NOVAFCSH
FACULDADE DE CIÊNCIAS SOCIAIS E HUMANAS
UNIVERSIDADE NOVA DE LISBOA

A Europa sob Ataque:
A Transnacionalização dos Desafios Cibernéticos na Modernidade Líquida

Relatório de Estágio

Mestrado em

Ciência Política e Relações Internacionais

Especialidade de Relações Internacionais

Versão corrigida e melhorada após defesa pública

Catarina de Barros Almeida
A Europa sob Ataque: A Transnacionalização dos Desafios Cibernéticos na Modernidade Líquida
2022

Agosto 2022

Relatório de Estágio apresentado para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Ciência Política e Relações Internacionais, realizado sob a orientação da Professora Doutora Teresa Ferreira Rodrigues

Aos meus pais, por me mostrarem que os gigantes são,
quase sempre, moinhos de vento.
À Dr.ª Florbela, pelo apoio incansável.

"A vida é um desempate permanente, e o que é preciso é jogar com limpeza e formosura em cada número da caprichosa roleta."

Miguel Torga, *Portugal*

Resumo do Relatório de Estágio

Intitulado *A Europa sob Ataque: A Transnacionalização dos Desafios Cibernéticos na Modernidade Líquida*, este relatório de estágio objetiva descrever as atividades realizadas no decorrer do estágio curricular realizado, entre novembro de 2021 e maio de 2022, na Embaixada de Portugal em Praga, tendo em vista a conclusão do Mestrado em Ciência Política e Relações Internacionais.

O estágio curricular pressupôs a aplicação prática dos ensinamentos teóricos adquiridos na componente letiva do Mestrado, bem como o desempenho de funções de carácter profissional relevante, tendo possibilitado, igualmente, o contacto direto e aprofundado com as atividades concretizadas numa Embaixada.

Neste relatório de estágio, além de se descrever as tarefas, regulares e pontuais, desenvolvidas ao longo do mesmo, analisa-se o impacto da globalização nos ciberataques ocorridos na Europa, entre 2000 e 2020, com especial atenção para o cibercrime, o ciberterrorismo e as ciberguerras.

Palavras-chave: embaixada, ciberataques, globalização, ciberespaço, cibersegurança, Europa

Abstract of the Internship Report

Entitled *Europe under Attack: The Transnationalization of Cyber-Challenges in Liquid Modernity*, this internship report aims to describe the activities undertaken during the curricular internship carried out between November 2021 and May 2022, at the Embassy of Portugal in Prague, in view of the completion of the master's degree in Political Science and International Relations.

The curricular internship aimed at the practical application of the theoretical lessons acquired in the teaching component of the masters, as well as the performance of functions of relevant professional nature, has also made possible the direct and in-depth contact with the activities carried out in an Embassy.

In this internship report, besides describing the regular and occasional tasks developed during the internship, the impact of globalisation on cyberattacks in Europe between 2000 and 2020 is analysed, with particular attention to cybercrime, cyberterrorism, and cyber wars.

Keywords: embassy, cyberattacks, globalization, cyberspace, cybersecurity, Europe

Índice

Introdução

A conceção leibniziana de que vivemos, a todo o instante, no 'melhor dos mundos possíveis', tem permeado a forma como perspetivamos a época em que existimos. Contudo, é impraticável que esta harmonia universal permaneça intocada pelos naturais e irreprimíveis desafios acarretados pela constante evolução global. Um dos exemplos máximos deste progresso é o processo de globalização que, com os seus benefícios e desafios inatos, tem moldado a sociedade que hoje conhecemos no 'melhor dos mundos possíveis'.

Desta forma, a globalização – que o sociólogo Anthony Giddens (1990, p. 64) definiu "*as the intensification of worldwide social relations which link distant localities in such a way that local happenings are shaped by events occurring many miles away and vice versa*" – é um fenómeno que impacta diretamente várias dimensões sociais, originando, concomitantemente, vantagens e desafios sociais, políticos, securitários, económicos e culturais, entre outros. Enquanto alguns reconhecem neste fenómeno, benefícios como a facilidade de trocas comerciais, o encurtamento de distâncias espaciais e temporais e o aumento de uma cultura cosmopolita, proporcionada por um mundo global (Baylis, Smith e Owens, 2014, p. 11), outros identificam na globalização uma forma de capitalismo, a última fase do imperialismo ocidental e um instrumento facilitador do aumento de criminalidade (Baylis, Smith e Owens, 2014, pp. 11-12).

Poderemos, então, afirmar que a globalização tem favorecido as transgressões criminais e, especialmente, a ocorrência ciberataques? A preocupação com a segurança e a criminalidade – em particular com os ciberataques – tem ganho, para Estados-Nação, indivíduos, organizações, entre outros, crescente importância nos anos recentes. A evolução tecnológica, acompanhada de um processo de globalização em que as fronteiras terrestres se mostram cada vez mais difusas, abriu espaço a novas formas de ameaça. Estes fatores, aliados a um gradual processo de desburocratização onde o ciberespaço ganha relevância, à democratização do acesso a dispositivos informáticos e à crescente dependência, pública e privada, da *internet* – numa época de contínua virtualização de atividades mundanas –, permitem que todos os detentores de um dispositivo informático sejam um ciberatacante em potencial, uma realidade que representa uma dificuldade acrescida à sua contenção para Estados, sociedade civil, órgãos de polícia criminal e gabinetes de combate ao cibercrime.

Partindo da preocupação com o aumento de criminalidade – em particular dos ciberataques, identificados pelos Estudos de Segurança como uma significativa

preocupação hodierna –, o principal objetivo desta pesquisa é investigar se a globalização foi fomentadora de ciberataques na Europa entre 2000 e 2020, num processo que se estende, anterior e ulteriormente, para além do tempo hodierno, e que demonstra ser um desafio securitário para a defesa europeia.

O estágio curricular realizado na Embaixada de Portugal em Praga, promove a aplicação prática dos ensinamentos teóricos obtidos na componente letiva da Área de Especialização em Relações Internacionais do Mestrado em Ciência Política e Relações Internacionais, permitindo, concomitantemente, o desempenho de funções de carácter profissional relevante, através de atividades ligadas à diplomacia político-económica, ao apoio consular à comunidade portuguesa e à interação com outras embaixadas e entidades locais.

Assim, o presente relatório trata, primeiramente, questões referentes à realização do estágio curricular de seis meses na Embaixada de Portugal em Praga, fazendo o enquadramento institucional do Ministério dos Negócios Estrangeiros e da Embaixada e analisando, posteriormente, as relações luso-checas e a diáspora portuguesa na República Checa. No capítulo dedicado à realização do estágio curricular descrevem-se, igualmente, as diversas atividades levadas a cabo no decorrer do mesmo, bem como a ocorrência de ciberataques no passado recente da República Checa.

Num momento posterior, este relatório – alicerçando-se nos Estudos de Segurança – investiga a ocorrência de ciberataques na Europa e a possível influência da globalização nestes eventos, numa investigação acompanhada por questões referentes à evolução tecnológica, à literacia digital e à cooperação interinstitucional na promoção da ciberdefesa europeia. Discutir-se-á também como a globalização tem promovido a transnacionalização dos desafios, especificamente dos ciberataques, abordando-se, posteriormente, os três grandes núcleos dos ataques cibernéticos: o cibercrime, o ciberterrorismo e as ciberguerras, com o foco sempre direcionado para o impacto destes desafios em solo europeu. Por fim, investiga-se que lições podem ser retiradas dos ciberataques sofridos e da atuação europeia relativamente aos mesmos, e de que forma a Europa pode utilizar o inevitável processo de globalização em prol de uma coesão e cooperação internacional promotora de uma Europa ciberneticamente resiliente, que trabalhe conjuntamente para a ciberdefesa comunitária.

I. Estágio curricular na Embaixada de Portugal em Praga

1.1. Enquadramento institucional

1.1.1. O Ministério dos Negócios Estrangeiros

Localizado no Palácio das Necessidades, em Lisboa, o Ministério dos Negócios Estrangeiros é, desde 1820, o ramo da Administração Pública encarregue da coordenação e execução da política externa portuguesa. Para essa execução, contribuem todos os dias os colaboradores colocados na sua sede, mas também os que asseguram a representação de Portugal em países estrangeiros e organizações internacionais.

De acordo com o *Portal Diplomático*[1], sítio *online* do Ministério dos Negócios Estrangeiros, a Rede Diplomática portuguesa é, atualmente, constituída por 133 postos, divididos em 76 embaixadas, 48 consulados e 9 representações e missões permanentes junto de organizações internacionais. Ainda assim, e apesar da vasta representação portuguesa no mundo, pode assumir-se que a Europa é a grande destinatária destas Missões – acolhendo 29 das 76 Embaixadas portuguesas existentes –, observando-se uma notória sub-representação diplomática nacional nos restantes continentes.

Todavia, se a Europa é o continente que acolhe mais Embaixadas de Portugal, o continente americano é aquele onde está localizado um maior número de consulados honorários – 82 de um total de 226 –, sendo o Brasil o país que acolhe o maior número destas representações (26). Não obstante, importa salientar que os Cônsules Honorários, apesar de terem funções de defesa dos direitos e interesses do Estado Português e dos seus nacionais, não são competentes para a prática de atos consulares (Consulado Geral de Portugal em Nova Iorque, s.d.), não fazendo parte da carreira diplomática portuguesa ou do pessoal administrativo adstrito ao Ministérios dos Negócios Estrangeiros.

Quanto à sua estrutura organizacional, o Ministério dos Negócios Estrangeiros é, desde março de 2022, liderado pelo Ministro João Gomes Cravinho – sucessor do ex-Ministro Augusto Santos Silva –, coadjuvado pelo Secretário de Estado dos Negócios Estrangeiros e da Cooperação, pelo Secretário de Estado das Comunidades Portuguesas e pelo Secretário de Estado da Internacionalização.

Sob a administração direta do Estado português, ainda que sob a direção do Ministério dos Negócios Estrangeiros, encontram-se também, a Secretaria-Geral do Ministério dos Negócios Estrangeiros – liderada pelo Embaixador Álvaro Mendonça e Moura –, a Direção-Geral de Política Externa – liderada pelo Embaixador Rui Vinhas –,

[1] Para mais informações *vide* https://portaldiplomatico.mne.gov.pt/.

a Direção-Geral dos Assuntos Europeus – liderada pela Embaixadora Helena Malcata –, a Direção-Geral dos Assuntos Consulares e das Comunidades Portuguesas – liderada pelo Embaixador Luís de Almeida Ferraz – e a Inspeção-Geral Diplomática e Consular – liderada pela Ministro plenipotenciário de 1ª classe Maria José Morais Pires.

1.1.2. A Embaixada de Portugal em Praga

Localizada naquele que é tido como o 'bairro diplomático' de Praga, devido à considerável quantidade de representações diplomáticas ali situadas, a Embaixada de Portugal em Praga é um serviço periférico externo que abriga, para além da sua secção diplomática – encarregue das relações bilaterais nas suas múltiplas vertentes (Portal Diplomático, s.d.a) –, uma secção consular – dedicada à prestação de serviços de assistência e socorro, registo e notariado e emissão de documentos de identificação e viagem, a nacionais residentes no estrangeiro (Portal Diplomático, s.d.a).

A Embaixada de Portugal em Praga é, assim, a única Missão diplomática portuguesa na República Checa, não se localizando naquele país, dissemelhantemente de outros Estados europeus, outros tipos de representações, como é o caso de Consulados Gerais ou Vice-Consulados, ocorrência justificada pela relativamente diminuta comunidade portuguesa residente naquele território.

Não obstante o reduzido número de portugueses a residir na República Checa, importa salientar que a jurisdição da Embaixada de Portugal em Praga, se estende apenas a território checo, sendo que os países seus vizinhos, isto é, a Alemanha, a Áustria, a Eslováquia e a Polónia, têm as suas próprias Missões diplomáticas portuguesas. Também por este motivo, a Embaixada de Portugal na República Checa – presente na, anteriormente na Checoslováquia, desde 1974 – é relativamente pequena, quando comparada com outras Missões portuguesas situadas na Europa e no Mundo, sendo composta por apenas quatro funcionários – dois pertencentes à carreira diplomática – Chefe de Missão e Chefe de Missão Adjunto – e dois pertencentes à categoria de pessoal administrativo.

1.2. Relações luso-checas

Depois de estabelecidas as primeiras relações diplomáticas com a, à época, Checoslováquia, em 1921, Portugal continuou, ao longo do século XX, o seu trabalho de fortalecimento desta relação bilateral. Importa, contudo, salientar que a 17 de agosto de 1937, Portugal cortou relações diplomáticas com a Checoslováquia depois daquele

governo ter embargado um fornecimento de armas para o Exército Nacional (Portal Diplomático, s.d.b). Estas relações viriam a ser restabelecidas a 27 de junho de 1974, tendo, em novembro do mesmo ano, o diplomata Francisco Quevedo Crespo tomado posse como Encarregado de Negócios, encetando a representação diplomática portuguesa na atual República Checa.

Mas será igualmente importante salientar que relações bilaterais entre Portugal e República Checa não têm apenas carácter diplomático, mas também económico e comercial. Assim, de forma a promover as últimas, em 2016, com o apoio da Embaixada de Portugal em Praga, foi fundada a Câmara de Comércio Checo-Portuguesa (em língua checa, *Česko-Portugalská Obchodní Komora*), cujo principal objetivo é "*promover o desenvolvimento dos negócios entre as empresas checas e portuguesas e incentivar as entidades não-comerciais nas suas actividades na República Checa e em Portugal*." (Câmara de Comércio Checo-Portuguesa, s.d.).

Ademais, a representação portuguesa na República Checa faz-se ainda sentir nos setores do turismo e da educação. No que se refere ao primeiro, localiza-se em Praga, no mesmo prédio que a Embaixada, uma representação do Turismo de Portugal, que tem como objetivo promover turisticamente o nosso país junto da sociedade checa. Quanto à educação e difusão da língua portuguesa na República Checa, Praga acolhe, desde 2004 (Instituto Camões, s.d.), o único centro de língua portuguesa no país, existindo, contudo, leitorados de português nas mais importantes cidades universitárias checas. Ambos os organismos trabalham em estreita colaboração com a Embaixada de Portugal em Praga.

1.3. Diáspora portuguesa na República Checa

Oficialmente, a comunidade lusa na República Checa é, como supramencionado, relativamente reduzida, existindo, oficialmente, em 2021, 816 cidadãos nacionais (Portal Diplomático, s.d.b) com morada naquele país. Contudo, os funcionários da Embaixada, estimam que, entre cidadãos consularmente inscritos e não-inscritos, residam, atualmente, naquele território cerca de dois mil portugueses.

A razão para esta falta de estatística oficial prende-se com o facto de o cidadão português médio, que se encontra temporária ou permanentemente deslocado na República Checa, não proceder à sua inscrição na secção consular da Embaixada de Portugal em Praga, o que não permite à mesma avançar números concretos relativamente à presença nacional naquele país. Todavia, nesta estimativa de dois mil portugueses crê-se que cerca de metade corresponderá, anualmente, ao número de

estudantes nacionais temporariamente deslocados em território checo com o objetivo de prosseguirem a totalidade dos seus cursos superiores nas universidades do país, e não aos estudantes em mobilidade ao abrigo do programa Erasmus+ ou outros semelhantes. Importa salientar que o referido corpo estudantil, na sua maioria alunos de Medicina, se encontra espalhado por diversas cidades checas, nomeadamente, Praga, Plzen, Brno, Hradec Králové e Olomouc, conhecidas pelas suas grandes comunidades universitárias.

1.4. Relatório de atividades desenvolvidas no decorrer do estágio

1.4.1. Atividades Regulares:

- Elaboração de telegramas

O trabalho numa missão diplomática implica a regular comunicação das mais diversas situações para o seu país de origem, isto é, para o seu Ministério dos Negócios Estrangeiros. Este relato regular, feito através de telegramas, é, por defeito, diário, podendo até, consoante a necessidade, ocorrer diversas vezes por dia. Por razões de confidencialidade, não se poderá elaborar neste relatório, a especificidade das matérias tratadas nesses telegramas, podendo, no entanto, revelar-se que a sua maioria versa sobre atualizações da política interna e externa do país onde está instalada a Missão Diplomática – no caso a República Checa –, bem como assuntos relativos a cidadãos portugueses residentes ou de passagem pela República Checa e, nos tempos hodiernos, atualizações permanentes da constante alteração de medidas relativas à COVID-19.

- Acompanhamento de *briefings* para o Conselho Europeu, Conselho dos Assuntos Gerais, Conselho de Justiça e Assuntos Internos, Conselho dos Negócios Estrangeiros, entre outros.

Todos os meses têm lugar diversas reuniões organizadas pelo Conselho Europeu. A esse propósito, e em preparação para as mesmas, os Estados acreditados enviam às Missões diplomáticas que representem países da UE, um documento informativo relativo às suas posições para o Conselho que se realizará. Contudo, o governo da República Checa para além difundir as suas posições por documento escrito, promove também, para determinados Conselhos – como é o caso do Conselho dos Assuntos Gerais (CAG) ou do Conselho de Justiça e Assuntos Internos (JAI) –, *briefings* presenciais ou virtuais. A divulgação das posições checas relativamente ao Conselho dos Negócios Estrangeiros (CNE), Conselho do Ambiente ou Conselho da Agricultura e Pescas, não é, habitualmente, acompanhada de *briefing* presencial ou virtual.

- Acompanhamento permanente da política interna e externa da República Checa

Uma das muitas responsabilidades das missões diplomáticas é acompanhar a política interna e externa dos países onde estão creditadas. Assim, ao longo do meu estágio, acompanhei diariamente, através da leitura da *FleetSheet* e do *website* noticioso *CTK* (*Česká Tisková Kancelář* ou *Czech News Agency*) as informações publicadas, sendo que a leitura destes segmentos informativos por parte dos colaboradores de uma Embaixada, tem sempre como objetivo encontrar informações de interesse que devam ser reportadas à capital do país da missão diplomática. Por essa razão, a informação mais relevante retirada destes e órgãos noticiosos, para além de ser alvo de telegrafia sempre que necessário, é também apresentada e discutida semanalmente, nas reuniões de coordenação da Embaixada de Portugal em Praga.

- Acompanhamento da criação e evolução do recém-indigitado governo checo

Nos dias 8 e 9 de outubro de 2021 ocorreram, na República Checa, eleições legislativas. O resultado destas eleições demonstrou que o partido *ANO* – identificado na República Checa como partido populista –, de que o anterior Primeiro-Ministro, Andrej Babiš, é líder, tinha ganho as eleições sem, no entanto, conseguir obter a maioria absoluta. Esta situação política levou a que as restantes forças mais votadas 'unissem esforços' e, assim, fosse possível formar governo através de uma coligação de cinco partidos. Desta forma, a nova era governativa da República Checa tornou-se particularmente interessante de acompanhar, não só pelo elevado número de partidos em coligação, mas também pelo facto de alguns destes terem concorrido às eleições já coligados. Assim, a coligação *SPOLU* (palavra que em português significa 'juntos') foi integrada pelos partidos *ODS* (Partido Democrático Cívico), *KDU-ČSL* (União Democrática e Cristã – Partido Popular Checoslovaco) e *TOP 09* (partido criado em 2009, de ideologia liberal e conservadora, cuja sigla remete para as palavras *tradição*, *responsabilidade* e *prosperidade*) – identificados como ideologicamente de direita e de centro-direita – e pela coligação liberal progressiva de centro, *Piratí a Starostové* (em português, 'Piratas e Mayors'), formada pelos partidos *Piráti* (trata-se de um partido progressista e liberal cujo nome significa 'Piratas') e *STAN* – abreviatura de *Starostové a nezávislí* (em português, 'Mayors e Independentes').

