Direito e Segurança* nº6, 2015.

aparente incapacidade do exercício de pleno controlo sobre um novo domínio" (Moniz, 2019).

O ciberespaço funciona como veículo de transmissão de ideias e liberdades públicas, e até pode ser utilizado como instrumento da paz universal[4], isto é, pode ser visto como um espaço onde todos os cidadãos podem partilhar os seus argumentos de forma igual, sejam estes de cariz político, movimentos sociais, ou apenas a disseminação de assuntos que geram polémica. Por estas características, o ciberespaço é um meio apelativo para os grupos terroristas pois o acesso à Internet é algo que está disponível para todos.

De acordo com o Instituto de Defesa Nacional (2013)[5], o ciberespaço tem um carácter dinâmico, que está em constante mudança, pois, com passar do tempo, a tecnologia vai progredindo, o que desencadeia a descoberta de novas vulnerabilidades e ameaças que se vão alterando consecutivamente. Outra característica é a alta capacidade para produzir danos físicos, dado que há a possibilidade de atingir uma ampla gama de indústrias e dispositivos na medida em que, atualmente, a tecnologia é o "braço direito" de muitos setores industriais e de empresas, tornando-se, por isso, um alvo.

De enunciar também a transversalidade do ciberespaço, pois uma ação que provenha do domínio cibernético pode afetar outros domínios das sociedades, sejam estas áreas políticas, económicas, sociais e, principalmente, na segurança e defesa dos Estados. As Forças Armadas, por exemplo, dependem cada vez mais da utilização do ciberespaço para conduzir todo o plano das operações, seja para explorar a capacidade dos adversários ou mesmo para uma resposta ofensiva[6].

Ainda que assistamos a ataques terroristas convencionais, o ciberespaço assume um papel cada vez mais relevante para terroristas, na medida em que começou a ser utlizado como uma ferramenta de intimidação. Quando estes grupos querem propagar a sua ideologia através da Internet, a informação flui sem controlo ou impedimento alcançando maiores audiências. No entanto, também pode ser utilizado pelos Estados como forma de sabotagem política, como aconteceu na Geórgia, em 2008, quando o governo georgiano foi atacado por *hackers,* que investigações indiciaram ter sido promovido pelas

[4] Santos, Lino e Armando Guedes. "Breves reflexões sobre Poder e Ciberespaço*"*. *Revista de Direito e Segurança* nº6, 2015.
[5] Instituto Nacional de Defesa (IDN). "Estratégia da Informação e Segurança no Ciberespaço". *Cadernos IDN* nº12, 2013.
[6] Brito, Luís. "A Evolução Tecnológica Militar na Era da Informação". *Revista Militar*, janeiro, 2010.

autoridades da Rússia, causando um prejuízo económico de cerca de mil milhões de dólares[7].

As organizações terroristas usufruem destas vantagens que o ciberespaço proporciona, nomeadamente para recrutamento e para disseminação da informação. Não existindo barreiras, não há maneira de travar o que é dito ou escrito, e, principalmente, em regimes democraticamente abertos, "onde a liberdade de expressão é pilar, assistimos a estratégias camufladas que têm como objetivo perturbar a segurança nacional" (Moniz, 2019).

Falamos de algo que já não se materializa, que não é visível. Neste momento é tudo executado *online*, desde o planeamento até à execução do plano. Em regimes democráticos, a informação na Internet está livremente disponível a qualquer momento, não há um limite nem censura que separe conteúdos; já em regimes autoritários, "há a colocação de filtros que impedem certas pesquisas e o acesso e partilha de temas considerados contrarrevolucionários" (Santos e Guedes, 2015). O ataque de 11 de setembro de 2001, com todos os cenários retratados pelas imagens publicadas, constitui um perfeito exemplo do que o terrorismo representa: destruição, medo e mortes; estas mesmas imagens foram bastante poderosas e mais eficazes para os terroristas, na medida em que instigam o medo e o caos. Assiste-se à utilização do ciberespaço para potenciar as ações terroristas e os Estados criaram a consciência que "a ciberguerra, ou a possibilidade de ciberataques, representa uma ameaça sem igual, e, particularmente, uma ameaça que ainda não é possível travar" (Sanger, 2018).

Tendo em conta que o terrorismo e a sua extensão tecnológica, o ciberterrorismo, assumem uma crescente importância nas sociedades contemporâneas pela sua maior dependência no ciberespaço, importa definir estes conceitos. No entanto, essa é uma tarefa complexa, uma vez que as definições disponibilizadas diferem de especialistas para especialistas, não havendo assim uma definição consensual, o que prejudica, por exemplo, a definição sobre o que realmente é um ataque ciberterrorista e a consequente resposta ao nível da prevenção e proteção por parte das autoridades, sejam elas políticas, de segurança, ou outras.

[7] Kakachia, Kornely. "A Guerra dos Cinco Dias". *Relações Internacionais,* 2008.

Nesta linha de pensamento, será de mencionar que uma eventual confusão concetual sobre ciberterrorismo num setor tão importante como os *media* pode contribuir para a desinformação, ou seja, se os órgãos de comunicação social não tiverem acesso a informação especializada clara sobre ciberterrorismo poderão veicular informação errónea.

Por outro lado, desempenham um papel fundamental na "disseminação e amplificação da audiência dos atentados terroristas" (Novais, 2012). Trata-se de uma mediação do terrorismo, onde vemos que esta vertente tecnológica se tornou como uma arma para os terroristas, que "beneficiam da credibilidade e do impacto nos consumidores de notícias dos media e tentam manipular no sentido de difundirem mensagens que lhes permite alcançar audiências maiores do que aquelas afetadas pelo atentado terrorista" (Novais, 2012).

De acordo com Dorothy Denning (2000) ciberterrorismo é:

> "a associação do ciberespaço e do terrorismo. Trata-se de ataques ou da ameaça de ataques ilegais a computadores, redes e às informações armazenadas no sistema em que estes atuam, quando feito para intimidar ou coagir um governo ou o seu povo em prol de objetivos políticos ou sociais. Além disso, para se qualificar como ciberterrorismo, um ataque deve resultar na violência contra pessoa ou bens, ou pelo menos causar sérios danos para gerar medo. Os ataques que levam à morte ou lesão corporal, explosões, ou perdas económicas graves seriam exemplos. Já os ataques que interrompem os serviços não essenciais ou os que são geralmente considerados apenas incómodos não seriam ataques ciberterroristas[8]".

No que diz respeito às OI, o Centro de Excelência NATO para a Ciberdefesa Cooperativa (CCDCOE) define ciberterrorismo como o "uso politicamente motivado de computadores e tecnologias de informação para causar perturbações severas ou medo generalizado na sociedade". A Agência da União Europeia para a Formação Policial (CEPOL), definiu, em 2018, ciberterrorismo como o:

> "uso de computadores ou tecnologias relacionadas com a intenção de causar danos, com o objetivo de coagir a população civil e influenciar a política do

[8] Weimann, Gabriel. "Cyberterrorism. How Real is the Threat?". *United States Institute of Peace*. Washington, 2004.

> governo alvo ou afetar a sua conduta. Além disso, o ciberterrorismo, que deve ser diferenciado de *hacking* e da ciberguerra, tem como alvo as Infraestruturas Críticas. Existem ligações, bem como discrepâncias entre o ciberterrorismo e o terrorismo em geral, que, inevitavelmente, afetam resposta ao contra- terrorismo em ambos os casos."

Ao nível nacional, o Centro Nacional de Cibersegurança (CNCS) adotou a definição disponibilizada pela Agência da União Europeia para a Cibersegurança (ENISA) que explica que "existe cada vez mais uma convergência entre terrorismo e ciberespaço. Ao mesmo tempo que têm como motivação a realização de ciberataques, os ciberterroristas têm como objetivos o recrutamento e a monetarização. Não obstante este uso instrumental do ciberespaço, o principal objetivo deste agente de ameaças, em última análise, é a realização de ciberataques por razões típicas de grupos terroristas."

De forma geral, todos concordam em que o principal objetivo destes atos terroristas é infligir danos que comprometam ou mesmo destruam alvos para causar grandes impactos físicos e psicológicos e que o seu combate deve ser cada vez mais urgente. Nesta sequência, importa percebermos como é que os atores descritos se enquadram e exercem o seu poder no ciberespaço.

1.2. Atores e campos de ação

Segundo Joseph Nye, "a difusão do poder no domínio cibernético é representada pelo grande número de atores e pela redução relativa dos diferenciais de poder entre eles"[9]. Para entendermos as dinâmicas que ocorrem no ciberespaço, convém entendermos quem está por detrás delas, ou seja, quem são os atores. Nye defende três tipos de agentes do ciberespaço: Estados, organizações com redes estruturadas e indivíduos com redes pouco estruturadas.

Em relação aos Estados e os seus respetivos governos, estes desempenham um papel determinante no ciberespaço pois são os responsáveis pela sua legislação, dado que este domínio necessita de quadros legais próprios de forma a evitar a sua utilizado de maneira

[9] Nye, Joseph. "Cyber Power". *Cambridge: Belfer Center for Science and International Affairs*, Harvard Kennedy School, 2010.

coerciva[10]. Para exemplos concretos, Nye relembra-nos o episódio dos protestos em Xinjiang, China, no ano de 2009, em que várias pessoas da etnia uigur, uma etnia minoritária dos povos turcos reconhecida pela China, se manifestaram para demonstrar o seu descontentamento perante a falta de ação do governo chinês na morte de trabalhadores desta etnia na província de Guandong. Para retaliar, o governo chinês decidiu privar 19 milhões de residentes de acederem a mensagens de texto e a chamadas internacionais (Nye, 2010: pág 8).

No compartimento das organizações com redes estruturadas, encontramos as duas faces da moeda: engloba-se as grandes empresas multinacionais como a Microsoft e a Google, como também estão incluídas as organizações criminosas com grande poder tecnológico e financeiro que conseguem o recrutamento e o financiamento suficiente para se expandirem e, por conseguinte, alcançam mais audiências e resultados. A título de exemplo, a Al-Qaeda, usufruindo das novas ferramentas tecnológicas, abandonou a sua estrutura hierárquica e restrita geograficamente, e passou a ser um forte rede global e com grande capacidade de influência[11] , dado que lhe foi permitida a capacidade de explorar vulnerabilidades e de propaganda com o uso da Internet.

Por fim, Nye refere os indivíduos sem redes estruturadas que são fruto de um dos fatores intrínsecos ao ciberespaço – a possibilidade de entrada sem qualquer barreira. Há uma extrema facilidade, que se revela perigosa, na maneira como todos os indivíduos podem interagir na rede global sem que haja uma distinção entre os criminosos e os outros agentes mencionados. Assistimos à utilização do ciberespaço com fins maliciosos, ligados a cibercrimes com o objetivo de lucrar economicamente através de várias tipologias de ataques, desde *phishing* a *randsomware*.

A tabela 1, inserida abaixo, demonstra os diferentes agentes e o seu exercício de poder no ciberespaço que sintetiza as ideias elaboradas neste subcapítulo.

[10] Moniz, Paulo. "Terrorismo e Violência política: como combater o Ciberterrorismo e a Radicalização." *IDN – Nação e Defesa*, Caderno nº152. Lisboa, 2019.
[11] Ibid, pág. 65.

Table 3: Relative Power Resources of Actors in the Cyber Domain

A. Governments

1. Development and support of infrastructure, education, intellectual property.
2. Legal and physical coercion of individuals and intermediaries located within borders.
3. Size of market and control of access; eg. EU, China, US
4. Resources for cyber attack and defense: bureaucracy, budgets, intelligence agencies
5. Provision of public goods; eg. regulations necessary for commerce
6. Reputation for legitimacy, benignity, competence that produce soft power

Key Vulnerabilities: High dependence on easily disrupted complex systems, political stability, reputational losses

B. Organizations and highly structured networks

1. Large budgets and human resources; economies of scale
2. Transnational flexibility
3. Control of code and product development, generativity of applications
4. Brands and reputation

Key Vulnerabilities: Legal, intellectual property theft, systems disruption, reputation loss (name and shame)

C. Individuals and lightly structured networks

1. Low cost of investment for entry
2. Virtual anonymity and ease of exit
3. Asymmetrical vulnerability compared to governments and large organizations

Key Vulnerabilities: Legal and illegal coercion by governments and organizations if caught

Figura 1 – Recursos de Poder dos Atores no Ciberespaço[12]

Segundo o relatório "Cibersegurança em Portugal – Riscos e Conflitos"[13] elaborado pelo CNCS no ano de 2020, é possível identificarmos três agentes geradores de ameaças no contexto português, sendo estes os cibercriminosos, agentes estatais e os *hacktivistas*. No que concerne aos cibercriminosos, são grupos ou mesmo indivíduos que têm como foco a extorsão, a atividade fraudulenta e, muitas vezes, o propósito de obter informação privilegiada, procurando misturar-se com atores estatais de forma a não serem detetados.

Os atores estatais também representam um peso importante, consistindo a sua ação na contratação de grupos cibercriminosos ou conferindo-lhes patrocínios de modo a obterem as informações que pretendem. Trata-se de práticas de ciberespionagem, cujo objetivo consiste na extração de informação, seja de teor político ou para comprometer o sistema de segurança do alvo. Os *hacktivistas* têm como objetivo destabilizar os sistemas através

[12] Fonte da tabela 1: Nye, Joseph. "Cyber Power". *Cambridge: Belfer Center for Science and International Affairs*, Harvard Kennedy School, 2010.

[13] "Relatório Riscos & Conflitos 2020", *Centro Nacional de Cibersegurança*, junho 2020. Disponível em: https://www.cncs.gov.pt/docs/relatorio-riscos-conflitos-2020.pdf

de sabotagens e causar danos significativos que se repercutem na reputação das organizações ou indivíduos. Focam-se nas vulnerabilidades e expõem-nas de forma a promover a sua mensagem de ativismo sociopolítico.

No geral, todas estas atividades cibercriminosas têm motivações político-ideológicas, pois maioritariamente destinam-se a fragilizar e a atacar a soberania governamental do Estado-alvo. As principais vítimas destes ataques são os organismos do Estado, ou empresas que detenham algum tipo de controlo ou poder comercial e/ou industrial e, por essa razão, são escolhidas. Empresas de telecomunicações podem tornar-se vítimas, como pudemos observar em 2022 nos ataques ao Grupo Impresa e à Vodafone, cujos respetivos serviços foram interrompidos com o objetivo de restringir o tecido de comunicações em Portugal. Em janeiro, o Grupo Impresa foi alvo de um ciberataque que foi reivindicado pelo *Laspsus$ Group*. O site do jornal Expresso, do canal de televisão SIC e SIC Notícias ficaram em baixo e vários subscritores do jornal Expresso receberam um e-mail com informações falsas de que os seus respetivos dados estavam comprometidos[12].

No caso da Vodafone, o ataque começou na noite de 7 de fevereiro por volta das 22h00 com a disrupção das comunicações de dados, SMS e de voz na rede fixa, tendo-se prologado até ao dia seguinte, o que impactou uma percentagem significativa de clientes desta rede[13].

Estes acontecimentos vieram mostrar como é necessário continuar com o investimento na cibersegurança, sendo que Portugal já se posiciona, desde 2020, no top 20 do Ranking do Índice Global de Cibersegurança, como podemos observar na figura abaixo.

[12] "Ataque Impresa: como um sistema vulnerável destrói parte da memória cultural de um país" *It Security*, fevereiro 2022. Disponível em: https://www.itsecurity.pt/news/x-ray/ataque-impresa-como-um-sistemavulneravel-destroi-parte-da-memoria-cultural-de-um-pais

[13] "Vodafone Portugal diz que foi alvo de ato terrorista" *IT Security*, fevereiro 2022. Disponível em: https://www.itsecurity.pt/news/news/vodafone-portugal-foi-alvo-de-ciberataque

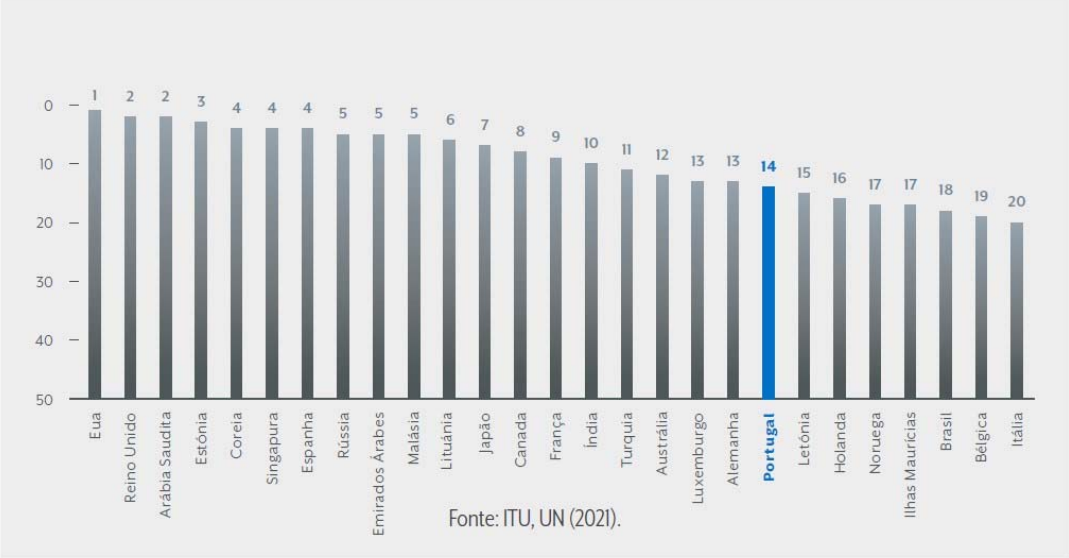

Figura 2 – Ranking do Índice Global de Cibersegurança[14]

1.3. Tipos de ciberataques e estratégias de combate

O mundo tem vindo a enfrentar ameaças cibernéticas cada vez mais potentes que se revelam cada vez mais perigosas, tornando a ideia de uma guerra virtual cada vez mais plausível. Os terroristas, atualmente, não necessitam de bombas ou armas de fogo para causar danos, pois através de um computador conseguem paralisar estruturas militares, políticas e económicas de um país ou mesmo de um continente inteiro.

No último relatório elaborado pela ENISA denominado "*Threat Landscape Overview (ETL)*"[15], podemos observar que durante os anos 2020 e 2021 os ataques à cibersegurança aumentaram não só em número, mas também nos respetivos impactos, tendo sido relatados entre abril de 2020 e julho de 2021, 198 incidentes no setor da administração pública/governo, 152 incidentes relativos a prestadores de serviços digitais, 151 no público em geral, 143 no setor da saúde e 97 no setor financeiro/bancário, como podemos observar na Figura 3.

[14] "Relatório Cibersegurança em Portugal – Economia" *Centro Nacional de Cibersegurança*, maio 2022. Disponível em: https://www.cncs.gov.pt/docs/relatorio-economia2022-obciber-cncs.pdf

[15] "ENISA Threat Landscape 2021" *ENISA*, outubro 2021. Disponível em: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021.

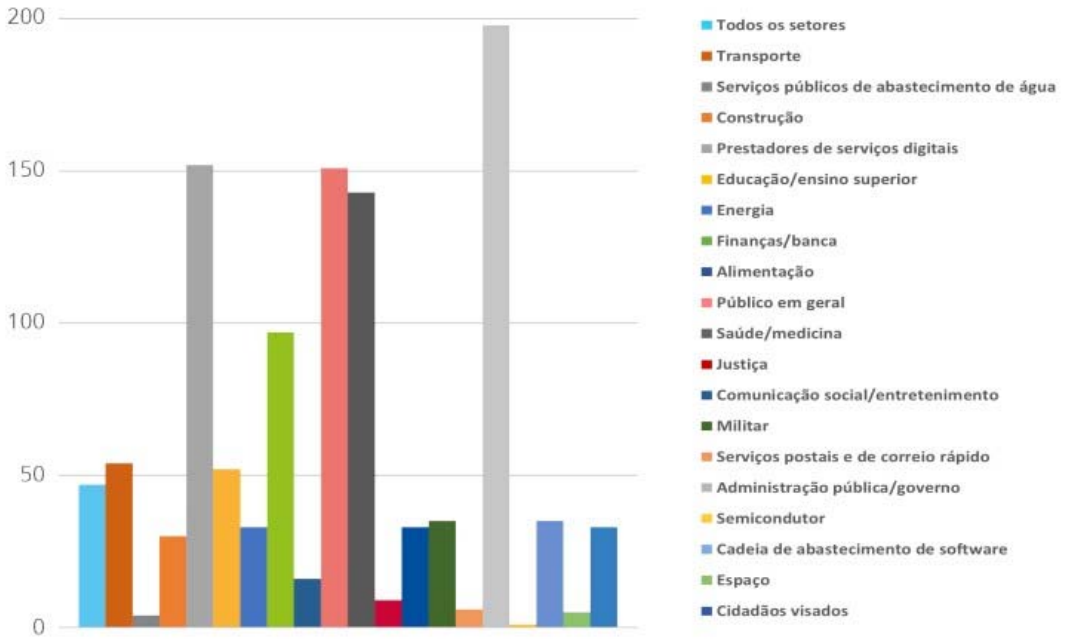

Figura 3 – Setores-alvo por número de incidentes cibernéticos no período 2020-2021[16]

O período pandémico serviu como catalisador de ataques cibernéticos, com uma adaptação ao "novo normal", abrindo assim caminho para a exploração das vulnerabilidades das organizações e empresas que já haviam investido na transição digital e se tornaram mais expostas a estes ataques. Uma nova tendência notada pela ENISA traduziu-se na ciberespionagem nos setores farmacêuticos e de pesquisa médica, onde os criminosos eram encarregues de encontrar informações relacionadas com a recuperação e desenvolvimento das vacinas.

A *Mandiant Threat Intelligence* rastreou várias atividades de ciberespionagem relacionadas com a pesquisa e a reposta à COVID-19 em grupos vietnamitas, chineses, norte-coreanos, iranianos e russos. Os grupos[17] que praticaram esta ciberespionagem estão ativos há anos e outrora foram bem-sucedidos nos seus objetivos – como exemplo, foi notada atividade do grupo chinês "APT41" em janeiro de 2020 afetando empresas farmacêuticas, como também pouco tempo depois o grupo vietnamita "APT32" conduziu

[16] "Relatório ENISA sobre o cenário das ameaças de 2021" *ENISA*, outubro 2021. Disponível em: https://www.enisa.europa.eu/publications/etl-2021/enisa-threat-landscape-2021-2022-final_pt.pdf/view

[17] Denomina-se *Advanced Persistent Threats* (APTs) aos diferentes grupos de cibercriminosos espalhados pelo mundo que utilizam técnicas de invasão contínuas, clandestinas e sofisticadas para obter acesso a um sistema e permanecer nesta durante um longo período de tempo.
What Is an Advanced Persistent Threat (APT)?" *Kaspersky*. Disponível em: https://www.kaspersky.com/resource-center/definitions/advanced-persistent-threats

uma campanha direcionada a entidades públicas e privadas chinesas de forma a tentar obter informações sobre a gestão e monitorização do surto pandémico[18].

Numa outra nota, os cibercriminosos aproveitaram esta janela de oportunidade pandémica para explorar o interesse, a preocupação e a curiosidade das pessoas atraindo-as através de técnicas de *phishing*[19] para obter ganhos financeiros. Desta forma, observou-se a criação de *fake news* sobre o vírus através de anúncios e websites relacionados com as possíveis curas e outras medidas de prevenção sendo o objetivo destes esquemas convencer a população a comprar medicamentos falsos que prometiam ser a solução.

Para além destas práticas maliciosas, e com base na análise proporcionada por esta agência, identificamos alguns tipos de ataques cibernéticos que merecem destaque devido à sua crescente ocorrência, e ao seu impacto. O *ransomware* é uma das ameaças mais populares no seio da cibersegurança, através da qual os cibercriminosos encriptam os dados de uma organização e exigem um pagamento em troca da devolução daqueles dados. Um dos ataques mais conhecidos deste tipo ocorreu em maio de 2017 apelidado de *"Wanna Cry"*. Este ataque foi possível devido a uma falha de segurança do sistema Windows que foi publicamente exposta numa fuga de dados pela Agência Nacional de Segurança dos EUA (NSA) orquestrada pelo grupo de *hackers* denominado *Shadow Brokers*. Este ataque de *ransomware* atingiu cerca de 230 mil computadores em todo o mundo, com especial foco no Serviço Nacional de Saúde do Reino Unido (NHS) onde muitos hospitais foram obrigados a encerrar os seus sistemas informáticos, causando uma interrupção no atendimento dos pacientes e na realização de algumas cirurgias[20].

Outra prática maliciosa mencionada neste relatório é o *malware*, destinado a executar um processo não autorizado que irá impactar na confidencialidade, integridade ou na disponibilidade de um sistema, sendo qualquer um destes o objetivo primário dos atacantes. A título de exemplo, no ano de 2010, um tipo de *malware* denominado *Stuxnet* foi descoberto nas centrais nucleares iranianas e causou a interrupção contínua de urânio

[18] "M-Trends 2021" *Fireeye Mandiant Services*, 2021. Disponível em: https://content.fireeye.com/mtrends/rpt-m-trends-2021

[19] A ENISA define *phishing* como um "meio de persuadir as vítimas a divulgar informações confidenciais como dados bancários e de cartões de crédito. O ataque geralmente assume a forma de e-mail de SPAM, sites maliciosos, parecendo ser de uma forma legítima como um banco ou uma rede social". Disponível em: https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/phishing-spear-phishing

[20] "O que é o WannaCry?" *Avast Academy*, fevereiro 2020. Disponível em: https://www.avast.com/pt-br/cwannacry

no programa nuclear do Irão, que estava sob monitorização das OI desde o início do milénio.

Podemos identificar também outro tipo de ataques que comprometem estas mesmas vertentes de um sistema, os *Distributed Denial-of-Service* (DDoS) que constituem umas das ameaças mais letais para a Informação Tecnológica (IT). Neste caso, observa-se o esgotamento dos recursos causando diminuições no desempenho, perda de dados e interrupções dos serviços. Exemplo deste tipo de ataque ocorreu em 2007, na Estónia e em 2008 na Geórgia, tendo-se verificado ataques a infraestruturas críticas como bancos nacionais, *websites* governamentais e serviços de comunicação. Os ataques deixaram marcas avassaladoras nestes dois países e foram desencadearam o reforço das medidas de cibersegurança.

Neste ETL, a NSA inclui na vertente das ameaças, pela primeira vez, as campanhas de desinformação que circulam na Internet e são impulsionadas pelo aumento do uso das plataformas sociais e órgãos de comunicação social *online*, bem como pelo aumento da presença de cidadãos e empresas *online* durante a pandemia COVID-19. É através desta corrente tecnológica que os grupos terroristas conseguem alcançar mais audiência e influenciar a esfera psicológica das pessoas.

A Al-Qaeda é um grupo terrorista que combina a propaganda no ciberespaço com as tecnologias avançadas de comunicação para "criar uma forma muito sofisticada de guerra psicológica" (Weimann, 2004). A Internet expandiu significativamente as oportunidades para os terroristas garantirem a publicidade das suas ideologias e objetivos, permitindo-lhes ter o controlo direto sobre o conteúdo das mensagens que querem transmitir, e, desta maneira, conseguirem manipular a sua imagem e a dos seus inimigos.

Abordam-se, de seguida, as estratégias de combate ao ciberterrorismo apoiadas por Irving Lachow (2009), que as definiu em três tipos – no plano físico, informacional e cognitivo.

No plano físico, a estratégia concretiza-se através da danificação das infraestruturas utilizadas pelos extremistas, como os canais de Internet e as comunicações. O objetivo é negar ou interromper estes serviços de maneira a tentar eliminar a presença terrorista *online*. Todavia, esta estratégia revela-se perigosa, pois pode atingir infraestruturas que também são utilizadas pela maior parte dos Estados, que albergam milhares de dados. Assim, torna-se necessária uma análise precisa e minuciosa na definição do alvo, o que, por si, é uma tarefa difícil.

Uma alternativa mais eficaz e controlada seria, por exemplo, solicitar aos operadores de serviços, aquando da identificação dos criminosos, para desativar os serviços que estão a ser utilizados maliciosamente. Contudo, isto pode tornar-se confuso pois a maior parte dos terroristas ativos no ciberespaço usufruem de uma camuflagem que lhes permite não serem notados. Pode-se considerar ainda uma outra alternativa, como a vigilância destas infraestruturas sem que haja a disrupção física dos serviços, mas isto implica uma possível violação dos direitos inerentes de uma sociedade democrática, uma vez que, quanto mais controlo houver, menos confiança haverá nos governantes. Desta maneira, esta estratégia não pode ser tomada como eficaz no longo prazo, pois como a maior parte destas infraestruturas se situa no continente americano e no continente europeu, ao tentar-se afetar estas infraestruturas poderiam ser também lesados outros serviços, correndo assim o risco de ser considerado um ato de guerra.