De facto, indigitar um governo com tantos partidos só foi possível porque os líderes desses mesmos partidos tomaram posse não apenas como ministros, mas também na qualidade de Vice-Primeiro-Ministro. A par deste facto, o novo governo checo enfrentou, ainda antes da sua indigitação, diversas polémicas tendo a mais notória sido o facto de o Presidente da República Checa, Miloš Zeman, se ter recusado durante algum

tempo a indigitar Jan Lipavský – escolhido pelo Primeiro-Ministro Petr Fiala – para Ministro dos Negócios Estrangeiros.

Na realidade, as escolhas de Petr Fiala – líder do *ODS* e Primeiro-Ministro da República Checa desde 17 de dezembro de 2021 – suscitaram muitas dúvidas não só neste país da Europa Central, mas também nos restantes países europeus, mormente, nos que são também parte da União Europeia. De facto, não só veio a verificar-se que a maioria dos ministros indigitados não têm experiência governativa – ainda que tenham experiência política, por terem feito, na sua maioria, parte da Câmara dos Deputados checa –, como também se descobriu que grande parte dos novos governantes ou não fala inglês ou tem um fraco conhecimento desta língua, o que rapidamente suscitou dúvidas quanto ao seu desempenho nas futuras reuniões ministeriais do Conselho Europeu.

- Criação e atualização de ficheiro com informações relativas a governantes checos

Perante a indigitação do novo governo checo no dia 17 de dezembro de 2021, tornou-se clara a necessidade recolher e tratar informação acerca dos seus integrantes. A compilação deste *dossier* teve como objetivo, não só permitir a rápida consulta de informação relativa aos governantes por parte dos colaboradores da Embaixada, mas, principalmente, permitir que o Embaixador de Portugal para a República Checa se apresentasse nas reuniões com os recém-empossados governantes, munido de toda a informação possível acerca dos mesmos. Assim, fui encarregue, pelo Embaixador Luís de Almeida Sampaio, de proceder a essa recolha e tratamento de informação, tendo, entre os dias 17 de dezembro de 2021 e 12 de janeiro de 2022, dedicado parte do meu tempo à elaboração deste *dossier*. A atualização da referida informação continuou a ser feita nos meses subsequentes, objetivando-se que os futuros estagiários da Embaixada de Portugal em Praga continuem este projeto.

- Participação em reuniões com estudantes portugueses na República Checa

Ainda que, tal como anteriormente referido, não existam números oficiais sobre a diáspora portuguesa na República Checa, estima-se que cerca de metade dos cidadãos nacionais presentes neste país sejam estudantes do ensino superior. Apesar das reuniões entre a Embaixada de Portugal em Praga e os estudantes portugueses terem lugar, costumeiramente, em setembro, época de arranque do ano letivo, no ano de 2021, por motivos vários, não se observou essa regularidade.

Apesar disso, a Embaixada de Portugal em Praga procurou juntar um número considerável de estudantes portugueses na República Checa, tanto estudantes que estão

a realizar a totalidade do seu curso superior neste país, como estudantes do programa Erasmus+, de forma a possibilitar a reunir virtualmente com os mesmos. Esta primeira reunião, realizada no dia 13 de dezembro de 2021, e na qual estive, juntamente com os restantes estagiários da Embaixada, presente, teve como objetivo primordial dar a conhecer a Missão e os seus colaboradores aos estudantes portugueses. Da mesma forma, foi objetivo desta reunião, transmitir a mensagem de que a Embaixada de Portugal em Praga é um ponto de ajuda essencial para os cidadãos portugueses residentes na República Checa, indo o seu escopo de atuação muito para além das funções consulares, mais conhecidas do público geral.

Nesta primeira reunião, os estudantes deram a conhecer as suas preocupações relativamente a vários temas, nomeadamente, à falta de ligações aéreas entre Portugal e a República Checa a preços acessíveis, à falta de apoio psicológico gratuito em língua inglesa, bem como o seu desejo relativamente à existência de uma maior cooperação entre as universidades checas e portuguesas que lhes permita estagiar em hospitais portugueses[2].

Apesar de nesta primeira reunião ter sido claro que, por parte de alguns estudantes, não havia a perfeita noção do que é o âmbito de ação de uma Embaixada, tentou-se, da melhor maneira possível, ir ao encontro dos seus pedidos, contactando-se psicólogos portugueses residentes na República Checa e dando a conhecer a estes estudantes a existência de gabinetes de psicologia e apoio ao estudante internacional nas suas universidades. Da mesma forma, no que respeita à temática das viagens entre Portugal e República Checa, tentámos auxiliar os estudantes na elaboração de um manifesto, a enviar a algumas companhias aéreas, que objetivou reivindicar a existência de valores mais competitivos dos bilhetes de avião para os estudantes portugueses residentes na República Checa.

Nesta primeira reunião foi ainda dado a conhecer a existência do 'Manual de Sobrevivência do Estudante', elaborado pela Embaixada de Portugal em Praga e direcionado aos estudantes portugueses, documento que compila variadíssimas sugestões para melhorar o dia a dia e a integração dos portugueses que se encontram deslocados na República Checa por motivos de estudos.

[2] De recordar que a maioria dos estudantes permanentes, isto é, os que realizam todo o seu curso superior na República Checa, são estudantes do curso de Medicina.

- *Focal Point* da Embaixada para a Presidência Francesa do Conselho da União Europeia

O ano de 2022 iniciou outra fase das presidências tripartidas do Conselho da União Europeia, sendo que, desta feita, o trio se iniciou com França, a que se segue a República Checa e, posteriormente, a Suécia.

A Presidência do Conselho da União Europeia é um acontecimento raro para cada país, uma vez que, tendo de passar a presidência por todos os Estados-membros se torna longo o período de interregno para cada um, razão pela qual, o semestre em que um Estado detém a Presidência do Conselho da União Europeia é, por defeito, altamente dinâmico. A Presidência Portuguesa da União Europeia (PPUE), em 2021, foi, para todas as missões diplomáticas portuguesas sitiadas na União Europeia, um momento de grande dinamismo, tendo a Embaixada de Portugal em Praga organizado, entre janeiro e junho de 2021, variadíssimos eventos no âmbito deste projeto.

A Presidência Francesa do Conselho da União Europeia, que decorreu entre janeiro e junho de 2022, objetivou igualar a dos seus congéneres. Posto isto, a Embaixada de França em Praga contactou, em novembro de 2021, as restantes missões diplomáticas presentes em Praga, e cujos países fazem parte da União Europeia, para que indicassem o seu ponto de contacto relativamente à Presidência Francesa. Posto isto, na nossa Embaixada, essa nomeação recaiu sobre mim, sob a supervisão do Dr. Eduardo Rafael, Chefe de Missão Adjunto.

- Elaboração da *newsletter* mensal relativa a atividades promovidas pela Embaixada, bem como pelo Instituto Camões em Praga e representação do Turismo de Portugal em Praga

A Embaixada de Portugal em Praga, num projeto inovador iniciado em outubro de 2021, traçou como objetivo disponibilizar mensalmente, tanto à comunidade portuguesa na República Checa como a todo e qualquer cidadão que se interesse por Portugal e pela atividade da Embaixada de Portugal em Praga, uma *newsletter* em língua inglesa. Esta *newsletter* relata, primordialmente, os eventos preparados pela Embaixada de Portugal em Praga ou aqueles em que se fez representar por um dos seus diplomatas ou estagiários. Assim, estas notícias, de índole eminentemente político-diplomática, cultural e turística, dão a conhecer à comunidade os eventos em que Portugal esteve representado, bem como futuras atividades, relacionadas com o nosso país, que venham a acontecer na República Checa. Por esta razão, ajudei, ao longo do meu estágio à

elaboração das diversas *newsletters* publicadas, tendo a mesma ficado, no mês de abril de 2022, exclusivamente ao meu encargo[3].

- Preparação/organização das visitas de cortesia recebidas na Embaixada

Quando um novo Chefe de Missão se apresenta no posto que lhe foi atribuído, é costume das práticas diplomáticas que o mesmo preste visitas de cortesia aos seus homólogos. Posto isto, e partindo sempre o pedido do Embaixador recém-chegado, o Embaixador Luís de Almeida Sampaio recebeu, durante o meu período de estágio na Embaixada de Portugal em Praga a visita de cortesia de quatro Chefes de Missão, nomeadamente, e por esta ordem, do Embaixador dos Países Baixos, da Embaixadora de Israel do Embaixador do Peru e da Embaixadora do Brasil. Por esta razão, e fazendo parte das minhas funções assistir o Embaixador de Portugal em Praga na organização da sua agenda, foi também minha função preparar as visitas de cortesia e receber, na Embaixada de Portugal, os Chefes de Missão que realizaram esse pedido.

- Receção e envio de resposta à apresentação das Cartas de Credenciais

Da mesma forma que é costume diplomático a prestação das visitas de cortesia que se acabam de descrever, também é prática comum que, aquando da apresentação de um Chefe de Missão num novo posto, todas as Missões Diplomáticas acreditadas nesse país sejam informadas da apresentação das suas Cartas de Credenciais ao presidente daquele Estado, no caso Miloš Zeman.

As Cartas de Credenciais são um documento emitido pelo Estado acreditante – que deve ser entregue ao Presidente do Estado acreditado –, comprovativas da nomeação do Chefe de Missão para aquele posto determinado. Após a receção e aprovação das Cartas de Credenciais por parte do Presidente do país recetor, o Chefe de Missão passa, assim, a estar oficialmente acreditado para exercer funções na sua Missão Diplomática. Após esta apresentação, é da competência da Missão Diplomática informar as restantes missões acreditadas no seu território de influência quanto à chegada do novo diplomata. Posto isto, é costume as restantes missões, após serem oficialmente informadas da apresentação das Cartas de Credenciais, reconhecerem esta chegada, enviando uma resposta de boas-vindas ao novo Chefe de Missão. Desta forma, durante o meu estágio na Embaixada de Portugal em Praga, rececionei várias vezes este tipo de informação, tendo, sempre que necessário, preparado a resposta adequada às mesmas.

[3] Esta *newsletter* correspondente ao mês de abril de 2022 poderá ser vista no seguinte *link*: https://6g8gi.r.ah.d.sendibm4.com/mk/mr/cLW3F2aC9qsi9qlaZGiZR9cafyn2ihkc99xXJtLOqT5-OHZ1xCg-oMriQT8lji5Kg7Jv8cX8cjMMqVuOisG6PEjNawroDyq3MCSwXIFrauheYvoBPduosdCsP3gyix3LdfvZGg

1.4.2. Atividades pontuais:

- *Working lunch* dos Chefes de Missão da União Europeia com a Presidente da Câmara dos Deputados da República Checa, Markéta Pekarová Adamová

No dia 24 de novembro de 2021, teve lugar, em Praga, um *working lunch* organizado pela Embaixada da Eslovénia em Praga, no âmbito da Presidência Eslovena do Conselho da União Europeia. Este almoço de trabalho foi um momento de encontro e discussão entre a recém-empossada Presidente da Câmara dos Deputados da República Checa, Markéta Pekarová Adamová, e os chefes das missões diplomáticas dos países da União Europeia com representação diplomática na República Checa. Enquanto estagiária da Embaixada de Portugal em Praga, tive a oportunidade de assistir a esta reunião onde se discutiram várias temáticas relativas à União Europeia, à 'nova era' política vivida pela República Checa, bem como o que se podia esperar da Presidência Checa do Conselho da União Europeia, a ter lugar entre julho e dezembro de 2022. Neste encontro discutiu-se ainda a possibilidade de se assistir a um maior envolvimento da República Checa no projeto europeu, nomeadamente através da adoção da moeda única por parte deste país, tendo também sido discutida a necessidade da existência de uma maior representação do género feminino nas instituições europeias e checas, mas, sobretudo, na política em geral.

- Preparação do Mercado de Natal

A preparação do Mercado de Natal, organizado pela Câmara Municipal de Praga 6, território onde a Embaixada de Portugal em Praga se localiza, foi um dos primeiros projetos no qual fui envolvida assim que iniciei o meu estágio. A participação da nossa Embaixada neste mercado tinha dois objetivos principais. Primeiramente, dar a conhecer a atividade cultural portuguesa em Praga, através de uma apresentação musical organizada pelo Instituto Camões em Praga, depois, recolher verbas, através da venda de artigos doados por empresas portuguesas, que seriam posteriormente entregues a uma instituição de solidariedade social checa. Nesta ação, que decorreria no dia 27 de novembro de 2021 e onde também estariam presentes outras missões diplomáticas acreditadas na República Checa e com sede no território da Câmara Municipal de Praga 6, a Embaixada de Portugal estaria representada pelos seus estagiários. Contudo, devido ao forte agravamento da situação pandémica registada na República Checa no fim de novembro de 2021, o evento acabou por ser cancelado pela entidade organizadora, o que impediu a angariação de verbas para as entidades de apoio social escolhidas.

- Ajuda à preparação de conferência na *Anglo-American University*

No início de dezembro de 2021, o Embaixador Luís de Almeida Sampaio recebeu – por parte de Liliana Torres-Muga, atual professora da *Anglo-American University*, em Praga, e antiga embaixadora do Peru para a República Checa – o convite para ser orador numa das suas aulas. Esta *guest-lecture*, que teve lugar no dia 10 de dezembro de 2021, contou com a presença de alunos de Relações Internacionais e teve como principal foco a Presidência Portuguesa do Conselho da União Europeia, intitulando-se "Europe and the World after the Pandemic – A Vision of the Portuguese Presidency of the European Union".

Tendo isto em conta, fiquei encarregue, desde o momento em que o Embaixador de Portugal foi contactado pela sua antiga colega, de ser o ponto de contacto na Embaixada de Portugal para a preparação desta *guest-lecture*. Desta forma, coordenei com a professora da instituição a deslocação do Embaixador Luís de Almeida Sampaio, tendo-me também, no dia 10 de dezembro de 2021, deslocado atempadamente à *Anglo-American University* com o objetivo de preparar a chegada do Embaixador de Portugal para que a aula em questão transcorresse da melhor maneira.

- Gravação da mensagem de Natal do Embaixador Luís de Almeida Sampaio

No dia 10 de dezembro de 2021, na sequência de um pedido de colaboração da revista *Czech & Slovak Leaders* para o envio de uma mensagem de Natal dos Chefes das Missões Diplomáticas acreditadas na República Checa, dirigi-me, acompanhada pelo Embaixador Luís de Almeida Sampaio e por outros estagiários, ao centro da cidade de Praga com o objetivo de proceder à gravação da já mencionada comunicação. Além da mensagem de Natal que foi publicada pela revista *Czech & Slovak Leaders*, foram ainda gravadas mensagens de Natal, em língua portuguesa e inglesa, para publicar nas redes sociais da Embaixada de Portugal em Praga. Estas mensagens revelaram-se um sucesso, tendo sido muito apreciadas pela publicação *Czech & Slovak Leaders*, bem como pelos seguidores das redes sociais da Embaixada.

- Preparação e envio de mensagens de Natal da Embaixada Portuguesa em Praga às restantes Missões Diplomáticas e serviços governamentais checos

A quadra festiva é, por regra, um momento de confraternização e envio de felicitações e desejos de boas festas. Por essa razão, fui incumbida de preparar e enviar para as Missões Diplomáticas acreditadas em Praga, bem como para diversos serviços governamentais, pessoas e instituições de interesse, a mensagem de boas festas da Embaixada de Portugal em Praga.

- Preparação de reuniões com os recém-indigitados elementos do governo checo e acompanhamento do Embaixador Luís de Almeida Sampaio

Na sequência da indigitação do novo governo checo, o Embaixador Luís de Almeida Sampaio expressou a sua vontade de reunir com vários elementos do recém-eleito executivo. Assim, e tendo em vista a possibilitação destas reuniões, contactei os responsáveis dos gabinetes dos governantes identificados, preparando e organizando o agendamento das mesmas.

Ademais, e tendo o Embaixador de Portugal demonstrado vontade em fazer-se acompanhar por outro elemento da Embaixada na maioria das reuniões, acabei por acompanhá-lo à reunião com o Ministro da Educação checo, Petr Gazdík. Estaria também prevista a minha presença nas reuniões com Marian Jurečka (Vice-Primeiro-Ministro e Ministro do Trabalho e dos Assuntos Sociais) e Zbyněk Stanjura (Ministro das Finanças), mas estas acabaram, por diversos motivos, canceladas pelos gabinetes dos respetivos ministros. Todavia, participei ainda numa reunião com Marek Ženíšek, Presidente da Comissão de Negócios Estrangeiros da Câmara dos Deputados da República Checa.

Estas reuniões objetivaram a apresentação de cumprimentos por parte do Embaixador de Portugal para a República Checa, fazer o balanço das relações bilaterais na área de atuação de cada Ministério e discutir a futura presidência checa do Conselho da União Europeia.

- *Focal point* para a estadia e atuação da pianista Maria João Pires em Praga

Janeiro de 2022 trazia consigo a vinda de Maria João Pires, renomada pianista portuguesa, a Praga. Apesar do convite para a atuação, prevista para o dia 8 de janeiro de 2022, na sala de espetáculos *Rudolfinum*, ter surgido por parte da *Orquestra Sinfónica de Praga* (comummente conhecida por *FOK*), a deslocação da pianista à capital checa acontecia sob os auspícios da Embaixada de Portugal em Praga. Posto isto, encarregou-me o Embaixador Luís de Almeida Sampaio de ser o ponto de contacto entre o dramaturgo da *FOK*, Martin Rudovský, que convidou Maria João Pires, e a Embaixada de Portugal em Praga.

Contudo, sucedeu que no dia 30 de dezembro de 2021 recebemos a informação de que, após uma digressão pela Suíça – em que já lhe teria sido muito difícil apresentar-se no seu último evento programado –, Maria João Pires não se encontrava em condições de atuar em Praga, razão pela qual o seu espetáculo seria cancelado, tendo o espaço cultural de dia 08 de janeiro de 2022 sido preenchido pelo pianista russo Alexander

Melnikov. Ainda assim, apesar do cancelamento da pianista, a Embaixada de Portugal em Praga não deixou de ser representada, tendo comparecido ao evento o Chefe de Missão Adjunto, bem como eu e outro estagiário.

- Ajuda à preparação do voto antecipado para as eleições legislativas de 2022

Na sequência do chumbo do Orçamento de Estado de 2022, foram convocadas eleições legislativas antecipadas. Para o efeito, ficou determinado que as mesmas, quando ocorridas em território nacional, teriam lugar no dia 30 de janeiro de 2022. Já os eleitores recenseados em Portugal, mas temporariamente deslocados no estrangeiro, para poderem votar, tiveram de recorrer ao Direito ao Voto Antecipado, exercido nos dias 18, 19 e 20 de janeiro de 2022.

Posto isto, enquanto estagiária da Embaixada de Portugal em Praga, apesar de não me encontrar a realizar o meu estágio nos serviços consulares, fiz, com os restantes estagiários, parte da mesa de voto. Durante o processo do voto antecipado realizei não só as atividades necessárias à devida recolha e validação dos votos dos cidadãos portugueses temporariamente deslocados no estrangeiro, como também tive, nos dias que se seguiram, a responsabilidade de preparar o envio, para território nacional, dos votos recolhidos nesta fase do processo eleitoral.

- Acompanhamento da visita de estudo de estudantes do *Liceu de Rokycany* à Embaixada e ao Instituto Camões em Praga

No dia 12 de janeiro de 2022, a Embaixada de Portugal em Praga recebeu a primeira turma de estudantes checos a aprender português como língua estrangeira. Os estudantes, que se deslocaram da cidade de Rokycany até Praga, visitaram da parte da manhã a Embaixada de Portugal, onde ouviram os funcionários e os estagiários falar um pouco das suas funções, e visitaram, da parte da tarde, o Instituto Camões em Praga.