Outro tipo estratégia é o informacional. As ações neste nível são concentradas nos armazéns virtuais de segurança da informação, mais concretamente na sua confidencialidade, integridade e disponibilidade. Os principais atores neste plano são as agências governamentais pois são estas que vão que monitorizar a atividade dos grupos terroristas *online* e vão poder decifrar o conteúdo das mensagens de modo a prevenir ataques. Entende-se que esta estratégia é mais fácil de ser levada a cabo, dado que não inclui quaisquer interrupções de serviços ou danos colaterais. No entanto, todas as ações de controlo acarretam a sua dificuldade, pois estamos num domínio (ciberespaço) onde há uma facilidade no contorno de medidas de segurança, podendo assim, os terroristas mudar a sua localização e arranjar outras cifras de mensagens que podem ser impossíveis de perceber.

Por fim, o tipo cognitivo. Entende-se como o plano mais sofisticado uma vez que as estratégias têm que atuar na esfera da perceção dos cidadãos, isto é, têm que ter influencia na tomada de decisões. A título de exemplo, as campanhas de "contrapropaganda" são uma forma de reduzir a atração às organizações terroristas, de modo a evitar que mais pessoas sejam recrutadas. Para esta estratégia ser bem-sucedida é necessária uma articulação entre os governantes e os órgãos de comunicação social para que se mantenha o equilíbrio entre a liberdade de imprensa e a importância do tratamento da informação, evitando assim a transmissão de *fake news*.

É sabido que, para alcançar isto com máxima eficácia, os Estados têm de reforçar a educação, essencialmente na parte da promoção dos valores que devem reger uma sociedade, mas também o desenvolvimento da autonomia dos cidadãos para que estes sejam capazes de classificar, por si próprios, a qualidade da informação disponível. A abundância da contrainformação que circula no ciberespaço exige a criação de medidas estruturais que controlem esta dinâmica, porém as ameaças são cada vez mais emergentes e atuais, o que não deixa muito tempo para as políticas surtirem efeito.

2. O Ciberterrorismo como tática de guerra

2.1. A guerra no séc. XXI

No sentido mais tradicional, a guerra caracteriza-se pela competição e pela hostilidade que é mantida pelas partes envolvendo o uso da violência em larga escala em função de um objetivo entendido como incompatível[20]. Focando-nos na transição do século XX para o século XXI, identificamos quatro tipos de guerras que marcam as relações internacionais contemporâneas, a saber, as guerras clássicas, a Guerra Fria, as "novas guerras" e a guerra global contra o terror[21].

As primeiras, as guerras clássicas, foram teorizadas por Carl von Clausewitz no século XIX que as caracterizou como o combate entre os Estados com o objetivo de, usando a força física, compelir o adversário à sua vontade, derrubando-o e tornando-o incapaz de retaliar com um novo ataque[22]. As Guerras Napoleónicas entram nesta categoria, pois Napoleão Bonaparte lutou até aos seus inimigos sucumbirem à sua vontade.

Esta forma de violência registou-se com menor frequência no pós-II Guerra Mundial no período designado de Guerra Fria, entre 1947–1991, que opôs as duas mais poderosas potências mundiais na altura: os Estados Unidos da América (EUA) e a União Soviética (URSS), detentoras de armamento nuclear, um novo elemento no contexto bélico. Entende-se que esta arma de destruição total teve o poder de mudar o paradigma dos conflitos tradicionais, dado que o confronto num campo de batalha resultaria na destruição total mútua. Para evitar um tal confronto, mas na disputa de poder e de influência

[20] Cravo, Teresa Almeida. "Mudanças e continuidades na conceptualização da guerra". *Janus*, 2014.
[21] Ibid, pág. 82.
[22] Clausewitz, Carl Von. "Da Guerra". *Edições Europa/América*. Lisboa, 1997.

internacional, os EUA e a URSS envolveram-se em guerras periféricas, fora dos seus territórios, num cenário em que ambos aproveitavam qualquer oportunidade para aumentar o seu domínio no mundo.

É neste contexto que, em 1949, foi criada a NATO com o fim de unir militarmente os países do Ocidente sob a direção dos EUA, constituindo um sistema de defesa coletiva através do qual os seus Estados-Membros concordam com a defesa mútua em caso de um ataque externo a um dos membros dessa aliança. Em resposta à criação da NATO, a URSS estabeleceu o Pacto de Varsóvia, assinado em 1955, consistindo numa aliança militar entre os países socialistas do leste europeu.

Mary Kaldor designou os conflitos do pós-Guerra Fria de "novas guerras". Nos anos 90, assistiu-se a um aumento de guerras civis e a um declínio de confrontos armados entre os Estados. As guerras civis, segundo a autora, são completamente opostas ao paradigma clássico das guerras inter-Estados, pois ocorrem dentro das fronteiras de um Estado e constituem uma ameaça à segurança interna. Kaldor distingue estas "novas guerras" das anteriores indicando que as diferenças entre a guerra, o crime organizado e a violação em massa dos direitos humanos deixaram de ser tão precisas[23]. Nesta conceptualização de guerra, desaparece a visão do campo de batalha, os alvos passam a ser civis e as táticas não são as convencionais (confronto entre exércitos/forças armadas dos Estados), mas sim atividades ilícitas, como por exemplo, ações terroristas.

Outro ponto que difere entre os "novos" e os "velhos" conflitos reside nos objetivos. Anteriormente, a motivação consistia sobretudo na conquista territorial, por razões ideológicas ou pela autodeterminação; atualmente, há uma panóplia de motivos para a deflagração dos conflitos, como razões éticas, religiosas, raciais e económicas. Kaldor argumenta que "as velhas guerras foram travadas por interesses geopolíticos ou ideológicos (democracia ou socialismo) e as novas guerras são travadas em nome da identidade (ética, religiosa ou tribal)"[24].

A última conceptualização da guerra surge com os ataques terroristas nos EUA em setembro de 2001 e a denominada guerra global contra o terror. Neste contexto, as

[23] Kaldor, Mary. "New and Old Wars – organized violence in a global era". *Stanford University Press*, 3º Edição, 2012.
[24] Pereira, João Paulo. "Os Conflitos do Pós-Guerra Fria, Novas ou Velhas Guerras?" *Revista Militar* nº2630, 2021.

ameaças não se baseiam num sistema bipolar (da Guerra Fria), nem se trata de ações confinadas a um país; trata-se de guerras com um alcance geográfico abrangente, não delimitado, consequência da globalização[25].

Estes ataques vieram evidenciar como os tempos mudaram no que respeita a uma "declaração de guerra". Anteriormente, assistíamos a confrontos militares entre forças armadas adversárias e quem detivesse a supremacia militar seria a vencedora. Na nova guerra, ainda que o país atacado possa ser uma potência militar poderosa, como é o caso dos EUA, existem novos instrumentos e táticas que não procuram uma vitória decisiva naquele momento, mas provocam danos de uma enorme magnitude, não só materiais como também imateriais, incutindo o medo e transtornos psicológicos à sociedade, levando-a a viver aterrorizada, e provocando a perda de vidas em nome de um objetivo político.

Tornou-se muito mais difícil a identificação de uma ameaça, mencionada antes por Clausewitz como a "névoa da guerra". As organizações terroristas não expõem as suas forças ao mundo, na sua maioria não se constituem como exércitos regulares, por isso, não se sabe bem qual é a sua composição. Esta é a questão mais complexa do terrorismo, não existe um "rosto", o inimigo é desconhecido, o que resulta numa fraca identificação entre quem é o agressor e quem não o é, tornando todo o mundo num cenário de batalha.

O terrorismo moderno não poderá ser considerado como uma forma de guerra, mas sim como uma tática de guerra, sendo uma tática "a ciência/arte de utilizar, da melhor forma, os meios militares do ambiente operacional e das facilidades proporcionadas pela técnica e tendo em vista reduzir o adversário pelo combate ou pela ameaça do combate" (Cabral Couto, 1982). Apresenta-se como um fenómeno de violência política, que utiliza métodos violentos para afirmar o seu posicionamento através do ataque contra o Estado, visando frequentemente a sociedade.

Ao longo do tempo, da mesma maneira que a guerra foi evoluindo, também o terrorismo foi registando mutações. Durante este milénio, o ciberterrorismo tem-se apresentado como uma das táticas mais usadas e eficazes. É uma crescente ameaça que se revela como uma grande vantagem para um Estado que detenha um grande poder tecnológico. Se o terrorismo tradicional já não tinha qualquer tipo de fronteiras, então o ciberterrorismo

[25] Kaldor, Mary. "New and Old Wars – organized violence in a global era". *Stanford University Press*, 3º Edição, 2012.

consegue ser ainda mais perigoso pelo facto de ser silencioso e invisível nas suas estratégias e efeitos. Nos tempos de Clausewitz, ambas as partes envolvidas tinham os meios para usar a força, no caso do ciberterrorismo não se verifica isso pois há uma dificuldade acrescida para retaliar quando a deteção do ataque pode ser tardia e a identificação do atacante pode ser difícil ou impossível.

Conclui-se, assim, que o ciberterrorismo é uma tática de guerra do séc. XXI e serão dados exemplos desta nova realidade com os ciberataques apresentados e analisados nos subcapítulos seguintes, nomeadamente, os que se verificaram na Estónia, na Geórgia e no Irão.

2.2. Ciberataques como tática de guerra

2.2.1. Estónia, 2007

No ano de 2007, o conceito de ciberguerra tomou uma posição mais visível quando foram realizados os ciberataques contra diversas infraestruturas críticas e *soft targets* da Estónia. O ciberterrorismo e a cibersegurança deixaram o plano abstrato e transitaram para o domínio concreto da defesa daquele país e de muitos outros Estados, bem como das OI que passaram a olhar para o ciberespaço como um novo campo de batalha que não estavam preparados para defender.

A Estónia, com uma população de 1,3 milhões de habitantes, está entre as sociedades digitalmente mais avançadas desde que se tornou num estado independente da União Soviética, em 1991. Conforme a organização *Freedom House,* este país europeu é dos países com as democracias mais abertas e liberais, conferindo assim liberdade económica, de expressão, de imprensa e na Internet. Os avanços tecnológicos foram cruciais na reconstrução da Estónia após a restauração da sua independência.

Em 1996, foi lançado o Programa *Tiger Leap* que tinha como objetivo modernizar o sistema educacional estoniano, usando assim a tecnologia em proveito do desenvolvimento social. Este programa tinha como pilares desenvolver os computadores e a Internet, a formação básica de professores e proporcionar material didático eletrónico na língua nativa para as instituições de ensino[26]. Para alcançar estes mesmos objetivos,

[26] "Estonia is a digital society" *Visit Estonia*, setembro 2020. Disponível em: https://www.visitestonia.com/en/why-estonia/estonia-is-a-digital-society

foi criada a Fundação *Tiger Leap* em 1997, uma fundação de investimentos tecnológicos apoiada pelo governo estoniano que permitiu o fornecimento de computadores e acesso à Internet em todas as escolas o que originou que estas mesmas expandissem os sistemas informáticos no final da década.

Em 2001, criou-se uma plataforma de integração nacional, a *X-Road,* que combinava os setores públicos e privados de forma a operarem harmoniosamente e que atualmente é a espinha dorsal da e-Estónia[27]. Vive-se numa sociedade altamente digitalizada, onde qualquer tarefa burocrática pode ser executada *online*. Isto também contém os seus riscos, pois "quanto mais tecnologicamente desenvolvido um país é, mais vulnerável se torna a um ciberataque contra as suas infraestruturas críticas" (Weimann, 2004).

Durante vários anos, a Estónia desenvolveu serviços como o e-*Tax Board,* onde os estonianos podem declarar os seus impostos *online* muito mais rapidamente, o i-*voting* que permite maximizar a acessibilidade às eleições locais e gerais, de modo a poderem votar num computador, o e-*Health* que permitiu melhorar a qualidade e a eficiência dos cuidados de saúde ao registarem, eletronicamente, os dados de um paciente de forma a reduzir a burocracia envolvida e dando acesso a informações imediatamente no caso de emergências[28]. Como resultado, este país adotou o termo e-Estónia que se referia ao movimento que tinha como finalidade facilitar a interação governo-população através de mecanismos tecnológicos[29].

No relatório da NATO *Strategic Communications Centre of Excelence* (NATO StratCom)[30] elaborado sobre o ataque de 2007 contra a Estónia, descreve-se o que motivou estes ciberataques em larga escala. O memorial "*The Bronze Soldier*", erguido em Tallinn no ano de 1982, tornou-se um ponto de conflito após 1991 entre estonianos nacionalistas e estonianos pró-Kremlin. Para os primeiros, simbolizava a opressão a que foram submetidos pela União Soviética, para os segundos, representava a coragem dos soldados do Exército Vermelho. Por decisão do governo, a estátua foi removida do centro de Tallinn em 2007, o que provocou grandes tumultos e protestos do lado russo. No

---

[27] "This is the story of the world's most advanced digital society" *e-Estonia*. Disponível em: https://eestonia.com/story/

[28] Ibid.

[29] "How it all began? From Tiger Leap to digital society! *Education Estonia*. Disponível em: https://www.educationestonia.org/tiger-leap/

[30] "2007 cyber-attacks on Estonia" *NATO StratCom*, junho 2019.
Disponível em: https://stratcomcoe.org/cuploads/pfiles/cyber_attacks_estonia.pdf

mesmo dia em que a estátua foi removida, os ciberataques começaram a dar os seus primeiros sinais.

Tratou-se de ataques DDoS conjugados com um programa malicioso que permite o controlo dos sistemas informáticos infetados (*Bonets*) o que faz com que o seu efeito seja mais destrutivo. Os setores públicos e privados estonianos foram altamente afetados. Páginas eletrónicas governamentais, de bancos e de meios de comunicação social tiveram de ser encerrados temporariamente, o que resultou num apagão nacional sem qualquer acesso a uma estrutura informática. A Internet é um elemento-chave das infraestruturas críticas nacionais de um Estado e a interrupção na disponibilidade de qualquer serviço que dela dependa, terá consequências rápidas, profundas e, por vezes, irreversíveis.

Ainda no relatório da StratCom, podemos observar uma intensa análise sobre a estratégia lógica destes ataques, isto é, por muito disruptivos que sejam os ataques DDoS, havia um risco previsível de acontecerem, pois, apesar de este país ter a tecnologia como a sua pedra angular, esta mesma condição torna a Estónia num alvo mais vulnerável. Rain Ottis, analista de ciberoperações, defende que este ataque foi coordenado com hostilidade pela parte da Rússia, pois coincidiu com a mudança programada do monumento em Tallinn[31].

Entende-se que o objetivo principal era responder à realocação do memorial "*The Bronze Soldier*", de maneira a impactar negativamente a segurança nacional da Estónia. Tratouse de um exercício de poder para testar as ciberarmas, levando Sanger (2018) a concluir que "tal como as armas nucleares, estas são um grande equalizador" (pág.34). A capacidade de "desligar" o acesso de uma nação soberana à Internet é uma maneira do atacante demonstrar como o próprio governo estoniano e as OI em que o país se insere que não têm os meios para se defenderem dos adversários e de, assim, contribuir para o enfraquecimento da confiança nos governos, em particular.

Para além de infligir a redução de confiança nas instituições públicas e privadas, estas ações hostis vieram demonstrar como a Federação Russa pode causar danos à distância sem recorrer aos métodos convencionais como as forças militares ou políticas. É de ressaltar que a Rússia foi "dos países que se adaptaram mais depressa e que alcançaram

[31] "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective" Rain Ottis, *CCDCOE*. Disponível em: https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf

mestria no uso destas vertentes tecnológicas e Moscovo tem mostrado ao mundo como funciona esta forma híbrida de guerra" (Sanger, 2018).

No que toca à NATO, este acontecimento serviu como um teste aos seus ideais de defesa e como estes foram aplicados nesta situação. O então Ministro dos Negócios Estrangeiros estoniano, Urmas Paet, pediu auxílio sob a jurisdição da NATO, na medida em que acreditava que estes ciberataques estavam a ameaçar a segurança nacional estoniana e, por conseguinte, também a segurança da Aliança. O Tratado de Washington indica que a NATO deve defender um Estado-Membro e, neste caso, parecia tratar-se do início de uma ciberguerra[32].

Porém, havia alguma discordância se o artigo n.º 5 do Tratado de Washington[33] se poderia aplicar dado que, tecnicamente, não resultaram destes ataques nem feridos ou mortos e nem a destruição ou dano de nenhuma propriedade. Assim, os líderes desta Aliança não atuaram sob a jurisdição deste artigo, mas enviaram um conjunto de peritos em cibersegurança para ajudar a reparar os danos e recuperar as infraestruturas atacadas, não tendo sido assim reconhecido como um ato de guerra. O caso da Estónia é elucidativo pois demonstra como foi difícil a conjugação de leis antiquadas às novas tecnologias e, principalmente, na dificuldade que existia quanto ao que era se considerava e o que era realmente um ato ciberterrorista[34].

Pela Carta das Nações Unidas, um Estado poderia participar numa guerra de forma justificada em caso de sofrer uma "agressão", ou seja, por ter sofrido "o uso da força contra o [seu] território (…)". O problema é que esta disposição da Carta apenas se foca na esfera geográfica, de fronteiras físicas. Todavia, os ciberataques provam que não é necessário vermos uma ameaça a olho nu para haver a necessidade de intervenção de uma

---

[32] Singer, Peter e Allan Friedmann. "Cybersecurity and Cyberwar: What Everybody Needs to Know". *Oxford: Oxford University,* 2014.

[33] *As Partes concordam em que um ataque armado contra uma ou várias delas na Europa ou na América do Norte será considerado um ataque a todas, e, consequentemente, concordam em que, se um tal ataque armado se verificar, cada uma, no exercício do direito de legítima defesa, individual ou coletiva, reconhecido pelo artigo 51.° da Carta das Nações Unidas, prestará assistência à Parte ou Partes assim atacadas, praticando sem demora, individualmente e de acordo com as restantes Partes, a ação que considerar necessária, inclusive o emprego da força armada, para restaurar e garantir a segurança na região do Atlântico Norte. Qualquer ataque armado desta natureza e todas as providências tomadas em consequência desse ataque serão imediatamente comunicados ao Conselho de Segurança. Essas providências terminarão logo que o Conselho de Segurança tiver tomado as medidas necessárias para restaurar e manter a paz e a segurança internacionais*".
Disponível em: https://www.nato.int/cps/en/natohq/official_texts_17120.htm?selectedLocale=pt

[34] Singer, Peter e Allan Friedmann. "Cybersecurity and Cyberwar: What Everybody Needs to Know". *Oxford: Oxford University,* 2014.

OI. Foi, aliás, neste sentido que o incidente na Estónia iniciou um novo capítulo na cibersegurança, pois a Estónia passou de um país vítima de ciberataques massivos a um país líder na cibersegurança.

Foi este inesperado catalisador que levou à criação do Manual de Tallinn, pelo CCDCOE, tornando-se uma ferramenta essencial que desenvolve o direito internacional no campo das operações cibernéticas. Constitui um conjunto de regras não vinculativas com o objetivo de contribuir para a contextualização dos direitos de autodefesa que um Estado pode ter durante este tipo de conflitos[35].

No entanto, mesmo com a elaboração deste manual, verifica-se a existência de uma "área cinzenta" no que à punição de ciberataques nas OI e seus Estados-Membros diz respeito: "a Estónia queria que a NATO declarasse que a sua soberania tinha sido violada, o que teria envolvido o artigo n.º 5. No mundo virtual se calhar foi posta em causa (a sua soberania), mas não no mundo físico" (Singer e Friedmann, 2014).

Em 2008, a Estónia adotou a primeira estratégia nacional para a cibersegurança que, atualmente, já se encontra na sua terceira edição. Foi o primeiro documento que reconhecia a interdisciplinaridade da cibersegurança e a necessidade de ações coordenadas nessa área. Na primeira edição, em vigor de 2008 até 2013, a estratégia baseava-se, principalmente, em reduzir as vulnerabilidades inerentes ao ciberespaço no país como um todo, sendo necessária para o efeito a implementação de planos de ação nacionais e de cooperação internacional.

Encontramos[36] as primeiras diretrizes redigidas pelo governo estoniano para fortalecer a cibersegurança: o desenvolvimento e implementação em larga escala de um sistema de medidas de segurança, criação de medidas para aumentar as competências na cibersegurança, bem como para melhorar o quadro jurídico de apoio à cibersegurança, fortalecer a cooperação internacional e aumentar a consciência pública sobre o que é a cibersegurança e como devemos agir.

Tudo isto veio sublinhar como era urgente trabalhar no futuro neste setor. Demonstrou-se a importância de, mais do que encontrar os culpados dos ataques, assumir as responsabilidades na proteção e prevenção destas ameaças do ciberterrorismo devendo

[35] "The Tallin Manual", *CCDCOE*. Disponível em: https://ccdcoe.org/research/tallinn-manual/
[36] "Cyber Security Strategy" *Ministry of Defence*, 2008.
Disponível em: file:///C:/Users/Utilizador/Downloads/EE_NCSS_2008_en.pdf

ser estas uma das principais preocupações das OI. No seio das agendas da UE e da NATO, a cibersegurança assumiu-se como uma das principais prioridades globais, como iremos verificar no próximo capítulo.

2.2.2. Geórgia, 2008

Apesar de todos os esforços feitos para travar as ameaças cibernéticas, um ano depois, em 2008, mais um país Europeu, a Geórgia, sofreu um ataque cibernético de grande envergadura, também com origem na Federação Russa. Estudando a história deste país localizado no Cáucaso, a Geórgia "sempre manteve uma relação de tensão com a Rússia pois esta última sempre considerou a Geórgia como parte da esfera da influência do Kremlin devido à sua localização e tamanho. Após a dissolução da União Soviética em 1991, a Geórgia, como a Estónia, declarou a sua independência" (Clarke and Knake, 2012).

Em 1993, a Geórgia perdeu o controlo de duas regiões, a Ossétia do Sul e a Abecásia que, com o apoio russo, quiseram declarar-se como governos independentes apesar de ainda serem reconhecidas internacionalmente como parte da Geórgia. Com a eleição de Vladimir Putin para Presidente da Federação Russa, em 2003, a situação complicou-se ao ponto de, no ano de 2008, rebeldes da Ossétia do Sul terem voltado a entrar em conflito com a Geórgia, tendo "em agosto desse ano, as forças de Ossétia bombardeado aldeias novamente com o apoio da Rússia e, previsivelmente, o exército georgiano retaliou bombardeando também a capital de Ossétia. Desta forma, deu-se início à conhecida guerra Russo-Georgiana" (Clarke and Knake, 2012).

Exatamente no mesmo estilo que em 2007 com a Estónia, a Geórgia foi vítima de ciberataques DDoS nos seus *websites*, mas com uma diferença – estes mesmos ataques estavam a acompanhar uma campanha militar e "foi a primeira vez que uma operação de ataque contra uma rede de computadores (ARC) de grande escala foi executada em conjunto com importantes operações terrestres" (Shakarian, 2011). Importa então analisar mais detalhadamente como se sucedeu esta guerra "híbrida".

Note-se que os *hackers* russos selecionaram o governo georgiano como o centro de gravidade para focar os seus ataques primários, e, posteriormente, alargaram o seu perímetro de atuação. Identificam-se, assim, duas fases nesta campanha de ataques

cibernéticos que se estenderam pelo dia anterior à invasão: numa primeira instância, os ataques foram direcionados a websites do governo e aos *media* locais, já numa segunda fase os alvos ampliaram-se, tendo sido atingidas várias instituições financeiras, escolas e *media* ocidentais[37].

No início dos ataques, o site oficial do governo foi desconfigurado com a inserção de fotografias de Adolf Hitler na tentativa de associar a imagem do presidente georgiano Mikheil Saakashvili à imagem do ditador alemão. Além disso, "vários hackers russos utilizaram endereços de correio eletrónico de políticos georgianos, disponíveis ao público, para iniciar uma campanha de proliferação de mensagens eletrónicas (*spam*)" (Danchev, 2008). Estes ataques foram de tal maneira lesivos que a Geórgia perdeu, por vários dias, a capacidade de comunicar na sua própria comunidade, mas também com a comunidade internacional.

Segundo Kenneth Corbin (2009), a finalidade primordial dos ataques cibernéticos era silenciar a Geórgia da comunidade internacional através do seu isolamento nos meios de comunicação, impedindo-a de contar ao mundo o que estava a acontecer. Ainda segundo este autor, o objetivo de isolar a Geórgia do mundo exterior também explica os ataques aos bancos georgianos na segunda onda de ataques cibernéticos. O sistema financeiro foi seriamente afetado e esses ataques desencadearam uma resposta automática da maioria dos bancos estrangeiros, que "encerraram as suas conexões com o setor bancário georgiano. Sem acesso ao sistema de compensação europeu, as operações bancárias da Geórgia ficaram paralisadas" (Clarke and Knake, 2012).

No entendimento de Shakarian, os objetivos eram específicos e estavam bem delineados na medida em que os *hackers* tinham mais capacidades para instalar o "caos tecnológico". Evitaram causar danos permanentes às redes georgianas, principalmente nos sistemas de *Supervisory Control and Data Acquistion* (SCADA) e nos *Industrial Control System* (ICS). Estes sistemas são os pilares das infraestruturas críticas, onde assentam oleodutos, sistemas de tratamento e distribuição de águas, redes de energias e uma interrupção neste setor causaria enormes repercussões ao país.

O facto de estes ciberataques terem acompanhado as operações bélicas faz-nos perceber que houve uma "coordenação bastante precisa para alcançar os objetivos pretendidos pelo

[37] Shakarian, Paulo. "The 2008 Russian Cyber Campaign Against Georgia". *Academia*, 2011.

governo russo" (Menn, 2008). As operações no ciberespaço estavam já delineadas antes de haver um confronto no domínio físico, o que implicou um processo de preparação intensiva muito anterior a julho de 2008. Através deste esforço combinado, os russos quiseram provar, como no caso da Estónia, que a Geórgia não tinha capacidades para defender o seu território soberano, seja no domínio físico ou no ciberespaço, como também quiseram degredar a legitimidade do governo perante o mundo. No entanto, este acontecimento levou a uma aproximação do país tanto à UE como a NATO.

A partir daquele momento, ficou visível que as operações no ciberespaço deviam ser tomadas como tão ou mais importantes como as operações nos outros domínios. O ajuste que se assistiu na coordenação dos ataques encaixou perfeitamente na estratégia geopolítica levada a cabo pelos agressores tendo assim começado um novo objeto de estudo no seio da segurança e defesa dos Estados: a ciberguerra.

Desta forma, e como base na análise do artigo de David Hollis *"Cyberwar Case Study: Georgia 2008"*[38], podemos salientar algumas lições sobre estes ciberataques. A primeira consiste no facto de governos que detêm um enorme ciberpoder, como é o caso do governo russo ou chinês, terem a possibilidade de empregar *hackers* com motivações patrióticas para atingir os alvos pretendidos. Neste sentido, os hackers são instruídos por uma autoridade superior controlada pelos governos no sentido de hostilizar os adversários, desenvolvendo as suas técnicas no ciberespaço de maneira a atacá-los com eficácia, e praticando exercícios preliminares das suas capacidades. É necessário haver um maior controlo nas comunicações, por exemplo, nos *chats* de *hackers* a fim de intercetar estas atividades maliciosas.

Uma segunda lição a extrair é que uma nação agressora precisa sempre de identificar os alvos no ciberespaço antes de conduzir uma operação militar. Os ataques que estão planeados fisicamente necessitam de ser testados para experimentar a sua eficácia, como se se tratasse de um ensaio antes do grande "espetáculo". No futuro, as nações necessitarão sempre de conduzir atividades de reconhecimento e sondagens no ciberespaço, de modo a coordenar as operações cibernéticas com as operações militares convencionais. Conclui-se, assim, que as organizações nacionais devem investir nas suas

[38] Hollis, David. "Cyberwar Case Study: Georgia 2008". *Small Wars Journal*, 2011.

"cibercapacidades" de forma a desenvolver competências defensivas no ciberespaço para detetar operações antes que seja tarde demais.

Uma terceira lição a retirar deste conflito, baseia-se na maneira como foi habilmente gerido. O facto de ter sido orquestrado um "apagão" repentino das atividades do ciberespaço numa região específica poderá fornecer um indicador de que poderá acontecer um ataque convencional. Também poderá ser usado como uma distração, criando assim uma confusão na defesa ao ataque real. Isto gerou o pânico na população georgiana, o que dificultou ainda mais a resposta militar.

Por fim, Hollis diz-nos que é do interesse de cada governo observar o *status* dos *hackers* na sua comunidade interna. Se houver ataques diretos aos *hackers* por parte de outros *hackers* de uma nação agressora, muito provavelmente isto significará que há potenciais hostilidades entre os Estados noutros domínios sem ser no ciberespaço. Também alerta para outros governos, mesmo que não estejam envolvidos no conflito em si, terem a consciência da comunidade de *hackers* existente no seu país, pois isto pode impedir que a nação seja arrastada para o conflito. Vivemos num mundo onde existem *hackers* que, mesmo que usem tecnologia de baixo nível, conseguem realizar uma quantia considerável de danos a nível nacional e estratégico.

Estas lições ilustram como há uma necessidade contínua de investir na defesa do ciberespaço. Estas ameaças e riscos aos quais a nossa sociedade está exposta não podem ser ignorados ou negligenciados pois se o forem, podemos estar a abrir caminho para um "*Pearl Harbor* digital"[39]. Estamos perante um domínio que está em constante mudança, e desta forma, "o ritmo da implementação de processos e mecanismos de segurança dificilmente acompanha a dinâmica das vulnerabilidades, materializando uma área privilegiada de guerra assimétrica" (Viegas Nunes, 2004).

[39] Nunes, Viegas. "Ciberterrorismo: Aspetos de Segurança." *Revista Militar*, nº10, outubro, 2004.

2.2.3. Irão, 2010

Em 1950, o Irão lançou um programa nuclear que suscitou desconfiança na comunidade internacional relativamente às finalidades desta atividade. Pela parte dos iranianos, sempre houve a negação de qualquer acusação de que estavam a trabalhar em armamento nuclear, afirmando que tinham objetivos pacíficos e o nuclear destinava-se à produção de energia e ao desenvolvimento da medicina[40].

Em 1970, este país tornou-se um dos membros signatários do Tratado de Não-Proliferação de Armas Nucleares (TNP), o que lhe conferia alguma privacidade nas informações sobre o programa nuclear, tendo agravado ainda mais as suspeitas na comunidade internacional. Em 2005, a Agência Internacional de Energia Atómica (AIEA) acusou o Irão de não cumprir com os acordos e de evitar a realização das inspeções internacionais ao seu programa nuclear. Este assunto já tinha sido objeto de várias Resoluções da ONU[4041] e da UE, tendo esta última aplicado sanções económicas e financeiras contra o Irão, como restrições ao comércio de diversos produtos – proibindo a sua exportação e o congelamento de ativos do Banco Central iraniano com o objetivo de cessar esta atividade ilícita[42].

No ano de 2010, foi descoberto um *worm*[43] denominado *Stuxnet* que consiste num programa de computador sofisticado desenhado para penetrar e apoderar-se do controlo de sistemas remotos de forma quase autónoma. Este tipo de *malware* veio representar uma nova geração de ciberataques contra alvos selecionados. O *Stuxnet* foi usado para atacar as instalações nucleares iranianas em Natanz, tendo sido considerado como uma "arma de guerra que deixou o mundo virtual e atacou no mundo real" (Chen, 2014).

Segundo Sanger (2012), houve uma colaboração entre Israel e os EUA no desenvolvimento do *Stuxnet* com a intenção de desacelerar a produção de urânio por parte

---

[40] Foltz, Andrew. "Stuxnet, Schmitt Analysis, and the Cyber 'Use-of-Force". Debate. *JFQ,* 2012.
[41] Do Conselho de Segurança da ONU, foram emitidas as resoluções 1737 (2006), 1747 (2007), 1803 (2008) e 1929 (2010) todas com o principal objetivo de obrigar o Irão a cessar o enriquecimento de urânio para fins de proliferação nuclear.
[42] "Medidas restritivas da UE contra o Irão" *Conselho da União Europeia*. Disponível em: https://www.consilium.europa.eu/pt/policies/sanctions/iran/
[43] A ENISA define *worm* como um "*tipo de malware que tem a capacidade de se espalhar sem qualquer ação humana. Um worm geralmente explora pontos fracos, como vulnerabilidades do sistema operacional ou senhas fracas para se espalhar pelas redes de computadores"*. Disponível em: https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/malware

do Irão sem que fosse detetada a presença deste *malware*. O especialista alemão Ralph Lagner descreveu o *Stuxnet* como um cibermíssil teleguiado que foi usado para desmantelar o programa nuclear do Irão[44].

Mais detalhadamente, o *Stuxnet* foi construído com "quatro vulnerabilidades de dia zero[45]", ou seja, vulnerabilidades desconhecidas que não permitiram o desenvolvimento de instrumentos que as combatessem a tempo, o que abriu caminho a um acesso mais facilitado aos sistemas operacionais. O facto de este vírus ter sido construído com as quatro vulnerabilidades mostra-nos que os seus criadores tinham bastantes recursos e queriam garantir que o *Stuxnet* se infiltrava no alvo pretendido, e caso não o identificasse, tinha a capacidade de se autodestruir[46].

O *Stuxnet* dirigia-se a alvos que não estavam conectados à Internet pública e esta penetração exigia o uso de dispositivos intermediários, como *pendrives*, para conseguir o acesso à rede privada dos sistemas[47]. Visava controlar os sistemas industriais (SCADA), mais especificamente, os sistemas das centrais nucleares iranianas que se pretendiam atacar. Desta forma, um intermediário introduziu manualmente o *worm* num dos computadores dos cientistas iranianos e daí foi lançado o ataque, provocando o mau funcionamento das centrifugadoras das centrais.

Lagner descreve que o efeito foi tão eficaz como usar explosivos contra a instalação[48]. Na verdade, mostrou-se ainda mais eficaz dado que o *Stuxnet* permaneceu por mais de um ano nas redes iranianas sem que fosse notado, levando os cientistas a crer que as suas centrifugadoras apenas teriam avarias aleatórias. Aliás, esta terá sido a parte mais brilhante deste *malware*, que não só corrompeu o processo como escondeu os seus efeitos e explorou os sistemas sem qualquer problema ou impedimento[49].

Porém, estes ataques não foram suficientes para travar o programa nuclear do Irão, que foi restabelecido pouco tempo depois, o que revelou que as vulnerabilidades da central de

---

[44] Farwell, James e Rafal Rohozinski. "Stuxnet and the Future of Cyber War". *Survival*, 2011.

[45] Uma vulnerabilidade de dia zero é uma vulnerabilidade de software descoberta primeiro pelos invasores antes que o fornecedor tome conhecimento da mesma. Disponível em: https://www.kaspersky.com/resource-center/definitions/zero-day-exploit

[46] Singer, pág. 115.

[47] Farwell, pág. 24.

[48] Ibid, pág. 25.

[49] Singer, pág. 117.

Natanz não eram tão grandes quanto os criadores do *worm* pensavam, tendo sido gastos avultados recursos financeiros que não conseguiram atingir os objetivos pretendidos[50]. O que não era expectável para os criadores do *Stuxnet* era a sua proliferação para além de Natanz, o que permitiu que vários outros cibernautas tivessem acesso a este novo instrumento provocando vários ataques a outros alvos. O *Stuxnet* infetou mais de 60 mil computadores, sendo a maioria concentrados no Irão, mas também na Índia, Indonésia, China, Azerbaijão, Coreia do Sul, Malásia, EUA, Austrália, Finlândia e Alemanha[51].

Entende-se que o objetivo dos EUA era neutralizar esta central em Natanz, mas através de métodos não convencionais, ou seja, desencorajar ataques militares e tentar convencer Israel que havia maneiras mais eficazes e menos dispendiosas do que lançar ataques aéreos no Irão[51]. Assim, optou-se por usar o ciberpoder como uma estratégia de segurança e defesa o que representou uma nova maneira de resolver antigos conflitos com novos recursos. Michael Hayden, que fora uma figura importante nas primeiras experiências dos EUA com ciberarmas, afirmou que "havia no *Stuxnet* qualquer coisa que recordava agosto de 1945 – uma referência ao lançamento da bomba atómica em Hiroxima e Nagasáqui – estava a deixar claro que se iniciara uma nova era" (Sanger, 2018).

Como mencionado, este plano não teve o resultado idealizado e, por tentar usar um *malware* não detetável, colocou em causa a credibilidade norte-americana no cenário internacional, tendo os EUA sido acusados de usar uma ciberarma contra outro Estado soberano[52]. O facto deste *worm* ter "escapado" para a Internet, tornando-se acessível a qualquer cibernauta, faz-nos entender que os EUA também podiam sofrer um ataque do género contra as suas próprias infraestruturas críticas, ou seja, estrategicamente, o *Stuxnet* não foi bem concebido[53].

A utilização do ciberespaço como um meio para atingir um fim político torna-se cada vez mais real e apelativo. Não obstante o facto de ser mais "prático", pois não envolve operações militares e pode ser executado à distância, nem sempre é eficaz e pode gerar um efeito inverso – o próprio ator do ataque pode tornar-se o alvo da sua própria criação, como poderia ter sido o caso do *Stuxnet*. Atenta-se que a opção dos EUA, relativamente à utilização do seu ciberpoder, ficou bastante exposta na medida em que pode ter

[50] Foltz, Andrew. (2012). *"Stuxnet, Schmitt Analysis, and the Cyber 'Use-of-Force"* Debate. *JFQ*.
[51] Farwell, pág. 24.
[52] Clarke, Richard A., e Robert Knake. "Cyber war: the next threat to national security and what to do about it". 2º edição. *HarperCollins*. New York, 2012.
[53] Ibid, pág. 296.

desencadeado uma nova tendência a seguir por outros Estados, que se sentem legitimados a fazê-lo. Da mesma forma, outros atores não-estatais podem projetar o seu ciberpoder no sistema internacional, criando assim mais vulnerabilidades e novas ameaças que acabam em danos reais.

3. O papel das Organizações Internacionais na prevenção e proteção do ciberterrorismo

Com a figura abaixo pretende-se mostrar como funciona a articulação entre as instituições nacionais com as OI que Portugal integra, nomeadamente a União Europeia e a NATO.

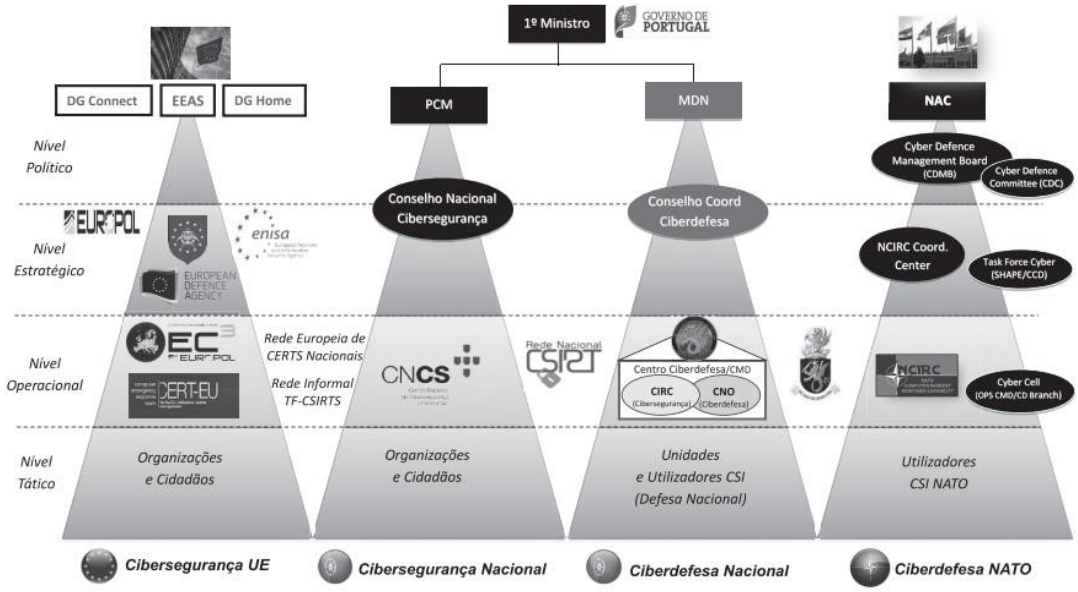

Figura 4 – Visão Orgânica para a Cibersegurança e Ciberdefesa: Articulação Nacional e Internacional[54]

Neste sentido, consegue-se identificar os organismos encarregues da cibersegurança como também da ciberdefesa, sendo estas duas componentes essenciais e complementares à defesa nacional. Ambas as áreas são interdependentes e entendem-se como o "conjunto

[54] "Contributos para uma Estratégia Nacional de Ciberdefesa" *Instituto de Defesa Nacional (IDN)* caderno nº28, abril de 2018.
Disponível em: https://www.idn.gov.pt/pt/publicacoes/idncadernos/Documents/2018/idncadernos_28.pdf

de atividades que ocorrem no ciberespaço, de prevenção, monitorização e reação a ameaças"[55]. No entanto, defendem vertentes diferentes – a cibersegurança defende das ameaças que coloquem em risco o bem-estar e a salvaguarda dos direitos dos cidadãos e organizações, já a ciberdefesa encarrega-se das ameaças que ponham em risco a soberania nacional. Em Portugal, a cibersegurança é assegurada pelas Forças de Segurança e os Serviços de Informações, já a ciberdefesa compete às Forças Armadas.

Sendo que o ciberespaço é um "território" no qual é difícil estabelecer limites e responsabilidades, é fundamental que as respostas às ameaças presentes sejam desenvolvidas em cenários de cooperação entre todos. Daqui resulta a criação de órgãos competentes dentro das OI que estão em contacto com as entidades nacionais de cada EM de forma a ser possível reforçar as sinergias e elaborar uma resposta concisa e eficaz em cenários de crise. Existe, assim, um consenso de que a nossa sociedade moderna apenas sobreviverá às novas ameaças híbridas se colocarmos a proteção do ciberespaço na consciência de cada um.

Vejamos, então, a jornada percorrida por estas duas OI e quais os principais elementos que defendem as infraestruturas críticas internacionais e nacionais.

3.1. A União Europeia

A União Europeia (UE) considera o ciberespaço como uma "área de justiça" onde se refletem os direitos humanos, a liberdade de expressão, a privacidade e a proteção dos dados pessoais, que devem ser preservados através do esforço conjunto de todos os Estados-Membros (EM) em prol de tornar este domínio cibernético mais seguro[56]. Apenas com a entrada do milénio e com o consequente desenvolvimento tecnológico é que o ciberespaço começou a ser considerado como uma matéria de segurança, pois "os ataques informáticos passaram a ser entendidos como cibercrimes" (Barrinha, 2018).

Neste sentido, em 2001 foi organizada, pelo Conselho da Europa, a Convenção de Budapeste (também conhecida como a Convenção Europeia do Cibercrime) pois, cada vez mais, era notório que as TIC estavam a desenvolver-se a um ritmo acelerado e a

[55] Ibid, pág. 23.
[56] "Estratégia da Informação e Segurança no Ciberespaço". *Instituto Nacional de Defesa (IDN).* Caderno nº12, 2013. Disponível em: https://comum.rcaap.pt/bitstream/10400.26/7757/1/idncaderno_12.pdf

sociedade crescentemente sujeita à sua dependência. Tornou-se necessário rever as medidas de cibersegurança de cada Estado de forma a reduzir os riscos a que estes estavam expostos tecnologicamente. Assim, em 23 de novembro de 2001, foi aprovada pelos EM europeus bem como por países fora da UE, nomeadamente, o Canadá, Japão, África do Sul e Estados Unidos da América (EUA) que colaboraram também na elaboração da Convenção.

As Partes envolvidas nesta Convenção tinham como objetivo:

> "impedir atos praticados contra a confidencialidade, integridade e disponibilidade de sistemas informáticos, de redes e dados informáticos, bem como a utilização fraudulenta desses sistemas, redes e dados, assegurando a incriminação desses comportamentos (…) e a adoção de poderes suficientes para combater eficazmente essas infrações, facilitando a deteção, a investigação e o procedimento criminal relativamente às referidas infrações, tanto a nível nacional como internacional, e estabelecendo disposições materiais com vista a uma cooperação internacional rápida e fiável[57]".

Outro passo foi tomado com a criação da ENISA, em 2004, que veio contribuir para a ciberpolítica da UE com o objetivo de apoiar a fiabilidade dos serviços e processos de TIC com novos mecanismos de cibersegurança como também para contribuir para a cooperação entre os Estados Membros e os respetivos organismos da UE para que fosse possível preparar a Europa para futuros desafios cibernéticos"[58].

A ENISA marcou a diferença pois, um dos seus primeiros atos, foi redefinir a cibersegurança como uma responsabilidade partilhada e, neste sentido, ajudou a construir o Sistema Europeu de Partilha e Alerta de Informação (EISAS), um quadro estratégico a ser implementado nos EM que tinha como objetivo educar os indivíduos, pequenas e médias empresas a protegerem-se de ameaças cibernéticas. Desta forma, contribuía-se não só para a segurança nacional, como também para uma infraestrutura de comunicação

[57] "Convention on Cybercrime" *Conselho da Europa*, 2001. Disponível em: https://rm.coe.int/1680081561
[58] "Sobre a ENISA" *ENISA*. Disponível em: https://www.enisa.europa.eu/about-enisa/about/pt

pública mais resiliente[59]. Assim, em 2006, a UE adotou uma estratégia que promovia o diálogo, a cooperação e o fortalecimento para uma sociedade segura e informada[60].

Apesar desta eficiente trajetória da UE, não houve meios suficientes para travar o conhecido ciberataque à Estónia no ano seguinte (2007). Como estudado, foi um dos marcos mais vincados na história da cibersegurança que veio pôr em causa todas as estratégias alguma vez adotadas pelas OI. Criou-se uma maior consciência do perigo (imprevisível e eminente) de um ciberataque e, como consequência, a UE adotou a cibersegurança como uma preocupação prioritária.

Desta forma, na Estratégia Europeia em Matéria de Segurança de 2008 elaborada pelo Conselho da UE, adverte que "A estratégia da UE para uma sociedade da informação segura, adotada em 2006, visava combater a cibercriminalidade. No entanto, os atentados contra sistemas informáticos tanto privados como governamentais que ocorreram nos Estados Membros, vieram conferir a este tipo de criminalidade uma nova dimensão, revelando o seu potencial como uma nova arma económica, política e militar"[61]. Era necessário investir mais no domínio emergente para conseguir alcançar um maior nível de cooperação internacional.

Numa nota informativa, também em 2008, Portugal criou uma rede Nacional de *Computer Security Incident Response* (CSIRT), constituindo assim um "fórum de excelência para partilha de informação de carácter operacional[62]". Atualmente, é composta por mais de 40 entidades de diversos setores da sociedade, como de infraestruturas de energia (EDP, GALP, REN), bancárias (Banco CTT, Santander, Novo Banco), de telecomunicações (Vodafone, Altice, NOS, NOWO), empresas de cibersegurança (CIPHER, S21SEC, SECURENET), de águas (Grupo Águas de Portugal), como também são parte integrante algumas universidades (Instituto Politécnico de Bragança, ISCTE, Universidade de Aveiro, Universidade do Algarve), como também se menciona que as Forças Armadas Portuguesas são membro constituinte desta rede desde do ano da sua criação.

---

[59] "EISAS Basic Toolset" *ENISA*, outubro 2011.
Disponível em: https://www.enisa.europa.eu/publications/eisas-basic-toolset

[60] "A Strategy for a Secure Information Society – Dialogue, partnership and empowerment" *Commission of the European Communities*, 2006. Disponível em: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0251:FIN:EN:PDF

[61] "Estratégia Europeia em Matéria de Segurança – Uma Europa segura num mundo melhor" *Conselho da União Europeia*, 2008. Disponível em: https://www.consilium.europa.eu/media/30824/qc7809568ptc.pdf

[62] "Rede Nacional de CSIRT" *Centro Nacional de Cibersegurança*.
Disponível em: https://www.cncs.gov.pt/pt/csirt/

No ano de 2010, foi apresentada uma nova revisão da estratégia de segurança de forma a reforçar a anterior. Nesta versão revista[63], foram mencionadas as ameaças comuns e respetivos desafios para a segurança interna da UE bem como as respostas a dar a esses mesmos desafios. Referem-se os fenómenos que são transfronteiriços, dando uma especial enfâse ao terrorismo, em todas as suas formas, e à cibercriminalidade que, cada vez mais, representa uma ameaça mundial e anónima para os sistemas de informação. A UE assumiu como uma prioridade a antecipação da ameaça, ou seja, a EUROPOL e outras agências europeias, como a ENISA, assumiram um papel mais presente e focado na avaliação da ameaça para encontrar respostas atempadas e adequadas.

Ainda no ano de 2010, a UE iniciou os seus esforços para definir ciberterrorismo aquando do ataque *Stuxnet* dirigido contra o Irão. Este ataque potenciou a vulnerabilidade dos sistemas de computadores ligados às infraestruturas da UE, o que veio acelerar o processo de preparação contra estes ataques antes que os grupos terroristas adquirissem as capacidades para direcioná-los contra as infraestruturas europeias.

Já em 2013, foi publicada uma estratégia apenas incidindo sobre a cibersegurança intitulada "Estratégia da UE para a Cibersegurança: um ciberespaço aberto, seguro e protegido". O objetivo desta estratégia focava-se em uniformizar as capacidades de cibersegurança dos EM uma vez que apenas 13 adotaram oficialmente estratégias de cibersegurança nacionais, sendo possível notar diferenças na preparação, conhecimento e segurança de estratégias entre estes. Foi realçada a importância de criar um "mercado único digital" com o objetivo de consumidores e empresas tirarem pleno partido das oportunidades oferecidas pela Internet e tecnologias digitais com a devida segurança[64].

Com a evolução tecnológica, tornou-se necessária uma maior segurança no ciberespaço e, desta forma, foram criadas as Equipas de Resposta a Emergências Informáticas (CERT-UE) como modo de investimento na prevenção, deteção, resposta e inteligência às ameaças cibernéticas. Estas equipas trabalham em articulação com as outras agências da UE como também "cooperam com as equipas de resposta a emergências informáticas nacionais (tanto dentro da UE como em países terceiros) e com parceiros internacionais,

---

[63] "Estratégia de Segurança interna da União Europeia – Rumo a um modelo europeu de segurança" *Conselho da União Europeia*, 2010.
Disponível em: https://www.consilium.europa.eu/media/30754/qc3010313ptc.pdf
[64] "A nova estratégia para o Mercado Único Digital da União Europeia" *EUR-LEX,* 2015. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=LEGISSUM:3102_3

o que ajuda a melhorar o nível de intercâmbio de informações dentro e fora da União Europeia"[65].

Na Figura 5, infra, encontramos o mapa atual de CERT-UE instalados pelos países de cor azul escura.

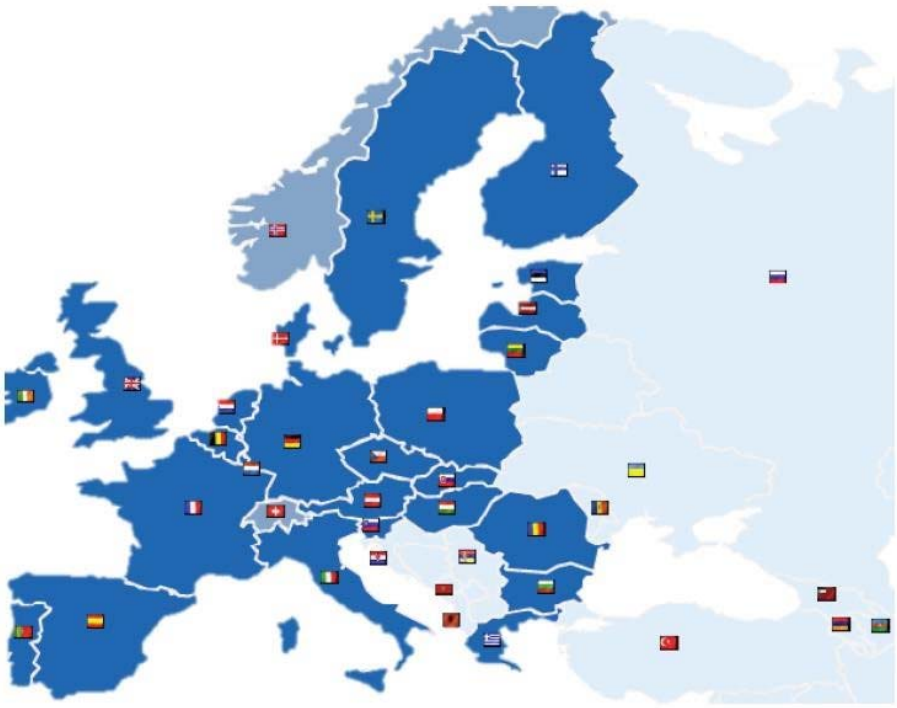

Figura 5 – Mapa de CERT-UE (países com cor azul escura)[66]

Em Portugal, entendeu-se também a importância da proteção da soberania e defesa dos interesses nacionais no âmbito do ciberespaço. Neste raciocínio, foi elaborada, em 2015 e pela primeira vez, a Estratégia Nacional para a Segurança do Ciberespaço (ENSC). Nesta estratégia, procura-se "estabelecer a importância de uma coordenação operacional ágil, construir uma permanente atualização da legislação; proteger as infraestruturas

[65] "Estratégia da União Europeia para a cibersegurança: um ciberespaço aberto, seguro e protegido", *Comissão Europeia*, 2013. Disponível em: https://eur-lex.europa.eu/legalcontent/PT/TXT/PDF/?uri=CELEX:52013JC0001&from=PT

[66] "New CERTs Inventory and updated may now available" *ENISA*, 2013. Disponível em: https://www.enisa.europa.eu/news/enisa-news/new-certs-inventory-and-updated-map-now-available

críticas (…) e estimular a investigação e o desenvolvimento e sublinhar a utilidade da cooperação nacional e internacional nos diversos domínios de atuação para Portugal"[67].

Em 2016, é aprovada uma Diretiva Europeia (UE 2016/1148) ou Diretiva para a Segurança das Redes e da Informação (SRI) que se tornou numa peça fundamental na arquitetura da cibersegurança. A sua finalidade reside, sobretudo, na importância da preparação dos EM e na capacidade de estarem prontos para reagir e combater um ciberataque, adotando medidas como "designar uma ou mais autoridades nacionais competentes, identificar um ponto de contacto único e identificar os operadores de serviços essenciais de setores críticos, como o da energia, transportes, financeiros, bancário, saúde, da água e das infraestruturas digitais"[68]. Visa, assim, garantir uma maior cooperação entre os organismos da UE com as Equipas de Resposta a Incidentes de Segurança de Computadores (CSIRT) de cada país para que seja possível aumentar ainda mais a sensibilização para este tema.

Também neste ano, a UE criou o Regulamento Geral sobre a Proteção de Dados (RGPD) pois na sequência da Carta dos Direitos Fundamentais da UE, "todos os cidadãos da União Europeia têm direito à proteção dos seus dados pessoais"[69] dado que, um ciberataque pode comprometer essas informações as quais podem ser utilizadas para fins maliciosos. Representa uma medida essencial na era digital e veio reforçar a segurança dos cidadãos de forma proteger as suas atividades, sejam estas, por exemplo, de teor comercial, no espaço europeu.

Ao nível nacional, em 2018 foi adotada a Lei nº46/2018 que transpôs esta mesma diretiva europeia. A lei estabelece o Regime Jurídico da Segurança do Ciberespaço e aplica-se às "entidades da Administração Pública, aos operadores de infraestruturas críticas, aos operadores de serviços essenciais, aos prestadores de serviços digitais, bem como a quaisquer outras entidades que utilizem redes e sistemas de informação, nomeadamente, no âmbito da notificação voluntária de incidentes"[70]. Na sequência deste Regime, o

---

[67] "A Estratégia de Cibersegurança para Portugal" *Centro de Investigação Jurídica do Ciberespaço*, 2015. Disponível em: https://www.cijic.org/2015/10/09/a-estrategia-de-ciberseguranca-para-portugal/

[68] "Diretiva do Parlamento Europeu e do Conselho relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União" *EUR-LEX*, 2016. Disponível em: https://eurlex.europa.eu/legalcontent/PT/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.POR&toc=OJ:L:2016:194TOC

[69] "A proteção de dados na UE" *Comissão Europeia*. Disponível em: https://ec.europa.eu/info/law/lawtopic/data-protection/data-protection-eu_pt

[70] "Regime Jurídico" *Centro Nacional de Cibersegurança*. https://www.cncs.gov.pt/pt/regime-juridico/

Centro Nacional de Cibersegurança (CNCS) e o Centro de Estudos para Resposta e Tratamento de Incidentes em Computadores (CERT.PT) foram consagrados como a Equipa de Resposta a Incidentes de Segurança Informática Nacional.

Em paralelo, no ano de 2019, Portugal adotou uma nova revisão da Estratégia Nacional de Segurança do Ciberespaço (ENSC) que está em vigor até 2023. Os objetivos desta estratégia baseiam-se em "maximizar a resiliência (…) promover a inovação (…) gerir e garantir recursos de forma a contribuir e garantir a alocação de recursos adequados para a edificação e sustentação da capacidade nacional para a segurança do ciberespaço"[71].