- Preparação e organização da visita de trabalho a Brno

Em dezembro de 2021, chegou à Embaixada de Portugal em Praga um convite da *Universidade de Masaryk*, localizada na cidade checa de Brno, para que o Embaixador Luís de Almeida Sampaio fosse orador numa conferência com realização prevista para março de 2022. Perante este convite, que o Embaixador de Portugal prontamente aceitou, verificou-se que esta seria uma excelente oportunidade para que o Embaixador pudesse, à margem da conferência, visitar outras entidades locais. Para isso, fui incumbida de organizar logisticamente (transporte e alojamento) a viagem, agendar reuniões com as entidades identificadas e, ainda, preparar uma visita a Slavkov u Bruna, local da Batalha de Austerlitz.

- Preparação de reunião com o Presidente do Tribunal de Contas checo, Miroslav Kala, e acompanhamento do Embaixador Luís de Almeida Sampaio

No dia 02 de fevereiro 2022, o Embaixador de Portugal para a República Checa deslocou-se ao Tribunal de Contas da República Checa com o objetivo de reunir com o Presidente do mesmo. Neste processo, tive como principal função contactar este organismo, solicitando que o seu Presidente recebesse o nosso Embaixador, procedendo, posteriormente, às necessárias ações de cooperação para que este encontro transcorresse da melhor maneira. A reunião foi um sucesso, tendo o Presidente do Tribunal de Contas Checo – também presidente da *European Organization of Supreme Audit Institutions* (*EUROSAI*) – referido haver o objetivo de organizar, em Praga, no verão de 2022, uma reunião pós-Congresso, onde estaria também presente o Juiz Conselheiro José Tavares, atual Presidente do Tribunal de Contas Português.

- Presença no *debriefing* da Cimeira União Europeia-União Africana.

No dia 21 de fevereiro de 2022, teve lugar no *Office of the Government* – equiparável, em Portugal, à Residência Oficial do Primeiro-Ministro, visto ser neste edifício que são ocorrem diversas reuniões governamentais e são recebidos governantes de países estrangeiros – o *debriefing* da Cimeira União Europeia-União Africana, presidido pela, à data, *Sherpa* da República Checa, Jolana Mungengová.

Apesar de este *debriefing* ter tido como principal objetivo abordar a cimeira que tinha ocorrido em Bruxelas nos dias 17 e 18 de fevereiro de 2022, vários outros assuntos foram discutidos para além disso, visto que este foi o primeiro evento oficial do Primeiro-Ministro checo, Petr Fiala. Assim, neste *debriefing* – onde estiveram presentes os Chefes de Missão da União Europeia acreditados em Praga – Jolana Mungengová deu também a conhecer como terá sido a receção de Fiala em Bruxelas, com Ursula von der Leyen a demonstrar-se bastante calorosa no acolhimento deste novo Chefe de Governo. Neste encontro, ocorrido no contexto da Cimeira União Europeia-União Africana, mas cujas conversações foram muito para além das relações Europa-África, Petr Fiala e Ursula von der Leyen discutiram também a transição energética da República Checa e a sua dificuldade, devido às suas características naturais, em produzir energia renovável solar e marítima; discutiram a futura presidência checa – a ter lugar na segunda metade de 2022 – e, relativamente a esta, os desafios que se lhe impõem, bem como os projetos que o governo checo tenciona levar a cabo no decorrer da mesma. Por fim, discutiram a necessidade de capacitar os ministros checos – na sua maioria governamentalmente inexperientes –, tendo a Presidente da Comissão Europeia

demonstrado a maior disponibilidade para ajudar nessa tarefa. A par da Cimeira União Europeia-União Africana e do encontro de Petr Fiala com Ursula von der Leyen, discutiu-se ainda a reunião do Primeiro-Ministro checo e do Chanceler austríaco, o confronto russo-ucraniano, os recentes problemas e violações de direitos na Hungria e na Polónia, a possibilidade do conflito na região do Donbass poder deixar vários países da Europa central, nomeadamente a República Checa, com o fornecimento de gás diminuído, a retirada das tropas do Mali e a sua realocação para outros países e a situação da Embaixada da República Checa em Kiev.

1.5. Os Ciberataques na República Checa: Ocorrências no passado recente

Tendo em conta que a parte investigativa deste relatório se centra na análise de ciberataques e que o estágio curricular a que este relatório se refere ocorreu na República Checa, será também interessante analisar a ocorrência destes eventos neste território, dando-se, no caso, prioridade à análise dos incidentes situados num período temporal mais recente, ao invés do período decorrido entre 2000 e 2020.

Assim, e observando que, em março de 2020, a sociedade foi assolada por uma pandemia global, impera perceber de que forma esta terá afetado, em termos cibernéticos, a República Checa. Durante o período pandémico, praticamente todos os países tecnologicamente avançados observaram um acréscimo no número de ocorrências que colocaram em causa a segurança cibernética, e a República Checa – país de origem da *Avast Software*, empresa que desenvolveu o antivírus *Avast* – também não 'escapou' a esta situação que, naquele território, afetou, sobretudo, unidades de saúde e instituições governativas. De facto, logo no mês de março de 2020, "*Czech officials in Prague have been hit by a large-scale cyberattack, according to the city's mayor*." (Euronews, 2021, s. p.), ataque que foi, desde logo, reportado à *NÚKIB* (*Národní úřad pro kybernetickou a informační bezpečnost*) – "*the central administrative body for cyber security, including the protection of classified information in information and communication systems and cryptographic protection*" (NÚKIB, s. d., s. p.), criada em agosto de 2017. No seguimento desta ocorrência, a, à época, Ministra do Trabalho e dos Assuntos Sociais, Jana Maláčová, "*told the Czech media that the ministry had also been targeted, without giving further details*." (Euronews, 2021, s. p.).

Além deste ataque às entidades governativas, "*Early in the healthcare crisis, a number of Czech hospitals were hacked with ransomware*." (ITA, 2021, s. p.), como foi

o caso do Hospital Universitário de Brno – a segunda maior unidade hospitalar da República Checa – que, em março de 2020, sofreu um ataque cibernético, que obrigou a bloquear toda a rede informática do hospital, a transportar pacientes críticos para outros hospitais (Security Magazine, 2020, s. p.) e a adiar cirurgias programadas (BÎZGĂ, 2020, s. p.). No mês seguinte, também os hospitais de Ostrava e Olomouc foram alvos de ataques informáticos (Lopatka e Muller, 2020, s. p.).

Na República Checa, "*Outdated computer systems have been one of the biggest problems for securing Czech government cyber assets*." (International Trade Association, 2021, s. p.), o que, aliado à cada vez maior ameaça dos ciberataques à segurança nacional, levou, semelhantemente a outros países, à implementação de uma Estratégia Nacional para a Segurança Cibernética (em checo, *Národní strategie kybernetické bezpečnosti České Republiky*), documento que vigorará entre 2021 e 2025.

II. Europa sob ataque: A emergência dos ciberataques e a defesa europeia

O século XX foi um período de mudança abrupta, não só no continente europeu, mas em todo o mundo. Tendo isto em conta, e apesar das 'fronteiras' de análise deste relatório se limitarem ao impacto que os ciberataques[4] tiveram na Europa entre 2000 e 2020, será praticamente impossível fazê-lo cingindo-nos apenas a esses anos. Para tanto, será antes necessário 'viajar' aos Estados Unidos da década de 60 do século XX, mais especificamente ao ano de 1962, onde, em plena Guerra Fria, nascia no *Massachussets Institute of Technology* (*M.I.T.*) o fenómeno global que hoje denominamos de *internet*.

Pela visão de Joseph Carl Robnett Licklider, ou simplesmente J. C. R. Licklider, professor do *M.I.T.*, surgiu o ideal de '*Galactic Network*', "*a concept that envisioned a "globally interconnected set of computers through which everyone could quickly access data and programs from any site*."" (Virkar, 2016, p. 3), tendo Licklider rapidamente ingressado na *Defense Advanced Research Project Agency* (*DARPA*), levando consigo a sua idealização. Na mesma época, um engenheiro polaco-americano que trabalhava na *RAND Corporation*, Paul Baran, demonstrou preocupação com a possibilidade de um líder de um Estado inimigo poder vir a ser tentado a tirar vantagem "*of the ease with*

[4] Toma este trabalho por definição, no que respeita aos ciberataques, ou ataques cibernéticos, a conceptualização presente no glossário do *Computer Research Resource Center* (s.d., s.p.): "An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.".

which military communications could be disrupted, and launch a pre-emptive nuclear strike on the USA circumventing its current digital arrangement." (Virkar, 2016, p. 3).

Assim, resultante da vontade de Licklider em criar uma '*Galactic Network*', da preocupação securitária de Baran e de uma parceria público-privada[5] nasce, em 1966, o projeto *ARPANET* (*Advanced Research Projects Agency Network*), declarado operacional em 1971. O objetivo deste projeto era fazer pesquisa "*on military defence related issues efficient by enabling researchers and their government sponsors to share resources without having to physically deliver them*." (Virkar, 2016, p. 3). Contudo, aquilo que hoje conhecemos como *internet*, mudou muito relativamente à forma como surgiu, tendo dois fatores contribuído para esta mutação. Em primeiro lugar, a *ARPANET* era baseada "*on a decentralized and open architecture which presupposed no concept of central ownership and control*." (Aas, 2007, p. 161), em segundo lugar, este projeto saiu rapidamente da exclusiva esfera militar.

No início dos anos 80 do século XX, o foco da *ARPANET* estava na "*interoperability and reliability as a means of communication and potential command and control in the event of an emergency*." (Winterfeld e Andress, 2013, p. 1). Chegados a meados da década de 90 do século XX – derivada da *ARPANET* – surge a *World Wide Web*, posteriormente difundida à sociedade civil em condições onde "*the Net was able to grow rapidly as anyone could add to the architecture by adding a new service*." (Aas, 2007, p. 161).

Assim, há duas vertentes da *internet* que é preciso notar. Por um lado, o seu carácter algo libertário – fruto da sua característica de rede aberta, totalmente editável e construível – que lhe dá uma particularidade que Katja Franco Aas (2007, p. 161) identificou como ingovernável. Por outro, há a faceta do poder, isto é, "*The Internet has after all its origins in Arpanet, a computer network set up by the US Defense Department in order to build its military might in the Cold War race*" (Castells, 2001 cit. por Aas, 2007, p. 154). Assim, a própria origem da *internet*, ou seja, o facto de esta ter sido criada no decorrer na Guerra Fria e usada para fins de defesa militar, mostra que a mesma é, acima de tudo, um instrumento de poder. Terá sido um instrumento de poder que ajudou a defender os Estados Unidos da América na Guerra Fria, mas é também, atualmente, um instrumento de poder que pode ser usado para atacar.

[5] Os únicos quatro computadores existentes ligados à rede estavam no instituto privado *Augmentation Research Center* (parte do, à época, *Stanford Research Institute*), na *University of California, Los Angeles*, na *University of California, Santa Barbara* e na *University of Utah School of Computing*.

Mas a *internet* não foi o único ponto de mudança no século passado, tendo também a globalização sido causadora de notórias alterações na vida quotidiana. Relativamente a este facto, Turner (2010, p. 3) refere que o tema da globalização "*has in the last two or three decades become established as the key topic of the social sciences*". Assim, e estabelecendo desde já o que aqui se entende por globalização, tomar-se-á por definição deste vocábulo, a apresentada por Baylis, Smith e Owen (2014, p. 9) que identifica a globalização como um "*process of increasing interconnectedness between societies such that events in one part of the world increasingly have effects on peoples and societies far away*.".

No entanto, pode desde já afirmar-se que a perceção perante o fenómeno da globalização não é consensual, tendo sido ao longo dos tempos fator de discórdia entre académicos, representantes políticos e sociedade civil. Esta discórdia assenta no facto de que críticos e proponentes da globalização "*tend to see the phenomenon as either intrinsically bad or automatically good. Some therefore prefer not to use 'globalization' at all, and talk of transnationalization in order to avoid over-generalization*" (Aas, 2007, p. 4). Esta falta de consensualidade assente, sobretudo, na dicotomia benefícios-malefícios que acompanha a globalização, levou Katja Franco Aas (2007, p. 110) a referir que a globalização "*has for a long time been associated with insecurity … and the proliferation of various forms of global risks*.", tendo da também John P. Sullivan (2014, p. 162) mencionado que determinados analistas utilizam o termo 'globalização desviante' para se referirem a atividades ilegais, como é o caso do tráfico de armas ou de pessoas, inevitavelmente favorecidas pelo desenvolvimento da globalização. Sobre esta insegurança aportada pela globalização e característica dos anos 90 do século XX, Anthony Giddens (2001, cit. por Booth, 2014, p. 16) expressou-se com as seguintes palavras: "*Something very new is happening in the world*.", com Booth (2014, p. 16) a completar com "*And it is not necessarily beningn*.". Assim, a década de 90 é, mais uma vez, objeto de referência. Tratou-se de uma época de profundas mudanças em que, ao desenvolvimento gradual da globalização, se juntou, como supramencionado, a abertura da *World Wide Web* à sociedade civil. Estes dois fatores, já de si poderosos quando em singularidade, encontraram na década de 90 do século XX o espaço ideal para o seu robustecimento uno e dual. Verificou-se uma influência mútua que exacerbou benefícios e malefícios de ambas as partes, fazendo suscitar, em grande medida, um dos temas mais preocupantes deste início de século: os ciberataques.

Esta influência recíproca observa-se a partir da libertação da *internet* da exclusiva esfera militar – evento parcialmente responsável pelo facto de a globalização se ter tornado, como já referira Turner, num dos principais objetos de estudo académico –, permitindo alcançar pessoas e conteúdos em lugares distantes, e revelando e encorajando um ideal de aldeia global (Gelernter e Regev, 2010, p. 63). Seria precisamente esta ideia de 'aldeia global' – cunhada por Herbert Marshall McLuhan –, uma sociedade que beneficiava da tecnologia para chegar a um ponto em que as fronteiras físicas perderam a sua importância de outrora, que viria a fazer com que o novo milénio fosse marcado por uma recém-identificada preocupação estatal relativamente aos riscos securitários acarretados por esta nova 'modernidade líquida'.

A noção de 'modernidade líquida' surgiu do pensamento do sociólogo polaco Zygmunt Bauman, que identificou a sociedade contemporânea global como vivendo numa modernidade líquida, leve e fluída. Partindo da conceitualização de Bauman, pode dizer-se que a globalização permitiu uma maior liberdade de circulação de pessoas e bens, bem como uma maior facilidade de troca de informações, promovendo um esforço conjunto para a melhoria de várias áreas de conhecimento na sociedade, entre elas, a tecnologia. Mas é precisamente em virtude do desenvolvimento tecnológico que surgem as primeiras questões relativas ao advento dos ciberataques. Sendo a *internet* e as novas tecnologias fortes utilizadoras de redes interconectadas de informação e, consequentemente, de partilha de dados, a informação passou a estar à distância de um clique, sem a barreira física da distância geográfica, outrora existente, no que Nunes (2016, p. 202) identificou como "*uma rede global … onde as fronteiras geográficas têm cada vez menos relevância*.". A este propósito, Goldsmith (2011, p. 3) acrescentou que a *internet* "*is a borderless medium over which people can communicate globally and instantaneously in ways that seem to resist geographically based regulation*.".

Posto isto, verifica-se que a preocupação – transversal a todo o globo – tem permeado os últimos anos, importando antes de mais perceber que ciberataques são, de uma forma geral, levados a cabo com recurso a meios e/ou dispositivos informáticos, dividindo-se em três grandes núcleos de atuação: o cibercrime, o ciberterrorismo e as ciberguerras. Habitualmente, o mais verificado é o cibercrime, comummente praticado num âmbito doméstico – estando, no entanto, a sua perpetração a nível internacional a crescer de forma exponencial –, por e contra cidadãos comuns. Ainda assim, ciberataques podem também ocorrer numa escala global e transfronteiriça, onde na

maioria dos casos, são os Estados-Nação e relevantes instituições públicas ou privadas as visadas dos ataques.

Tendo isto em conta, há muito que os Estudos de Segurança identificaram os ciberataques e, em particular, o cibercrime[6] como uma das principais preocupações da atualidade. De facto, a "*dependência tecnológica dos Estados e das sociedades cria uma percepção de vulnerabilidade*." (Geraldes, 2019, p. 91), o que levou Estados-Nação a tentarem colmatar esta sensação de insegurança com a securitização do ciberespaço, após uma tomada de consciência da importância do mesmo tanto para instituições estatais ou privadas, como para a sociedade civil. Contudo, e apesar de os Estudos de Segurança terem, há muito, identificado os ciberataques como um tema de análise de particular importância, essa consciencialização por parte de Estados-Nação e de organizações internacionais não é assim tão antiga. Tendo isto em conta, e apesar de os ciberataques serem percecionados como um acontecimento gravoso e, na maioria das vezes, extremamente oneroso, estes têm um enquadramento jurídico relativamente recente quando comparados com delitos que têm, exclusivamente, o espaço físico como local de atuação, havendo ainda muito esforço a ser feito em prol da penalização dos mesmos.

O facto de os ciberataques atingirem, na maioria das vezes, a sociedade civil, fez com que esta rapidamente tomasse conhecimento deste fenómeno. Não obstante tal consciencialização, a maioria da população continua frequentemente a mutar os conceitos de *ciberataque* e *cibercrime* como se de uma coisa una se tratasse, numa confusão que mais não é do que um resultado de paronímia. Se por um lado o público em geral se encontra mais vulnerável a transgressões altamente perturbadoras da vida privada, como é o caso do roubo de identidade, de dados, de ficheiros informáticos ou de informações bancárias – infrações que no escopo dos ciberataques são tipificadas como cibercrimes –, países e organizações são mais frequentemente atingidos por ciberterrorismo ou as ciberguerras.

Apesar da consciencialização europeia para os desafios colocados pelos ciberataques, esta não foi resultado de uma preocupação securitária. De facto, a

[6] A definição de cibercrime não é consensual, no entanto, tomará o presente trabalho como definição a fornecida pelo *Centro Europeu da Cibercriminalidade* da *Europol*: "A cibercriminalidade consiste nos atos criminosos que são cometidos *online* utilizando computadores e redes de comunicações (como, por exemplo, a *Internet*)" (EUR-Lex, 2014, s.p.).

cibersegurança[7] ganhou destaque entre as principais preocupações europeias, mais especificamente da União Europeia, "*no início dos anos 1990, mas não como matéria de segurança*." (Geraldes, 2019, p. 100), antes como preocupação económica, visto que, "*A segurança informática era essencial para o desenvolvimento das economias europeias e para a concretização do Mercado Único."* (Geraldes, 2019, p. 101). Posto isto, poder-se-á considerar que a globalização económica lançou as bases para uma política de ciberdefesa europeia, com a recém-descoberta realidade global a levar também à perceção de que os ciberataques se tratavam "*de uma criminalidade com uma dimensão supranacional, não se limitando às fronteiras da soberania dos Estados-Nação, fluida, flutuante, múltipla, volátil e mimética*" (Elias, 2016, p. 119).

Perante esta nova realidade global, que na Europa ganhava dimensão, tornou-se premente incrementar a ciberdefesa europeia recorrendo à adoção de medidas de combate aos ciberataques. Esta ciberdefesa europeia, foi sobretudo implementada pela União Europeia, que adotou desde cedo medidas para se defender enquanto instituição, e para defender os Estados-membros que a integram. Desta forma, tendo em vista a dissuasão do avanço de ciberataques, que eram ainda recentes, mas já se adivinhavam altamente onerosos para Estados-Nação, União Europeia e sociedade civil, em 2001 – por iniciativa do Conselho da Europa –, tem lugar a Convenção de Budapeste, também conhecida como Convenção sobre o Cibercrime. Esta Convenção, assinada e/ou ratificada por países europeus e por alguns outros Estados-Nação não europeus, foi o primeiro tratado internacional a visar matérias relativas ao cibercrime.