Em 2020, surge uma nova necessidade de desenvolvimento de estratégias e ações na área da cibersegurança. A pandemia do COVID-19 veio acelerar a dependência de ferramentas e serviços digitais, o que muito contribuiu para o aumento de ciberataques às infraestruturas críticas de todo o mundo. Fred Cohen afirmou que "quanto menos ligados ao mundo estivessem os nossos computadores, menos risco de infeção" teriam[72].

A pandemia, que levou ao confinamento de milhões de pessoas em casa, teve como consequência o acesso dos trabalhadores às suas empresas e organizações a partir das suas casas, usando as redes de Internet domésticas que têm um baixo nível de segurança, sendo que "não é de espantar que tenha havido um aumento generalizado de ataques cibernéticos, com o FBI a dar conta de um crescimento de 300% no número de queixas relativas a ataques informáticos, um cenário que se espalhou pelo mundo fora" (Barrinha, 2020).

Deste modo, em 2020, a estratégia da cibersegurança teve como objetivo "preservar uma Internet global e aberta, mediante a utilização e o reforço de todos os instrumentos e recursos disponíveis, a fim de garantir a segurança e proteger os valores europeus e os direitos fundamentais de cada um de nós[73]". O que existe de novidade nesta estratégia, assenta no conceito de desenvolver um "ciberescudo", isto é, "um conjunto de operações de segurança que utilizam a Inteligência Artificial (IA) e a aprendizagem automática para

[71] "Estratégia Nacional de Segurança do Ciberespaço" *Portugal Digital*, 2019. Disponível em: https://portugaldigital.gov.pt/acelerar-a-transicao-digital-em-portugal/conhecer-as-estrategias-para-atransicao-digital/estrategia-nacional-de-seguranca-do-ciberespaco/

[72] Lin, Herb. "Cybersecurity Lessons from the Pandemic, or Pandemic Lessons from Cybersecurity" *LAWFARE*. Disponível em: https://www.lawfareblog.com/cybersecurity-lessons-pandemic-or-pandemiclessons-cybersecurity

[73] "Noca estratégia de cibersegurança da UE e novas regras para aumentar a resiliência das entidades críticas físicas e digitais – Perguntas e respostas" *Comissão Europeia,* 2020. Disponível em: https://ec.europa.eu/commission/presscorner/detail/pt/qanda_20_2392#cybersecurity

detetar indícios precoces de ciberataques iminentes e que permitem adotar medidas antes que sejam causados quaisquer danos"[74]. Para além do "ciberescudo", pretendia-se criar uma "ciberunidade conjunta", que tinha a finalidade de trabalhar na atual cooperação entre as instituições, órgãos e agências da UE com as autoridades dos Estados Membros em prol de aproximar as cibercomunidades para criar uma frente mais resiliente às ameaças ou incidentes graves[75].

Em 2021, foi desenvolvida uma nova estratégia de cibersegurança da UE, incentivada pela Comissão Europeia, para a década digital na qual se reconhece a transformação digital como uma prioridade estratégica como também é mencionado que se prevê um aumento significativo de dispositivos ligados à Internet até 2024, o que irá criar uma maior exposição às ciberameaças. Também nesta estratégia considera-se o aumento das ameaças híbridas que se têm mostrado através de campanhas de desinformação e de ciberataques contra instituições democráticas os quais têm dificultado os processos democráticos[76].

No caso português, surge o decreto-lei nº65/2021[77], que representa um passo fundamental para a cibersegurança portuguesa. Este decreto vem regulamentar certos aspetos da lei nº46/2018 e, principalmente, tem a missão de distribuir responsabilidades, pois como afirma João Alves, atual Coordenador do Departamento de Regulação, Supervisão e Certificação do CNCS, "a garantia de um elevado nível de segurança do ciberespaço é do interesse de todos os cidadãos e atores, públicos ou privados, envolvidos"[78].

Importa notar que, para a implementação desta lei, é necessária uma maior cooperação entre as organizações e também que estas tenham a maturidade e a consciência de que toda a preparação que devem ter para dar resposta aos incidentes contribuirá não só para a ciberesiliência nacional, como para a afirmação de Portugal no domínio do ciberespaço. Deve-se abandonar as práticas mais isolacionistas e continuar a trabalhar para ser possível aguentar as futuras crises que aparecerão.

---

[74] Ibid.

[75] Ibid.

[76] "Estratégia de cibersegurança da UE para a década digital" *Parlamento Europeu*, 2021. Disponível em: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0286_PT.pdf

[77] "Decreto-lei nº65/2021, de 30 de junho" *CNCS*. Disponível em:https://www.cncs.gov.pt/docs/decretolei-65-2021.pdf

[78] "Decreto-lei 65/2021: um pequeno passo para o homem, um salto gigante para as organizações nacionais" *It Security*, 2022. Disponível em: https://www.itsecurity.pt/news/compliance/decreto-lei-652021-umpequeno-passo-para-o-homem-um-salto-gigante-para-as-organizacoes-nacionais

Em 2022, urge a necessidade da aprovação da proposta de revisão da Diretiva SRI em termos de alargamento da sua aplicabilidade. Assim, o objetivo desta revisão (Diretiva SRI 2) foca-se em reforçar as obrigações de cibersegurança alargando-as a novos setores que tenham uma função fundamental para a economia, tais como os setores da energia, transportes, saúde, setor bancário, infraestruturas digitais, registos de domínios de alto nível (…)[79].

As políticas de cibersegurança que têm sido desenvolvidas e implementadas pela UE neste século são bem mais abrangentes do que a mera proteção contra ciberataques terroristas, tendo como principal objetivo posicionar a UE como uma autoridade internacional e líder no combate às ameaças cibernéticas do futuro. Os avultados investimentos realizados desde o início do milénio permitiram que a UE se assumisse como um exemplo global no combate ao ciberterrorismo. No entanto, a evolução da tecnologia é de tal forma vertiginosa que a UE deverá continuar a acompanhar esta dinâmica, investindo mais recursos humanos e materiais de forma a aumentar a resiliência aos fenómenos de ciberterrorismo nos seus EM bem como a nível global.

3.2. A NATO

A NATO assume-se como a maior aliança militar do mundo, baseada no Tratado do Atlântico Norte, de 1949, que tem como objetivo a defesa coletiva dos seus Aliados em caso de um ataque iminente a algum destes[80]. É considerada como a organização internacional que mais recursos tem mobilizado no combate às ameaças cibernéticas e na proteção do ciberespaço. Desta forma, importa conhecermos os antecedentes que levaram a NATO a alcançar a atual relevância no âmbito da ciberdefesa.

No final da década 90, a sede da NATO em Bruxelas foi vítima de ciberataques do tipo DDoS aquando do seu envolvimento na Guerra dos Balcãs[81]. *Hackers* sérvios conseguiram negar o acesso ao principal servidor da *World Wide Web* da sede, no qual

[79] "Nova estratégia de cibersegurança da UE e novas regras para aumentar a resiliência das entidades críticas físicas e digitais – Perguntas e respostas" *Comissão Europeia*, 2020. Disponível em: https://ec.europa.eu/commission/presscorner/detail/pt/qanda_20_2392

[80] "O que é a NATO?" *NATO*. Disponível em: https://www.nato.int/nato-welcome/index_pt.html

[81] A Guerra dos Balcãs consistiu em vários conflitos bélicos ocorridos no final da década de 90 entre vários países (Sérvia, Grécia, Montenegro, Turquia, Roménia e Bulgária) pela posse dos restantes territórios que antes estavam sob o domínio do Império Otomano.

era feita a atualização da informação da operação diplomática levada a cabo pela NATO no Kosovo. Como resultado, este servidor ficou inoperável durante vários dias e os sistemas de *e-mail* da Aliança receberam milhares de mensagens de *spam* por dia[82], provocando danos consideráveis nas operações em curso.

Após o ataque terrorista do 11 de setembro de 2001 nos EUA, tornou-se ainda mais premente a necessidade de rever as estratégias de defesa da NATO face aos métodos pouco convencionais e inovadores utilizados nos ataques e que se foram propagando quer pelo mundo físico quer pelo virtual. Assim, a segurança no ciberespaço, bem como o termo cibersegurança, "entraram, progressivamente, na lista de preocupações das principais potências mundiais" (Barrinha e Carrapiço, 2016). Neste sentido, o primeiro passo dado nessa missão foi concretizado com a Cimeira de Praga no ano de 2002.

Nesta cimeira deu-se início à transformação do conceito estratégico da NATO para fazer frente a um novo tipo de ameaças. Um dos temas centrais foi a segurança da informação das infraestruturas da NATO, área que apresentava vulnerabilidades e que representava um desafio às capacidades da Aliança. A Cimeira de Praga foi reconhecida como "um marco que veio transformar a NATO. Daqui resultaria uma Aliança mais bem orientada para os novos desafios provocados pelo terrorismo e pela disseminação de armas de destruição maciça.

Neste sentido, foi criada uma unidade operacional vocacionada para combater as ameaças emergentes, denominada *NATO's Response Force* (NRF), que era constituída por um "grupo de força tecnologicamente avançada, flexível, desdobrável, interoperável e sustentável na terra, mar e ar, pronto para se mover rapidamente para onde fosse necessário conforme decidido pelo Conselho, como também seria um catalisador para focar e promover melhorias nas capacidades Aliança"[83].

Dentro desta mesma equipa, foi desenvolvida, em 2004, outra vertente que se focava mais na segurança da informação das infraestruturas da NATO, denominada *NATO Computer Incident Response Capability* (NCIRC). Este centro, sedeado em Mons, na Bélgica, tinha

[82] "Serbs lauch cyberattack on NATO" *FCW*, 1999. Disponível em: https://fcw.com/1999/04/serbs-launchcyberattack-on-nato/195288/
[83] Ibid.

como objetivo "proteger as próprias redes da NATO fornecendo apoio centralizado e ininterrupto na defesa cibernética"[84].

Em 2006, realizou-se a Cimeira de Riga na qual foram discutidos os desafios de segurança do século XXI. Um dos resultados desta Cimeira foi a elaboração do documento "Orientação Política Global" que reforçou a ideia da transformação da estratégia da NATO e da continuidade de adaptação das suas forças combatentes, bem como o "estabelecimento das prioridades relativas às capacidades de planeamento e informações da NATO" (IDN, 2013). Deste modo, foi decidido o desenvolvimento e implementação de uma rede segura onde fosse viável "a partilha de informações, dados e inteligência das operações da Aliança, de forma a proteger os principais sistemas de informação contra ciberataques"[85].

Com os ciberataques à Estónia em 2007, a NATO, do mesmo modo como sucedeu com a UE, percebeu que os ciberataques representavam uma nova geração de conflitos e hostilidades com consequências que poderiam ser devastadoras. As infraestruturas críticas dos países atacados necessitavam não só da proteção estatal, como também, e cada vez mais, da proteção das organizações em que se inseriam. Neste sentido, a NATO criou um órgão responsável pela consulta, comando e controlo da política de ciberdefesa, denominado "NC3B" que iria dedicar-se ao aperfeiçoamento da política de ciberdefesa com vista ao desenvolvimento do conceito.

Neste seguimento, em 2008, foi constituído em Tallinn, o Centro de Excelência para a Ciberdefesa Cooperativa (CCDCOE), com a missão de prestar apoio aos países membros e à própria NATO nos campos de pesquisa, treinos e exercícios de ciberdefesa para que fosse possível manter o foco nas áreas mais críticas, tais como a estratégia, operações, direito e tecnologia[86].

O CCDCOE começou por ser desenvolvido em resultado do ciberataque massivo que a Estónia sofreu, sendo atualmente responsável pelo maior e mais complexo exercício internacional de ciberdefesa, o *Locked Shields*. Ian West, chefe do Centro de Segurança Cibernética da NATO, considera este exercício "uma oportunidade única para os participantes praticarem a proteção dos seus sistemas nacionais e das infraestruturas

[84] "Cyber Defence" *NATO*. Disponível em: https://www.nato.int/cps/en/natohq/topics_78170.html
[85] "Riga Summit Declaration" *NATO,* 2006.
Disponível em:https://www.nato.int/cps/en/natohq/official_texts_37920.htm?selectedLocale=en
[86] "About Us" *CCDCOE*. Disponível em: https://ccdcoe.org/about-us/

críticas, sendo um exercício realizado sob condições de intensa pressão com equipas combatendo várias séries de sofisticados e intensos ciberataques"[87].

Um dos documentos mais importante que este centro elaborou foi o Manual de Tallinn (já mencionado acima no capítulo da Estónia, 2007), que versa o modo como o Direito Internacional pode ser aplicado no ciberespaço. Portugal é membro do CCDCOE desde 2018.

Em 2010, teve lugar a Cimeira de Lisboa que assinalou novas evoluções na ciberdefesa da Aliança: foi aprovado um novo Conceito Estratégico, abrindo caminho para a revisão da Política de Ciberdefesa da NATO.

Neste Conceito Estratégico denotou-se a urgência e a crescente preocupação com os vários ciberataques que assolavam os Aliados, determinando que a Aliança "desenvolverá mais profundamente a capacidade de prevenir, detetar e defender e recuperar de ciberataques, incluindo o uso do processo de planeamento da NATO para melhorar e coordenar as capacidades nacionais de ciberdefesa"[88].

Com a Cimeira de Chicago, em 2012, ocorreu uma outra revisão, mas desta vez à Política de Segurança da Informação da NATO. Nesta mesma, foi incluído o tópico da ciberdefesa e, de igual modo, surgiu também a Agência de Comunicações e Informações da NATO (NCIA) que engloba o Centro de Segurança Cibernética o qual atuava como um *hub* para a partilha de informações cibernéticas, treinos e experiências para todos os Aliados bem como para as Nações Parceiras[89].

Em 2014, na Cimeira de Gales, a NATO reconheceu que era necessário um endossamento da Política de Ciberdefesa, recordando que a defesa das próprias estruturas da NATO e o auxílio aos Aliados de forma a incentivá-los a desenvolver mecanismos de defesa para as suas redes nacionais, faziam parte da responsabilidade da ciberdefesa da Aliança[90].

A Política de Ciberdefesa defende que o Direito Internacional deve ser aplicado no ciberespaço, como versa o Manual de Tallinn. Outro ponto importante desta política foi

---

[87] "Exercise Locked Shields 2022 Concludes" *SHAPE-NATO,* 2022. Disponível em: https://shape.nato.int/news-archive/2022/exercise-locked-shields-2022-concludes

[88] "Active Engagement, Modern Defence" *NATO*, 2010. Disponível em: https://www.nato.int/cps/fr/natohq/official_texts_68580.htm?selectedLocale=en

[89] "NATO'S Cyber Security Centre" *NCIA-NATO.*
Disponível em : https://www.ncia.nato.int/what-wedo/cyber-security.html

[90] "Wales Sumit Declaration" *NATO,* 2014.
Disponível em: https://www.nato.int/cps/en/natohq/official_texts_112964.htm

que "uma decisão sobre um ciberataque levaria à invocação do 5.º artigo e seria tomada pelo Conselho do Atlântico Norte caso a caso"[91].

Dois anos depois, em 2016, realiza-se a Cimeira de Varsóvia onde o ciberespaço é reconhecido como o novo domínio de operações e, por conseguinte, os Aliados comprometeram-se a reforçar as suas capacidades de ciberdefesa através do *Cyber Defense Pledge*[92]. Este compromisso pretendia desenvolver a gama de capacidades de defesa das infraestruturas da NATO de forma a reforçar as competências e criar uma maior consciência entre todos os participantes da defesa, desde o nível nacional até ao nível organizacional.

Ainda nesta cimeira, a UE e a NATO estabeleceram vários acordos de cooperação nas áreas conectadas à ciberdefesa. Neste sentido, em fevereiro de 2016, foi estabelecido um Acordo Técnico sobre a Ciberdefesa entre o NCIRC e o CERT-UE que "fornecia uma estrutura para troca de informações e compartilhamento de melhores práticas entre as equipas de resposta a emergências"[93]. Este acordo funcionaria como um exemplo do trabalho conjunto entre as duas OI para reforçar a segurança dos seus EM e Aliados de modo a incentivá-los a investir no combate às ameaças híbridas emergentes (físicas e virtuais).

Em 2018, na Cimeira de Bruxelas, a contínua preocupação com o ciberespaço resultou num reforço de todas as medidas tomadas nas cimeiras anteriores, com especial enfoque na cooperação internacional, nomeadamente entre a NATO e a UE, tendo resultado na criação do Centro de Operações do Ciberespaço (CyOc) sedeado em Bruxelas. Este centro representaria um fortalecimento das estruturas da Aliança para "fornecer consciência situacional e coordenação da atividade operacional da NATO no ciberespaço, incluindo o planeamento de exercícios e operações"[94].

A sua principal finalidade seria melhorar a resposta da Aliança aos ciberataques, de modo a conseguir coordenar as capacidades cibernéticas com as capacidades militares convencionais. Adicionalmente, foi introduzido na cimeira o tema do uso distorcido da

---

[91] Ibid.

[92] "Enquadramento da Ciberdefesa" *República Portuguesa – Defesa Nacional.* Disponível em: https://www.defesa.gov.pt/pt/pdefesa/ciberdefesa/enquadramento

[93] "Relatório sobre o estado das capacidades de ciberdefesa" *Parlamento Europeu.* Disponível em: https://www.europarl.europa.eu/doceo/document/A-9-2021-0234_PT.html

[94] "Cyber defence at the 28th NATO Summit in Brussels, 11-12 July 2018" *CCDCOE*, 2018. Disponível em:https://ccdcoe.org/incyder-articles/cyber-defence-at-the-28th-nato-summit-in-brussels-11-12-july2018/

tecnologia pelas organizações terroristas, tendo a NATO concordado em continuar a melhorar as suas capacidades e tecnologias através da adoção de uma nova política de dados biométricos que permitia identificar as personalidades terroristas de todo o mundo.

Também em 2018, a NATO e a UE assinaram uma declaração conjunta, na qual definiam a visão conjunta sobre como poderiam colaborar para enfrentar as ameaças em prol da segurança transatlântica nos domínios explanados na Figura 6[95].

Figura 6 – Domínios de cooperação UE-NATO[96]

Embora nos últimos anos se tenha intensificado o debate mais amplo sobre o desenvolvimento de possíveis normas de comportamento ou conjunto de medidas de construção de confiança no domínio da segurança e da cibersegurança, não devemos esquecer que a maioria das questões e desafios prementes neste domínio têm raízes na adoção e revisão nacional e na implementação de princípios acordados multilateralmente.

Em 2020, Portugal inaugurou a Academia de Comunicações e Sistemas de Informações da NATO, localizada em Oeiras, com o objetivo de proporcionar formações e treinos na área da cibersegurança e reforçar o desempenho português nas missões da Aliança. O

[95] "Cooperação UE-NATO" *República Portuguesa – Defesa Nacional".*
Disponível em: https://www.defesa.gov.pt/pt/pdefesa/due/uenato
[96] Ibid.

facto de Portugal ter sido escolhido para acolher esta academia contribui, por um lado, para a soberania nacional e, por outro, para a afirmação de Portugal no contexto internacional.

A título de exemplo, Portugal alberga o exercício CIBER PERSEU que se "destina a exercitar e avaliar a capacidade de resposta do Exército, face à ocorrência de ciberataques de âmbito nacional e internacional, que podem escalar para uma Crise no Ciberespaço"[97]. Estes exercícios constroem uma maior motivação para todos os Estados apostarem no investimento das suas capacidades de cibersegurança e permitem também o aprofundamento do conhecimento dos mecanismos de resposta às ameaças ciberterroristas.

Em 2021, dá-se uma nova Cimeira da NATO em Bruxelas onde foram enfatizadas as crescentes ameaças cibernéticas à segurança dos Aliados. Para que fosse possível enfrentar este imparável crescimento, aprovou-se a *Comprehensive Cyber Defence Policy*, que serve de suporte á Política de Ciberdefesa da NATO. Nesta declaração, as Nações concordaram que um ciberataque poderá desencadear a invocação do artigo 5, sendo necessária a avaliação pelo Conselho de caso para caso[98]. Isto representa uma nova mudança no seio da Aliança pois se nos recordarmos do caso da Estónia, onde não se agiu sob a jurisdição do artigo 5 por falta de danos "reais", atualmente é reconhecido que os impactos das atividades cibernéticas maliciosas podem constituir um ataque armado.

Em junho de 2022, deu-se a Cimeira de Madrid onde foi aprovado o novo Conceito Estratégico da NATO. Este focava-se, maioritariamente, no reconhecimento da Rússia como a ameaça mais significativa à segurança da Aliança à luz dos acontecimentos com a Ucrânia, mas também identifica o ciberespaço e as tecnologias emergentes e disruptivas como uma ameaça que necessita de ser contida através da cooperação e do compromisso de adoção que todos devem assumir relativo à ciberdefesa[99].

Em setembro, o Estado-Maior-General das Forças Armadas (EMGFA) foi vítima de um ciberataque que resultou no desvio de documentos classificados da NATO que outrora

---

[97] "Exercício CIBER PERSEU 19" *Academia Militar*. Disponível em: https://academiamilitar.pt/ciberperseu-19.html

[98] "Cimeira da NATO: Impacto para a BTID" *idD Portugal Defence,* 2021. Disponível em: https://www.iddportugal.pt/cimeira-nato-impacto-btid/

[99] "Conceitos Estratégicos" *NATO,* 2022. Disponível em: https://www.nato.int/cps/en/natohq/topics_56626.htm

tinham sido enviados a Portugal[100]. O Serviço de Informações dos EUA alertou as entidades portuguesas que os documentos estavam expostos na *dark web*[101], facto que comprometeu as informações classificadas como confidenciais. Estas situações colocam em causa a credibilidade de uma nação, mostrando o quão fundamental é a prevenção, bem como a cooperação entre organizações nacionais e internacionais.

A NATO tem vindo a combater o terrorismo há várias décadas e prevenir o ciberterrorismo deve ser simplesmente uma extensão da sua política atual. Denote-se que a ameaça terrorista de índole fundamentalista islâmica que ganhou mais mediatismo e requereu mais medidas de segurança desde o início do século XXI, era, por si só, complexa e alarmante, mas hoje estamos perante perigos muitos maiores e em várias frentes. A ciberdefesa está cada vez mais exposta a ameaças iminentes e, nesse sentido, deve ser trabalhada e potencializada por OI como a Aliança Atlântica.

[100] "Documentos portugueses da NATO apanhados à venda na darkweb" *Diário de Notícias*, 2022. Disponível em: https://www.dn.pt/sociedade/documentos-portugueses-da-nato-apanhados-a-venda-nadarkweb--15146671.html

[101] A *dark web* é o coletivo oculto de sites da Internet acessíveis apenas por um navegador especializado. É usada para manter a atividade da internet anónima e privada, o que pode ser útil em aplicativos legais e ilegais. Enquanto alguns a usam para evitar a censura do governo, também é conhecida por ser utilizada para atividades altamente ilegais.
Disponível em: https://www.kaspersky.com/resource-center/threats/deep-web

4. Recomendações

Com base no estudo realizado e de forma a aprofundar os temas tratados através do conhecimento e experiência de diversos especialistas e entidades que atuam na área da cibersegurança e áreas conexas, foram entrevistados, quer por escrito, quer presencialmente, o Professor Doutor José Tribolet, Professor Catedrático do Instituto Superior Técnico (IST), a Dra. Dalila Araújo, vice-Presidente do Observatório de Segurança, Criminalidade Organizada e Terrorismo (OSCOT), o Dr. João Pacheco, Fundador e CEO da empresa Cyberprotech, o Dr. José Casinha, Chief Information Security Officer da empresa OutSystems, o Dr. Bruno Castro, fundador e CEO da empresa VisionWare, o Dr. Francisco Nina Rente, cofundador da empresa Art Resilia e da empresa The Rock - Cybsecurity, o Sistema de Informações e Segurança (SIS) e o Dr. Pedro Mendonça, coordenador do Observatório de Cibersegurança do Centro Nacional de Cibersegurança (CNCS). Foram ainda solicitadas entrevistas a outras personalidades e instituições que se encontram identificadas na Tabela 4 do Apêndice V, mas das quais não foi possível receber resposta.

O guião das entrevistas e as respostas encontram-se, respetivamente, nos Apêndices II e III. O Apêndice IV consiste na análise de conteúdo das entrevistas. Como resultado desta metodologia, sistematizou-se um conjunto de recomendações que se apresentam no presente capítulo.

O ciberespaço é, cada vez mais, um ambiente estratégico para a segurança dos Estados, sendo o ciberpoder um importante índice para avaliar as suas capacidades de ataque e de defesa. A cibersegurança deverá constituir uma prioridade da agenda política dos Estados, atendendo à evolução vertiginosa dos ataques cibernéticos nas duas últimas décadas.

A sofisticação das técnicas de ataque e o incremento dos meios tecnológicos ao dispor das organizações terroristas poderão, num futuro próximo, conseguir provocar danos de magnitude igual ou superior aos do ataque terrorista de 11 de setembro nos EUA. Se um ataque tão paradigmático como esse ocorresse no ciberespaço, teria o poder de parar o mundo.

Vivemos numa era onde a informação é considerada um trunfo que devemos preservar a todo o custo. Importa não esquecer que grande parte das informações, seja a nível estatal,

organizacional e civil, estão armazenadas no ciberespaço, o que as torna suscetíveis a ciberataques que as podem desviar, danificar ou destruir. A proteção das infraestruturas digitais deve estar presente nas estratégias de cibersegurança dos Estados, na medida em que poderemos sofrer um ciberataque massivo que comprometa a integridade dos dados pessoais dos cidadãos, o que colocará em causa o ordenamento do espaço virtual, afetando o funcionamento da sociedade, e, no limite, causar uma severa crise social.

No que toca às OI, estas funcionam como as "guardiãs" dos seus membros, pelo que deverão continuar a melhorar as suas políticas de proteção e prevenção do ciberespaço. O caminho traçado pelas organizações estudadas, a UE e a NATO, contribuiu para serem consideradas como um exemplo a seguir em todo o mundo. No entanto, é necessário reforçarem a sua cooperação, adotando uma comunicação mais transparente para aumentar a eficácia da defesa aos ataques que têm uma natureza híbrida, isto é, os ataques ao mundo físico são complementados com os ataques ao mundo virtual. Deste modo, o planeamento coordenado e a partilha de informação assumem particular importância pois, sem estes, tornar-se-á muito mais difícil construir uma frente que não vergue aos desafios atuais.

A dimensão global do ciberespaço não é compatível com a prática de uma cultura de defesa isolacionista, ou seja, o facto de se proteger apenas um determinado número de pessoas ou países não assegura a sua invulnerabilidade a ataques cibernéticos. Deve-se adotar uma filosofia de proteger os seus, mas também proteger todos, pois só assim veremos conquistas concretas na área da segurança e da defesa. A criação de sinergias a nível internacional é fundamental e, neste sentido, também o é a utilização de metodologias cruzadas entre os organismos, recorrendo à combinação das respetivas ferramentas tecnológicas.

Respeitando uma ordem *top-down*, tanto a UE como NATO, devem continuar a desenvolver políticas e a emanar orientações no âmbito da cibersegurança para serem implementadas pelos seus EM. No caso da UE, é fundamental prosseguir na melhoria dos instrumentos jurídicos, como se observou com a Diretiva da Segurança das Redes e da Informação (SRI) e com o Regulamento Geral sobre a Proteção de Dados (RGPD). Também se conclui que é necessária a aplicação da regulamentação da cibersegurança às empresas do setor privado em geral, questão que não se encontra ainda legislada. As

vulnerabilidades existentes neste setor foram bastante visíveis no período da pandemia, pelo que urge implementar mecanismos adicionais de segurança aos já existentes.

No caso da NATO, tendo esta organização uma doutrina mais defensiva do que a UE, deve continuar a focar a sua missão na preparação cibernética através de exercícios e de simulações que ajudem os seus membros a maturarem as suas capacidades de ciberdefesa, tendo sempre em vista o objetivo comum: a proteção e a prevenção.

Em Portugal, a cibersegurança ainda é vista como um tema com muita margem para evoluir, sendo necessário fazer um maior esforço a nível nacional de forma a afirmarmo-nos no ciberespaço como uma nação mais preparada para o futuro. Um dos aspetos fundamentais a considerar é a implementação de um adequado ordenamento jurídico do espaço virtual, sendo muito importante o desenvolvimento de um inventário de entidades informacionais, estruturado segundo regras constitutivas próprias e arquivado em segurança.

Por outro lado, Portugal apresenta ainda um défice de ferramentas tecnológicas que é necessário superar de modo a acompanhar a constante evolução das tecnologias, pois as que estão a ser utilizadas revelam-se insuficientes à luz dos últimos ataques cibernéticos durante o ano de 2022.

Em termos de políticas de segurança e de defesa, há ainda um longo caminho a percorrer, quer em termos legislativos, quer em termos de sensibilização dos cidadãos. Sendo certo que estão bem definidas as normas e orientações que as forças militares e de segurança devem cumprir em caso de ataques por terra, mar e ar, não se encontram ainda suficientemente densificadas as ações a tomar em caso de ciberataques massivos.

O conceito de defesa em Portugal tem sido interpretado, tradicionalmente, como a defesa do território físico. No entanto, face ao aumento dos ciberataques que temos vindo a sofrer bem como ao crescente perigo das suas consequências, é fundamental o aumento da nossa ciberesiliência que passará por uma distribuição de responsabilidades pelos diversos organismos que atuam nesta área (serviços de informações, estruturas judiciais, Forças Armadas, Centro Nacional de Cibersegurança, rede nacional de CSIRT e empresas de cibersegurança, entre outros) bem como uma adequada articulação entre todos.

Portugal não sofreu, ainda, um ataque ciberterrorista de grande extensão, mas importa sublinhar que os fenómenos de cibercriminalidade como o *ransomware*, o *phishin*g e o

cyberbullying têm aumentado de forma exponencial, sobretudo durante e após a pandemia de Covid-19.

A formação da sociedade civil e o seu envolvimento em ações com vista à sensibilização e conhecimento do ciberespaço devem ser objetivos de carácter prioritário para qualquer Estado. As campanhas de sensibilização para os perigos no ciberespaço contribuem, de forma significativa, para a defesa dos ciberataques dado que, se um cidadão estiver informado e adotar as medidas de segurança que lhe foram ensinadas, estará em condições de proteger o ciberespaço.

É notório o hiato que existe entre a evolução da tecnologia e a formação das pessoas e que deve ser urgentemente diminuído, na medida em que as sociedades tornar-se-ão cada vez mais digitais. Num contexto de uma guerra virtual, todos nós, como intervenientes no ciberespaço, temos a responsabilidade de conhecermos os seus perigos. Para que tal aconteça, é necessário haver um reforço na formação e na educação dos cidadãos de modo a aumentar a sua perceção sobre os danos que um ciberataque poderá gerar. Da mesma forma que somos educados a não atravessar a estrada quando o semáforo está vermelho, também deveremos aprender a razão da cibersegurança ser tão determinante para o bom funcionamento da sociedade.

Neste âmbito, será necessário mobilizar recursos tecnológicos e financeiros para que as pessoas aprendam a proteger-se, ou seja, é necessário evoluir para o conceito de "defesa popular" que se aplica na defesa do território físico. Se pensarmos nos ciberataques já perpetuados a infraestruturas críticas de vários países, concluímos que é urgente criar ou aumentar os "exércitos" de cibernautas para assegurar a segurança dos Estados.

Conclusão

Como foi possível verificar ao longo da dissertação, o fenómeno da guerra está em constante evolução, a par com a evolução tecnológica que introduziu novas formas de ameaças e riscos na segurança das nações, de que o ciberterrorismo é um bom exemplo.

A transição digital criou o ciberespaço, um novo domínio operacional que se constitui, cada vez mais, como um meio facilitador de ações terroristas. Com a análise que foi feita ao longo da dissertação, demonstrou-se que, no séc. XXI, o terrorismo e a sua extensão tecnológica, o ciberterrorismo, assumem uma crescente importância nas sociedades contemporâneas pela sua maior dependência do ciberespaço. Para uma melhor perceção das dinâmicas que estão na base do ciberterrorismo, identificaram-se os agentes geradores de ameaças que atuam no ciberespaço, podendo agrupar-se em atores estatais, organizações criminosas e indivíduos – habitualmente designados de *hackers*.

Os atores estatais desempenham um papel determinante, quer seja na vertente ofensiva, quer seja na vertente defensiva, na medida em que têm ao seu dispor recursos humanos, tecnológicos e financeiros que lhes permitem desencadear ataques cibernéticos de elevada magnitude. Conforme se analisou nos casos de estudo apresentados, os ataques à Estónia (2007) e à Geórgia (2008) perpetrados pela Rússia infligiram danos e prejuízos significativos a estes países. Também o ataque ao Irão, alegadamente desencadeado pelos EUA e Israel, foi bem elucidativo do quanto o ciberpoder dos Estados é fundamental para atingir objetivos de defesa.

Relativamente às organizações criminosas, concluiu-se que as suas atividades cibercriminosas têm, frequentemente, motivações político-ideológicas, observando-se uma aposta na propaganda com vista ao recrutamento de pessoas e ao *crowdfunding* das suas ações, de modo a expandirem-se para além das fronteiras físicas. É o caso da organização terrorista Al-Qaeda que combina a propaganda no ciberespaço com as tecnologias avançadas de comunicação para alcançar uma maior diversidade de audiências.

Os *hackers* são, na sua maioria, indivíduos que levam a cabo um tipo de cibercriminalidade com objetivos de extorsão financeira, de interrupção de serviços de comunicações ou de obtenção de informação privilegiada, através de várias tipologias de ataques, desde o *phishing* ao *randsomware.* Os "hacktivistas", como os *Anonymous,* são

grupos que agem contra organismos estatais ou privados para combaterem o que consideram ser violações dos direitos de um povo. Conclui-se, assim, que há uma linha bastante ténue que separa as ações que se podem classificar de ciberterrorismo daquelas provenientes do "hacktivismo", sendo que a distinção apenas poderá ser claramente feita através da análise dos objetivos subjacentes aos ataques e ao *modus operandi* utilizado.

O ataque cibernético massivo à Estónia foi paradigmático e constituiu uma viragem na forma como os Estados e as OI passaram a tratar os temas do ciberterrorismo e da cibersegurança, tendo contribuído para o desenvolvimento das suas estratégias de defesa e segurança neste domínio. O ciberespaço constituiu-se como um novo "campo de batalha" que urgia defender, tornando-se uma prioridade para a UE e para a NATO a implementação de políticas mais consentâneas face a uma nova realidade.

A considerável evolução no que concerne às políticas de segurança e defesa no ciberespaço posicionou a UE como uma autoridade reconhecida a nível internacional nesta matéria. Foram criadas instituições como a Agência da União Europeia para a Cibersegurança (ENISA) e a Agência da União Europeia para a Cooperação Policial (EUROPOL), que constituem excelentes exemplos para a necessária articulação entre os diversos EM da UE para lidar com o ciberterrorismo.

Também os avultados investimentos em meios tecnológicos contribuíram para que a UE se assumisse com um exemplo a nível global. Presentemente, a UE encontra-se a rever a Diretiva Relativa à Segurança das Redes e da Informação (SRI), com vista a melhorar a resposta face à evolução das ameaças que foi catalisada pelo período pandémico. Pretende-se que a nova legislação venha reforçar a gestão e a cooperação dos EstadosMembros no que respeita aos riscos e incidentes cibernéticos, bem como alargar o âmbito da aplicação das regras de cibersegurança a um conjunto de atores que não se encontram ainda abrangidos, como é o caso das empresas privadas na sua generalidade. Denotou-se, ao longo do estudo, o carácter dinâmico das matérias relacionadas com o ciberespaço, o que obriga a que as OI as acompanhem de uma forma contínua e empenhada.

Relativamente à NATO, considerada como a organização internacional que mais recursos tem mobilizado no combate às ameaças cibernéticas e na proteção do ciberespaço, desenvolver organismos – como o Centro de Excelência NATO para a Ciberdefesa

Cooperativa (CCDCOE), o Centro de Operações do Ciberespaço (CyOc), a Agência de Comunicações e Sistemas de Informações da NATO (NCIA) –, que têm vindo a fortalecer as vertentes da cibersegurança e ciberdefesa com sucesso.

A cooperação internacional, nomeadamente entre a NATO e a UE, é uma das pedras basilares para o sucesso da implementação das suas políticas de segurança e defesa e das quais Portugal é beneficiário enquanto membro das duas organizações. Deste modo, revela-se fulcral que ambas continuem a partilhar informações, métodos e ferramentas para que seja possível travar e evitar ciberataques como os que se descreveram nesta dissertação.

Portugal dispõe em território nacional, desde 2020, da Academia de Comunicações e Sistemas de Informações da NATO, que proporciona treinos e formação na área da cibersegurança, como é também vocacionada para reforçar o desempenho português nas missões da Aliança. O exercício "CIBER PERSEU", da responsabilidade das Forças Armadas portuguesas, destinou-se a avaliar a capacidade de resposta face à ocorrência de ciberataques de âmbito nacional e internacional, que podem escalar para uma crise no ciberespaço. Nesta dissertação foi também abordado o papel determinante das instituições portuguesas em matéria de cibersegurança, entre as quais se destacam o CNCS, o OSCOT, o SIS e o IDN.

Salienta-se que a cibersegurança e a ciberdefesa são áreas interdependentes e complementares que incluem um "conjunto de atividades que ocorrem no ciberespaço, de prevenção, monitorização e reação a ameaças" (IDN, 2018). No entanto, o conceito de cibersegurança difere do conceito de ciberdefesa, sendo o primeiro vocacionando para a defesa das ameaças que coloquem em risco o bem-estar e a salvaguarda dos direitos dos cidadãos e a ciberdefesa é entendida como a defesa das ameaças que coloquem em perigo a soberania da nação.

Com base nas pesquisas e análises realizadas na presente dissertação, foi identificado um conjunto de especialistas e entidades públicas e privadas que atuam na área da cibersegurança e áreas conexas a quem foi proposta uma entrevista estruturada. As entrevistas tiveram como objetivo aprofundar os conhecimentos adquiridos, cujas respostas muito contribuíram para selecionar um conjunto de recomendações relevantes baseadas no conhecimento e na experiência dos interlocutores.

As recomendações abrangem diversas áreas, destacando-se i) a necessidade de priorização das políticas dos Estados no que respeita à cibersegurança, ii) o reforço do papel das OI na prossecução e implementação dessas políticas, iii) a importância da cooperação ao nível internacional para além da já estabelecida entre a UE e a NATO envolvendo também outras potências mundiais, iv) a melhoria da legislação que regula os vários atores do ciberespaço, e v) a sensibilização e formação dos cidadãos para a prevenção e defesa dos ciberataques.

No diagnóstico feito pela maioria dos entrevistados, sublinha-se o estado ainda deficitário do desenvolvimento da cibersegurança em Portugal, concluindo-se que o nosso país tem ainda um caminho longo a percorrer nesta matéria. Considera-se determinante para a segurança e defesa de Portugal no ciberespaço a mobilização de mais recursos quer humanos, quer tecnológicos, quer financeiros que reforcem os organismos com competências nestas áreas, incluindo as próprias Forças Armadas que devem desempenhar um papel mais preponderante na ciberdefesa da nação.

Depreendeu-se ao longo do estudo feito que, atualmente, há uma facilidade preocupante no acesso ilegal a informações privilegiadas dos Estados que podem criar, no limite, crises de soberania. Até ao ano de 2024, espera-se que mais de 22,3 mil milhões de dispositivos em todo o mundo estejam ligados à Internet[102], sendo fácil de antever o aumento da competição entre os atores do ciberespaço na procura de novos meios de comunicação, novas tecnologias, novas táticas cibernéticas, em suma, na procura de novas formas de usar e exponenciar o seu ciberpoder.

O ciberterrorismo é um perigo real e imediato. Devemos encará-lo como uma tática de guerra no séc. XXI com um potencial para alcançar níveis de destruição que ainda são inimagináveis, mas que podem deixar de o ser a curto prazo. Um ataque ciberterrorista massivo poderá causar danos bem superiores aos causados pelos ataques terroristas "tradicionais", sendo premente a adoção de uma cultura de proteção cibernética cada vez mais eficiente. Este fenómeno criou tensões nas relações internacionais difíceis de controlar, estaremos sempre a um *click* de uma ciberguerra. Torna-se, assim, primordial que o mundo se prepare para esta realidade, pois à luz de todos os acontecimentos estudados, é algo que poderá a acontecer a qualquer momento.

[102] "Cibersegurança: como combate a UE as ciberameaças" *Conselho da União Europeia*. Disponível em: https://www.consilium.europa.eu/pt/policies/cybersecurity/

Bibliografia

Livros:

Barrinha, André e Helena Carrapiço. "Cibersegurança". *Segurança Contemporânea*, Pactor, 2016.

Clarke, Richard A., e Robert Knake. "Cyber war: the next threat to national security and what to do about it". 2º edição. *HarperCollins*. New York, 2012.

Clausewitz, Carl Von. "Da Guerra". *Edições Europa/América*. Lisboa, 1997.

Duque, Raquel, Diogo Noivo e Teresa Almeida e Silva. "Segurança Contemporânea". *Pactor*, 2016.

Guiora, N. Amos. "Global Perspectives on Cyber Security". *Routledge Editors*, 2017.

Kaldor, Mary. "New and Old Wars – organized violence in a global era". *Stanford University Press*, 3º Edição, 2012.

Nye, Joseph. "Cyber Power". *Cambridge: Belfer Center for Science and International Affairs*. Harvard Kennedy School, 2010.

Sanger, David. "Confront and conceal: Obama's secret wars and surprising use of American power". *Crown Publishes*. New York, 2012.

Sanger, David. "The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age". *Crown Publishes*. New York, 2018.

Singer, Peter e Allan Friedmann. "Cybersecurity and Cyberwar: What Everybody Needs to Know". *Oxford: Oxford University*, 2014.

Taylor, W. Robert. "Cybercrime and Cyberterrorism". *Pearson Editors*, 2017.

Weimann, Gabriel. "Cyberterrorism. How Real is the Threat?" *United States Institute of Peace*. Washington, 2004.

Whittaker, David J. "The Terrorism Reader". *Routledge*. New York, 2001.

Artigos científicos:

Couto, Abel Cabral. "Elementos de Estratégia". *IAEM*. Lisboa, 1989. Cravo, Teresa Almeida. "Mudanças e continuidades na conceptualização da guerra". *Janus*, 2014.

Danchev, Dancho. "Coordinated Russia vs Georgia cyberattack in progress" *ZDNET*, 2008.

Farwell, James e Rafal Rohozinski. "Stuxnet and the Future of Cyber War". *Survival*, 2011.

Foltz, Andrew. "Stuxnet, Schmitt Analysis, and the Cyber 'Use-of-Force" Debate. *JFQ*, 2012.

Hollis, David. "Cyberwar Case Study: Georgia 2008". *Small Wars Journal*, 2011.

Nunes, Viegas. "Ciberterrorismo: Aspetos de Segurança." *Revista Militar*, nº10, 2004.

Pereira, João Paulo. "Os Conflitos do Pós-Guerra Fria, Novas ou Velhas Guerras?" *Revista Militar* nº2630, 2021.

Santos, Lino e Armando Guedes. "Breves reflexões sobre Poder e Ciberespaço". *Revista de Direito e Segurança* nº6, 2015.

Shakarian, Paulo. "The 2008 Russian Cyber Campaign Against Georgia". *Academia*, 2011.

Tomé, António. "A Segurança e a Defesa no Ciberespaço". *ResPublica,* nº15, 2015.

Relatórios/Declarações de Organizações Nacionais e Internacionais:

"Active Engagement, Modern Defence" *NATO*, 2010.
Disponívelem:https://www.nato.int/cps/fr/natohq/official_texts_68580.htm?selectedLocale=en

"A Estratégia de Cibersegurança para Portugal" *Centro de Investigação Jurídica do Ciberespaço*, 2015.
Disponível em: https://www.cijic.org/2015/10/09/a-estrategia-de-ciberseguranca-paraportugal/

"Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective" Rain Ottis, *CCDCOE*.
Disponívelem:https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf

"A nova estratégia para o Mercado Único Digital da União Europeia" *EUR-LEX*, 2015.
Disponívelem:https://eur-lex.europa.eu/legalcontent/PT/TXT/?uri=LEGISSUM:3102_3

"A proteção de dados na UE" *Comissão Europeia*, 2016.
Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/data-protectioneu_pt

"A Strategy for a Secure Information Society – Dialogue, partnership and empowerment" *Commission of the European Communities*, 2006.
Disponívelem:https://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0251:FIN:EN:PDF

"Cibersegurança" *Instituto da Defesa Nacional (IDN)* caderno nº133, 2012.
Disponívelem:https://www.idn.gov.pt/pt/publicacoes/nacao/Documents/NeD133/NeD133.pdf

"Contributos para uma Estratégia Nacional de Ciberdefesa" *Instituto da Defesa Nacional (IDN)* caderno nº28, 2018.
Disponívelem:https://www.idn.gov.pt/pt/publicacoes/idncadernos/Documents/2018/idncadernos_28.pdf

"Convention on Cybercrime" *Conselho da Europa*, 2001.
Disponível em: https://rm.coe.int/1680081561

"Cyber Defence at the 28th NATO Summit in Brussels, 11-12 July 2018" *CCDCOE*, 2018. Disponível em: https://ccdcoe.org/incyder-articles/cyber-defence-at-the-28thnato-summit-in-brussels-11-12-july-2018/

"Cyber Security Strategy" *Ministry of Defence*, 2008. Disponível em: file:///C:/Users/Utilizador/Downloads/EE_NCSS_2008_en.pdf

"Diretiva do Parlamento Europeu e do Conselho relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União" *EURLEX*,2016.
Disponívelem:https://eurlex.europa.eu/legalcontent/PT/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.POR&toc=OJ:L:2016:194TOC

"EISAS Basic Toolset" *ENISA*, outubro 2011.
Disponível em: https://www.enisa.europa.eu/publications/eisas-basic-toolset

"ENISA Threat Landscape 2021" *ENISA*, outubro 2021.
Disponível em: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021.

"Enquadramento da Ciberdefesa" *República Portuguesa – Defesa Nacional,* 2018.
Disponível em: https://www.defesa.gov.pt/pt/pdefesa/ciberdefesa/enquadramento

"Estratégia da Informação e Segurança no Ciberespaço". *Instituto Nacional de Defesa (IDN)*. Caderno nº12, 2013.
Disponívelem: https://comum.rcaap.pt/bitstream/10400.26/7757/1/idncaderno_12.pdf

"Estratégia da União Europeia para a cibersegurança: um ciberespaço aberto, seguro e protegido", *Comissão Europeia*, 2013.

Disponívelem:https://eurlex.europa.eu/legalcontent/PT/TXT/PDF/?uri=CELEX:52013JC0001&from=PT

"Estratégia de Segurança interna da União Europeia – Rumo a um modelo europeu de segurança" *Conselho da União Europeia*, 2010.

Disponível em: https://www.consilium.europa.eu/media/30754/qc3010313ptc.pdf

"Estratégia Europeia em Matéria de Segurança – Uma Europa segura num mundo melhor" *Conselho da União Europeia*, 2008.
Disponível em: https://www.consilium.europa.eu/media/30824/qc7809568ptc.pdf
"European Union Terrorism Situation and Trend Report" *Europol*, 2021.
Disponívelem:https://www.europol.europa.eu/cms/sites/default/files/documents/tesat_2021_0.pdf

"Exercício CIBER PERSEU 19" *Academia Militar*.
Disponível em: https://academiamilitar.pt/ciber-perseu-19.html

"Exercise Locked Shields 2022 Concludes" *nc-NATO*, 2022.
Disponível em: https://shape.nato.int/news-archive/2022/exercise-locked-shields-2022concludes

"Global Terrorism Index 2020: Measuring the Impact of Terrorism" *Institute for Economics & Peace*, 2020.
Disponível em: http://visionofhumanity.org/reports

"Medidas restritivas da UE contra o Irão" *Conselho da União Europeia*, 2014.
Disponível em: https://www.consilium.europa.eu/pt/policies/sanctions/iran/

"M-Trends 2021" *Fireeye Mandiant Services*, 2021.
Disponível em: https://content.fireeye.com/m-trends/rpt-m-trends-2021

"NATO'S Cyber Security Centre" *NCIA-NATO*.
Disponível em : https://www.ncia.nato.int/what-we-do/cyber-security.html

"New CERTs Inventory and updated may now available" *ENISA*, 2013.
Disponível em: https://www.enisa.europa.eu/news/enisa-news/new-certs-inventory-andupdated-map-now-available

"Nova estratégia de cibersegurança da UE e novas regras para aumentar a resiliência das entidades críticas físicas e digitais – Perguntas e respostas" *Comissão Europeia*, 2020.
Disponívelem:https://ec.europa.eu/commission/presscorner/detail/pt/qanda_20_2392#cybersecurity

"Prague Summit 2002 – Selected Documents and Statements" *NATO*, 2002.
Disponível em: https://www.nato.int/docu/0211prague/speeches-e.pdf

"Rede Nacional de CSIRT" *Centro Nacional de Cibersegurança*.
Disponível em: https://www.cncs.gov.pt/pt/csirt/

"Regime Jurídico" *Centro Nacional de Cibersegurança*.
Disponível em: https://www.cncs.gov.pt/pt/regime-juridico/

"Relatório Cibersegurança em Portugal – Economia" *Centro Nacional de Cibersegurança*, maio 2022.
Disponível em: https://www.cncs.gov.pt/docs/relatorio-economia2022-obciber-cncs.pdf
"Relatório Riscos & Conflitos 2020", *Centro Nacional de Cibersegurança*, junho 2020.
Disponível em: https://www.cncs.gov.pt/docs/relatorio-riscos-conflitos-2020.pdf

"Relatório sobre o estado das capacidades de ciberdefesa" *Parlamento Europeu,* 2021.
Disponível em: https://www.europarl.europa.eu/doceo/document/A-9-20210234_PT.html

"Riga Summit Declaration" *NATO*, 2006.
Disponívelem:https://www.nato.int/cps/en/natohq/official_texts_37920.htm?selectedLocale=en

"Terrorismo e Violència Política" *Instituto da Defesa Nacional (IDN)* nº152, 2019.
Disponível em: https://www.idn.gov.pt/pt/publicacoes/nacao/Paginas/NeD152.aspx

"The Tallin Manual", *Centro de Excelência da NATO para a Ciberdefesa Cooperativa (CCDCOE).*
Disponível em: https://ccdcoe.org/research/tallinn-manual/

"Wales Sumit Declaration" *NATO,* 2014.
Disponível em: https://www.nato.int/cps/en/natohq/official_texts_112964.htm

"2007 cyber-attacks on Estonia" *NATO StratCom*, junho 2019.
Disponível em: https://stratcomcoe.org/cuploads/pfiles/cyber_attacks_estonia.pdf

"V Seminário IDN Jovem" *Instituto da Defesa Nacional (IDN),* caderno º36, 2019.
Disponívelem:https://www.idn.gov.pt/pt/publicacoes/idncadernos/Documents/Texto%20integral/idncadernos_36.pdf

Outros conteúdos online:

"Estonia is a digital society" *Visit Estonia*, setembro 2020.
Disponível em: https://www.visitestonia.com/en/why-estonia/estonia-is-a-digitalsociety

"How it all began? From Tiger Leap to digital society" *Education Estonia*. Disponível em: https://www.educationestonia.org/tiger-leap/

"O que é o WannaCry?" *Avast Academy*, fevereiro 2020.
Disponível em: https://www.avast.com/pt-br/c-wannacry

"This is the story of the world's most advanced digital society" *e-Estonia*. Disponível em: https://e-estonia.com/story/

"What is the Deep and Dark Web?" *Kaspersky*, 2018.
Disponível em: https://www.kaspersky.com/resource-center/threats/deep-web
Imprensa:

"Ataque Impresa: como um sistema vulnerável destrói parte da memória cultural de um país" *It Security,* fevereiro 2022.
Disponível em: https://www.itsecurity.pt/news/x-ray/ataque-impresa-como-um-sistemavulneravel-destroi-parte-da-memoria-cultural-de-um-pais

"Decreto-lei 65/2021: um pequeno passo para o homem, um salto gigante para as organizações nacionais" *It Security*, 2022.
Disponível em: https://www.itsecurity.pt/news/compliance/decreto-lei-652021-umpequeno-passo-para-o-homem-um-salto-gigante-para-as-organizacoes-nacionais

"Documentos portugueses da NATO apanhados à venda na darkweb" *Diário de Notícias*, 2022. Disponível em: https://www.dn.pt/sociedade/documentos-portugueses-da-natoapanhados-a-venda-na-darkweb--15146671.html

"Estratégia Nacional de Segurança do Ciberespaço" *Portugal Digital*, 2019.
Disponível em: https://portugaldigital.gov.pt/acelerar-a-transicao-digital-emportugal/conhecer-as-estrategias-para-a-transicao-digital/estrategia-nacional-deseguranca-do-ciberespaco/

"Expert: Cyber-attacks on Georgia websites tied to mob Russian government" *Los Angeles Times*, 2008.
Disponível em: https://www.latimes.com/archives/blogs/technology-blog/story/200808-13/expert-cyber-attacks-on-georgia-websites-tied-to-mob-russian-government

HELLER, Nathan. "Estonia, the Digital Republic". *The New Yorker,* 2017.
Disponível em: https://www.newyorker.com/magazine/2017/12/18/estonia-the-digitalrepublic

"Serbs lauch cyberattack on NATO" *FCW*, 1999.
Disponível em: https://fcw.com/1999/04/serbs-launch-cyberattack-on-nato/195288/

"Vodafone Portugal diz que foi alvo de ato terrorista" *IT Security,* fevereiro 2022. Disponível em: https://www.itsecurity.pt/news/news/vodafone-portugal-foi-alvo-deciberataque

Apêndices

Apêndice I

Tabelas cronológicas dos trabalhos cibersecuritários na UE e na NATO

União Europeia	
2001	Convenção de Budapeste (Convenção do Cibercrime)
2004	Criação da ENISA
2006	Implementação do EISAS
2007	Ataques cibernéticos à Estónia
2008	Estratégia Europeia em Matéria de Segurança
2010	Revisão da Estratégia em Matéria de Segurança
2012	Criação dos CERT-UE
2013	Estratégia Europeia para a Cibersegurança
2015	Estratégia digital de Mercado Único
2016	Elaboração da Diretiva Europeia SRI
2018	Implementação do RGPD
2020	Revisão da Estratégia Europeia para a Cibersegurança
2021	Estratégia de Cibersegurança da UE para a década digital
2022	Revisão da Diretiva SRI (SRI 2)

Tabela 1 – Ordem cronológica dos trabalhos cibersecuritários na União Europeia

NATO	
2002	Cimeira de Praga
2004	Criação do NCIRC
2006	Cimeira de Riga
2007	Ataques cibernéticos na Estónia
2008	CCDCOE / 1º edição do Manual de Tallinn
2010	Cimeira de Lisboa / Novo Conceito Estratégico / 1º *Locked Shields*
2012	Cimeira de Chicago / Criação da NCIA
2014	Cimeira de Gales
2016	Cimeira de Varsóvia / *Cyber Defense Pledge*
2018	Cimeira de Bruxelas / Criação do CyOc / Declaração de Cooperação EU-NATO
2020	Inauguração da Academia de Comunicações e Sistemas de Informações da NATO em Oeiras
2021	Cimeira de Bruxelas / *Comprehensive Cyber Defence Policy*
2022	Cimeira de Madrid / Novo Conceito Estratégico

Tabela 2 - Ordem cronológica dos trabalhos cibersecuritários na NATO

Apêndice II

Guião matriz de entrevistas

Guião matriz de entrevistas

1. Como caracteriza o ciberespaço em termos de potencialidades e vulnerabilidades?

2. Considera possível acontecer no ciberespaço um ataque tão paradigmático como outro 9/11?

3. Qual deveria ser a prioridade no ramo da cibersegurança dos Estados?

4. Na sua ótica, como é que podem as Organizações Internacionais, como a UE e a NATO prevenir e proteger os seus Estados-membros de ciberataques terroristas?

5. Considera que Portugal, nomeadamente a vertente estatal encarregada pela proteção contra estas ameaças, encara o ciberterrorismo como uma ameaça real?

Apêndice III

Entrevistas

Entrevista

Prof. Doutor José Tribolet

(Professor Catedrático do Instituto Superior Técnico – IST)

1.Como caracteriza o ciberespaço em termos de potencialidades e vulnerabilidades?

2.Considera possível acontecer no ciberespaço um ataque tão paradigmático como outro 9/11?

3.Qual deveria ser a prioridade no ramo da cibersegurança dos Estados?

4.Na sua ótica, como é que podem as Organizações Internacionais, como a UE e a NATO prevenir e proteger os seus Estados-membros de ciberataques terroristas?

5.Considera que Portugal, nomeadamente a vertente estatal encarregada pela proteção contra estas ameaças, encara o ciberterrorismo como uma ameaça real?

O espaço virtual é populado por entidades. Tal como as frases que construímos na nossa linguagem corrente, na qual usamos nomes e verbos, no espaço virtual temos as entidades virtuais (nome) e os verbos (ações ou funcionalidades que se podem desencadear). O espaço virtual é, assim, formado por um sistema de muitas entidades que estão interligadas em rede, ocorrendo dinâmicas que o fazem funcionar em conjunto.