A Convenção de Budapeste teve como objetivo principal, não apenas incentivar a cooperação internacional e aperfeiçoar técnicas de investigação, mas também uniformizar o direito internacional e transpor, para os ordenamentos jurídicos dos países que a ratificaram, decisões e punições relativas ao cibercrime. Contudo, alguns académicos demonstram-se céticos perante a real aplicação dos objetivos desta Convenção. Para isso, Goldsmith (2011, p. 4) opta por referir um estudo, datado de 2009, do *National Research Council* onde se defende a ideia de que uma nação signatária pode recusar cumprir "*with its obligations under the Convention on fairly broad grounds, and the convention lacks an enforcement mechanism to assure that signatories will indeed cooperate in accordance to their obligations*.". Ademais, o

[7] Importa mencionar que, conceptualmente, a União Europeia e os Estados Unidos da América utilizam a palavra *cybersecurity* para se referir tanto ao seu âmbito técnico como governativo/holístico. Em Portugal, a palavra *cibersegurança* aproxima-se de um nível técnico, enquanto o termo *segurança no ciberespaço* compreende a área governativa/holística.

mesmo autor (2011, p. 3) argumenta que a Convenção sobre o Cibercrime é, de uma maneira geral, percecionada como malsucedida, tendo apenas obtido consenso relativo aos crimes informáticos através da adoção de definições vagas sujeitas a diferentes interpretações por diferentes Estados, notando ainda que, mesmo com esta imprecisão, muitas nações fizeram uso do seu direito de reserva no que respeita a determinados artigos desta Convenção. Goldsmith (2011, p. 4) refere igualmente que a inaplicabilidade internacional desta Convenção se torna ainda mais notória, uma vez que "*Every nation was invited to join, but only the United States and two-thirds of Council of Europe states have ratified the treaty*.", fazendo com que deste facto se retire o ensinamento de que os Estados "*significantly disagree about what digital practices should be outlawed and are deeply skeptical about even the weakest forms of international cooperation in this area*." (Goldsmith, 2011, p. 3). Até ao momento apenas 66 países ratificaram a Convenção de Budapeste[8]. Contudo, e na consciência de que a Convenção de Budapeste, apesar de benéfica não é instrumento suficiente para as necessidades contemporâneas de combate a ciberataques, e porque as autoridades judiciárias e policiais dos países que ratificaram esta Convenção têm verificado obstáculos relacionados com o acesso a provas eletrónicas, em junho de 2017 foram iniciadas negociações para o *Second Additional Protocol* que terá como objetivo assegurar uma melhoria na cooperação internacional, esperando-se que este Protocolo fique disponível para ratificação em maio de 2022 (European Comission, 2019). Da mesma forma, a Comissão Europeia (2019) refere que:

> The negotiations on the Second Additional Protocol focus on 4 key elements: measures to improve international cooperation between law enforcement and judicial authorities – including on legal assistance between authorities ("mutual legal assistance"); cooperation between authorities and service providers in other countries; conditions and safeguards for access to information by authorities in other countries; and other safeguards, including data protection requirements.

Mas a Convenção de Budapeste não foi o único instrumento internacional criado com o objetivo de melhorar a segurança cibernética da Europa. Após os

[8] O facto de a Convenção de Budapeste não ter um nível de adesão suficientemente expressivo para uma adequada aplicabilidade que permita a realização dos seus objetivos, levou, em parte, a que em dezembro de 2019, a Resolução 74/247 da Assembleia Geral das Nações Unidas estabelecesse "an open-ended *ad hoc* intergovernmental committee of experts and representative of all regions, to elaborate a comprehensive international Convention on countering the use of information and communications technologies for criminal purposes." (Giovannelli, s.d., para. 1). No dia 29 de junho de 2021, a Rússia apresentou o seu primeiro projeto de Convenção.

ciberataques à Estónia, em 2007 – os quais analisaremos mais à frente –, os países europeus, apoiados pela *Organização do Tratado do Atlântico Norte* (*NATO*), rapidamente entenderam que a cibersegurança e a ciberdefesa era prioridades fundamentais neste início de século. Desta forma, em 2008, observou-se a criação do *NATO Cooperative Cyber Defence Centre of Excellence* (*NATO CCD CEO*)[9] e, em 2013, depois do convite do *NATO CCD CEO* a vários académicos, foi publicado o *Manual Tallinn*, um documento não vinculativo, que versa sobre a aplicação da lei internacional no contexto da cibercriminalidade.

Assim, será praticamente impossível analisar a temática da ciberdefesa e dos ataques cibernéticos na Europa sem abordar, especificamente, a preocupação da União Europeia no que respeita aos desafios que representam os ciberataques. Objetivando garantir a sua ciberdefesa e a repelir o avanço dos ciberataques, a União Europeia cedo adotou medidas para se defender e defender os Estados-Nação que a compõem, bem como garantir a cibersegurança e incrementar a confiança dos seus cidadãos nas redes digitais e sistemas de informação. Posto isto, para além da proposta da Convenção de Budapeste, ocorrida em 2001, nos anos subsequentes verificaram-se variadas ações de promoção da cibersegurança e ciberdefesa europeias. Em 2004, é criada a *The European Union Agency for Cybersecurity* (*ENISA*), localizada em Atenas, com o objetivo de transferir conhecimento "*from the Cybersecurity community to the user groups for the purpose of strengthening cyber defense*." (Skopik, Settani e Fiedler, 2018, p. 138). Em 2013, entra em vigor a Estratégia da União Europeia para a Cibersegurança, com o objetivo de "*orientar a resposta política da União às ciberameaças e aos riscos para a cibersegurança*" (Parlamento Europeu e Conselho da União Europeia, 2019, p. 17), sendo criado, no mesmo ano, o *European Cybercrime Centre* (*EC3*)[10] que ficou sob a alçada da *Europol*. Em 2014, este órgão de polícia criminal reforçou o seu empenho na investigação do cibercrime, tendo criado a *Joint Cybercrime Action Taskforce* (*J-CAT*), que passou a fazer parte do *EC3*. Ademais, em 2007, a *Europol* criou o *Europol Working Group on the Harmonisation of Cybercrime Investigation Training*, com o objetivo primário de providenciar "*experience and knowledge to further enhance the*

[9] O *NATO CCD CEO* encontra-se situado em Tallinn, capital da Estónia. A escolha da localização deste centro de excelência da *NATO* não foi apenas consequência dos ataques ocorridos na Estónia em 2007. De facto, "Estonia had proposed the creation of a "cyber excellence center" in Tallin as far back as 2003, prior to the country's official accession to NATO." (Socor, 2008).

[10] O *European Cybercrime Centre* publica, anualmente, o *Internet Organised Crime Threat Assessment* (*IOCTA*), um relatório estratégico "on key findings and emerging threats and developments in cybercrime" (Europol, 2021).

coordination of cybercrime training, by identifying opportunities to build the capacity of countries to combat cybercrime" (European Cybercrime Training and Education Group, s. d.). Mais tarde, em 2009, a denominação deste grupo foi alterada para *European Cybercrime Training and Education Group* (*ECTEG*) e, a 24 de novembro de 2016, em Bruxelas, este grupo foi oficializado "*através da assinatura da escritura pública de constituição desta organização internacional sem fins lucrativos*"[11] (XXI Governo – República Portuguesa, 2016). O *ECTEG* objetiva, assim, "*apoiar o esforço desenvolvido pelas polícias e magistrados dos Estados membros da União Europeia na luta contra a cibercriminalidade*." (XXI Governo – República Portuguesa, 2016).

Assim, o *ECTEG*, fundado pela *Comissão Europeia* e a trabalhar em estreita cooperação com o *EC3* da *Europol* e o *CEPOL* (*Collège Européen de Police ou European Union Agency for Law Enforcement Training*), "*is composed of European Union and European Economic Area Member States law enforcement agencies, international bodies, academia, private industry and experts.*" (European Cybercrime Training and Education Group, s. d.). Além dos instrumentos supramencionados, vários países europeus, comunitários e extracomunitários, contam com um gabinete *CERT* (*Computer Emergency Response Team*) ou *CSIRT* (*Cyber Security Incident Response Team*). Os gabinetes *CERT*, "*typically contain the Incident Response Teams responsible for the response cycle – Protect, Detect, React, and Recover. This is very similar to the military OODA Loop (Observe, Orient, Decide, and Act).*" (Winterfeld e Andrews, 2013, p. 11).

Nos tempos recentes, permeados por constantes mutações e agravamentos dos desafios securitários, têm sido notórios os esforços dedicados por parte da União Europeia à promoção da sua segurança interna. A este propósito, Katja Franco Aas (2007, p. 146) referiu o seguinte:

> Nevertheless, there seems also to be growing evidence of the relative autonomy of the transnational policing networks from the individual nation states. The development has been pronounced in the context of the European Union and its emerging structures of 'freedom, security and justice'. The Tampare Summit in 1999, the gradual expansion of Europol

[11] O Estado português, representado aquando da assinatura da escritura pública pela Política Judiciária, tornou-se cofundador deste grupo, assumindo também o cargo de sercetário-geral, o que permite ao país "a participação ativa nas linhas de orientação para uma resposta formativa de vanguarda na investigação criminal dos novos desafios apresentados pelo cibercrime e ciberterrorismo" (XXI Governo – República Portuguesa, 2016).

> and the current mobilizations against terrorism have moved the issues of European police co-operation from the relative periphery to be one of the main motors of European co-operation and integration. As Walker (2003: 121) aptly puts it, internal security has changed from a 'poor cousin of European integration' to a mature member of the family, in some regards 'vying for the mantle of head of the family'. The creation of a common European arrest warrant, the newly established network of judicial authorities – Eurojust, the creation of a common European border control agency (Frontex) and the Police Chiefs Operational Task Force – are only some of the newly institutionalized forms of this development.

Posto isto, e tendo em conta o elevado número de agências – dedicadas ao combate aos ciberataques – criadas pela União Europeia, pode concluir-se que, para este organismo, o desafio cibernético contemporâneo é de fundamental importância, o que se comprova pelo facto de a *Europol*, considerar que os mercados em que se observa franco crescimento e dinamismo "*são: o tráfico de drogas sintéticas e de substâncias psicoativas, a contrafação de bens diversos, a cibercriminalidade e os crimes ambientais*." (Elias, 2016, p. 130). Em 2016, a União Europeia publicou a sua primeira legislação para a cibersegurança: a Diretiva (UE) 2016/1148.

Mas, não será possível analisar o combate aos ataques cibernéticos e a promoção da cibersegurança na Europa, sem fazer o mesmo exercício relativamente à realidade portuguesa. Tendo em conta o já mencionado carácter contemporâneo e dinâmico dos ciberataques, não espanta que a sua tipificação criminal em Portugal seja, à semelhança de outras jurisdições, recente. Todavia, urge salientar que Portugal foi pioneiro nesta matéria, publicando, em 1991, a Lei da Criminalidade Informática (Lei n.º 109/91, de 17 de agosto)[12]. Ainda que esta lei não possa ser enquadrada como de combate a ciberataques[13], demonstrava já a vontade do Estado Português em penalizar crimes que recorriam a meios informáticos e/ou ocorriam em sistemas em rede.

Assim, com a manifesta desatualização da Lei da Criminalidade Informática, devido ao crescente número de ciberataques – que se vinham a revelar cada vez mais

[12] Diploma revogado pela Lei n.º 109/2009, de 15 de setembro, vulgo Lei do Cibercrime.

[13] Para uma melhor apreciação da Lei da Criminalidade Informática, é preciso enquadrar a mesma no período temporal da sua publicação. Apesar de este diploma excluir da sua área de abrangência os crimes praticados com recurso à *internet*, contemplando apenas os delitos que recorriam a dispositivos informáticos, importa salientar que a *internet* era, em 1991, em Portugal, uma ferramenta utilizada apenas por certos nichos da sociedade, não estando, diferentemente da atualidade, acessível à generalidade da população, razão pela qual a Lei n.º 109/91 foi, na sua época, manifestamente inovadora.

onerosos para as suas vítimas, fossem elas Estados-Nação, instituições privadas ou cidadãos –, com o incremento da globalização na Europa e com os acontecimentos de 2007 na Estónia, o Estado português viu-se compelido a atualizar a sua lei relativa ao crime informático. Assim, em 2009, surge a Lei do Cibercrime (Lei n.º 109/2009, de 15 de setembro), que viria a revogar a Lei da Criminalidade Informática e que vigora até hoje, tendo transposto para o ordenamento jurídico interno – quase na sua totalidade[14] –, o acordado na Convenção de Budapeste, em 2001.

Concomitantemente, como instrumentos de combate ao cibercrime em Portugal, em 2011, foi criado o *Gabinete do Cibercrime* – que se encontra sob a alçada direta do *Ministério Público*. Em 2015, foi estabelecida a *Unidade Nacional de Investigação da Criminalidade Informática*, que viria a ser substituída[15] pela *UNC3T* (*Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica*), integrada na *Polícia Judiciária*[16] – num modelo semelhante ao usado no *EC3* (*European Cybercrime Center*) da *Europol*. Procedeu-se também à criação do *Centro Nacional de Cibersegurança* (através do Decreto-Lei n.º 69/2014), onde estão integrados o *Observatório de Cibersegurança* e o *CERT.PT.*, sob a direta supervisão do *Gabinete Nacional de Segurança*. O *Centro Nacional de Cibersegurança* é ainda autor do *Quadro Nacional de Referência para a Cibersegurança* (*QNRCS*), que possibilita organizações a "*reduzir o risco associado às ciberameaças, disponibilizando as bases para que qualquer entidade possa cumprir os requisitos mínimos de segurança das redes e sistemas de informação*" (Centro Nacional de Cibersegurança, 2021).

Ademais, deu-se também a criação do *Centro de Ciberdefesa* – exclusivamente dedicado à proteção de informações militares – através do Despacho n.º 13692/2013. Em 2019, a Resolução do Conselho de Ministros n.º 92/2019, no âmbito da estratégia governativa dos anos vindouros, atualizou e aprovou a *Estratégia Nacional de Segurança do Ciberespaço* (*ENSC*), a ser implementada até 2023[17].

Ainda dedicadas, até certo ponto, à identificação atempada de ciberataques, estão as unidades afetas ao *Serviço de Informações da República Portuguesa* (*SIRP*),

[14] O Estado português reservou o direito de não transpor para o seu ordenamento jurídico questões relativas à extradição de cidadãos nacionais, por já estarem contempladas no *Código Penal Português*.
[15] Esta substituição deu-se apenas um ano depois da criação da *Unidade Nacional de Investigação da Criminalidade Informática* e ficou consagrada no Decreto-Lei n.º 81/2016, de 28 de novembro.
[16] Este órgão de polícia criminal detém a competência reservada para a investigação de crimes informáticos, prevista na Lei da Organização da Investigação Criminal, Artigo 7.º, n.º 3, alínea *l)*.
[17] A Estratégia Nacional de Segurança do Ciberespaço 2019-2023 sucedeu à Estratégia Nacional de Segurança do Ciberespaço 2015-2019.

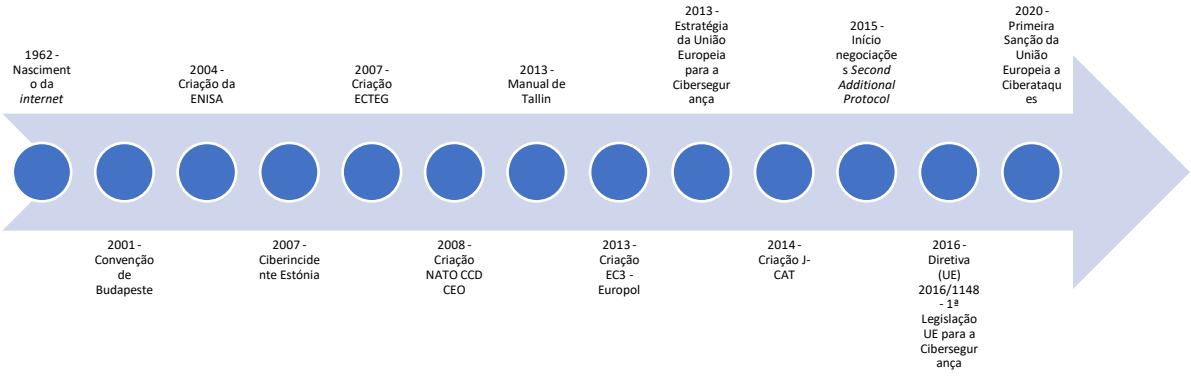
que através da sua atuação permitem identificar e bloquear ciberataques ocorridos em território português ou que possam perigar a segurança nacional.

É ainda de salientar que o Ministério da Defesa Nacional (2013, p. 31976) "*antecipa como grande tendência no ambiente de segurança global, o potencial devastador dos ataques cibernéticos, identificando o ciberterrorismo e a cibercriminalidade como ameaças e riscos prioritários*", estando também o cibercrime referenciado como crime de investigação prioritária, no Artigo 3.º da Lei-Quadro da Política Criminal (Lei n.º 55/2020), em vigor desde 1 de setembro de 2020.

Posto isto, para que se possa avaliar verdadeiramente o impacto da globalização nos ataques cibernéticos ocorridos na Europa entre 2000 e 2020, importa recolher e analisar dados e informações relativos à quantidade e ao grau de perigosidade dos ciberataques ocorridos neste território e período temporal.

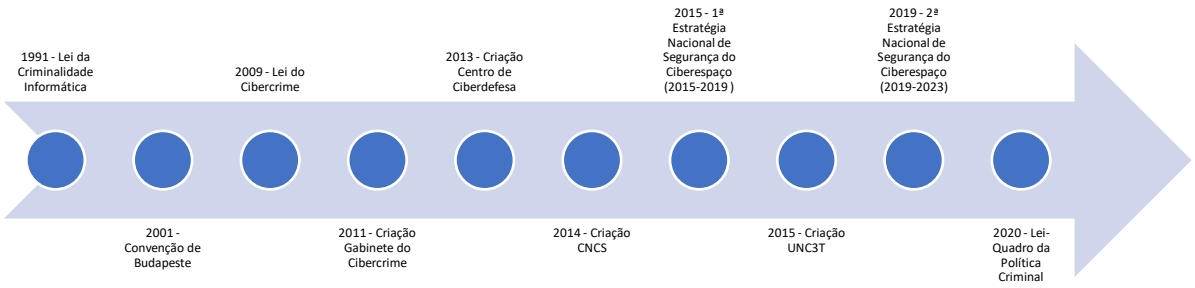
Ainda que órgãos de soberania, órgãos de polícia criminal e académicos já estivessem alerta para a ameaça imposta pelos ciberataques, tendo mesmo o *2006 Riga summit* "*listed possible cyber attacks among the asymetric threats to the common security and acknowledge the need for programs to protect information systems over the long term*" (Socor, 2008), a sociedade civil europeia só 'despertou' verdadeiramente para este alerta em 2007, ano que ficou marcado pelo mais expressivo ciberataque que teve lugar em solo europeu entre 2000 e 2020. Na base deste acontecimento, ocorrido na Estónia, esteve a decisão do governo daquele país em mudar a localização de uma estátua – representativa de um soldado soviético e comemorativa da libertação estoniana da influência Nazi – para um local menos exposto da capital, determinação que despoletou a revolta social da minoria russa radicada naquela nação báltica.

Fig. 1: Cronologia de eventos significativos da História cibernética europeia



Fonte: Elaboração própria

Fig. 2: Cronologia de eventos significativos da História cibernética portuguesa



Fonte: Elaboração própria

Na noite de 26 para 27 de abril de 2007, Tallin foi palco de inúmeros tumultos e detenções, com o país a ser assolado por uma onda de motins e um ataque ciberterrorista[18] levado a cabo por "*digital activists from the Russian diaspora*" (Herzog, 2011, p. 5). O ano de 2007 ficou na História como aquele em que diversas instituições estonianas sofreram um *denial-of-service* (DoS)[19], um ciberataque que teve o objetivo de fazer *crash* nos sistemas informáticos estonianos[20], através de uma multiplicidade de dispositivos que, coordenadamente e através de um grande número de visitas concomitantes – para as quais os respetivos *sites* não estavam preparados – levaram ao *shutdown* de *websites* de jornais e emissoras, "*of all government ministries, two major banks, and several political parties. At one point, hackers even disabled the parliament email server*." (Herzog, 2011, p. 6).