Nas organizações, para que o seu funcionamento seja adequado, deve existir um nível de *awareness* (*entreprise self awareness)* suficiente, ou seja, aplica-se o conceito de "consciência de si" e cada empresa deve ter um grau específico desta consciência. Este conhecimento é ajudado com o *empowerement* que a tecnologia colocou ao nosso dispor.

Fazendo uma analogia com o mundo físico, onde visualizamos o mundo que existe ao nosso redor (prédios, pessoas, etc.) e as suas interações, também o mundo virtual tem "coisas" que se traduzem por "n" suportes tecnológicos que se relacionam entre si e que vão alterando o seu estado momento a momento. Tanto os indivíduos como as organizações vivem, cada vez mais, no espaço virtual à medida que a tecnologia vai evoluindo. Ou seja, o mundo físico e o virtual estão cada vez mais sincronizados, os eventos no primeiro repercutem-se no segundo e vice-versa com cada vez mais velocidade.

O dia-a-dia das pessoas e organizações passa-se, ocorre e depende das atividades no ciberespaço. Também as técnicas de guerra foram evoluindo, ao longo dos anos, sendo cada vez mais sofisticadas, vivendo-se agora tempos onde o ciberespaço é um espaço natural para utilizar os novos instrumentos de ataque. Por pouco dinheiro se conseguem desenvolver instrumentos que podem ser armas poderosas para causar graves danos e mortes.

Vivemos hoje na era biónica, uma combinação da era biológica com a era eletrotónica, a vida futura tem a base do carbono (a base biológica) e a base de sílica/ótica/quântica que é a base com que funcionam os computadores.

--

O ordenamento do território é fundamental para um coletivo humano ter consciência do património que tem, do que precisa para viver, dos seus *assets*, da maneira como estão organizados e quais as regras para sua adequada utilização.

A humanidade tem um património importante de pensamento jurídico, de pensamento sobre ordenamento do território. Para vivermos em sociedade é necessário um mínimo de ordenamento, de "arrumação" que nos permita ter comportamentos previsíveis e saber distinguir os que se encontram dentro das normas estabelecidas dos que estão fora das mesmas.

O espaço virtual não tem ordenamento e é urgente que tenha. Para que seja operacionalizado, é necessário criar as entidades informacionais (nomes) que devem ser preservadas, defendidas e resilientes a perturbações do ciberespaço. Essas bases de entidades informacionais (ex. cada indivíduo, prédio, automóvel, terreno, etc. é uma entidade informacional (EI) com atributos que os definem inequivocamente) são estruturadas segundo regras constitutivas próprias e arquivadas com segurança (por ex., em máquinas que não estão ligadas nem à Internet para não comprometer a sua segurança). Essas bases (ou inventário) traduzem o estado desse conjunto de EI num determinado momento de tempo.

A elaboração e proteção do inventário constituem a base primordial para construir o ordenamento do território virtual. O inventário deve conter a informação mais atualizada possível das EI de forma devidamente verificável, estável e deve ser preservada e

guardada de uma forma segura – sobretudo de forma a impedir infiltrações via net. Para o proteger, é necessário um conjunto de funcionalidades/aplicações/software que permitam executar um conjunto de ações nas EI de modo a possibilitar a recuperação de capacidades no caso de haver perturbações profundas nos sistemas informáticos.

--

Hoje em dia, existe uma tendência para analisar a problemática das atividades no ciberespaço levando estes assuntos para o âmbito puramente tecnológico, ou seja, é amplamente defendido que são necessárias mais ferramentas tecnológicas, que é necessário mais armamento, mais Forças Armadas. Ou seja, o conceito de defesa sempre foi pensado ao nível físico, quem se pretende defender e qual o território, mas este pensamento ainda não evoluiu, em Portugal, para o espaço virtual.

Quando se está a falar de segurança dos indivíduos e das organizações, é primordial colocar as seguintes questões também no espaço virtual: o que é Portugal no espaço virtual? Quais são os seus *assets* no território virtual? O que se pretende defender? Porquê? De quem? Por outro lado, é fundamental perceber: quem é o meu inimigo? O que pretendo atacar? Como?

Em Portugal, como podem as estruturas que superintendem as questões de segurança dar um complemento às populações para se defenderem? O que será necessário mudar para aumentar a proteção civil quando se tratar de ataques no ciberespaço?

Quando se pensa em termos de nação, é determinante sabermos o que é essencial preservar para que o nosso país possa ter uma vida normal segundo o regime político que escolhemos (no nosso caso, o regime democrático), defender a nossa sociedade das perturbações profundas que ocorrem no ciberespaço e encontrar uma metodologia objetiva para este efeito.

Nos ataques informáticos, geralmente as redes de comunicações ficam afetadas, caso do último ataque informático à Vodafone. Também se verificam, com alguma frequência, ações que impedem o acesso de determinadas entidades às redes (aconteceu em Portugal nos hospitais, tendo os funcionários ficado impedidos de aceder aos dados clínicos dos doentes). Estas ações causam danos enormes, por isso é muito importante preservar as funcionalidades mínimas de segurança nas infraestruturas informáticas, protegendo-as e isolando-as para garantir o limiar mínimo de prestação de serviços à sociedade.

Numa aproximação *bottom – up* de toda esta problemática, é preciso dar base à nação, ou seja, é necessário que as pessoas tenham conhecimento de "quem é dono de quê". Por exemplo, a informação que está nos notariados é importantíssima e tem de ser preservada dado que, caso seja destruída ou alterada, assistiríamos a um reordenamento do país face à ausência de informação credível que nos permitisse verificar a veracidade dos factos, instalando-se uma enorme conflitualidade no país. Por exemplo, um contrato é uma entidade informacional *per si* e deve ser preservado, situação que não está minimamente pensada no nosso sistema de registos e notariado, o que é assustador e muito perigoso nos dias de hoje.

Passando do nível nacional para o das empresas, é também muito importante ser preservada a informação e o estado de "sanidade" das suas aplicações informáticas. No entanto, praticamente nenhuma organização sabe exatamente qual é o *software* que tem a correr, devido às contantes alterações que resultam dos mecanismos automáticos concebidos pelos fabricantes para fazer os *updates.* Assim, é muito difícil ter atualizado o registo dos sistemas que, a cada momento, estão a correr nos computadores.

No entanto, também há excelentes exemplos de *software,* como o que foi construído para fazer a gestão do espaço aéreo mundial: no espaço aéreo, há milhares de aviões a cruzar os ares que comunicam com torres de controlo onde estão pessoas de várias nacionalidades que usam diversas legislações, mas têm como base um *software* percetível para todos. Existe ainda um *software* disponível para todas as pessoas que mostra, em tempo real, os trajetos dos aviões que estão a voar por todo o mundo. Estes exemplos demonstram que é necessário um estado de *awareness* sistémico fundamental, ou seja, no mundo da informática é preciso saber responder às perguntas básicas: quem (o agente), o quê (a ação), como (o modo), quando (o tempo) e porquê (o motivo) para construir um sistema que responda às necessidades da sociedade no espaço virtual.

Para refletir sobre as consequências que podem ter as alterações maliciosas em sistemas informáticos que são usados pela maioria das pessoas, observem-se as seguintes situações:

- Como temos a garantia que o cálculo dos nossos impostos que foi feito pelos sistemas informáticos das Finanças cumpre a lei? Esses cálculos são algoritmos que estão definidos, mas podemos sempre questionar: demonstre-me que o software que está a correr hoje cumpre a lei atual, demonstre-me que o software não foi alterado por alguém

que criou uma exceção para um determinado NIF fazendo com que o algoritmo executado não é o correto, mas sim outro criado para fins fraudulentos;

- Um determinado banco ficou na posse de prédios (casos de hipotecas que não se cumpriram, portanto, o banco ficou com esses bens). Passados uns anos, o banco pretendia vender os prédios, mas quando o processo chegou à conservatória e ao notário verificouse que os imóveis não estavam registados como propriedade do banco, mas sim em nome de outra entidade, impossibilitando a venda. Após uma investigação judicial que demorou vários anos, concluiu-se que houve uma interação interna de operadores que conseguiram fazer esta fraude;

Se for provocada uma perturbação informática que afete o tráfego de Lisboa por 48h, poderá gerar uma congestão de trânsito enorme, as ambulâncias ficariam imobilizadas, gerando o caos na cidade.

Face a estes e muitos outros exemplos de perturbações no espaço virtual que põem em causa a qualidade de vida (e a própria vida) das pessoas, é prioritário que as pessoas entendam que a defesa do ciberespaço é tão importante como a defesa do espaço físico. A força do povo na defesa da sua terra, do país, é fortíssima porque implica uma ligação profunda do ser humano ao seu espaço de vida, à sua sobrevivência. O problema é que o espaço virtual não é a "nossa terra", o espaço virtual é muito mais difícil para o ser humano perceber e visualizar, não se apercebendo dos perigos a que está exposto.

Para uma consciencialização destes "perigos escondidos", é importante desenvolveremse *serious games* de modo que, ao longo do processo educativo, as pessoas pudessem experienciar disrupções profundas no espaço virtual. Por exemplo, o que poderia acontecer se suas propriedades fossem passadas para o nome de outras pessoas? Deste modo, aprenderiam a "sobreviver" a ataques virtuais, o que seria bastante pedagógico dado que só passando por estas situações se pode efetivamente aprender a defendermonos delas.

Com o passar do tempo, estamos cada vez mais a viver no espaço virtual, mas não temos a consciência exata de onde está e o que se está a fazer para nos defendermos dos ataques.

O facto de não existirem Forças Armadas em Portugal para a defesa do ciberespaço é uma situação muito assustadora e irresponsável dos decisores políticos.

É necessário formar um "exército" de milhares de *maquis* informáticos para lutarem no ciberespaço, o que implicaria uma opção nacional de imersão massiva de muita gente na aprendizagem de conceitos do ciberespaço e de exercícios para a sua defesa. Está a ser feito um trabalho muito meritório no Centro Nacional de Cibersegurança e nas Forças Armadas no envolvimento da sociedade civil nesta área. No entanto, estas ações não são suficientes, não chegam à "massa popular", por isso devia ser feita uma mobilização das pessoas, uma "chamada às armas" ainda mais quando sabemos que, nos dias de hoje, há países em outras geografias (por exemplo, Rússia, China, Japão, etc.) nos quais existem milhares de pessoas completamente fluentes nestas tecnologias e muito preparadas para enfrentarem o desafio dos ataques informáticos.

Há um vazio de pensamento político de Portugal sobre um assunto tão importante e tão premente, os decisores não só não têm formação nem preparação nesta área (questões ultrapassáveis dado que têm peritos que os podem aconselhar) mas também (e sobretudo), não têm vontade para pensar em soluções de grande escala envolvendo recursos significativos. Limitam-se a pensar em soluções tecnológicas implementadas por especialistas e confiam que as Forças Armadas "nos salvem" ou que as organizações internacionais nos venham proteger. Por outro lado, nem sequer está consagrado na Constituição a defesa militar e a proteção civil no ciberespaço.

O estado de arte em Portugal na defesa do seu ciberespaço é uma situação verdadeiramente assustadora.

Abordando agora o nível mundial, existem diversos tipos de Internet: a Internet do mundo ocidental, a Internet dos chineses, dos russos, etc, ou seja, os Estados vão tomando conta de determinados espaços internéticos. No entanto, não conseguem controlar a internet porque a capacidade de resistência do povo que sabe usar a tecnologia acaba por conseguir usar meios ilícitos de comunicação para organizar as suas ações.

No caso dos sistemas financeiros mundiais, não foram concebidos com a escala e âmbito que têm nos dias de hoje. A partir dos anos 90, as diversas praças financeiras mundiais foram aumentando e articulando-se entre si, mas nunca se criou uma estrutura de governação e de regulação adequada, o que constitui uma enorme vulnerabilidade aproveitada para grandes fraudes financeiras.

A Lei de Proteção de Dados, adotada por vários países do mundo ocidental, é bastante ineficaz quando aplicada na prática dado que o processo de apagar dados é bastante

complexo na medida em que existem muitos *backups* legais e não legais que, praticamente, inviabilizam o desaparecimento dos ficheiros de dados. Por outro lado, esta lei ficou muito aquém do tema sobre o qual é verdadeiramente importante dispor de legislação: o ordenamento do espaço virtual, a sua monitorização e o seu policiamento.

Os juristas deviam legislar sobre a existência de entidades virtuais que não são pessoas individuais ou coletivas. Por exemplo, se definirmos uma propriedade rural como uma entidade virtual (ou seja, uma *persona* jurídica) devia ser possível atribuir-lhe um conjunto de atributos que a definem e protegem, ou seja, essa propriedade possuiria um conjunto de agentes informáticos que preservam a sua integridade, que denunciam tentativas de violação da sua integridade e que mantêm a sua coerência. Desta forma estaremos a implementar o princípio da "defesa popular". Imaginemos o seguinte caso: se alguém quiser alterar o dono da propriedade rural, a entidade rural virtual (designada por "agente ativo") questiona o individuo que pretende executar a alteração da seguinte forma (por exemplo): "Quem é o senhor?" "É alguma autoridade que esteja a executar algum processo legítimo que levou à alteração da propriedade?" "Que evidências tem para executar esse processo?" Só após um determinado conjunto de rotinas, a ação seria (ou não) validada.

Outro exemplo de defesa popular: um automóvel, sendo definido como uma entidade informacional (EI), tem uma determinada quilometragem. Se alguém quiser alterar o número de Km, a EI automóvel questionará o individuo responsável por essa alteração por forma a validar a ação, apenas permitindo que ocorra se concluir que é legítima. Concluindo, é muito importante que os cidadãos tenham a capacidade de, proactivamente, validar ações que interferem com as nossas vidas e bens, o que significa que a defesa não deve ser centralizada num *software,* mas sim distribuída à sociedade civil.

É absolutamente fundamental implementar o princípio de "distribuir defesa", este princípio devia fazer parte da legislação básica que regula o ciberespaço, exatamente da mesma maneira como o direito à defesa civil se encontra há muitos anos consagrado na nossa legislação.

Entrevista

Dra. Dalila Araújo

(Vice-Presidente do Observatório de Segurança, Criminalidade Organizada e Terrorismo - OSCOT)

1.Como caracteriza o ciberespaço em termos de potencialidades e vulnerabilidades?

2.Considera possível acontecer no ciberespaço um ataque tão paradigmático como outro 9/11?

3.Qual deveria ser a prioridade no ramo da cibersegurança dos Estados?

4.Na sua ótica, como é que podem as Organizações Internacionais, como a UE e a NATO prevenir e proteger os seus Estados-membros de ciberataques terroristas?

5.Considera que Portugal, nomeadamente a vertente estatal encarregada pela proteção contra estas ameaças, encara o ciberterrorismo como uma ameaça real?

A definição de ciberespaço é difícil. O ciberespaço é um ambiente complexo onde se cruza a informação e onde agem determinados circuitos digitais. Cada vez mais o cidadão comum, as infraestruturas do Estado, a Administração Pública, a prestação de serviços, as economias interagem no ciberespaço e nessa medida o ciberespaço passa a ser um ecossistema, como o é a terra, o ar e o mar. Não tenho dúvidas que a transição digital criou uma outra matriz, criou o ciberespaço com potencialidades, mas também com vulnerabilidades, representando um espaço de ameaças e riscos.

As matérias relativas ao ciberespaço não são novas, mas não têm tanta maturidade que nos permitam hoje a ter muitas certezas. Por vezes, confunde-se ciberterrorismo com cibercrime, que são realidades distintas.

O ciberataques que conhecemos mais vulgarmente são atos criminais que, geralmente, têm como resultado a indisponibilidade de um serviço, ou o *ransomware* ou o *phishing*, ou seja, tudo o que se classifica como cibercrime - atos ilícitos que ocorrem no ciberespaço.

A cibercriminalidade é completamente diferente do ciberterrorismo. Tal como o entendemos hoje, um ataque terrorista tem como objetivos provocar vítimas, provocar o caos, provocar danos em grande escala, amedrontar e aterrorizar as pessoas.

O terrorismo é o crime que mais aterroriza as pessoas, elas têm a perceção do que é o terrorismo e medo de virem a ser vítimas de ataques. Poderá até haver mais vítimas mortais devido, por exemplo, a acidentes rodoviários, mas o medo dos ataques terroristas sobrepõe-se a quaisquer outras realidades, mesmo que impliquem um número muito superior de mortes.

Relativamente ao ciberterrorismo, o cidadão comum não tem grande perceção do que se trata nem tão pouco fica aterrorizado, como acontece com os ataques terroristas no mundo físico. A perceção que existe sobre as consequências de um ataque de ciberterrorismo é muito inferior à perceção do risco de um ato terrorista "tradicional". Porquê? Porque também o tema é relativamente recente.

Quanto à pergunta se o ciberterrorismo pode provocar um ataque de uma escala tal que possa provocar tantos danos como o 11/09, eu diria que é evidente que sim. Há uma assimetria de meios muito grande, ou seja, no limite, um indivíduo isoladamente com um computador pode provocar um ataque terrorista nas infraestruturas críticas de um Estado. No entanto, é preciso que haja muitos recursos no meio físico para que um ataque ciberterrorista tenha o mesmo impacto e a mesma adversidade dos ataques que ocorrem presentemente no mundo material.

Claro que, do ponto de vista do seu potencial, o ciberterrorismo tenderá a ser mais sofisticado, tenderá a ser mais organizado, aliás, ele já o é – isso é público, estão identificados *sites* de organizações terroristas que tentam criar uma rede de *hackers* para que possa servir de interface para a sua ação terrorista. Portanto, o ciberterrorismo poderá, de facto, alcançar até uma escala superior aos ataques terroristas "tradicionais" dado que os recursos tecnológicos estão em constante evolução, são muitos e admito que a Segurança e a Defesa não acompanharam ainda o potencial que a tecnologia tem para fins de guerra tecnológica.

Há um conjunto de prioridades, um conjunto de ações que têm que ser rápidas: a própria União Europeia não está parada, em 2016 fez a primeira Diretiva para os EstadosMembros que era uma diretiva orientadora das ações que a Administração Pública e os prestadores de serviços em *cloud* para serviços públicos deveriam implementar nos seus sistemas

tecnológicos de modo a salvaguardarem os dados, as prestações de serviços e as infraestruturas críticas.

Esta Diretiva foi transposta nos Estados-Membros, sendo que em Portugal deu já origem a um conjunto de políticas: temos uma Estratégia Nacional para o ciberespaço que está em vigor até 2023. No entanto, as empresas privadas não estão obrigadas a implementála, situação que terá de ser corrigida dado que as empresas privadas são o suporte de infraestruturas críticas como, por exemplo, algumas existentes na área da Saúde e dos Transportes. Muitas destas infraestruturas tecnológicas estão na "mão" de privados e, se não houver regulamentação que obrigue estas empresas a integrarem mecanismos para se protegerem de ataques de cibercrime ou mesmo de natureza terrorista, então ficará ao critério de cada uma o sistema de segurança.

Em suma, a União Europeia (UE) procedeu bem quando fez esta Diretiva, Portugal tem uma Estratégia Nacional, tem um Centro Nacional de Cibersegurança e tem também um regime jurídico da segurança no ciberespaço que define um conjunto de matérias relativas à certificação dos prestadores de serviços que estão associados às infraestruturas críticas. A UE já anunciou que este ano vai rever a Diretiva e, provavelmente, irá alargar a sua obrigatoriedade de aplicação às empresas.

De facto, no mundo em rede onde nós vivemos, existe uma complexidade e uma conectividade tais que a legislação e as obrigações emanadas da União Europeia têm de ser mais rígidas, mais assertivas na proteção do ciberespaço. Em Portugal, houve um exemplo recente de um ataque dirigido a um *player* de telecomunicações que presta serviços a um hospital, provocando sérios danos no funcionamento dos seus serviços do hospital, facto que demonstra bem a importância da questão da regulamentação das empresas privadas.

A natureza do ciberterrorismo não se compadece com atos isolados, o ciberterrorismo tem uma dimensão global, ele corre na Internet, a "rede das redes". A União Europeia e os Estados Unidos da América têm trabalhado muito nesta área, é absolutamente necessária uma cooperação entre organizações de forma a produzir normas gerais. Do ponto de vista da tecnologia, se a União Europeia não obrigar os fabricantes a introduzir um conjunto de mecanismos de proteção nos dispositivos eletrónicos que comercializa, não é o cidadão que os compra que depois o vai fazer: por exemplo, se comprar um *iPhone* e o telemóvel

não vier com os dispositivos de segurança, pode ser vítima de um ataque. Isto aplica-se a um *IPhone,* a um computador ou a um qualquer *device*.

É fundamental desenvolver uma ação concertada no quadro da União Europeia, no caso de Portugal, e uma forte articulação com outras geografias, nomeadamente, com os Estados Unidos da América e mesmo com outros países, como a Índia ou da China. Claro que estes últimos têm os sistemas tecnológicos de acordo com a sua natureza política, conseguindo um maior controlo sobre estes. No entanto, a tecnologia não se compadece com planos políticos, no ciberespaço as guerras não são como as guerras tradicionais no mundo físico, existe uma assimetria enorme de velocidade e duração que exige uma abordagem à escala global rapidamente.

Considera que o período pandémico veio exponenciar as vulnerabilidades a nível nacional?

Claro que sim e há estatísticas que provam isso. De um momento para outro, as pessoas que tiveram que pegar nos seus PC e fazer o seu trabalho em casa e as empresas não estavam preparadas do ponto de vista da segurança para que este trabalho pudesse ser feito em casa porque em casa nós usamos o nosso Wi-Fi doméstico que não tem a proteção que tem o outro sistema de acesso aos dados ou de acesso à Internet como as empresas já podem ter. Portanto, a vulnerabilidade resultou do facto de um momento para o outro as pessoas que passaram a trabalhar nas suas casas e as empresas não estarem não estarem dotadas nos computadores dos seus colaboradores, não os terem apetrechado de VPN, porque muitas empresas não têm VPN não há nada disso.

Esta dimensão das empresas ou dos prestadores serviços públicos que não estavam preparados do ponto de vista tecnológico e de segurança para prevenir os ciberataques que foram mais que muitos: o Centro Nacional de Cibersegurança já apresentou estatísticas, o próprio Ministério Público também, portanto os ataques ciber do *phishing,* do *ransomware*, da captura de dados subiu exponencialmente. E não subiu tanto porque muitas pessoas não sabem onde vão comunicar estes eventos.

Por outro lado, nós também começámos a fazer a nossa vida recorrendo às compras online, passámos a fazer muito mais interação online e ainda não estávamos preparados. Os *hackers,* nesse quadro, tinham aí um potencial enorme, eles também estavam nas suas casas, nas profundezas da *darkweb* e tiveram um potencial enorme de *ransomware*, de *phishing,* de uns *hackers* ativistas porque as pessoas não têm cultura de cibersegurança.

Eu costumo dar este exemplo nas minhas aulas porque é um exemplo muito simples: quando nós temos carta de condução e se andarmos a conduzir, nós sabemos que temos que fazer um determinado conjunto de coisas para nos protegermos, ao nosso automóvel e também protegermos os outros, ou seja, ensinaram-nos a andar nas estradas. Mas ninguém nos ensinou a andar no ciberespaço, ninguém nos ensinou a forma como nos conduzimos no ciberespaço, ninguém nos ensina a identificar os *sites*, não ensinam as crianças nem a nós próprios nem o cidadão comum como é que se protegem de um ciberataque.

Portanto a pandemia, quer por via das empresas e foi uma mudança substancial da vida de todos nós, propiciou e aumentou os ciberataques. Não estamos a falar de ciberterrorismo, mas estamos a falar de cibersegurança, o que é uma dimensão também do ciberespaço.

Entrevista

Sistema de Informação e Segurança (SIS)

1. Como caracteriza o ciberespaço em termos de potencialidades e vulnerabilidades?

A crescente dependência da tecnologia e da informação por parte de pessoas e Estados torna-nos vulneráveis à ameaça do ciberespaço, que é muitas vezes utilizado como um local privilegiado para atividades com elevado risco na salvaguarda de segurança interna e dos interesses nacionais.

A ameaça cibernética com recurso a ações de intrusão ou de acesso ilegal no ciberespaço, por parte de agentes hostis, tem registado um crescimento exponencial nos últimos anos,
por consequência da exploração massiva das vulnerabilidades instituídas pela expansão do s canais informais e institucionais de trabalho remoto.

Com efeito, a pandemia, o consequente confinamento social e a resultante migração da generalidade da população para trabalho, estudo e socialização em ambiente remoto, conduziram a uma expansão da superfície de ataque ao dispor do cibercrime internacional, num fenómeno agora categorizado como a "Revolução Industrial do Cibercrime".

Sobressaem, nesse âmbito, as ciberactividades ilícitas com origem em atores não estatais, quaisquer que sejam as motivações subjacentes (criminalidade, lucro, ideologia ou propagação da violência subversiva ou terrorista), por via de ações maliciosas contra pessoas e instituições.

2. Considera possível acontecer no ciberespaço um ataque tão paradigmático como outro 9/11?

O termo ciberterrorismo, quando entendido como a utilização do ciberespaço por organizações terroristas para a condução de ações violentas, digitais ou cinéticas, não é consensual entre a comunidade das informações e, mesmo, entre a comunidade de cibersegurança.

A principal motivação para este quadro dogmático decorre da ausência de pressupostos empíricos, do passado distante e/ou recente, de ações terroristas violentas de escopo

digital, muito embora seja rotineiro o recurso ao ciberespaço por organizações terroristas, para efeitos de capacitação logística, de recrutamento ou de radicalização.
Tem sido possível observar o incremento da ameaça da Cibercriminalidade internacional empenhada na execução de operações extorsionistas ou de fraude contra alvos com forte dependência na disponibilidade digital, sendo igualmente visível a forte expressão digital dos extremismos ideológicos ou de protagonismo mediático,
muitas vezes associada ao *hacktivismo,* ao ciberativismo e ao cibervandalismo, de natureza radical ou terrorista.
Por sua vez, é tendencialmente crescente o recurso a atividades de Ciberespionagem, de elevada sofisticação operacional, enquanto variante da espionagem dita tradicional, por acesso remoto a sistemas e infraestruturas informáticas alheias, para recolha e exportação de informação sensível e/ou classificada, de teor político, militar, científico e económico.

Nesse domínio, determinados atores hostis à segurança do ciberespaço procuram prosseguir as suas determinações estratégicas por via da
tentativa de exfiltração de informação classificada ou privilegiada e da construção de mecanismos sub-reptícios de disrupção.

3. Qual deveria ser a prioridade no ramo da cibersegurança dos Estados?

Estados adversários (e seus *proxies*) das alianças políticas e militares que Portugal integra, têm prosseguido estratégias de reforço das suas capacidades de projeção de força e de recolha de informações por via remota e à escala global. Essa tendência tem-se verificado sobretudo nos últimos três anos, em que o volume e a gravidade deste tipo de ações contra interesses e instituições públicas e privadas têm apresentado acrescidos sinais de intensificação.

De entre estes avultam as ameaças desenvolvidas através de vastas campanhas de alcance global, com uma ofensiva indiscriminada de recolha de informações por via cibernética contra alvos de natureza política e militar, bem como contra instituições cuja atividade se insere em áreas de natureza científica e económica.
Em virtude da especificidade da desmaterialização e dispersão geográfica das estruturas que compõem o ciberespaço, tratam-se de atividades maioritariamente desenvolvidas fora de território nacional, mas que aqui se projetam com grande intensidade.

Acrescentam-se repetidos indícios de recurso ao ciberespaço de interesse nacional para o alojamento de plataformas ofensivas utilizadas contra alvos locais e externos, enquanto se levam a cabo linhas de atuação ofensiva para a condução de operações clandestinas de desinformação digital de espectro local ou universal ao longo das várias plataformas de *social media* e canais *online*.

Considerando que, à semelhança de outros países, Portugal tem sido vítima regular de ciberataques que, em número e severidade crescentes, afetam a confid encialidade, a integridade e a disponibilidade de infraestruturas públicas e privadas det erminantes para o normal funcionamento de instituições e de serviços essenciais, justifica - se a necessidade de desenvolver uma resposta eficaz, de âmbito estratégico, de forma a prevenir a ocorrência de incidentes no ciberespaço, garantindo a cibersegurança.

No cumprimento da sua missão, o SIS desenvolve esforços de avaliação da ameaça cibernética, presente e emergente, relativa à segurança de informação e de comunicações de elevada sensibilidade, em permanente cooperação com as entidades públicas com responsabilidades na promoção da cibersegurança interna, nomeadamente com o Centro de Ciberdefesa das Forças Armadas, o Centro Nacional de Cibersegurança e a Polícia Judiciária.