Apesar de a autoria dos ataques cibernéticos de 2007, ter sido reivindicada pelo "*pro-Kremlin youth group Nashi in Transnistria*" (Keating, 2010), os reais perpetradores dos ataques posteriores nunca foram verdadeiramente identificados, uma vez que a Comissão Europeia e os especialistas informáticos da NATO nunca encontraram provas credíveis do envolvimento do Kremlin (Herzog, 2011, p. 6). Contudo, analisando o grau de insurgência da comunidade russa no que respeita à decisão do governo de Tallin, é certo que, conquanto não tenha havido envolvimento direto do governo russo, "*much of the attack was the result of mass mobilization by ethnic Russian volunteers from all over the world*" (Gelernter e Regev, 2010, p. 62).

[18] A Estónia referiu, à época, que os incidentes se trataram de atos terroristas (Johnson, 2015a, p. 178).

[19] Um ataque semelhante a este, com recurso aos mesmos métodos, viria a ocorrer na Geórgia em julho de 2008, tendo ficado desta feita comprovada a autoria russa.

[20] O impacto foi particularmente notório porque há muito que o governo estoniano desburocratizou a nação através de sistemas informáticos, pelo que um ciberataque desta dimensão 'paralisou' o país.

Graças à rápida ajuda da *NATO* e da *UE*, bem como dos seus especialistas informáticos, a Estónia conseguiu recuperar os seus sistemas informáticos. Todavia, surgia agora uma preocupação premente: quais eram as implicações de um ataque cibernético desta dimensão para os restantes países europeus? E que ensinamentos podiam – e deviam – ser retirados deste acontecimento? Era importante colocar estas questões, porque tal como referiu Herzog (2011, p. 11), "*The severity of the Estonian cyber attacks served as a wake-up call to the world*". Mas este incidente cibernético não foi apenas uma chamada de atenção, demonstrou uma faceta da globalização que até então poucas vezes tinha sido observada: a sua capacidade de promover ações disruptivas, em infraestruturas críticas, através do uso de sistemas informáticos e da tecnologia.

Os ciberataques de 2007 também evidenciaram as vulnerabilidades dos países da NATO, das suas instituições e, até mesmo, da própria NATO quanto à disrupção ou penetração dos seus sistemas informáticos (Socor, 2008). Assim, observando a gravidade do ciberincidente, os países europeus, na sua maioria membros da NATO, perceberam que imperava reforçar os sistemas informáticos das suas instituições governamentais, bem como os sistemas de importantes instituições privadas – onde se incluíam, entre outros, instituições financeiras ou de abastecimento de bens de primeira necessidade. O ataque cibernético à Estónia compeliu os países europeus a unirem esforços tanto para proteger o seu ciberespaço como para encontrar soluções para que os culpados de um eventual futuro ataque não ficassem por punir. Assim, a prioridade era legislar e regulamentar de maneira a travar e evitar ataques cibernéticos vindouros, tendo, por essa razão, o papel de atuação da *ENISA* e da *Europol* sido incrementado.

Em 2015 e, mais tarde, em 2016, também a Ucrânia seria atacada, desta feita através do acesso remoto aos centros de controlo de duas companhias de distribuição de eletricidade. A autoria destes ciberataques tem sido atribuída à Rússia – em mais um caso de *hacktivismo* – como maneira de retaliação à progressiva europeização e afastamento ucraniano do governo russo, tendo também estes ciberataques servido de demonstração de força cibernética (Park, Summers e Walstrom, 2017).

Explorando mais aprofundadamente a temática do *hacktivismo*, é possível perceber que este teve um forte impacto nos ataques cibernéticos, tanto numa perspetiva global como europeia. A pletora de motivações dos *hacktivistas*, nomeadamente "*political views, cultural/religious beliefs, national pride, or terrorist ideology*" (Winterfeld e Andrews, 2013, p. 9), levou a que os ataques perpetrados por estes

indivíduos ou grupos[21] se tenham verificado cada vez mais frequentes, públicos e, não raras vezes, perniciosos. De facto, tal como refere Aas (2007, p. 161), a inicial perceção de que a *internet* não pode ser governada, "*went hand in hand with the view that it should not be governed, that governmental intervention was in many ways contrary to its spirit of freedom*". É precisamente esta 'ingovernabilidade' da *internet*, quer em termos próprios, quer por organismos externos, que proporcionou, e proporciona diariamente, ocasiões ideais para que os *hacktivistas* possam, irrestritamente, continuar a sua atividade. Contudo, urge chamar a atenção para a preocupação relativamente ao potencial ónus do *hacktivismo*, isto porque, tal como argumentaram Gelenter e Regev (2010, p. 69), na segunda metade dos anos 90 do século XX, tornou-se habitual ver a *internet* como a 'casa' da radicalização global do discurso político e do ativismo.

Assim, o facto de a *internet* ter surgido, como supramencionado, num formato suscetível a uma permanente edição por uma pluralidade de indivíduos, levou a que a mesma seja, inerentemente, um espaço sem leis, visto que a visão da *internet* "*as an open, boundless frontier had a certain affinity with neo-liberal thinking which similarly promoted the virtues of minimal state intervention*" (Aas, 2007, p. 161). Esta noção da *internet* como espaço apátrida e não subordinado a normas, é reforçada por McCormick (2013, p. 24) que referiu que se existe algum fator que une *hacktivistas* de várias gerações, é a crença de que a informação disponível na *internet* deve ser gratuita.

Em suma, os ciberataques ocorridos na Estónia, em 2007, não foram os primeiros ataques cibernéticos onde se constatou que a *internet* tinha sido uma ferramenta promotora e facilitadora da ação ativista. Ainda assim, o episódio ímpar que se verificou em 2007 foi, certamente, o mais oneroso ataque ocorrido em território europeu, perdurando até aos dias de hoje na memória comum deste continente.

Tendo em conta o referido anteriormente, urge analisar, de forma mais aprofundada e detalhada, a ocorrência de ciberataques na Europa entre os anos de 2000 e 2020. Para tal, utiliza-se, numa perspetiva europeia, os relatórios anuais *Internet Organised Crime Threat Assessment* (*IOCTA*)[22], publicados pelo *European Cybercrime Centre* (*EC3*) da *Europol*, os *Annual Incident Reports*[23], da *ENISA*, que sumarizam

[21] No que a este tema diz respeito, pode considerar-se que o grupo *Anonymous* é, mundialmente, o mais conhecido grupo hacktivista. A respeito do fenómeno hacktivista, Kremling e Parker (2017, p. 136) afirmaram que "Hacktivists, such as the group "Anonymous," engage in political action against a certain person, group, or even nation-state.".

[22] Os *Internet Organised Crime Threat Assessment* (*IOCTA*) foram disponibilizados, pela primeira vez, em 2011.

[23] Os *Annual Incident Reports* foram disponibilizados apenas entre 2011 e 2015.

significativos ciberincidentes denunciados à *ENISA* e à *Comissão Europeia* (ENISA, s.p.), bem como a lista do *Center for Strategic & International Studies*[24], que relata a cronologia dos mais significativos incidentes cibernéticos ocorridos desde o ano de 2006. Numa perspetiva nacional, escrutinar-se-ão os *Relatórios Anuais de Segurança Interna* (*RASI*)[25], cuja dados são obtidos com base nos dados registados, pelos órgãos de polícia criminal portugueses, no *Sistema Integrado de Informação Criminal* (*SIIC*), bem como os *Boletins do Observatório de Cibersegurança*[26], de publicação bimestral.

Assim, e porque aqui se tratam, primordialmente, os ciberataques ocorridos na Europa, importará analisar primeiramente os eventos ocorridos neste continente. De facto, e começando por analisar o *Internet Organised Crime Threat Assessment* (*IOCTA*), cuja primeira publicação teve lugar apenas no ano de 2011, percebe-se rapidamente o quão contemporânea é a preocupação com os desafios do ciberespaço. Se até 2011, a *Europol* publicava os *EU Organised Crime & Threat Assessment*, após esse ano, verificou-se o fortalecimento de uma preocupação securitária no domínio do ciberespaço, com o início da publicação de um relatório dedicado exclusivamente ao tratamento de dados relativos ao cibercrime. Todavia, é notório que o *IOCTA* 2011 mais não é que uma fase embrionária dos relatórios *IOCTA* a que temos acesso hodiernamente, não indo a extensão deste documento além das 11 páginas. Posto isto, e porque a utilização única do *IOCTA* para a análise devida do tema, demonstra ser manifestamente insuficiente, será concomitantemente analisado, o documento intitulado *Significant Cyber Incidents Since 2006*, disponibilizado pelo *Center for Strategic and International Studies* (*CSIS*).

Desta forma, globalmente, e segundo a informação disponibilizada pelo *CSIS*, a Europa não sofreu, até maio de 2007, nenhum ataque cibernético particularmente doloso. De facto, o primeiro grande incidente terá sido mesmo o ocorrido na Estónia que, segundo o *CSIS* (s.d., s.p.), criou um clima de medo nos países ciberdependentes. Em agosto do mesmo ano, informa-nos o mesmo relatório (*CSIS*, s.d., s.p.) que o Serviço Secreto britânico, os gabinetes do primeiro-ministro francês e da Chanceller

[24] O documento *Significant Cyber Incidents Since 2006* é uma lista disponibilizada pelo *CSIS*, fazendo um registo dos eventos em que se registaram incidentes cibernéticos desde o ano de 2006. Este documento, apesar de registar a maioria dos ciberataques de larga escala conhecidos, foca-se, maioritariamente, em ciberataques que têm como alvo agências governamentais, empresas relacionadas com a defesa e a tecnologia, e em ciberataques com contornos de crime económico, que tenham provocado perdas de mais de uma milhão de dólares americanos.

[25] O Ministério da Administração Interna publicou virtualmente o primeiro *Relatório Anual de Segurança Interna* (*RASI*) no ano de 2007, estando neste compilados dados referentes ao ano anterior.

[26] Os Boletins do Observatório de Cibersegurança apenas começaram a ser publicados em março de 2020.

Angela Merkel se queixaram à China na sequência de uma invasão das suas redes informáticas governamentais. De facto, os principais ciberataques de 2007, se não incluirmos o que teve lugar na Estónia, parecem ter tido origem na China, uma vez que, em setembro desse ano, as autoridades britânicas e francesas reportaram invasões aos seus sistemas informáticos, que se crê terem tido origem no Exército de Libertação Popular da China e em grupos de *hackers* chineses (CSIS, s.d., s.p.).

O ano de 2008 aparenta, tendo por base os dois relatórios que aqui se tratam, ter sido mais tranquilo no que respeita a ciberincidentes na Europa. Todavia, em maio, o Ministro da Justiça belga, acusou a China de *hackear* a rede informática do Governo belga (CSIS, s.d., s.p.). Em novembro de 2008, *hackers* invadiram a rede informática do *Royal Bank of Scotland*, clonando 100 cartões bancários e retirando 9 milhões de dólares de contas bancárias (CSIS, s.d., s.p.) e, ainda nesse ano, deputados britânicos foram alertados que *hackers* chineses poderiam, em nome do Parlamento Europeu, ter enviado *emails* com vírus informáticos (CSIS, s.d., s.p.).

Em 2009, no mês de fevereiro, aviões militares franceses não puderam descolar, depois de as bases de dados militares terem sido infetadas com o vírus *confickr* (CSIS, s.d., s.p.). Em junho do mesmo ano, Wolfgang Schaeuble, Ministro do Interior alemão, aquando da apresentação do relatório de segurança relativo ao ano anterior, referiu que a China e a Rússia estavam a aumentar os seus esforços de espionagem, bem como ciberataques a empresas alemãs (CSIS, s.d., s.p.).

Já em 2010, o serviço de segurança britânico *MI5*, alertou para o facto de que agentes infiltrados do Exército de Libertação Popular da China tinham abordado empresários britânicos, oferecendo-lhes *gadgets* eletrónicos infetados com *malware* (CSIS, s.d., s.p.). Em março do mesmo ano, a *NATO* e a *UE* relataram que o número de ciberataques contra sistemas informáticos tinha aumentado significativamente no último ano, com a Rússia e a China entre os principais responsáveis (CSIS, s.d., s.p.). Nesse mesmo mês, a Letónia sofreu um ciberataque, ao serem publicados os valores salariais dos seus governantes (CSIS, s.d., s.p.). No fim do ano, em dezembro, o Ministro dos Negócios Estrangeiros britânico deu conta de ciberataques perpetrados por uma potência estrangeira contra aquele Ministério (CSIS, s.d., s.p.).

Em 2011, ano em que o *IOCTA* foi disponibilizado pela primeira vez, o *CSIS* (s.d., s.p.) registou que *hackers* tinham invadido o mercado de comercialização de carbono da União Europeia. Em março, *hackers* entraram na rede informática do governo francês à procura de informação sobre as futuras reuniões do *G-20* (CSIS, s.d.,

s.p.). Na mesma época, e devido ao mesmo tema, a *Comissão Europeia* e o *Serviço Europeu de Ação Externa* foram alvos de uma alargada ação de ciberespionagem, onde teriam sido procurados documentos sobre a reunião do G-20 que se realizaria em Paris naquele ano (CSIS, s.d., s.p.). No mesmo ano, a polícia alemã e o *Bundeszollverwaltung* descobriram que as bases de dados usadas para localizar suspeitos de crimes graves e terrorismo vinham a ser *hackeadas* desde 2010 (CSIS, s.d., s.p.). Em novembro, os Serviços Secretos noruegueses relataram que 10 grandes empresas norueguesas, ligadas aos setores da defesa e da energia, tinham sido *hackeadas* (CSIS, s.d., s.p.).

No ano seguinte, 2012, a *BBC* reportou uma tentativa de disrupção do seu Serviço de Língua Persa (CSIS, s.d., s.p.) e o governo britânico denunciou invasões bem-sucedidas às redes informáticas do seu Ministério da Defesa (CSIS, s.d., s.p.). Em maio o diretor dos Serviços Secretos britânicos disse que uma empresa britânica tinha sofrido perdas estimadas em 800 milhões de libras resultantes de ciberataques (CSIS, s.d., s.p.).

Em 2013, um ano antes do *IOCTA* começar a ser disponibilizado com regularidade anual, o *CSIS* não registou um grande número de ciberataques em solo europeu, sendo apenas de salientar dois incidentes. O primeiro registo, datado de maio de 2013, dá conta de que durante um mês, os sistemas informáticos de empresas europeias fornecedoras de componentes automóveis foram invadidos por *hackers* não identificados (CSIS, s.d., s.p.), o segundo, ocorreu em novembro, quando o Ministro dos Negócios Estrangeiros finlandês reportou que as suas comunicações diplomáticas tinham sido *hackeadas* (CSIS, s.d., s.p.).

No ano de 2014, quando o *IOCTA* começa a ser publicado com regularidade anual, a problemática do cibercrime e dos ataques cibernéticos na Europa, começa a ser analisada de uma forma mais constante e focada, permitindo construir e robustecer progressivamente a investigação deste fenómeno, tendo sempre em vista perceber a forma como o mesmo impactou e continua, até à atualidade, a impactar este território. Se, por um lado, este *IOCTA* (Europol, 2014, p. 66) informa que a maioria da atividade ligada ao cibercrime, na Europa, se foca na Europa Ocidental e do Leste, por outro informa também que, à época, enquanto muitos ciberataques se originavam na Europa, a maioria destes era direcionada a jurisdições fora deste continente (Europol, 2014, p.67). Neste ano, observou-se também um maior número de ciberataques relativamente ao ano anterior. Em julho de 2014, "*Hackers in Eastern Europe breached energy sectors in the U.S., Spain, France, Italy, Germany, Turkey, and Poland in a major cyberespionage campaign.*" (CSIS, s.d., s.p.). Em setembro, cibercriminosos conseguiram acesso a 300

websites pertencentes a empresas e aos governos da Alemanha, Áustria e Suíça (CSIS, s.d., s.p.) e, em outubro de 2014, "*A five-year cyber espionage campaign attributed to Russia exploits a zero-day vulnerability in Windows software on computers used by NATO, the EU and the Ukrainian government*." (CSIS, s.d., s.p.).

Em 2015, por comparação ao relatório do ano anterior, o *IOCTA* já revelava uma maior incidência da atividade cibercriminosa na Europa, sendo referido que a infraestrutura TIC presente na Europa, particularmente na Europa Ocidental, é invadida por cibercriminosos que a permeiam de vírus informáticos para levar a cabo ciberataques dentro e fora do continente (Europol, 2015, p. 59). No que respeita a ocorrências específicas de ataques cibernéticos, o *CSIS* (s.d., s.p.) regista que, em janeiro de 2015, "*a German steel mill become the second recorded victim of a cyberattack causing physical destruction*. *The attack disrupted control systems so severely that a blast furnace could not be properly shut down*.". Em abril do mesmo ano, *hackers* que diziam pertencer ao *ISIS*, invadiram a rede da *TV5 Monde*, publicando no *website* e redes sociais do canal propaganda pró-*ISIS* (CSIS, s.d., s.p.). Em junho, foi revelado que *hackers* tinham invadido a rede do parlamento alemão, extraindo dados de mais de 20 000 contas dos seus membros (CSIS, s.d., s.p.). No mês seguinte, uma empresa – sediada em Itália – especializada na venda de equipamento de vigilância, viu serem roubados centenas de *gigabytes* de informação privada (CSIS, s.d., s.p.). Em novembro, "*Spies were found to have attempted to hack into the German, French, and Japanese submarine builders bidding for a contract to build Australia's new submarine fleet.*" (CSIS, s.d., s.p.) e, em dezembro, um ataque a empresas de energia do Oeste da Ucrânia, coordenado por *hackers* russos, deixou cerca de 225 000 pessoas sem energia durante 3 a 6 horas (CSIS, s.d., s.p.).

No ano de 2016, o *CSIS* registou um ainda maior número de notórios ciberataques em solo europeu. Apesar de o *IOCTA* deste ano não ter descrito este período, quando comparado com outros, como especialmente problemático, a lista disponibilizada pelo *CSIS* é longa. Em janeiro de 2016, o *Twitter* e o *email* pessoal do Primeiro-Ministro da República Checa foram *hackeados* (CSIS, s.d., s.p.) e, em março desse ano, o Ministério dos Negócios Estrangeiros da Finlândia "*discovered it had been the victim of a four-year breach in their computer network.*" (CSIS, s.d., s.p.). No mês seguinte, na Alemanha, o partido CDU sofreu um ciberataque por parte do um grupo de ciberespionagem russo (CSIS, s.d., s.p.), o que voltou a ocorrer em maio. Em julho, foi descoberto um novo tipo de *malware* utilizado em ciberespionagem, que seria

direcionado a companhias energéticas europeias, (CSIS, s.d., s.p.) e, em dezembro, "*Russian hackers targeted Ukraine's national power company, Ukrenergo, and shut down power to northern Kiev for over an hour.*" (CSIS, s.d., s.p.).