Neste domínio têm sido incrementados esforços de avaliação de ameaça cibernética relativa à segurança de informação e de comunicações de elevada sensibilidade e à introdução no quotidiano digital de novidades tecnológicas como a tecnologia de *blockchain*, a Inteligência Artificial, os equipamentos do universo da Internet das Coisas (IoT) e as futuras redes de telecomunicações de quinta geração (5G).
Em simultâneo, prosseguem-se linhas de investigação dedicadas a soluções tecnológicas com potencial disruptivo ou hostil, bem como para a identificação de vulnerabilidades com potencial de impacto na confidencialidade, na integridade e na disponibilidade de sistemas informáticos do espectro público e privado interno ou de infraestruturas críticas nacionais.

Merece a atenção especial do SIS, o desenvolvimento das condições securitárias das infraestruturas e dos sistemas que suportam o ciberespaço de interesse nacional, em colaboração com entidades detentoras ou gestoras de ativos digitais passíveis de serem

vitimados por ciberataques, como os titulares e administradores de infraestruturas informáticas associadas a serviços essenciais.

4. Na sua ótica, como podem as Organizações internacionais, como a UE e a NATO, prevenir e proteger os seus Estados-membros de ciberataques terroristas?

Os desafios são muitos e distintos. Pode dizer-se que o que está em causa é um conceito alargado e aglutinado de segurança que exige uma abordagem estratégica integrada e coordenada entre vários parceiros de segurança de forma a conter riscos. Deste modo, criar sinergias, clarificar e efetivar o sentido da política de segurança interna no espaço europeu constitui um objetivo relevante.

Para tanto, tem sido promovida uma reflexão ao nível doutrinal, técnico e operacional referente à evolução das ameaças à segurança interna, num exercício de interpretação atualista às características da missão a desenvolver.

E porque as atuais ameaças são globalizadas e partilhadas por todos, o desafio consiste agora em congregar diferentes instrumentos e capacidades, contribuindo para salvaguardar a segurança de um determinado Estado e a de países terceiros, através de um esforço acrescido de cooperação estratégica.

Outro grande objetivo passa por reforçar a cooperação operacional e a troca de informações entre as diversas autoridades, na definição de uma base legal comum, através da utilização de metodologias mais efetivas, com recurso a novas ferramentas e aplicações tecnológicas.

Nesse âmbito, entende-se a atual vulnerabilidade dos canais de comunicação exige uma acrescida interoperabilidade entre parceiros, com recurso a novas infraestruturas e serviços, capazes de fazer face à ameaça representada pela transformação digital e pela quebra de integridade e confidencialidade da informação transmitida.

5. Considera que Portugal, nomeadamente a vertente estatal encarregada pela proteção contra estas ameaças encara o ciberterrorismo como uma ameaça real?

Propomos, para esta questão, a leitura do discurso do Diretor do SIS por altura do recente seminário dedicado ao tema que se encontra na nossa página eletrónica: https://www.sirp.pt/noticias (**Ciberterrorismo - desafios, ameaças e consequências geopolíticas (6ª conferência terrorismo contemporâneo)**

Entrevista

Dr. Bruno Castro

(CEO e Fundador da empresa Visionware)

1 Como caracteriza o ciberespaço em termos de potencialidades e vulnerabilidades?

Se há 20 anos olhávamos para o conceito de ciberespaço com grande estranheza e algum esoterismo, hoje certamente quase todas as pessoas estão familiarizadas com o mesmo. Tornou-se uma terminologia corrente no nosso dia-a-dia, em paralelo com o mundo do ciberataque.

Como bem referiu na sua questão, existem potencialidades e vulnerabilidades, vantagens e desvantagens.

A primeira potencialidade/vantagem que o ciberespaço nos oferece é o acesso à informação. Deixaram de existir momentos ou serviços específicos onde nos podemos informar. Na internet, a informação corre 24/7. Coloca-nos em contacto com acontecimentos de outros cantos do mundo em segundos. E isso leva-me à segunda premissa: a proximidade e conexão – o ciberespaço torna-nos mais próximos, com possibilidade de contactos mais próximos uns com os outros.

Para além disso, o ciberespaço apresenta um conjunto de oportunidades de desenvolvimento de negócios e de uma sociedade mais moderna e capaz de corresponder aos desafios dos seus concidadãos.

Não obstante, apresenta muitas vulnerabilidades e grandes perigos.

Basta entrar na sua conta bancária online, aderir às redes sociais ou outros serviços, para ser passível de correr o risco de estar exposto a um potencial roubo das suas informações pessoais, tais como nome, morada, número de cartão de crédito, etc. Cada vez mais hackers – e cada vez mais facilmente - conseguem aceder a estas informações através de ligações não seguras ou plantando um software malicioso, o qual pode ser ativado se clicar num link (à partida) inofensivo. Basta uma fração de segundos.

Em geral, as desvantagens não ficam atrás das vantagens, devido à segurança e aos perigos inerentes desta sociedade em rede. Nunca se sabe quem está a aceder às suas informações pessoais e o que farão com elas.

2.Considera possível acontecer no ciberespaço um ataque tão paradigmático como outro 9/11?

Atualmente, encontramo-nos num mundo diferente daquele conhecíamos. Há 22 anos, aquando do virar do século, as ameaças que encontrávamos à nossa segurança e bem-estar eram, por si só, alarmantes e complexas. Hoje, estamos perantes perigos muito maiores, em várias frentes.

Vivemos num país democrático, partilhamos valores liberais e preservamos o respeito pela liberdades e garantias individuais. Contudo, como no ataque 9/11, há pessoas que não veem a realidade dessa forma. Se o 11 de setembro de 2001 é considerado, por muitos, o dia que mudou o mundo – com claras melhorias físicas à segurança coletiva -, talvez seria benéfico se compreendessemos o conceito de ameaça aos dias de hoje. E isso inclui a ameaça cibernética como uma das mais perigosas de todos os tempos.

Os sistemas bancários estão interligados. Os sistemas governativos também. A nossa sociedade é desginada como "sociedade em rede" por algum motivo. Um ataque a essa rede, seria capaz de deitar abaixo as defesas, e inevitavelmente, gerar uma série de episódios catastróficos, que podem ter ou não diretamente a ver com esse ataque.

Acima de tudo, é preciso que as pessoas estejam alertadas e precavidas. É preciso saberem que a segurança digital, que contempla os seus dados, é um alvo para muitos grupos criminosos e, inclusivamente, Estados.

3.Qual deveria ser a prioridade no ramo da cibersegurança dos Estados?

Acima de tudo, é necessário que os governantes percebam que o ciberespaço apresenta várias ameaças à democracia e aos principais fundamentos de um Estado soberano.

Depois, é necessário criar mecanismos efetivos para prevenir ciberataques: isso implica um constante controlo, deteção e defesa das vulnerabilidade e monitorização das ameaças.

4.Na sua ótica, como podem as Organizações Internacionais, como a UE e a NATO, prevenir e proteger os seus Estados-Membros de ciberataques terroristas?

A criação (e já existem) de departamentos e núcleos capazes de prevenir este tipo de ataques é fundamental. Lá está, volto a reforçar a palavra fundamental: prevenção.

A atividade diária da VisionWare demonstra que o fator humano continua a ser um dos grandes responsáveis pela consumação das ameaças e que estas tanto podem vir de fora, como de dentro da própria organização. Neste sentido, além de ser fundamental prepararse uma estrutura capaz de responder às ameaças que vêm do exterior, investindo na tríade de segurança (pessoas, processos e tecnologia), é fundamental olhar para dentro de cada organização, sensibilizar e formar as pessoas para que estas sejam conscientes e não se transformem em veículos de ameaça.

É necessário que existam campanhas de sensibilização para os perigos iminentes destes ataques, não só à população em geral, mas também junto dos governantes.

5.Considera que Portugal, nomeadamente a vertente estatal encarregada da proteção contra estas ameaças encara o ciberterrorismo como uma ameaça real?

Creio que Portugal tem dado um grande salto nesta matéria, sobretudo ao nível da mentalidade e mudança de mindset. No entanto, estamos (tal como grande parte dos Estados que compõem a União Europeia) a anos-luz dos Estados Unidos da América ou Israel, se quisermos explorar exemplos mais "ocidentais".

Sobretudo pela idade mais avançada da população portuguesa – e, em grande parte, pelo desinteresse nestas matérias -, o Centro Nacional de Cibersegurança tem realizado inúmeras ações de sensibilização, através da realização de cursos de e-learning para dotarem o cidadão com alguns conhecimentos nesta área (como uma "luta" pela literacia no digital). Temos também vários Observatórios multidisciplinares que estudam o ciberespaço e os seus perigos.

No entanto, quando falamos de ciberterrorismo, creio que o país não está devidamente preparado para responder positivamente a essa ameaça. Aliás, basta compreender, até pelos recentes acontecimentos, o quão relativamente fácil é a um cibercriminoso roubar informações confidenciais ao Estado português ou dados de clientes a empresas nacionais.

É uma realidade que, para nós, está distante ao nível da preparação e análise, mas cada vez mais próxima de poder vir a ser materializada contra os nossos interesses.

Entrevista

Dr. José Casinha

(Chief Information Security Officer da OutSystems)

1. Como caracteriza o ciberespaço em termos de potencialidades e vulnerabilidades?

O Ciberespaço é o "território" onde se governa o mundo nos dias de hoje. A dependência do Ciberespaço para o desenvolvimento da sociedade é por de mais conhecida e onde as oportunidades surgem todos os dias. Se se juntar o desenvolvimento de software como o motor do ciberespaço então diria que é aqui que a investigação e desenvolvimento assume a liderança da exploração do potencial do ciberespaço. O ciclo de vida da tecnologia é muito curto o que torna obsoleto muitos dos desenvolvimentos realizados deixando um rasto de vulnerabilidades que quando exploradas se podem tornar em ameaças.

2. Considera possível acontecer no ciberespaço um ataque tão paradigmático como outro 9/11?

Sim.

3. Qual deveria ser a prioridade no ramo da cibersegurança dos Estados?

Formar pessoas. Profissionalizar quadros para garantir a segurança dos cidadãos e das organizações. Em termos de comparação temos policias e forças militares que protegem a segurança física dos cidadãos e das organizações no território, mas o mesmo não se passa no Ciberespaço.

4. Na sua ótica, como podem as Organizações Internacionais, como a UE e a NATO, prevenir e proteger os seus Estados-Membros de ciberataques terroristas?

Devem ser parte integrante de um sistema de defesa que devem integrar estas organizações, juntamente com a estrutura organizada dos estados membros que deve incluir a sociedade civil também.

5. Considera que Portugal, nomeadamente a vertente estatal encarregada pela proteção contra estas ameaças encara o ciberterrorismo como uma ameaça real?

Sim, mas com um grande desafamento entre a palavra e os atos. Basta ver o que foi a ambição do Centro Nacional de Cibersegurança que pretendia vir a ser um organismo autónomo e ainda está sobre a tutela do Gabinete Nacional de Segurança cuja missão é diferente. A capacitação de organismo desta natureza requere equipas multidisciplinares ativas e focadas nestas temáticas, mas em Portugal o assunto é tratado por múltiplos organismos em múltiplas tutelas que vão deste o SIED, PJ, MAI, CNCS que acumulam o Ciberterrorismo com outras atividades.

Entrevista

Eng. Francisco Nina Rente

(Art Resilia: cybereslience e The Rock: cybersecurity)

1.Como caracteriza o ciberespaço em termos de potencialidades e vulnerabilidades?

Começando pelas potencialidades, o ciberespaço é, provavelmente, a maior criação da humanidade. É verdade que depende de muitas outras ciências de base, que demoraram séculos ou milénios a desenvolver, mas o ciberespaço é a verdadeira realidade aumentada, não no sentido de realidade aumentada como nós a conhecemos, mas é uma forma de aumentar as capacidades do ser humano para uma escala que ainda hoje em dia que não é conhecida.

A nível de comunicação, cognitivo, análise, presença, o ciberespaço será o plateau para a sociedade no futuro, quer seja ela contida no nosso planeta, mas principalmente quando se tornar interplanetária, pois é o ciberespaço que vai garantir a comunicação sem barreiras, a expansão cultural, a troca de capacidades cognitivas que no passado necessitavam e estavam dependentes de uma presença física.

Quanto as vulnerabilidades, como qualquer tecnologia ou criação humana pode ser usada fins ilícitos e um bom exemplo disso neste momento é a temática das redes sociais. As redes sociais foram criadas com um propósito, ou pelo menos era essa a intuição, mas neste momento já são mais as partes más do que boas. São o maior playground para grupos ciberterroristas. Esta será a maior vulnerabilidade do ciberespaço, a adulteração da humanidade.

2.Considera possível acontecer no ciberespaço um ataque tão paradigmático como outro 9/11?

O 11 de setembro não é nada comparado com o que pode ser feito com o ciberespaço. Conceptualmente, a nossa sociedade pode colapsar, no sentido de ficarmos sem energia, sem água, sem cadeias de alimentação, sem comunicações, sem nada. Qualquer sociedade, da mais evoluída à menos evoluída, tem uma dependência tecnológica do ciberespaço que permite um ataque avassalador.

É verdade que há muitas disciplinas sociopolíticas e não só que tentam mitigar este tipo de ameaças com regulamentações, com políticas que incentivam a evolução, a inovação, o investimento, mas ainda estamos muito aquém.

No final dos anos 80, início dos anos 90, houve um grupo de hackers que fez uma manifestação em frente ao senado americano dizendo que tinham descoberto uma maneira de mandar a internet abaixo em menos de uma hora, mas ninguém acreditou neles. Desta forma, o grupo fez prova de conceito, provaram que era possível. A parte mais "engraçada" desta história é que o problema que eles identificaram ainda hoje ainda não está resolvido e passaram mais de 40 anos. Foram feitos alguns remendos e criado alguns alertas para quem tentasse invadir outra vez, mas conceptualmente não foi resolvido.

Passaram-se 20 anos e há muita coisa a ser feita a nível técnico, político, académico, mas ainda assim o caminho é muito ténue, pois isto contrabalança muito com a obtenção de lucro.

3.Qual deveria ser a prioridade no ramo da cibersegurança dos Estados?

Proteger os seus cidadãos, por uma razão muito simples: como em qualquer guerra, a guerra ganha-se com os soldados rasos, não é com os generais. Num cenário de ciberguerra, todos nós somos soldados, no sentido de que as armas dos atacantes são os *smart devices*. O foco primordial, para além de proteger os cidadãos, é proteger as infraestruturas físicas.

4.Na sua ótica, como é que podem as Organizações Internacionais, como a UE e a NATO prevenir e proteger os seus Estados-membros de ciberataques terroristas?

Eu poria essas duas organizações em dois stocks diferentes. Aliás, juntaria a UE com a ONU e deixaria a NATO noutro patamar. A NATO é uma organização bélica, e sempre será. Os seus propósitos, a sua doutrina e a sua estratégia são orientadas à guerra. E a guerra é, como qualquer outro setor económico, uma "máquina de fazer dinheiro". Haverão poucos momentos na vida para comprovar o que estou a dizer como aquele que estamos agora a viver. A guerra na Ucrânia e a Rússia vai ser perpetuada por interesses económicos, tanto para os ucranianos, tanto para os russos, como também todos os europeus.

Uma nota interessante a analisar será como as grandes potências bélicas, como a França, Inglaterra, os EUA, a Rússia, Israel estão a ter menos impacto na recessão económica

porque o setor bélico está a crescer, pois esta a ser alimentado pela guerra. A NATO, quer seja no mundo real, quer seja no ciberespaço, terá sempre uma doutrina bélica independentemente de essa ser a prioridade ou não no momento.

A UE e a ONU, na minha perspetiva, terão uma missão muito mais larga, não necessariamente bélica, pela sua essência terão a preocupação primeiro pelas pessoas e depois eventualmente com os interesses económicos oriundos da guerra. Dito isto, na minha perspetiva, a UE tem vindo a fazer um caminho brilhante nos últimos anos, é líder mundial na implementação de regulamentação, que tem criado mudanças gigantes – por exemplo, o caso do GDPR que está focado na privacidade de dados, mas que é uma engrenagem importantíssima no contexto de combate à ciberguerra e ciberterrorismo. Enquanto que, por exemplo, a regulamentação americana é mais isolacionista e virada apenas para o país, sendo que isto não resulta na dinâmica do ciberespaço, a UE não olha às fronteiras, não olha às nacionalidades como deve ser feito.

O ciberespaço tem que ser lidado como por exemplo a saúde, tem que haver *cyberhealth, cyberhygiene*, que são noções e dimensões que têm que ser construídas para todos, sem distinções, sem ter em conta a geografia, a política pois se não irá funcionar. A omnipresença e a interligação que existe impede que qualquer coisa seja feita noutro sentido. Por isso, organizações como a ONU, como a UE e eventualmente a NATO nos seus âmbitos, têm que operar numa ótica de "proteger os seus, mas proteger todos".

5.Considera que Portugal, nomeadamente a vertente estatal encarregada pela proteção contra estas ameaças, encara o ciberterrorismo como uma ameaça real?

Sim. Portugal, felizmente, nunca teve assim grandes situações de ciberterrorismo. Este ano está a ser um bocado atípico, temos visto muitas atividades de cibercrime que pode extravasar um pouco para o ciberterrorismo pelo impacto e pela maneira como é feito. Desde serviços secretos a estruturas judiciais, polícias, as forças amardas, a parte civil com o CNCS, a rede nacional CSIRT constituem um conjunto de organismos que de uma ou outra maneira têm vindo a fazer trabalhos que têm sido casos de sucesso muito grandes a nível nacional que demonstram isso. Um país pequeno, com uma economia relativamente pequena, dá a cara a problemas como esses, ao contrário de outros países maiores que não o fazem. Dentro do possível, não estamos mal na luta contra o ciberterrorismo.

Entrevista

Dr. João Pacheco

(Fundador e CEO da empresa Cyberprotech)

1.Como caracteriza o ciberespaço em termos de potencialidades e vulnerabilidades?

O ciberespaço no século XXI tornou-se um espaço tão comum como o espaço "real" em que vivemos. Aliás, diria que existem cada vez mais pessoas a passar mais tempo no ciberespaço do que na sua própria vida lá fora!

Este dinamismo conta com aspetos positivos e com aspetos negativos.
Dentro dos aspetos positivos, temos o rápido e fácil acesso a milhares de informações e de dados de qualquer tipo, novas oportunidades de comunicação, inclusive a adoção do teletrabalho, da escola/universidade online e a oportunidade de partilharmos as nossas emoções em tempo real através das inúmeras plataformas de redes sociais existentes (que ainda são algumas!). Já aspetos negativos, temos a consequente redução da nossa privacidade e a utilização indevida das nossas informações pessoais, o acesso não supervisionado de menores no mundo digital (jogos violentos, bullying, conteúdo impróprio, etc.) que pode levar a que predadores tenham o seu "trabalho" simplificado nos seus atos ilícitos. Um dos aspectos mais negativos é o desenvolvimento do cibercrime (espionagem corporativa, roubo de identidade e de dados bancários, ciberbullying, pornografia infantil, roubo de dados privados e sensíveis, engenharia social, etc.), assim como a possibilidade de com apenas um ataque, bem direcionado, haver a hipótese de deitar abaixo ou de comprometer infraestruturas importantes ao funcionamento normal de organismos estatais e privados (ataques DDoS, Ransowares, Malware, injeção de SQL, etc.)

Apesar de tudo, na minha opinião, existem mais potencialidades do que vulnerabilidades no uso do ciberespaço - a World Wide Web uniu-nos de uma forma incrível e permitiu-nos chegar a sítios em segundos, onde outrora demoraríamos dias ou até semanas a chegar. Uma das maiores vulnerabilidades será o imenso tempo que passamos online

em vez de o passarmos offline, perdendo a essência de sermos seres sociáveis que vivem a vida no mundo real e não no mundo digital.

2. Considera possível acontecer no ciberespaço um ataque tão paradigmático como outro 9/11?

No ataque 9/11, foi um acontecimento devastador! A "Ground Zone" foi inteiramente física, edifícios, veículos, infraestruturas (como esgotos, luz e água possivelmente) e pessoas.

Nos dias de hoje, havendo um ataque no ciberespaço de tamanha magnitude, teria o poder de parar, literalmente, o mundo. Hoje em dia, praticamente está tudo online e interligado: com o desenvolvimento e integração das IA´s (Inteligências Artificiais) existe agora também a automatização de processos e de aparelhos - os IoT´s (Internet of things).
Como é expressado no relatório "Cyberterrorism How Real Is the Threat?" redigido por *Gabriel Weimann* em 2004 - *"É importante distinguir entre o ciberterrorismo e "hacktivismo", um termo cunhado por estudiosos para descrever o casamento de hacking com ativismo."*

Muitas vezes é difícil perceber a linha que separa entre hacktivismo e ciberterrorismo. Grupos como Anonymous, que dizem ser a favor dos direitos do povo perante os seus governantes, já usaram táticas mais "ligeiras", como o Projeto Chanology ou o caso de Chris Forcand e Operação DarkNet; e já usaram a sua força contra organismos estatais e privados, como e, 2011 na Primavera Árabe, Operação Egito, Operação Tunísia e Operação Síria entre outras, e Vingar Assange, em resposta à pressão para com a WikiLeaks em 2010.

Temos um bom exemplo de que uma guerra cibernética está a ser travada no presente momento: a guerra Rússia/Ucrânia. Não apenas no mundo físico, com homens, veículos, armas e aviões, mas também no mundo cibernético, através de atividades de ciberespionagem, ataques de DDoS contra instituições, serviços e infraestruturas essenciais às comunicações e aos esforços de guerra de ambos os Países, de forma a comprometer o avanço de ambos os lados.

Mas sem dúvida, se um dia uma organização terrorista, ou entidades com atividades ilícitas tenham em mãos os meios e o conhecimento necessário para lançar um ataque no ciberespaço, complementando com outro ataque no mundo "físico", teremos uma receita para uma catástrofe que poderá ser, inclusive, de uma maior gravidade do que o ataque tão paradigmático como 9/11.

3. Qual deveria ser a prioridade no ramo da cibersegurança dos Estados?

Cada Estado deverá ter em atenção a sua própria realidade. Países como EUA e Inglaterra têm um orçamento mais alto e dedicado à cibersegurança do que, como por exemplo, os Países Baixos ou mesmo como Portugal.
Contudo, qualquer Estado deverá priorizar estruturas e processos que estejam ligados ao combate do cibercrime e à ciberdefesa e ter um plano de ação de estratégia nacional de segurança do ciberespaço em vigor.

Proteger as estruturas digitais do Estado e infraestruturas importantes ao funcionamento normal de organismos estatais, como hospitais, sistema de defesa, aérea militar, educação, área bancária, redes de energia e de águas, deverá ser um trabalho constante e prioritário.
No caso Português, a prioridade principal diria que passa por adquirirmos mais mão de obra e técnicos especializados para a área e de os distribuírem uniformemente pelo território Nacional: segundo o relatório de economia 2022 do CNCS, 58.2% dos técnicos encontram-se na área de Lisboa e Vale do Tejo e 15.5% na área Centro; seguindo-se o Norte, com 20.3%; em último vem a região Algarvia com 4.5% de efetivos e as Ilhas com apenas 1.5%, onde 42,4% tem 5 ou menos anos de experiência e 9.7% tema já uma vasta experiência com 21 ou mais anos de experiência.

Já é altura em que, desde bem cedo, deveríamos ter nas escolas uma disciplina dedicada ao tema, começar a consciencializar e a formar a juventude para que tenhamos um futuro mais preparado e consciencializado do que é certo e errado. Enquanto a Direção-Geral da Educação não toma uma posição mais proativa e atualizada, vai havendo entidades que estão a apostar em novos movimentos ou métodos alternativos de ensino e reclamam

ser mais focados nas crianças. Continua-se a "despejar" informação para todos de forma igual, quando não há duas crianças iguais, gostos e aptidões iguais.
A formação e atualização do corpo docente, deverá continuar a ser uma prioridade para que tenhamos profissionais aptos a reconhecer os indícios e a responder de forma mais amorosa, dando assim a oportunidade para um crescimento saudável, em vez da revolta que vai aumentando e é alimentada por grupos maliciosos e depois temos os "criminosos" que começam muito cedo.

4. Na sua ótica, como podem as Organizações Internacionais, como a UE e a NATO, prevenir e proteger os seus Estados-Membros de ciberataques terroristas?

Desde julho 2016, que a UE entrou na Fase Centralizadora da abordagem e perspetiva da UE para a Cibersegurança, que se define por medidas de centralização e elaboração de medidas e políticas; na postura de liderança; em ações horizontais, multiníveis e de maior integração; na legislação específica (Diretiva SRI, RGPD, Regulamento de Cibersegurança.) e no reforço da Ciberdefesa e combate a ameaças híbridas.
A UE tem Instrumentos Jurídicos próprios para ajudar a proteger os seus Estados-Membros, tais como a Diretiva SRI, o Regulamento da Cibersegurança da UE, tem uma vasta Base Jurídica para o efeito.

O combate às ciberameaças passou a fazer parte das prioridades da agenda política da UE, onde os ativos que carregam maior grau de importância são as infraestruturas críticas essenciais para o funcionamento da sociedade (como fornecimento de água e energia, hospitais, transportes, redes e sistemas de informação etc.).
No plano da prevenção, com a Diretiva Relativa à Segurança das Redes e da Informação (SRI), a resposta coordenada e de recuperação de incidentes tornou-se mais eficiente pois ao estabelecer uma série de medidas (tais como a obrigação de notificação de incidentes graves e de atender aos requisitos de segurança) para a prevenção e tratamento de ciber-incidentes nas infraestruturas críticas, essenciais para o funcionamento da sociedade, tornou mais fácil a partilha entre Estado-Membros de novos perigos e as suas soluções. Ou seja, houve um maior foco na preparação e na capacidade de resposta a grandes incidentes.

Apesar de tudo, continua a ser importante e necessária a atualização de políticas e processos para que cada vez seja mais fácil e simples a partilha de informações entre entidades responsáveis pela Cibersegurança de cada um dos Estados-Membros, sobretudo no que toca a mão de obra, pois é um sector onde continua escassa a mão de obra qualificada e especializada, o que leva a muitas vezes a um Burnout e consequente desistência de técnicos especializados na área.

5. Considera que Portugal, nomeadamente a vertente estatal encarregada pela proteção contra estas ameaças, encara o ciberterrorismo como uma ameaça real?

Portugal em termos de cibersegurança, tem uma rede na primeira linha de combate criada pelo Estado Português: A Rede Nacional CSIRT *(Computer Security Incident Response Team)* que vem englobar a Diretiva SRI da UE.

Foi criada com o intuito de demonstrar que a ameaça cibernética é real e potencialmente perigosa. Esta Rede Nacional é composta por membros que constituem um fórum de cooperação entre equipas de resposta a incidentes de segurança informática (CSIRT) em Portugal e tem como principal objectivo contribuir para a promoção de uma cultura de cibersegurança, tanto na criação de instrumentos necessários à prevenção e resposta rápida num cenário de ataque de grande dimensão, como na criação de indicadores e na recolha de informações sobre incidentes com vista à melhor identificação de contramedidas pró-ativas e reativas e claro, estabelecer laços de confiança entre elementos responsáveis pela segurança informática de forma a criar um ambiente de cooperação e assistência mútua no tratamento de incidentes e na partilha de boas práticas de segurança.

Para se pertencer a esta rede, existem certos requisitos obrigatórios que as empresas têm que cumprir, como por exemplo: ser pessoa coletiva com NIPC, a empresa deverá ter uma equipa CSIRT já formada e em funções.

Neste momento, empresas como a NOS; Altice; EDP; CGD; banco CTT; universidade do Algarve, do Minho e de Évora; a S21sec; a REN; a EY; Galp e muitos mais estão na linha da frente como membros da Rede Nacional CSIRT.

O aumento de ataques informáticos a Portugal tem vindo a aumentar neste ano, com o ataque à vodafone pelo grupo Lazarus e o ataque à Companhia Aérea portuguesa (TAP) onde milhares de dados de utilizadores foram roubados e posteriormente colocados a disposição da Dark web, a forte modernização das infraestruturas e a aposta em cada vez mais membros para a Rede Nacional CSIRT, mostra a forma natural que Portugal está a encarar o crime cibernético como um perigo cada vez mais emergentes.

Entrevista

Dr. Pedro Mendonça

(Coordenador do Observatório de Cibersegurança do Centro Nacional de Cibersegurança)

1.Como caracteriza o ciberespaço em termos de potencialidades e vulnerabilidades?

No ciberespaço não há uma territorialidade clara, ou fronteiras claras, é mais uma dispersão de servidores, de serviços que não obedecem às regras do território nacional clássico e isto traz vulnerabilidades, como, por exemplo, na identificação dos agentes de ameaça. Pode acontecer que um indivíduo ataque Portugal e nem sequer use um servidor português, pode estar em qualquer lado do mundo.