O *IOCTA* de 2017 revelou, interessantemente, que era "*perhaps unsurprising that majority of threats affecting the EU were identified by EU law enforcement as coming from within Europe, in fact more than all the regions outside Europe combined.*" (Europol, 2017, p. 69). Contudo, o mesmo relatório realçou que este facto talvez seja reflexo de uma maior cooperação entre agências policiais europeias (Europol, 2017, p. 69). Apesar disto, o documento não deixa de citar a empresa de segurança informática Panda Security (2017, cit. por Europol, 2017, p. 69) para referir que a Europa "*still has some of the lowest rates of attacked computers globally.*". Relativamente a ciberincidentes, o *CSIS* (s.d., s.p.) registou que, em janeiro de 2017, um instituto sueco dedicado à política externa acusou a Rússia de levar a cabo uma campanha de desinformação com o intuito de diminuir o apoio da população às políticas do governo sueco. No mês seguinte, um ciberataque levou à extração de 600 gigabytes de dados pertencentes a 70 empresas ucranianas, de variados setores (CSIS, s.d., s.p.). O mês de abril foi profícuo no registo de ciberataques, com especialistas em cibersegurança a identificar vários episódios de ciberespionagem, originados na China, contra empresas e governos europeus (CSIS, s.d., s.p.). No mesmo mês, uma empresa publica irlandesa sofreu um ciberataque (CSIS, s.d., s.p.). Em maio de 2017, milhares de *emails* e informações da campanha presidencial de Emmanuel Macron foram publicados após uma invasão, presumivelmente, russa (CSIS, s.d., s.p.). Em junho de 2017, quase 90 membros do parlamento britânico viram as suas contas de *email* comprometidas após um ciberataque (CSIS, s.d., s.p.). No mesmo mês, ciberatacantes russos invadiram as redes informáticas de parte da infraestrutura crítica ucraniana (CSIS, s.d., s.p.). Ainda em junho, na Dinamarca, "*A NotPetya ransomware attack shut down the port terminals of Danish shipping giant Maersk for two days*" (CSIS, s.d., s.p.) e, um grupo de *hackers* russos lançou uma campanha de *spear-phishing* contra Montenegro, após o país anunciar a decisão de se juntar à NATO (CSIS, s.d., s.p.). No mês de julho de 2017, um grupo de *hackers* atacaram um parceiro da italiana *UniCredit*, tendo acedido a dados de 400 000 clientes (CSIS, s.d., s.p.) e os dados da agência de transportes sueca sofreram um ciberataque, tendo sido comprometida informação confidencial militar (CSIS, s.d., s.p.). No mês de agosto, "*The Scottish Parliament suffered from a brute force cyberattack similar to the one that compromised the British Parliament in June.*" (CSIS,

s.d., s.p.). Em setembro de 2017, a Rússia comprometeu os smartphones pessoais de soldados da NATO que se encontravam em missão na Polónia e em países Bálticos (CSIS, s.d., s.p.). Em outubro, o Ministro da Defesa polaco disse que o país tinha repelido uma terceira tentativa de ciberataque, russa, contra infraestrutura crítica (CSIS, s.d., s.p.), tendo também a infraestrutura crítica de países da Europa do Leste sido atacada durante uma 'onda' de ciberataques por *ransomware* (CSIS, s.d., s.p.).

Relativamente ao ano de 2018, enquanto o *IOCTA* corroborou o seu antecessor ao referir que a maioria das "*cyber threats affecting Europe continue to emanate from within Europe, either domestically, or from other European countries.*" (Europol, 2018, p. 67), o relatório de ciberincidentes disponibilizado pelo *CSIS* relata um, ainda maior, número de ciberataques ocorridos na Europa. Em fevereiro de 2018, os *media* alemães relataram que um grupo de *hackers* russos tinha invadido as redes informáticas dos Ministérios dos Negócios Estrangeiros e do Interior alemães, conseguindo obter, pelo menos, 17 *gigabytes* de informação (CSIS, s.d., s.p.), enquanto em março, investigadores de cibersegurança revelaram que um grupo de *hackers* chineses tinha tentado aceder às redes de departamentos governamentais e organizações militares inglesas (CSIS, s.d., s.p.). Em abril, o Centro Nacional de Cibersegurança do Reino Unido denunciou tentativas de ciberataque à infraestrutura crítica do país (CSIS, s.d., s.p.). Em junho, um grupo de *hackers* russo teve como alvos indivíduos em França, Alemanha, Suíça e Ucrânia (CSIS, s.d., s.p.) e, ainda nesse mês, a polícia ucraniana revelou que *hackers* russos teriam atacado, sistematicamente, bancos e companhias de eletricidade ucranianas (CSIS, s.d., s.p.). No mês seguinte, membros dos serviços secretos ucranianos alegaram ter impedido um ciberataque russo a uma central de produção cloro no país (CSIS, s.d., s.p.). Ainda em julho, foi detetado, na Finlândia, um aumento nas tentativas de ciberataque durante o encontro entre Donald Trump e Vladimir Putin, em Helsínquia (CSIS, s.d., s.p.), enquanto "*Russian hackers were found to have targeted the Italian navy with malware designed to insert a backdoor into infected networks.*" (CSIS, s.d., s.p.). Em setembro desse ano, as autoridades suíças revelaram que espiões russos se teriam preparado para usar ferramentas cibernéticas contra o laboratório encarregue de analisar o agente químico usado para envenenar Sergei Skripal (CSIS, s.d., s.p.) e, também nesse mês, foi descoberto que *hackers* russos tinham atacado redes informáticas de instituições governamentais nos Balcãs, na Europa Central e do Leste (CSIS, s.d., s.p.). Em outubro 2018, os Serviços Secretos da Ucrânia anunciaram que um grupo russo tinha tentado atacar os sistemas TIC de grupos

governamentais do país (CSIS, s.d., s.p.) e, no mês seguinte, o *CERT* ucraniano identificou *malware* no sistema informático de agências estatais da Ucrânia, possível precursor de um ciberataque em maior escala (CSIS, s.d., s.p.). Ainda em novembro, a Ucrânia voltou a ser um alvo cibernético depois de a Rússia ter realizado ciberataques coordenados contra o governo e forças armadas ucranianas (CSIS, s.d., s.p.). No mesmo mês, as forças de segurança alemãs anunciaram "*that a Russia-linked group had targeted the email accounts of several members of the German parliament, as well as the German military and several embassies*" (CSIS, s.d., s.p.). Dezembro de 2018 foi também um mês com inúmeras ocorrências em termos cibernéticos, isto porque, os serviços secretos ucranianos bloquearam uma tentativa de disrupção russa contra o sistema da autoridade judicial da Ucrânia (CSIS, s.d., s.p.), a empresa italiana *Saipem* sofreu um ciberataque que desativou centenas dos seus servidores (CSIS, s.d., s.p.) e foi descoberta uma ação cibernética russa que tinha como alvo agências governamentais ucranianas e membros da NATO (CSIS, s.d., s.p.).

O ano de 2019 marcou o fim dos relatórios *IOCTA* como os conhecíamos até ao momento, deixando de estar presente o capítulo identificado como *The Geographic Distribution of Cybercrime*, decisão que levou a que a informação relativa ao continente europeu deixasse de estar sintetizada como anteriormente, passando este relatório a estar dividido por tipologias de crime que ocorrem no ciberespaço. Ainda assim, não obstante as mudanças no *IOCTA*, o *CSIS* continuou a disponibilizar os dados relativos aos ciberataques, permitindo perceber claramente que a incidência destes na Europa tem tido um exponencial aumento anual. Assim, o *CSIS* (s.d., s.p.) registou que, em janeiro de 2019, *hackers* tinham publicado detalhes pessoais, comunicações privadas e informações financeiras de centenas de políticos alemães (s.d., s.p.) e, ainda nesse mês, "*France attributed a cyberattack targeting the Ministry of Defense to a Russian based hacking group.*" (CSIS, s.d., s.p.). Em fevereiro, registou-se que a *Visma* – empresa finlandesa de *software* – foi atacada por *hackers* chineses que tentavam roubar dados dos clients da empresa (CSIS, s.d., s.p.). No mesmo mês, a Airbus revelou ter sido atacada por *hackers* chineses que roubaram informação pessoal de alguns trabalhadores europeus (CSIS, s.d., s.p.), enquanto foi também revelado que *hackers* com ligações aos serviços secretos russos tinham *hackeado*, na Europa, mais de 100 pessoas ligadas a grupos de promoção de democracia e segurança em eleições (CSIS, s.d., s.p.). Em março de 2019, "*Russian hackers targeted a number of European government agencies ahead of EU elections in May.*" (CSIS, s.d., s.p.). Em abril, a polícia finlandesa

identificou um ataque *DoS* contra um *website* usado para publicar resultados de eleições (CSIS, s.d., s.p.). No mesmo mês, na Lituânia, *hackers* levaram a cabo uma campanha de desinformação para desacreditar o Ministro da Defesa lituano (CSIS, s.d., s.p.) e, na Ucrânia, forças armadas e organizações governamentais, foram alvo de *hackers* da autoproclamada República Popular de Lugansk (CSIS, s.d., s.p.). Em agosto de 2019, a República Checa anunciou que o seu Ministro dos Negócios Estrangeiros tinha sido vítima de um ciberataque russo (CSIS, s.d., s.p.). No mês de setembro de 2019, *hackers* conduziram uma campanha de *phishing* contra Embaixadas e Ministérios dos Negócios Estrangeiros de países da Europa do Leste e Ásia Central (CSIS, s.d., s.p.) e, em outubro, "*A state-sponsored hacking group targeted diplomats and high-profile Russian speaking users in Eastern Europe*." (CSIS, s.d., s.p.). No mesmo mês descobriu-se que *hackers* russos tinham como alvo cibernético, desde 2013, Embaixadas e Ministérios dos Negócios Estrangeiros de diversos países europeus (CSIS, s.d., s.p.).

O ano de 2020 continuou a marcado por uma pletora de ataques cibernéticos em solo europeu. Desta forma, o *IOCTA* (Europol, 2020, p. 7) referiu que, ainda que a fraude *online* não seja recente, tem gerado mais preocupação por parte das autoridades policiais, sendo também afirmado que o *ramsomware* continua a ser uma das ameaças mais prementes para organizações pública e privadas na Europa. Assim, o relatório do *CSIS* (s.d., s.p.) revela que, em janeiro, um Estado-nação tinha atacado o Ministério dos Negócios Estrangeiros austríaco durante várias semanas, enquanto em abril de 2020, um grupo *hacker* russo lançou uma campanha de desinformação contra os governos estónio e georgiano (CSIS, s.d., s.p.) e o governo polaco deu a entender que a Rússia estava por trás de uma série de ciberataques à *War Studies University* polaca (CSIS, s.d., s.p.). Em maio de 2020, "*Cyber criminals managed to steal $10 million from Norway's state investment fund*" (CSIS, s.d., s.p.) e, no mesmo mês, as autoridades alemãs descobriram que um grupo de *hackers* ligado à FSB tinha comprometido as redes de infraestrutura crítica alemãs (CSIS, s.d., s.p.). Em julho, autoridades do Reino Unido anunciaram que acreditavam que a Rússia tentou interferir nas suas eleições de 2019 (CSIS, s.d., s.p.) e que tinha tentado roubar informações sobre o desenvolvimento da vacina contra a COVID-19 (CSIS, s.d., s.p.). Em agosto de 2020, representantes do governo ucraniano anunciaram que a Rússia tinha conduzido uma campanha de *phishing* em preparação para o seu Dia da Independência (CSIS, s.d., s.p.), ao mesmo tempo que *hackers* russos comprometeram *websites* noticiosos, publicando notícias falsas que objetivavam desacreditar a NATO perante polacos, lituanos e letões (CSIS, s.d., s.p.). Em setembro

de 2020, a Noruega anunciou que tinha conseguido 'travar' ciberataques aos *emails* de membros e funcionários do parlamento norueguês (CSIS, s.d., s.p.) e, no mesmo mês, um hospital alemão foi alvo de um ataque de *ransomware* que poderá ter levado à morte de um paciente (CSIS, s.d., s.p.). Em outubro de 2020, foi notório o aumento da incidência de ciberataques no continente europeu, sendo que nesse período, foi identificado um grupo dedicado à ciberespionagem que roubava, desde 2011, documentos de governos e empresas da Europa de Leste e Balcãs (CSIS, s.d., s.p.). No mesmo mês, grupos de *hackers* originários da China, Irão e Rússia, lançaram ciberataques contra entidades diplomáticas, organizações governamentais e não-governamentais, universidades, entre outros, com impacto em vários países europeus (CSIS, s.d., s.p.). Em dezembro, a *Agência Europeia do Medicamento* sofreu um ataque cibernético que almejou o acesso ilegítimo a dados relativos ao desenvolvimento da vacina para a COVID-19 (CSIS, s.d., s.p.). No mesmo período, *hackers* chineses atacaram os *emails* de membros e funcionários do parlamento finlandês (CSIS, s.d., s.p.) e, na véspera de Natal, "*hackers hit the Scottish Environment Protection Agency with a ransomware attack.*" (CSIS, s.d., s.p.).

Mas, para além dos ataques cibernéticos na Europa, impera também analisar os ciberataques ocorridos em Portugal, utilizando-se, para tal, o *Relatório Anual de Segurança Interna* (*RASI*), o principal meio de análise criminal em Portugal. Há semelhança do resto da Europa, torna-se notório que, em Portugal, os ciberataques não foram uma preocupação nos anos iniciais do século XXI, só se desenvolvendo uma análise mais aprofundada deste fenómeno passado o primeiro lustro do século. Assim, os crimes relacionados com ou ocorridos no ciberespaço, são mencionados, pela primeira vez, no *Relatório* de 2007, onde se verifica uma primeira abordagem à temática dos ciberataques ou, mais especificamente, ao ciberespaço, numa breve menção ao crime de burla informática, não se verificando, para além desta, nenhuma descrição ou referência pormenorizada relacionada com o que hoje denominamos de cibercrime. No *RASI* de 2008 (p. 211) constata-se uma dedicação um pouco mais aprofundada relativamente ao cibercrime, sendo referido o aumento do mesmo, bem como uma gradual especialização nesta prática criminosa.

O *RASI* de 2009, sofre uma clara remodelação face aos relatórios anteriores. A partir deste ano, o relatório anual de segurança interna passa a apresentar um capítulo dedicado às ameaças globais à segurança, onde se insere também a preocupação com os ciberataques e, especificamente, com o cibercrime. Assim, o *RASI* do ano em apreço,

refere um cenário de desafios colocados à segurança interna que resulta num "*esbatimento das fronteiras entre a segurança interna e externa*" (RASI, 2009, p. 31), assumindo-se também as ciberameaças como ameaças globais e à segurança dos Estados (RASI, 2009, p. 31).

O *Relatório* de 2010 identificou, novamente, as ciberameaças como uma ameaça global à segurança interna, caracterizando-as como um fenómeno de evolução negativa, sendo referido que a crescente monitorização das mesmas tornou possível a "*identificação de ciberatividades potencialmente hostis susceptíveis de ameaçarem a segurança nacional, sobrevindo indícios de que parte das mesmas poderão constituir iniciativas de base governamental*" (RASI, 2010, pp. 46-47).

O *RASI* de 2011 (p. 29), refere as ciberameaças como um dos "*desafios colocados à segurança dos Estados e de organizações, como é o caso da Aliança Atlântica*", considerando também que a preocupação com estes desafios deve ser catalisadora "*para a implementação de uma efetiva estratégia nacional neste domínio*." (RASI, 2011, p. 29) e propondo a "*aprovação de uma estratégia nacional de cibersegurança e de um centro nacional de cibersegurança.*" (RASI, 2011, p.33), sugestão essa que se viria a concretizar nos anos de 2015[27] e 2012[28], respetivamente.

Em 2012, o *RASI*, para além de, há semelhança dos relatórios anteriores, ter reconhecido as ciberameaças como um dos fenómenos em que se observam características de ameaça global, bem como um carácter potencialmente negativo para a segurança interna (RASI, 2012, p. 36), identificou também a "*multiplicidade de fatores de risco e de ameaças relacionadas com o ciberespaço, designadamente no âmbito do hacktivismo, da espionagem e do terrorismo.*" (RASI, 2012, p. 38). Este relatório vem demonstrar o carácter cada vez mais disruptivo dos ciberataques, com as ciberameaças num nível de alerta elevado (RASI, 2012, p. 41), uma vez que sobressaem as ações de indivíduos e organizações detentores de motivação e saber "*para desencadear operações que visam corromper ou desvirtuar o arquétipo securitário do nosso país e das organizações internacionais de que Portugal é membro.*" (RASI, 2012, p. 38).

Em 2013, o *Relatório Anual de Segurança Interna*, voltou a destacar a importância e a necessidade de seguir atentamente os desafios cibernéticos, referindo

[27] Ano em que foi publicado a Resolução de Conselho de Ministros n.º 36/2015, de 12 de junho, documento que aprovou a primeira Estratégia Nacional de Segurança do Ciberespaço, entretanto repensada e reformulada na Resolução de Conselho de Ministros n.º 92/2019, que publicou a Estratégia Nacional de Segurança do Ciberespaço 2019-2023.

[28] A Resolução do Conselho de Ministros n.º 42/2012, de 13 de abril, criou uma comissão instaladora, objetivando a criação e operacionalização do Centro Nacional de Cibersegurança.

que se verificou um aumento de atividade disruptiva nos "*domínios do hacktivismo, da espionagem e do terrorismo*" (RASI, 2013, p. 27), notoriamente levados a cabo por Estados e organizações que usam o ciberespaço para os seus propósitos maliciosos.

No ano de 2014, o *RASI* (2014, p. 114) aprecia, pela primeira vez, mais detalhadamente a cibercriminalidade, visto ser "*uma realidade que tem vindo a ganhar importância no contexto da criminalidade nacional.*". De facto, este relatório vem aprofundar a análise a ciberataques, dedicando uma maior atenção ao tratamento dos mesmos no nosso país. Assim, este *RASI* (2014, p. 114), refere que a *Polícia Judiciária* verificou, na última década, e em contraciclo com a criminalidade geral, um substancial aumento de casos de cibercrime, bem como de casos praticados com recurso a meios informáticos. Da mesma forma, e para além da utilização da *internet* para propósitos de espionagem, terrorismo ou *hacktivismo*, os quais já tinham sido referidos em relatórios de anos anteriores, este documento (RASI, 2014, p. 6) vem agora destacar "*a ameaça da natureza ciber que se manifesta no cibercrime organizado*". Ademais, importa ainda salientar que a atividade cibernética ocorrida no ano de 2014, em Portugal, foi algo diferente dos anos que lhe antecederam. Na verdade, apesar de se ter verificado um declínio na capacidade técnica dos grupos de *hackers* nacionais "*e uma menor capacidade de mobilização, as lacunas de segurança nas infraestruturas informáticas de diferentes serviços e/ou organismos públicos, permitiram operações hacktivistas com alguma gravidade e especial impacto mediático.*" (RASI, 2014, p.12).

O *RASI* de 2015 (p. 45) voltou a evidenciar, no que concerne aos crimes inseridos na área da criminalidade informática e praticados com recurso à tecnologia informática, um aumento dos mesmos, "*destacando-se o crime de burla informática e nas comunicações, que registou um aumento em relação a 2014*.". Todavia, relativamente a esta afirmação, o *RASI* expõe também um dado importante: este aumento pode ser explicado pelo facto de serem agora incluídos não só crimes informáticos – e estruturalmente conexos previstos na Lei do Cibercrime ou outra –, mas também os que "*tratando-se de crimes comuns, podem, em teoria, ser praticados com recurso à tecnologia informática*." (RASI, 2015, p. 45). Também a referência à criminalidade organizada transnacional e, no caso ao cibercrime organizado, que já havia sido feita no *RASI* de 2014, volta a ter lugar no *RASI* de 2015 (p. 78), sendo referido neste relatório que os desafios à segurança interna são também projetados "*no plano transnacional, num quadro de esbatimento das fronteiras entre a segurança interna e externa.*", razão

pela qual o *RASI* de 2015 (p. 83) observou uma "*sistemática construção, disseminação e a expansão*" do cibercrime organizado.

Em 2016, o *RASI* (2016, p. 31) admitiu que, em território português, se verificou um aumento generalizado da criminalidade informática, destacando os crimes de sabotagem informática, dano de dados informáticos e falsidade informática. De referir ainda que o *Relatório* de 2016 (p. 31), referiu, pela primeira vez, os ciberataques como um todo, dizendo que a sua motivação de base continuava a ser, na nua maioria, "*económica (v.g. extorsão, phishing, CEO fraud) e hacktivista (anonymous e movimentos semelhantes)*". Mas, o *RASI* de 2016 não foi apenas inovador devido à sua referência a ciberataques, tendo deixado também o alerta para o facto de que o "*crescimento explosivo de dispositivos conectados, dentro e fora das fronteiras ainda mal definidas da* Internet-of-Things, *poderá contribuir para um aumento da complexidade de criação de ataques*" (RASI, 2016, p. 75).

O *RASI* de 2017 (p. 29) destacou o aumento generalizado da criminalidade informática, particularmente, do crime de acesso ilegítimo ou indevido, devassa por meio informático, falsidade informática e sabotagem informática. Além do mais, este *RASI*, à semelhança do publicado em 2016, continuou a incluir, para além do simples relato e estatística dos crimes, sugestões e alertas, alertando, por isso, para o facto de que "*A ameaça de ciberespionagem tem vindo a agravar-se e vai continuar neste sentido.*" (RASI, 2017, p. 70), adiantando também que, no cibercrime, "*é cada vez mais usual a exploração de vulnerabilidades dos sistemas que contêm dados sensíveis dos seus utilizadores.*" (RASI, 2017, p. 73).

O *Relatório Anual de Segurança Interna* de 2018 identificou em Portugal, em tendência oposta ao que se descreveu anteriormente relativamente ao continente europeu, uma diminuição do número de crimes informáticos registados, tendo convergido "*para este resultado a diminuição verificada no crime de "acesso/interceção ilegítima" e no crime de "sabotagem"*" (RASI, 2018, p. 46). Verificou-se, concomitantemente, uma decrescência relativamente ao *hacktivismo*, continuando a observar-se uma contração das capacidades, e consecutiva redução de presença, dos atores nacionais tanto no plano interno como internacional (RASI, 2018, pp. 79-80). Todavia, apesar da diminuição registada de crimes informáticos, aumentou o "*número de incidentes de cibersegurança em todas as tipologias observadas.*" (RASI, 2018, p. 80). Na realidade, o *RASI* de 2018 torna-se primordial para a perceção da exposição portuguesa ao risco de ciberataques. Este documento alerta para o facto de os

"*incidentes atribuídos a agentes associados a Estados estrangeiros … [continuarem] a ser aqueles que se apresentaram com maior potencial de dano efetivo*." (RASI, 2018, p. 80), adindo que as ciberameaças originadas a partir destes atores estatais, "*continuaram a visar entidades nacionais maioritariamente com o propósito de comprometer sistemas pretendendo a obtenção não autorizada de informação*" (RASI, 2018, p. 80).

Por oposição ao ano anterior, 2019 verificou um aumento substancial da criminalidade informática, tendo concorrido "para este resultado o aumento verificado nos crimes de "*acesso/interceção ilegítima*", de "*sabotagem informática*" e de "*falsidade informática*"." (RASI, 2019, p.47). Por outro lado, este *RASI* (2019, p. 78) reiterou a vulnerabilidade cibernética portuguesa, referindo que, em matéria de ciberataques, existem diversos atores hostis, tanto estatais como não estatais que recorrem à ciberespionagem com o objetivo de aceder a matéria classificada, bem como "*sabotar, desestabilizar e afetar a credibilidade de entidades e indivíduos, com especial incidência em países do espaço euro-atlântico*". Da mesma forma, à margem das ações de espionagem tradicionais, registaram-se "*ações, cada vez mais sofisticadas, de ciberespionagem, hacktivismo e cibercriminalidade.*" (RASI, 2019, p. 80), tendo estas ações sido identificadas como um "*agravamento da ameaça à segurança da informação classificada e privilegiada*" (RASI, 2019, p. 81). No que se refere ao *hacktivismo,* no ano de 2019 registou-se, diferentemente dos anos anteriores, um aumento de incidentes, sendo de notar que, no último trimestre desse ano, se verificou uma maior ligação de atores nacionais aos seus congéneres internacionais, levando-os a integrar ações conjuntas, "*procurando maior protagonismo pessoal ou coletivo, em detrimento da marca ideológica que caracterizava as gerações precedentes.*" (RASI, 2019, p. 81). Neste *RASI* (2019, p. 81) citaram-se também preocupações perante o facto de Portugal ter sido incluído entre os alvos da cibercriminalidade exógena, perpetradora de campanhas massivas de *phishing* e *smishing*, preocupação à qual acresce a ameaça dos ciberataques de carácter extorsionista, que objetivam explorar vulnerabilidades defensivas e securitárias de instituições públicas e privadas, de forma a 'sequestrar' os respetivos sistemas informáticos.

O RASI de 2020, alude ao contínuo crescimento de ciberincidentes, justificando essa tendência com o aparecimento de novos elementos ligados à tecnologia. Terá sido o caso das criptomoedas, área em que se verificou um aumento de caso de extorsão em que, sob ameaça de divulgação de informação privada, se exigiram pagamentos avultados, através de moedas virtuais (RASI, 2020, pp. 66-67). Também a pandemia de

COVID-19, chegada a Portugal em 2020, acarretou novos desafios no campo da cibersegurança e ciberdefesa. De facto, em 2020, o *RASI* (p. 99), identificou, em contexto pandémico, operações cibernéticas ofensivas, realizadas por agentes estatais e não estatais, que visaram entidades públicas e privadas. Assim, em linha com o que aconteceu na restante dimensão do continente europeu, também em Portugal foram detetados inúmeros ciberataques contra "*instituições do setor de saúde, bem como operações de ciberespionagem contra entidades de investigação científica*" (RASI, 2020, p. 99), em campanhas pautadas por *phishing* e *smishing* bancário, *ransomware*, fraude digital e corrupção ao estilo de canais digitais remotos (RASI, 2020, p. 104). Assim, o *Relatório Anual de Segurança Interna* (2020, p. 104) voltou a ter um papel de alerta, referindo que não só se verificou uma tendência de agravamento do cibercrime, mas também, "*num futuro imediato, a possibilidade de multiplicação de eventos disruptivos, à escala global*". Não obstante, o *Eurostat* (2019, cit. por Boletim de Março, 2020, p. 1) refere que "*A percentagem de pessoas a experienciarem incidentes de segurança no uso da Internet para fins privados em Portugal está abaixo da média da UE.*". O *Boletim de Maio* (2020, p. 1) – publicado pelo *Observatório de Cibersegurança* – alerta, no entanto, para o facto de o número de incidentes cibernéticos registados em Portugal ter sofrido um aumento de 84%, entre os meses de fevereiro e março de 2020, enquanto no período de um ano – entre março de 2020 e março de 2019 – se registou um aumento em 176%. O *Boletim de Julho* (2020, p. 1), reiterou o impacto da pandemia COVID-19 no espaço cibernético, referindo que se registou, no decorrer do 1º semestre de 2020, um notório aumento, seguindo de diminuição, do número de ciberincidentes em Portugal – tendo o aumento coincidido com o período inicial de confinamento. Enquanto o *Boletim de Setembro* iterou a tendência de flutuação dos números, o *Boletim de Dezembro* (2020, p. 1) centrou a sua análise nos ataques à administração pública, referindo que, até outubro de 2020, a percentagem de ataques a este setor se centrou nos 33%, embora o número global de incidentes tenha aumentado.

Assim, e tendo em conta o supramencionado, é facilmente percetível que as primeiras duas décadas do século XXI foram marcadas por um crescendo na atividade cibernética de índole dolosa. Se, por um lado, não se verificou uma elevada preocupação com os ataques cibernéticos durante os primeiros anos deste século, não havendo registos aprofundados destes acontecimentos, nem tendo sido criadas agências ou grupos de investigação (nacionais ou internacionais) dedicados a este desafio, por outro, verificou-se a partir de 2004 – com a fundação da *ENISA* – um concreto

investimento dos países europeus e da *União Europeia*, no combate aos danos que esta nova realidade poderia trazer.

O facto de a entrada do século ter trazido sucessivos ataques cibernéticos nunca antes verificados na Europa, 'obrigou' à criação, não só de grupos de trabalho e agências dedicadas a esta nova realidade, mas também à instituição de convenções e tratados que permitissem iniciar sinergias entre os países assinantes e, para o que a esta análise interessa, entre os países europeus. Na verdade, o novo século não trouxe apenas uma maior visibilidade para o ciberespaço e para a utilização perniciosa do mesmo. O século em que vivemos proporcionou um maior conhecimento da globalização, consciencializando a maioria das sociedades de que este fenómeno é, em grande parte, um processo de causa-efeito que serve, não raras vezes, de 'acelerante' para as mais diversas situações de risco que ocorrem no mundo em que vivemos e, especificamente, na Europa. Assim, e tendo em conta o relatado anteriormente, torna-se bastante claro que, entre 2000 e 2020, há medida que os anos foram passando e nos fomos aproximando dos tempos em que vivemos, também tem aumentado o número de ataques cibernéticos registados. Apesar de tal se dever, eventualmente, à crescente consciencialização social, institucional, governamental e individual, existe também uma grande probabilidade de que o aumento dos ciberataques esteja igualmente ligado à gradual globalização que se tem verificado, emoldurada num mundo que está cada vez mais interligado e onde, a cada dia, existe um maior 'esbatimento' de fronteiras.

2.1. A Globalização e os ciberataques: A transnacionalização dos desafios

Os tempos contemporâneos não foram apenas moldados pelo aparecimento da *internet* e pela gradual transição digital. Tal como já referido, a globalização foi também um fator de suma importância para a reformulação da forma como vivemos, bem como para o gradual aumento da importância que as novas tecnologias têm nas nossas vidas. A propósito desta interligação, Gelernter e Regev (2010, p. 69) identificaram a globalização como um processo "*by which networks of interaction spread around the world – especially across national border – connecting diverse people, institution, ideas, and representations in increasingly complex patterns of interdependence*", já Kaldor (2012, p. 4) foca o seu pensamento, sobretudo, na dualidade e contraditoriedade deste processo, que envolve integração e fragmentação, homogeneização e diversificação, globalização e localização.

Assim, seguindo a ideia de Gelernter e Regev, observa-se que foi devido à globalização que se justificou o contínuo investimento no progresso tecnológico, tendo em vista a gradual difusão e acessibilidade a dispositivos informáticos. Por sua vez, estes dispositivos influenciaram a globalização ao permitirem e promoverem uma aproximação entre pessoas, grupos e sociedades num progressivo ato de superação das impossibilidades impostas pelas barreiras físicas. Todavia, a globalização não acarreta apenas a instantaneidade de comunicações, de fluxos económicos e facilidade na mobilidade. No extremo, pode também demonstrar malefícios revelados no incremento da atividade criminosa, em especial da criminalidade transnacional como são, não raras vezes, os ciberataques.

Esta 'faceta' perniciosa da globalização, muitas vezes identificada com o termo 'globalização desviante' (Sullivan, 2014, p. 162), é frequentemente relacionada com o crime transnacional – definido pela Organização das Nações Unidas (1995, p. 4) como um conjunto de ofensas "*whose inception, perpetration and/or direct or indirect effects involved more than one country*" – elemento de risco em termos securitários. A este propósito Baylis (2014, p. 240) defendeu também que a globalização parece ter efeitos negativos na segurança internacional, sendo frequentemente associada a "*fragmentation, rapid social change, increased economic inequality, terrorism, threats to cyber security, and challenges to cultural and religious identities*".

Assim, é verificável que o processo de globalização – que é sobretudo a interação entre o local e o global – crie processos de causa e efeito, como é o caso da exploração da globalização para o aumento, dispersão e descentralização da criminalidade. Esta utilização desviante da globalização provocou uma mudança no que se consubstanciava até ao momento como crime, permitindo o agravamento das tipologias há muito existentes, sendo elemento de auxílio ao surgimento de outras – como é o caso do cibercrime – e instigando, sobretudo, o crescimento exponencial do crime transnacional.

A este propósito, Ken Booth (2014, p. 12), na obra *The Handbook of Global Security*, aborda o conceito de *segurança* como não sendo estanque, uma vez que tem sido alargado "*since the end of the Cold War to include other referents, dangers, and strategies*" para além das que estavam até ao momento consagrados na conceção académica das Relações Internacionais, defensora de um conceito de segurança mais restrito focado "*on the so-called nation-state as the privileged referent, war as the ultimate danger, and successful military strategy as the basic mode of survival*" (Booth,

2014, p. 12). Posto isto, a segurança passou a ser elemento de preocupação não só dos Estados-Nação, mas também de pessoas individuais e coletivas.

Após a Guerra Fria, o conceito de segurança continuou a sofrer mutações, principalmente, com o incremento do crime transnacional. A este propósito Picarelli (2008, p. 453) refere que "*Since the 1990s, security experts have viewed transnational organized crime as a rising security threat*", dizendo o mesmo autor (2008, p. 461) que o crime organizado transnacional "*is a complex security threat that demands a multi-lavered approach and response*.".

O crime transnacional abalou de tal forma a perceção securitária do sistema internacional que este foi descrito por Ulsch (2014, p. 19) como "*The crime wave of the future*", sendo um tipo de crime que tem feito uso da "*technology and security with a fervor that even many major corporations have not*." (Ulsch, 2014, p. 20). A referida preocupação emergente, surgida no início dos anos 90 do século XX, levou a que a *Organização das Nações Unidas* fundasse, em 1997, o *United Nations Office on Drugs and Crime* (*UNODC*), com o objetivo de agregar os esforços dos Estados-membros "*against all forms of cross-border crime but specificallly to improve the fight against transnational organized crime*." (Picarelli, 2008, p. 464). Assim, objetivando combater rapidamente o crime transnacional, a *UNODC* organizou várias reuniões das quais resultou, em 2000, a Convenção das Nações Unidas contra a Criminalidade Organizada Transnacional, que procurava harmonizar "*legal codes and improve law enforcement capabilities in order to curtail cross-border crime*" (Picarelli, 2008, p. 465).

As características do crime organizado transnacional – que Winslow e Winslow (2010, p. 259) denominaram de *high-level crimes*, isto é, crimes que passam de fenómeno local a global, tendencialmente cometidos de forma massificada por grupos de indivíduos ou organizações e de uma maneira que identificamos comummente como crime organizado – foram, de facto, as razões pelas quais surgiu uma necessidade de harmonização legal entre os Estados. Entre estes instrumentos de harmonização surgiu a criação de instituições intergovernamentais e supranacionais, como é o caso da *Europol* e da *Interpol*, bem como, segundo Picarelli (2008, p. 465), a criação de *Mutual Legal Assistance Treaties* (*MLATs*), que objetivam harmonizar sistemas jurídicos distintos e promover a cooperação em extradições, investigações conjuntas e recolha de provas.

Contudo, apesar dos inúmeros esforços, continuam a existir claros desafios no que respeita à cooperação internacional para o combate ao crime transnacional, uma ideia corroborada por Picarelli (2008, p. 462) ao referir de forma inequívoca que, pela sua

essência apólida, os Estados não podem 'combater' os grupos que se dedicam à criminalidade transnacional sozinhos, crendo que a luta contra o crime organizado é, por definição, uma questão de segurança internacional. Ericson (2007, cit. por Aas, 2007, p. 106) atesta esta visão ao afirmar que "*The view is that borderless threats require borderless law enforcement across organizational entities nationally and internationally, and across categories of citizens and non-citizens*".

De facto, foi esta verificação do elevado grau de onerosidade dos crimes transnacionais, tanto em termos securitários como económicos – uma vez que o "*transnacional crime drains potencial tax revenues from the coffers of the states while forcing the states to dedicate more financial and human resources to border control and law enforcement*" (Picarelli, 2008, p. 462) –, que levou à urgência em simplificar a cooperação internacional – seja europeia ou global –, inerentemente deficitária.

A prosperidade da criminalidade transnacional estará escorada, precisamente, na deficiência de cooperação internacional e no processo de globalização, que permite, agora, que o crime transnacional se alforrie das fronteiras físicas, até há pouco tempo impugnadoras do seu desenvolvimento. A questão das fronteiras é, como já referido, fundamental no que respeita à criminalidade, e o melhor local que a mesma tem para prosperar é precisamente aquele que é inerentemente transfronteiriço e apátrida: o ciberespaço. Perante isto, Rattray (2009 cit. por Nye, 2010, p. 4) referiu que:

> The cyber domain is unique in that it is manmade, recent and subject to even more rapid technological changes than other domains. As one observer put it, "the geography of cyberspace is much more mutable than other environments. Mountains and oceans are hard to move, but portions of cyberspace can be turned on and off with the click of a switch.".

É devido a esta falta de barreiras geográficas do ciberespaço que se deve considerar que os ciberataques, em especial o cibercrime, podem ser incluídos no crime transnacional, devendo os ciberataques ser adicionados "*to the list of conventional threats facing states, groups, and individuals alike… [as they] have the ability to affect individual countries or the world*" (Mahmoud, 2013, p. 2).

Contudo, coloca-se o problema de a tecnologia estar a desenvolver-se muito mais rápido do que os processos legislativos necessários para dirimir o cibercrime (Skórzewska-Amberg, 2017, p. 82), sendo precisamente devido à natureza altamente mutável do ciberespaço, já anteriormente referida, e à utilização do mesmo para

benefício da criminalidade organizada transnacional, que é tão importante adotar medidas que incluam "*the widest possible range of behaviour in cyberspace*." (Skórzewska-Amberg, 2017, p. 68), o que a mesma autora (2017, p. 68) considera ser "*not only of utmost importance and urgency, but also a considerable challenge, especially from the point of view of criminal law.*". Assim, Skórzewska-Amberg (2017, p. 82) defende que a convergência entre sistemas legais e, especificamente a harmonização legislativa no contexto da cooperação internacional seriam do superior interesse dos Estados, dando como exemplo "*the EU legislation, which produces a legal framework for the domestic law of the Member States*.".

Tendo em conta o expresso, parece ser consensual que a última década do século XX trouxe, à comunidade internacional, uma preocupação securitária assente em três elementos: a massificação da utilização da *internet* pela sociedade, o crescente processo de globalização e o robustecimento da atividade criminosa através do crime organizado internacional. A ordem da enumeração não é aleatória, mas antes consequente. Consequência essa exacerbada todos os dias pela dependência global do ciberespaço. Foi precisamente esta dependência, o que levou a Resolução do Conselho de Ministros n.º 92/2019 (2019, p. 2890), aquando da aprovação da Estratégia Nacional de Segurança do Ciberespaço 2019-2023, a referir o seguinte:

> A tendência para um crescente aumento da dependência das tecnologias de informação e de comunicação … trouxeram, de igual modo, em sociedades conectadas como a nossa, oportunidades significativas para aqueles que pretendem comprometer as nossas redes e sistemas de informação com intuitos potencialmente perniciosos para o bem-estar da sociedade portuguesa.

2.2. Cibercrime: A nova criminalidade na era digital

O ciberespaço é, como referido anteriormente, "*a global space with no geographical boundaries*" (Bernik, 2014, p. 49). Por esta razão, é também um lugar que não se 'encaixa' facilmente no conceito Vestefaliano de *Estado*, razão pela qual os Estados acabam por ser, até certo ponto, incapazes de cumprir o ser papel securitário no ciberespaço (Yeo, Birch e Bengtsson, 2016, p. 239).

A falta de fronteiras, juntamente com o progresso tecnológico levou a que o crime organizado transnacional utilizasse o ciberespaço e a globalização em seu favor, para se

desenvolver e perpetrar atos ilegais, não apenas no mundo físico, mas também no virtual. Posto isto, pode dizer-se que a transformação digital acarretou, necessariamente, desafios securitários, algo corroborado por Aas (2007, p. 159) ao defender que "*Most commentators acknowledge the fundamental shift represented by the transnational nature of crime in digital environments.*"

No entanto, quanto tentamos perceber, através do estado da arte, o surgimento, frequência e impactes dos ciberataques em geral, e do cibercrime em particular, é facilmente percetível que existe na literatura uma lacuna sobre o tema. Isto porque, em razão do elevado número de autores e publicações fixadas nos Estados Unidos da América, a maioria do estudo e análise nesta área, é feita do ponto de vista norte-americano, acarretando uma grave deficiência no que respeita ao volume de estudos e investigações contextualizadas no continente europeu.