Para combater isto, criou-se um conjunto de metodologias que procuram, a partir de um conjunto de técnicas, táticas e procedimentos, identificar os atores da ameaça e, por vezes, consegue-se detê-los. Por exemplo, um ataque sofisticado, com muitos meios e bem coordenado, foi, provavelmente, orquestrado por um Estado, como vimos no caso do Irão com o vírus *Stuxnet*, no qual foram utilizadas tantas vulnerabilidades *zero days* que indicam que poderá ter sido um Estado a fazê-lo, apesar de não haver consenso mundial qual terá sido o responsável. Este é um dos aspetos que traz dificuldades e aspetos negativos ao ciberespaço.

Um outro aspeto é a complexidade tecnológica. O meio digital é particularmente complexo, os serviços digitais prestados têm milhões de linhas de código e cada vez que há um novo produto facilmente são introduzidas novas vulnerabilidades nos sistemas que ainda não foram estudadas. Devido a este facto, temos de fazer atualizações todas as semanas para detetar e evitar a retenção de tantas vulnerabilidades nos sistemas.

2.Considera possível acontecer no ciberespaço um ataque tão paradigmático como outro 9/11?

O ataque do 11 de setembro foi um ataque muito simbólico, não gostaria de fazer esta comparação com o ciberespaço. Já houve ataques paradigmáticos no ciberespaço, como por exemplo o *WannaCry*, os ataques à Estónia, ao Irão, os ataques dos *Anonymous*, os

ataques à Ucrânia, são todos ataques que vieram criar paradigmas, que vieram demonstrar a relevância do ciberespaço, que vieram marcar a História.

Há uma dificuldade na conceção do que é, realmente, um ato ciberterrorista nomeadamente, quem são os seus agentes. Se foram indivíduos que agiram por motivos político-ideológicos numa lógica puramente de *trolling,* estarão mais próximos daquilo a que denominamos "hacktivistas". Se, por outro lado, forem indivíduos que agiram por motivos económicos, ainda que estejam na fronteira entre o *trolling* e os benefícios económicos, será, no mínimo, cibercriminosos e não ciberterroristas.

A forma mais fácil de definir um ciberterrorista é, no fundo, alguém que pertence a um grupo terrorista que pratica ações no âmbito no ciberespaço. A verdade é que, grande parte das vezes, as ações são de recrutamento e de *crowdfunding*. É uma tarefa bastante difícil distinguir de "hacktivistas", sendo que, à partida, os indivíduos que praticam atos ciberterroristas procuram causar a disrupção total dos sistemas, provocar o medo nas pessoas. O "hacktivista" não procura bem isto, procura sabotar chamando a atenção, estando por detrás um motivo ideológico.

Existem ainda os *cyberoffender,* um termo usado pelo CNCS que não é consensual. Os *cyberoffender* são indivíduos que não têm motivos nem ideológicos, nem estratégicos nem financeiros, querem apenas "chatear". Podem até ter motivos emocionais, querem que lhes seja dada atenção praticando atos de *cyberbullying, stalking* ou *sextorcion*, é quase um fenómeno patológico.

3.Qual deveria ser a prioridade no ramo da cibersegurança dos Estados?

Devemos agir a vários níveis ao mesmo tempo. Se olharmos para a estratégia nacional, encontramos algumas respostas às várias necessidades. Deve-se agir na área da prevenção e proteção do fator humano, no reforço das autoridades, das forças policiais, das forças de defesa e da dimensão civil da cibersegurança, pois esta última é uma dimensão muito forte na medida em que estamos constantemente expostos aos riscos que existem no ciberespaço. Deve-se levar a cibersegurança a sério e perceber que esta já não é um mundo paralelo ao físico, é um espaço onde nós estamos e onde devemos agir com a mesma preocupação com que agimos no *offline*.

4.Na sua ótica, como podem as Organizações Internacionais, como a UE e a NATO, prevenir e proteger os seus Estados-Membros de ciberataques terroristas?

Tem sido feito muita coisa ao nível europeu, nomeadamente a diretiva SRI, a transposição para Portugal do regime jurídico do ciberespaço e prevê-se ainda uma nova versão desta diretiva com carácter mais abrangente. O CNCS tem uma boa articulação com as entidades nacionais e internacionais, incluindo com a NATO. Têm-se feito um grande esforço do ponto de vista da regulamentação para que novos aspetos sejam considerados na legislação existente.

5.Considera que Portugal, nomeadamente a vertente estatal encarregada da cibersegurança, encara o ciberterrorismo como uma ameaça real?

Por princípio, encara. Esta dimensão acaba por ser considerada em todos os esforços de prevenção e proteção, de preparação para a reação, de mitigação dos ciberataques, portanto diria que sim.

Apêndice IV

Tabela de análise de conteúdo

Temas	Categorias	Subcategorias	Entrevistados	Unidades de registo
Ciberespaço	Potencialidades e vulnerabilidades	- Dependência tecnológica	José Tribolet (IST)	*(…) tanto os indivíduos como as organizações vivem também no espaço virtual, cada vez mais, à medida que a tecnologia vai evoluindo e disponibilizada a todos nós (…)* *"(…) o mundo físico e o virtual estão cada vez mais sincronizados, os eventos do primeiro repercutem-se no segundo e vice-versa com cada vez mais velocidade (…)"*
			Dalila Araújo (OSCOT)	*(…) não tenho dúvidas que a transição digital criou outra matriz, criou o ciberespaço com potencialidades para ameaças e riscos (…)* *(…) cada vez mais as nossas vidas, a vida da administração pública, as infraestruturas do Estado, a prestação de serviços, as economias interagem no ciberespaço (…)*
		- Rapidez e acesso	Sistemas de Informação e Segurança (SIS)	*(…) mais do que um alvo ou uma ferramenta, o ciberespaço é indissociável do mundo real e constitui-se como um meio facilitador da ação terrorista (…)* *(…) a crescente dependência da tecnologia e da informação por parte das pessoas e Estados torna-nos vulneráveis ao ciberespaço (…)*
			João Pacheco (Cyberprotech)	*(…) tornou-se um espaço tão comum como o espaço "real" em que vivemos (…) diria que existem cada vez mais pessoas a passar tempo no ciberespaço do que na própria vida lá fora! (…)* *(…) rápido e fácil acesso a milhares de informações e dados de qualquer tipo, novas oportunidades de comunicação (…)*
			Bruno Castro (VisionWare)	*(…) o ciberespaço tornou-se uma terminologia corrente no nosso dia-a-dia, em paralelo com o mundo ciberataque (…)* *(…) o acesso à informação (…) na internet a informação corre 24/7 e isto leva-me à segunda premissa – a proximidade e conexão, o ciberespaço torna-nos mais próximos (…)*
		- Plataforma para o futuro	José Casinha (OutSystems)	*(…) o ciberespaço é o "território" onde se governa o mundo nos dias de hoje. A dependência do ciberespaço para o desenvolvimento da sociedade é por de mais conhecida e onde as oportunidades surgem todos os dias (…)* *(…) o ciclo da tecnologia é muito curto o que torna obsoleto muito dos desenvolvimentos realizados deixando um rasto de vulnerabilidades que quando exploradas se podem tornar em ameaças (…)*

			Pedro Mendonça (CNCS)	(…) *no ciberespaço não há uma territorialidade clara, ou fronteiras claras, é mais uma dispersão de servidores, de serviços que não obedecem às regras do território nacional clássico e isto traz vulnerabilidades, como por exemplo na identificação dos agentes de ameaça (…)* *(…) um outro aspeto será a complexidade tecnológica. O digital é particularmente complexo, os serviços prestados têm milhões de linhas de código, que cada vez que há um novo produto facilmente traz novas vulnerabilidades que ainda não foram estudadas. Por isto mesmo é que temos atualizações todas as semanas dos sistemas para evitar a retensão de tantas vulnerabilidades (…)*
			Francisco Nina Rente (Art Resilia & The Rock)	*(…) qualquer sociedade, da mais evoluída à menos evoluída, tem uma dependência tecnológica do ciberespaço que permite um ataque avassalador (…)"* *(…) a nível de comunicação, cognitivo, análise, presença, o ciberespaço será o plateau para a sociedade no futuro (…)* *(…) é o ciberespaço que vai garantir a comunicação sem barreiras, a expansão cultural, a troca de capacidades cognitivas que no passado necessitavam e estavam dependentes de uma presença física (…)*
Ciberterrorismo	Evolução da tipologia de ameaças	- Sofisticação das ameaças - 11 de setembro no ciberespaço	José Tribolet (IST)	*(…) como o ser humano aperfeiçoou ao longo de muitos anos as técnicas sofisticadas de matar outros, o ciberespaço é o espaço natural onde isto ocorre e cada vez mais democrático, por pouco dinheiro se conseguem ter instrumentos para usar (…)*
			Dalila Araújo (OSCOT)	*(…) do ponto de vista do seu potencial, o ciberterrorismo tenderá a ser sofisticado, mais organizado (…) poderá alcançar uma escala superior ao ataque terrorista tradicional dado que os recursos tecnológicos estão em constante dinâmica (…)* *(…) admito que a segurança e a defesa não acompanharam ainda aquilo que o potencial da tecnologia tem para fins ilícitos como um ataque terrorista (…)*
			Sistemas de Informação e Segurança (SIS)	*(…) tem sido possível observar o incremento da ameaça da Cibercriminalidade Internacional empenhada na execução de operações extorsionistas ou de fraude contra alvos com forte dependência na disponibilidade digital (…)* *(…) nesse domínio, determinados atores hostis à segurança no ciberespaço procuram prosseguir as suas determinações estratégicas por via da tentativa de exfiltração de informação classificada ou privilegiada e da construção de mecanismos sub-reptícios de disrupção (…)*
			João Pacheco (Cyberprotech)	*(…) nos dias de hoje, havendo um ataque de tamanha magnitude, teria o poder de parar, literalmente o mundo (…)* *(…) se algum dia, se uma organização terrorista ou entidades com atividades ilícitas tenham em mãos os meios e o conhecimento necessário para lançar um ataque no ciberespaço , complementando com outro ataque no mundo "físico", teremos uma receita para uma catástrofe que poderá ser, inclusive, de uma maior gravidade do que o ataque tão paradigmático como o 9/11 (…)*

			Bruno Castro (VisionWare)	*(…) há 22 anos, as ameaças que encontrávamos à nossa segurança e bem-estar eram, por si só, alarmantes e complexas, hoje estamos perante perigos muitos maiores, em várias frentes (…)* *(…) se o 11 de setembro é considerado, por muitos, como o dia que mudou o mundo – com claras melhorias físicas à segurança coletiva – talvez seria benéfico se compreendêssemos o conceito de ameaça aos dias de hoje (…) e isso inclui a ameaça cibernética como uma das mais perigosas de todos os tempos (…)*
			José Casinha (OutSystems)	*(…) seria possível acontecer no ciberespaço um ataque tão paradigmático como outro 9/11 (…)*
			Pedro Mendonça (CNCS)	*(…) o ataque do 11 de setembro foi um ataque muito simbólico, não gostaria de fazer esta comparação com o ciberespaço. Já houve ataques paradigmáticos no ciberespaço, como por exemplo o WannaCry, os ataques à Estónia, ao Irão, os ataques dos Anonymous, os ataques à Ucrânia, são tudo ataques que vieram criar paradigmas, vieram demonstrar a relevância do ciberespaço e marcar a história (…)*
			Francisco Nina Rente (Art Resilia & The Rock)	*(…) o 11 de setembro não é nada comparado com o que pode ser feito com o ciberespaço. Conceptualmente, a nossa sociedade pode colapsar, no sentido de ficarmos sem energia, sem água, sem cadeias de alimentação, sem comunicações, sem nada (…)* *(…) passaram-se 20 anos e há muita coisa a ser feita a nível técnico, político, académico, mas ainda assim o caminho é muito ténue, pois isto contrabalança muito com a obtenção de lucro (…)*
Organizações Internacionais	Prevenção e proteção	- Melhoria das políticas	José Tribolet (IST)	*(…) nas organizações, para que o seu funcionamento seja adequado, deve existir um nível de awareness (entreprise self awareness) suficiente, ou seja, aplica-se o conceito de "consciência de si" e cada empresa deve ter um grau específico desta consciência. Este conhecimento é ajudado com o empowerement que a tecnologia colocou ao nosso dispor (…)*
			Dalila Araújo (OSCOT)	*(…) a UE rapidamente vai ter que produzir mais orientações, mais enquadramento formal para os Estados-Membros para que eles sejam obrigados a agir (…)* *(…) no mundo em rede onde nós vivemos tem aqui a complexidade e uma conetividade de tal forma que a própria legislação e as obrigações da UE têm de ser mais rígidas, mais assertivas na proteção do ciberespaço (…)*
			Sistemas de Informação e Segurança (SIS)	*(…) está em causa o conceito alargado e aglutinado de segurança que exige uma abordagem estratégica integrada e coordenada entre vários parceiros de segurança de forma a conter riscos. Deste modo, criar sinergias, clarificar e efetivar o sentido da política de segurança interna no espaço europeu constitui um objetivo relevante (…)* *(…) reforçar a cooperação operacional e a troca de informações entre as diversas autoridades, na definição de uma base legal comum, através da utilização de metodologias mais efetivas, com recurso a novas ferramentas e aplicações tecnológicas (…)*

		- Cooperação	João Pacheco (Cyberprotech)	(…) a *UE tem instrumentos Jurídicos para ajudar a proteger os seus Estados-membros, tais como a Diretiva SRI, o regulamento da Cibersegurança da UE, tem uma vasta Base Jurídica para o efeito (…)* *(…) o combate às ciberameaças passou a fazer parte das prioridades da agenda política da UE onde os ativos que carregam maior grau de importância são as infraestruturas críticas essenciais para o funcionamento da sociedade (…)* *(…) continua a ser importante e necessária a atualização de políticas e processos para que cada vez seja mais fácil e simples a partilha de informações entre entidades responsáveis pela Cibersegurança de cada um dos Estados-Membros (…)*
			Bruno Castro (VisionWare)	*(…) além de ser fundamental preparar-se uma estrutura capaz de responder às ameaças que vêm do exterior, investindo na tríade de segurança (pessoas, processos e tecnologia), é fundamental olhar para dentro de cada organização, sensibilizar e formar as pessoas para que estas sejam conscientes e não se transformem em veículos de ameaça (…)*
			José Casinha (OutSystems)	*(…) deve ser parte integrante de um sistema de defesa que devem integrar estas organizações, juntamente com a estrutura organizada dos estados membros que deve incluir a sociedade civil também (…)*
			Pedro Mendonça (CNCS)	*(…) tem sido feito muita coisa ao nível europeu, nomeadamente a diretiva SRI, a transposição para Portugal do regime jurídico do ciberespaço, virá ainda uma nova versão desta diretiva mais abrangente. O CNCS tem uma boa articulação com as entidades nacionais e internacionais, nomeadamente a NATO. Têm-se observado um esforço do ponto de vista da regulamentação, para que estes aspetos sejam considerados (…)*
		- Evolução das estruturas organizacionais	Francisco Nina Rente (ArtResilia & The Rock)	*(…) a UE e a ONU, na minha perspetiva, terão uma missão muito mais larga, não necessariamente bélica, pela sua essência terão a preocupação primeiro pelas pessoas e depois eventualmente com os interesses económicos oriundos da guerra (…)* *(…) a UE tem vindo a fazer um caminho brilhante nos últimos anos, é líder mundial na implementação de regulamentação, que tem criado mudanças gigantes – por exemplo, o caso do GDPR que está focado na privacidade de dados, mas que é uma engrenagem importantíssima no contexto de combate à ciberguerra e ciberterrorismo (…)* *(…) a omnipresença e a interligação que existe impede que qualquer coisa seja feita noutro sentido. Por isso, organizações como a ONU, como a UE e eventualmente a NATO nos seus âmbitos, têm que operar numa ótica de "proteger os seus, mas proteger todos" (…)*

Cibersegurança	Revisão das prioridades	- Proteção da informação - Educação/ formação dos cidadãos	José Tribolet (IST)	*(…) é preciso dar base à nação, ou seja, é necessário que as pessoas tenham conhecimento de "quem é dono de quê". Por exemplo, a informação que está nos notariados é importantíssima e tem de ser preservada dado que, caso seja destruída ou alterada, assistiríamos a um reordenamento do país face à ausência de informação credível que nos permitisse verificar a veracidade dos factos, instalando-se uma enorme conflitualidade no país (…)*
			Dalila Araújo (OSCOT)	*(…) é necessária mais educação (…) quando nós temos carta de condução e se andarmos a conduzir, nós sabemos que temos que fazer um determinado conjunto de coisas para nos protegermos, ao nosso automóvel e também protegermos os outros, ou seja, ensinaram-nos a andar nas estradas. Mas ninguém nos ensinou como conduzir-nos no ciberespaço, ninguém nos ensina a identificar os sites, não ensinam crianças nem a nós próprios nem o cidadão comum como é que se protegem de um ciberataque (…)*
			Sistemas de Informação e Segurança (SIS)	*(…) o SIS desenvolve esforços de avaliação de ameaça cibernética, presente e emergente relativa à segurança de informação e comunicações de elevada sensibilidade (…)* *(…) neste domínio têm sido incrementados esforços de avaliação de ameaça cibernética relativa à segurança de informação e de comunicação elevada sensibilidade e à introdução no quotidiano digital de novidades tecnológicas como a tecnologia blockchain, Inteligência Artificial, os equipamentos do universo da Internet das Coisas (IoT) e as futuras redes de telecomunicações de quinta geração (5G) (…)*
			João Pacheco (Cyberprotech)	*(…) qualquer Estado deverá priorizar estruturas e processos que estejam ligados ao combate do cibercrime e à ciberdefesa e ter um plano de ação de estratégia nacional de segurança do ciberespaço em vigor (…) proteger as estruturas digitais do Estado e infraestruturas ao funcionamento normal de organismos estatais, como hospitais, sistemas de defesa, área militar, educação, área bancária, redes de energia e de águas (…)* *(…) no caso português, a prioridade diria que passa por adquirimos mais mão de obra e técnicos especializados para a área e de os distribuírem uniformemente pelo território nacional (…) deveríamos ter nas escolas uma disciplina dedicada ao tema, começar a consciencializar e a formar a juventude para que tenhamos um futuro mais preparado e a consciencializar o que é certo e errado (…)*
			Bruno Castro (VisionWare)	*(…) é necessário que os governantes percebam que o ciberespaço apresenta várias ameaças à democracia e aos principais fundamentos de um Estado soberano (…)*

		- Proteção das infraestruturas críticas	José Casinha (OutSystems)	*(…) formar pessoas. Profissionalizar quadros para garantir a segurança dos cidadãos e das organizações. Em termos de comparação, temos polícias e forças militares que protegem a segurança física dos cidadãos e das organizações no território, mas o mesmo não se passa no ciberespaço (…)*
			Pedro Mendonça (CNCS)	*(…) devemos agir a vários níveis ao mesmo tempo. Se olharmos para a estratégia nacional encontramos algumas respostas às várias necessidades. Deve-se agir na área da prevenção e proteção do fator humano, no reforço das autoridades das forças policiais, das forças de defesa e da dimensão civil da cibersegurança, pois esta última é uma dimensão muito forte pois estamos constantemente expostos ao risco do ciberespaço (…)* *(…) deve-se levar a cibersegurança a sério e perceber que esta já não é um paralelo, é um espaço onde nós estamos e onde devemos agir com a mesma preocupação com que agimos no offline (…)*
			Francisco Nina Rente (Art Resilia & The Rock)	*(…) proteger os seus cidadãos, por uma razão muito simples: como em qualquer guerra, a guerra ganha-se com os soldados rasos, não é com os generais. Num cenário de ciberguerra, todos nós somos soldados, no sentido de que as armas dos atacantes são os smart devices. O foco primordial, para além de proteger os cidadãos, é proteger as infraestruturas físicas (…)*
Estado de arte em Portugal	Nível de desenvolvimento	- Ordenamento jurídico	José Tribolet (INESC-ID)	*(…) o espaço virtual não tem ordenamento e é urgente que tenha (…) para que seja operacionalizado, é necessário criar as entidades informacionais (nomes) que devem ser preservadas, defendidas e resilientes a perturbações do ciberespaço. Essas bases estruturadas de entidades informacionais (…)* *(…) é amplamente defendido que são necessárias mais ferramentas tecnológicas, que é necessário mais armamento, mais Forças Armadas. Ou seja, o conceito de defesa sempre foi pensado ao nível físico, quem se pretende defender e qual o território, mas este pensamento ainda não evoluiu, em Portugal, para o espaço virtual (…)* *(…) seria necessário formar um "exército" de milhares de maquis informáticos para lutarem no ciberespaço, o que implicaria uma opção nacional de imersão massiva de muita gente na aprendizagem de conceitos do ciberespaço e de exercícios para a sua defesa (…)*
			Dalila Araújo (OSCOT)	*(…) nós temos orientações sobre a segurança e defesa naquilo que são os ataques por terra, ar e água, mas não temos ainda tão densificada uma orientação para a proteção dos ciberataques (…) aqui tem de haver sempre um plano do ponto de vista legal, do ponto de vista do ordenamento jurídico pois a natureza do ciberterrorismo não compadece com atos isolados, o ciberterrorismo é global, ele corre na internet (…)*

		- Entidades dedicadas à proteção cibernética		*(…) com as empresas a mesma coisa (…) proteger empresas que prestam serviços públicos, que tem informações sensíveis, que prestam serviços de segurança e defesa, pois o ciberterrorismo é um crime no ecossistema da informação, não é físico (…)*
			Sistemas de Informação e Segurança (SIS)	*(…) no caso português, falta quase tudo o que diz respeito às comunicações. Continuamos como o único país da Europa sem autorização legal para aceder aos dados de comunicações por parte dos serviços de informações (…)* *(…) o termo ciberterrorismo pode-se manifestar e gerar impactos relevante e significativos, os serviços de informações e as demais entidades nacionais com competências nesta matéria dispõem de mais um aliado: os responsáveis pela cibersegurança destas entidades que são a primeira linha de proteção dos sistemas e redes informáticas e de resposta em caso de incidente (…)* *(…) felizmente, e nas ultimas décadas, Portugal não foi palco da estratégia violenta de organizações terroristas ou extremistas (…) os serviços de informações e as forças de segurança estão a cumprir a sua missão (…) mas o momento atual encerra demasiadas incertezas securitárias que irão inevitavelmente alterar o quadro atual (…)*
			João Pacheco (Cyberprotech)	*(…) Portugal, em termos de cibersegurança, tem uma rede na primeira linha de combate criada pelo Estado Português: a rede nacional CSIRT, que vem englobar a Diretiva SRI da UE (…)* *(…) os aumentos de ataques informáticos a Portugal têm vindo a aumentar neste ano, com o ataque à Vodafone e à TAP onde milhares de dados de utilizadores foram roubados e posteriormente colocados a disposição na Dark Web, a forte modernização das infraestruturas e a aposta em cada vez mais membros para a rede CSIRT mostra a forma como Portugal está a encarar o crime cibernético como um perigo cada vez mais emergente (…)*
			Bruno Castro (VisionWare)	*(…) creio que Portugal tem dado um grande salto nesta matéria, sobretudo ao nível da mentalidade e mudança de mindset (…) no entanto, como a grande parte dos Estados que compõem a União Europeia, estamos a ano-luz dos EUA ou Israel (…)* *(…) no entanto, quando falamos de ciberterrorismo, creio que o país não está devidamente preparado para responder positivamente a essa ameaça. Aliás, basta compreender, até pelos recentes acontecimentos, o quão relativamente fácil é a um cibercriminosos informações confidenciais ao Estado português ou dados de clientes a empresas nacionais (…)*

			José Casinha (OutSystems)	*(…) Portugal encara o ciberterrorismo como ameaça real, mas com um grande desfasamento entre a palavra e os atos (…) basta ver o que foi a ambição do CNCS que pretendia vir a ser um organismo autónomo e ainda está sob a tutela do GNS cuja missão é diferente (…)* *(…) A capacitação de um organismo desta natureza requere equipas multidisciplinares ativas e focadas nestas temáticas mas em Portugal o assunto é tratado por múltiplos organismos em múltiplas tutelas que vão desde do SIED, PJ, MAI, CNCS que acumulam o Ciberterrorismo com outras atividades (…)*
			Pedro Mendonça (CNCS)	*(…) esta dimensão acaba por ser considerada em todos os esforços de prevenção, de preparação para a reação, de mitigação para ciberataques, portanto diria que Portugal encara o ciberterrorismo como uma ameaça real (…)*
			Francisco Nina Rente (ArtResilia & The Rock)	*(…) Portugal, felizmente, nunca teve assim grandes situações de ciberterrorismo. Este ano está a ser um bocado atípico, temos visto muitas atividades de cibercrime que pode extravasar um pouco para o ciberterrorismo pelo impacto e pela maneira como é feito (…)* *(…) desde serviços secretos a estruturas judiciais, polícias, as forças amardas, a parte civil com o CNCS, a rede nacional CSIRT constituem um conjunto de organismos que de uma ou outra têm vindo a fazer trabalhos que têm sido casos de sucesso muito grandes a nível nacional que demonstram isso (…)* *(…) um país pequeno, com uma economia relativamente pequena, dá a cara a problemas como esses, ao contrário de outros países maiores que não o fazem. Dentro do possível, não estamos mal na luta contra o ciberterrorismo (…)*

Tabela 1 – Tabela de Análise de Conteúdo das Entrevistas Realizadas

Apêndice V

Tabela de contactos

Entidade	Nome	Data de Envio	Insistências	Data da Resposta	Observações
Centro Nacional de Cibersegurança (CNCS)	Pedro Mendonça (Coordenador do Observatório de Cibersegurança)	28/08/2022	19/09/2022	27/09/2022	
Observatório de Segurança, Criminalidade Organizada e Terrorismo (OSCOT)	Dalila Araújo (Vice-Presidente)	28/08/2022	x	1/09/2022	
Instituto Superior Técnico (IST)	José Tribolet (Professor Catedrático)	28/08/2022	x	29/08/2022	
Sistema de Informação e Segurança (SIS)	x	28/08/2022	x	29/08/2022	
Instituto Superior de Ciências Sociais e Políticas (ISCSP)	Teresa de Almeida e Silva	28/08/2022	27/09/2022	2/09/2022	Perguntas enviadas por e-mail mas sem resposta

Polícia de Segurança Pública (PSP)	x	28/08/2022	x	22/09/2022	Necessária uma autorização a nível institucional e não a título particular
Guarda Nacional Republicana (GNR)	x	28/08/2022	x	7/09/2022	Pedido deferido mas sem resultado de resposta
Gabinete Cibercrime da Procuradoria-Geral da República de Portugal (PGR)	x	28/08/2022	x	x	Sem resposta obtida
Serviço de Informações Estratégicas de Defesa (SIED)	x	28/08/2022	21/09/2022	x	Sem resposta obtida
CyberProtech	João Pacheco (Fundador e CEO)	27/09/2022	x	27/09/2022	
VisionWare	Bruno Castro (Fundador e CEO)	27/09/2022	x	29/09/2022	

OutSystems	José Casinha (Chief Information Security Officer)	29/09/2022	x	12/10/2022	
Forças Armadas Comunicações & Eletronics Associations (AFCEA)		10/10/2022	24/10/2022		Sem resposta obtida
Microsoft		10/10/2022	24/10/2022		Sem resposta obtida
Edisoft		10/10/2022	24/10/2022		Sem resposta obtida
Wisdomit		10/10/2022	24/10/2022		Sem resposta obtida

SecureNet		10/10/2022	24/10/2022		Sem resposta obtida
Insígnia do Antigo Combatente – Defesa Nacional (DSCRP)		2/10/2022	x	12/10/2022	Direcionado para entidades que atuam diretamente no objetivo pretendido
Estado-Maior-General das Forças Armadas – Defesa Nacional (EMGFA)		12/10/2022	24/10/2022		Sem resposta obtida
Direção Geral da Defesa Nacional		12/10/2022			Sem resposta obtida
Unidade Nacional ContraTerrorismo da Polícia Judiciária (UNCT da PJ)		27/09/2022			Sem resposta obtida

Art Resilia	Francisco Nina Rente (Cofundador e CEO)	Contacto externo	x	Resposta afirmativa	
Agência da União Europeia para a Cooperação Policial (EUROPOL)		08/06/2022	x	9/06/2022	Pedido negado mas foi enviado um relatório com informações sobre o tema
Agência Europeia de Cibersegurança (ENISA)		08/06/2022	1/10/2022	15/10/2022	Enviadas as perguntas mas sem resposta
CERT-UE		08/06/2022	1/10/2022	07/11/2022	Pedido negado
Centro de Excelência da NATO para a Ciberdefesa Cooperativa (CCDCOE)		08/06/2022	1/10/2022		Sem resposta obtida