Não obstante, o que importa salientar é que o conceito de *cibercrime* é, sobretudo, fluido. Enquanto o autor Igor Bernik (2014, p. 55) afirma que o cibercrime se tornou um fenómeno difundido "*which is emerging in numerous cases that cannot be classified as criminal offenses due to the vagueness of definitions, misunderstandings or incomplete legal acts*", classificando-o como um problema sério que a sociedade moderna não pode ignorar, e Sam C. McQuade (2006, cit. por Khan, 2011, p. 92) definiu o cibercrime como sendo o "*use of computers or other electronic devices via information systems to facilitate ilegal behaviors*", Emilio C. Viano (2017, p. 4) defendeu que os cibercrimes são "*the digital editions of well-known, traditional offenses*". Apesar da referida fluidez conceptual, diversos autores acabam por comungar da ideia de que "*victims and their harms are at best of only marginal interest to the criminal law*" (Vincent, 2017, p. 27), sendo devido às características de base da lei penal, "*conceptually incompatible with recognizing and adjudicating cybercrimes.*" (Vincent, 2017, p. 27), que, anos após o seu surgimento, continua a ser tão difícil e moroso penalizar o cibercrime. Ademais, será também interessante partilhar a distinção feita por Lachow (2009, p. 439) entre *cibercrime* e *hacktivismo*, onde o autor refere que os mesmos são distinguíveis pela sua motivação, uma vez que "*In the case of cyber crime, the goal is economic gain, not political change, ego gratification, or civil disobedience*.".

Além da chamada de atenção, feita por Lachow, para as diferentes motivações no que respeita à perpetração de cibercrimes, Bernik (2014, p. 6) alertou também para a responsabilização dos colaboradores de empresas, uma vez que "*Employees are not only dangerous because of their malicious thoughts and actions directed against the*

company, but also because of their ignorance and negligence". Ainda assim, também de acordo com Bernik (2014, p. 25), o que faz os números do cibercrime prosperarem verdadeiramente serão a anonimidade e a dificuldade em sancionar este tipo de crimes, junção que será "*certainly the reason for individual forms of crime, which directly impair a certain person or more persons, an organization or even a country*.".

Contudo, relativamente à temática do cibercrime, uma das referências mais importantes feita por Bernik (2014, p. 14), autor da obra *Cybercrime and Cyberwarfare*, refere-se ao facto de as ofensas criminais não serem, recorrentemente, um evento isolado, mas poderem ser parte de um conjunto de ocorrências mais alargado. Bernik (2014, p. 29) refere mesmo que, se no passado os cibercriminosos agiam de forma independente, atualmente, trabalham de forma mais organizada e conectada. Esta ideia vem correlacionar a expansão do cibercrime com a expansão paralela do, já referido, crime organizado transnacional, uma vez que, segundo Bernik (2014, p. 30), a mesma situação que caracterizou a máfia no passado, "*is now characteristic of the cybercrime perpetrators' subculture; an individual approach to cybercrime is replaced by the system of organizations that reflect the hierarchichal structure typical of the mafia*.", afirmação apoiada por Kremling e Parker (2017, p. 135) ao referirem que o cibercrime evoluiu rapidamente para crime organizado "*with organizations headed by crime bosses employing an armada of experienced developers who create ever-more sophisticated malware and attack tactics. This is also referred to as the digital mob.*". A este propósito, Goodman (2010, p. 27) defende também que "*While society tends to think of traditional organized crime as distinct from hightech criminals and hackers, there is evidence to suggest that the boundaries are blurring.*".

Posto isto, Bernik (2014, p. 27) conclui que *"It would thus be useful to start profiling cybercriminals and get to know their organization, just as this is done with the perpetrators of classic criminal offenses*.", referindo ainda que prevenir o crescimento desmedido do cibercrime passa por combatê-lo com a ajuda de especialistas de diferentes áreas, "*such as psychology, criminal investigation, information security and similar, because only a sound knowledge of the problem and perpetrators can contribute to the successful fight against cybercrime.*" (Bernik, 2014, p. 28). Assim, o exposto, relativamente à correlação do cibercrime e do crime organizado internacional, ficou perfeitamente sintetizado nas seguintes palavras de Grabosky (2011, cit. por Aas, 2007, p. 159): "*virtual criminality is basically the same as terrestrial crime, only committed through a new medium – a case of 'old wine in new bottles'*.", ideia também

presente no artigo "Cybercrime, Cyberterrorism and Cyberwarfare", da autoria da causídica norte-americana Susan Brenner (2006, p. 455).

Brenner (2006, p. 455), à semelhança de Grabosky, explica esta analogia entre o cibercrime e a expressão '*old wine in new bottles*', referindo que o cibercrime "*constitutes nothing more than the commission of a traditional "crime", albeit by different means …, that is true for much of the cybercrime we have seen so far*". Brenner tem razão na sua defesa. Haverá, certamente, inúmeros crimes cometidos no ciberespaço, cuja perpetração é, também, perfeitamente exequível no 'mundo real'. Não obstante, é necessário analisar o artigo de Susan Brenner à luz do seu ano de publicação, 2006, época em que, apesar de os crimes cibernéticos serem já uma preocupação securitária nacional e internacional – o ataque na Estónia aconteceria apenas um ano depois –, não teriam ainda o nível de abrangência e perniciosidade hodierna. Por esta razão, Brenner acaba por cair na falácia de apresentar aos seus leitores uma visão simplista do que é, e pode ser, o cibercrime, levando, por consequência, a uma perigosa desconsideração das consequências deste tipo de ataque. É facto que os anos têm dado razão a Brenner no sentido de que *alguns* crimes cibernéticos são crimes tradicionais que tiveram a oportunidade de migrar para o ciberespaço, passando, assim, a ter dois espaços de atuação. Ainda assim, a 'abertura' do ciberespaço à sociedade civil permitiu também o advento de crimes até então inexistentes, como foi o caso dos ciberataques ocorridos com recurso a *phishing*, *ransomware*, ataques DoS (*denial-of-service*) ou ataques DDoS (*distributed denial-of-service*). Assim, devido à distinção de Brenner entre crimes tradicionais e cibernéticos, os exemplos anteriores são os únicos casos em que a autora (2006, p. 456) equacionaria a existência de cibercrimes.

Mas, na problemática do cibercrime, mais importante do que encontrar uma definição universal e inequívoca para o mesmo, é identificar as características gerais dos seus perpetradores, bem como perceber como é que o sistema internacional pode legislar e cooperar de forma efetiva para dirimir o cibercrime.

O cibercrime, a par da globalização, mais não é que uma consequência dos processos de causa-efeito, e a dificuldade em criar um sistema de cooperação internacional é prova disso mesmo. A este propósito Goodman (2010, p. 311) referiu que as sociedades mais tecnologicamente avançadas são também as mais vulneráveis ao cibercrime e as que mais têm a perder com a sua ocorrência, tudo resultado, na sua opinião, "*of the inability or unwillingness of developing countries to effectively detect, investigate, arrest, and prosecute cybercriminals*" (Goodman, 2010, p. 311). Bernik

(2014, p. 39) apoia esta afirmação ao referir que os *websites* "*on which they carry out their unlawful activities ... are usually placed on server in countries with inadequate laws, no international agreements and with less qualified law enforcement authorities*.". Bernik (2014, p. 3) vai mais longe e adianta uma explicação para a utilização de Estados menos desenvolvidos para o cometimento do cibercrime, ao referir que devido aos ganhos financeiros expectáveis, a quantia destinada "*for the committing of cybercrime is growing steadily, since profits are also increasing. In light of the economic problems faced by the developing world, the issue is ever growing*.", suscitando, assim, a ideia de que o cibercrime trará, a determinados países, mais benefício que malefício económico.

Contudo, há autores que apesar de não rejeitarem o pensamento de Goodman e Bernik, optam por dar ênfase a países em situações de desenvolvimento diferentes, ou seja, aos países que já tiveram oportunidade de viver uma fase de democratização da *internet* e da tecnologia, mas cujos níveis de cibersegurança não serão ainda suficientemente avançados. Este é o caso de Allison Peters e Amy Jordan (2019, p. 5) que, no seu artigo "Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime" – publicado no periódico associado ao *think tank Third Way* – sustentam a sua lógica num estudo realizado pelo *Center for Strategic and International Studies*, referindo que, apesar de o cibercrime ter diferentes impactos em países com diferentes níveis de desenvolvimento, os Estados que terão, de facto, maior perda financeira perante a ocorrência de cibercrimes serão os "*"mid-tier" countries that are increasingly becoming digitized but are still developing their cybersecurity capabilities, as opposed to those countries that tend to be most highly developed and have the most mature cybersecurity capabilities.*".

Se o desenvolvimento de legislação efetiva e uma melhoria na cooperação e coesão internacional parecem ser, para a maioria dos autores, os caminhos evidentes a percorrer no combate ao cibercrime e na melhoria da cibersegurança, outros sugerem outras opções. É o caso de Vanja Bajovic (2017, p. 99) – docente da Universidade de Belgrado e autora do capítulo "Criminal Proceedings in Cyberspace: The Challenge of Digital Era", presente na obra *Cybercrime, Organized Crime and Societal Responses. International Approache*s – que defende que o ciberespaço, enquanto lugar sem fronteiras, não pode ser regulado de uma forma apenas parcial – seja nacional ou regional –, devendo, pelo contrário, ser fiscalizado por entidades supranacionais com jurisdição exclusiva sobre o ciberespaço, referindo ainda que, semelhantemente aos estados "*that protect the order within their boundaries, cyber authorities must be*

authorized to 'deport' the person who breaks the law and prohibit him from entering this 'non-physical' territory.". Ocorre que a idealização de Bajovic não é apenas simplista, é utópica. Pensar que é possível 'deportar' alguém do ciberespaço ou não permitir a qualquer indivíduo, nos dias atuais, que entre no ciberespaço ou tenha acesso a um dispositivo eletrónico é, no mínimo, fantasioso. Bajovic (2017, p. 99) continua a sua explanação propondo que "*Instead of traditional usernames and passwords, fingerprints could be a new "passport" for the entrance into the cyberspace that provides easy, reliable and accurate identification of the offender*.". Turrini e Ghosh (2010, p. 14) mencionam brevemente esta idealização ao referirem que "s*ome researchers argue that computers may be redesigned with biometric data built into the basic configuration to strengthen authentication and defeat intrusion by cybercriminals*.". Mas esta obrigatoriedade do uso de dados biométricos – Bajovic refere explicitamente as impressões digitais – não será mais que uma quimera. Primeiro, será impraticável que todos os dispositivos eletrónicos existentes no mundo passem a ser acedidos, exclusivamente, através de impressões digitais. Depois, porque se nos remetermos aos chamados 'crimes tradicionais', a utilização de dactilogramas também nunca se mostrou infalível para a identificação do seu proprietário.

Posto isto, a solução para diminuir ou, pelo menos, tentar refrear o aumento dos cibercrimes, passará unicamente por ultrapassar aquilo que Bernik (2014, p. 14) referiu como "*One of the major challenges faced by law enforcement agencies in combating international cybercrime*": conseguir uma coordenação eficaz entre as diversas autoridades internacionais e os seus sistemas legais. Ideia corroborada por Katja Franco Aas (2007, p. 160) quando refere a natureza espacialmente distribuída do ciberespaço, bem como o facto de "*Different legislative systems and traditions are an obstacle to effective control and prosecution. What is prohibited in one jurisdiction may be legal in another*.". Preocupação idêntica perante a dissemelhança entre sistemas legais, foi expressada num acórdão (2000, cit. por Goodman, 2010, p. 333) emitido pelo *Tribunal de grande instance de Paris* e assinado pelo juiz Jean-Jacques Gomez – que ficou conhecido por *'juge de l'internet'* –, relativo ao processo que opôs a *Ligue Internationale Contre le Racisme et l'Antisémitisme* (*LICRA*) e a empresa *Yahoo*, e onde se podia ler que "*An average citizen abiding by the laws of his or her own country may abruptly find themselves subject to prosecution in a different country, where the laws are different*.". Será precisamente esta dificuldade em encontrar uma definição de cibercrime e um conjunto de pressupostos estanque, passíveis de utilização por todos os

Estados-Nação, que levam à eventual existência de situações como a exemplificada por Vincent (2017, p. 31), quando o autor fornece uma pletora de exemplos relativamente ao que pode constituir um cibercrime, mas termina a sua explanação com a certeza de que em certos países, os exemplos que dá, poderão nem mesmo "*count as cybercrimes but at most only as something like cyberwrongs*".

Assim, é notório que urge encontrar pontos-comuns que permitam travar o avanço galopante do crime organizado transnacional e do cibercrime. Como referiu Goodman, (2010, p. 334) "*Cybercrimes can occur in a fraction of a second. In contrast, extradition, evidence preservation orders, and mutual legal assistance treaties can take lot longer*". Noção apoiada por Peters e Jordan (2019, p. 2), quando mencionam que são necessários "*years of cooperation, significant resourcing, and dozens of national and international entities to impact only one element of a single cybercrime organization*.". É precisamente esta dificuldade em concatenar esforços entre agências internacionais e, em alguns países, até mesmo nacionais, que permite aos cibercriminosos, e às organizações com que colaboram, prosperarem, a cada dia, na sua atividade. Ainda assim, não creio que as referidas entropias, em termos de cooperação nacional, sejam observáveis em território português, onde, apesar de a lei definir categoricamente que a investigação do cibercrime é da exclusiva competência da *Polícia Judiciária*, é notória a concertação de esforços entre as mais diversas entidades nacionais – civis ou militares – para a atempada repressão ou posterior investigação destas ocorrências.

Mas, se por um lado já percebemos que penalizar os agentes que cometem cibercrimes, principalmente os que o fazem de forma organizada, é altamente moroso e desafiante, impera perceber que "*No matter how challenging and complex, cybercrimes are not beyond the reaches of society.*" (Goodman, 2010, p. 336). De facto, ainda de acordo com Goodman (2010, p. 336), o ciberespaço não é o primeiro nem o único "*policy domain which lies beyond the control of a single nation. International air traffic control, the law of the sea, and militarization of space have required concerted international cooperation and agreement.*". Assim, e se em tempos anteriores, foi possível chegar a acordo relativamente a diversas matérias, não há razão para que o mesmo não aconteça com o cibercrime. No entanto, Bernik (2014, p. 50) alerta-nos para um importante facto relativamente à cooperação internacional, quando, expressando-se sobre a Convenção de Budapeste, defende que a verdadeira dificuldade neste esforço conjunto verificar-se-á se países como a Rússia, a China, a Índia e outros semelhantes

não assinarem e ratificarem a Convenção, isto porque, "*attacks often come from these countries and prosecuting perpetrators is thus almost impossible*.".

Assim, a noção geral é que "*Individual responsibility, community cooperation, and international cooperation among states are therefore all necessary parts of a multi-faceted approach that is essential when responding to pressing global cybersecurity needs.*" (Yeo, Birch e Bengtsson, 2016, p. 239). Williams (2008, p. 1) referiu que os Estudos de Segurança envolvem interpreter "*the past (specifically how different groups thought about and practised security), understanding the present, and trying to influence the future.*". Esses ensinamentos têm de ser considerados. Como alertou Goodman (2010, 336) "*The world must work proactively now to prevent future crimes and protect the global population from this new menace of the twenty-first century*.".

Mas, se o cibercrime é uma preocupação premente no contexto de segurança e cooperação internacional, a abrangência dos ataques cibernéticos vai muito para além deste, razão pela qual "*We must not forget that cyberspace is [also] an effective weapon in the hands of terrorists*" (Bernik, 2014, p. 25).

2.3. Ciberterrorismo: O terror no ciberespaço

O ciberespaço pode, como expresso anteriormente, ser também permeado pelo terrorismo. A definição primária de *terrorismo* – que é deixada "*to the unilateral interpretation of states"* (Diaz-Paniagua, 2008, cit. por Marsili, 2019, p. 172) – centra-se no uso de violência por grupos que instigam o medo "*by attacking civilians and/or symbolic targets, for purposes such as drawing widespread attention to a grievance, provoking a severe response, or wearing down their opponent's moral resolve, to effect political change'*." (Kiras, 2014, p. 359). Contudo, nos anos 80 do século XX, "*Barry Collin, a senior research fellow at the Institute for Security and Intelligence in California, coined the term "cyberterrorism" to refer to the convergence of cyberspace and terrorism.*" (Denning, 2001, p. 281).

Mas, tal como no *cibercrime*, "*there is no consensus on a legal or academic definition of the derivate term "Cyberterrorism""*" (Marsili, 2019, p. 172). Contudo, na necessidade de encontrar uma definição apropriada para o mesmo, alguns autores propõem uma definição de ciberterrorismo adaptada, mas muito aproximada, à já referida definição de terrorismo proposta por Kiras. Este é o caso de Kremling e Parker (2017, p. 240), que aproximam a sua definição de ciberterrorismo, que aqui seguimos, de um ato intencional "*committed via computer or communication system and motivated*

by political, religious, or ideological objectives, against information, data, or computer systems/programs, intended to cause severe harm, death, or destruction to civilians.", definição acompanhada por Matusitz (2005, p. 137) que referiu que o ciberterrorismo "*is the intentional use of threatening and disruptive actions against computers, networks, and the Internet*.". Akhagar (2016, p. 266) adianta ainda que um ataque ciberterrorista "*should result in violence against persons or property, or at least cause fear and terror. That includes attacks against critical infrastructures.*", e Noble (2017, p. 70) acrescenta que um outro objetivo do ciberterrorismo é causar dano à reputação percecionada dos governos, ou seja, "*In other words, by causing embarrassment to the security services an enemy can promote an image of weakness and declare a victory for their cause*.". Assim, torna-se claro que o ciberterrorismo se trata do terrorismo internacional que, analogamente ao cibercrime, fruiu do avanço tecnológico de forma a beneficiar e atingir os seus intentos, motivo pelo qual alguns investigadores concluíram que o ciberterrorismo representa o futuro do terrorismo, podendo mostrar-se uma grave ameaça à segurança nacional, uma vez que os grupos terroristas "*are increasing their knowledge of technology and are actively recruiting individuals with IT skills and training*" (Kremling e Parker, 2017, p. 244).

Ainda assim, como referiu Kiras (2014, p. 358), "*Terrorism and globalization share at least one thing in common - both are complex phenomena open to subjective interpretation.*". Por essa razão, existem autores que não valoram, seja em detrimento da época em que partilharam as suas opiniões ou por crença própria, a existência de ciberterrorismo. Será o caso do autor Marco Marsili (2019, p. 173), defensor de que no terrorismo, tal como na guerra, impera a dispersão do medo e o uso de violência, não podendo, por isso, existir ciberterrorismo, uma vez que essa violência não é passível de transmutação para o ciberespaço. Ademais, Marsili (2019, pp. 173-174) completa a sua teorização referindo que a ação terrorista, para além de permeada por violência e medo, tem de ter motivações políticas, pelo que o terrorismo, apenas será assim categorizado, no eventual preenchimento destes três pressupostos. Não obstante, não podemos acompanhar o pensamento de Marsili, uma vez que a falácia do autor está em crer que o terrorismo tem de ser exclusivamente alavancado por divergências políticas, esquecendo que, na base do mesmo, estarão, mais frequentemente, oposições ideológicas ou religiosas. Todavia, mais bizarra será a opinião de Rogers (2008, p. 173), que considera que o terrorismo – na sua forma tradicional – "*is still a minor issue in terms of global human security*". Diremos, de forma não surpreendente, que não podemos concordar

com esta afirmação. O terrorismo pode, em termos de estatísticos, ser um dos ataques à segurança humana menos frequentes, mas em caso algum a sua frequência é diretamente proporcional à sua letalidade.

Em 2001, Dorothy E. Denning (2001, p. 281) perguntava retoricamente, no seu artigo "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy", o seguinte: "*Is cyberterrorism the way of the future?*". A autora (2001, p. 281) respondia à pergunta dizendo que, para um terrorista, a utilização do ciberespaço teria vantagens relativamente a métodos físicos, uma vez que podia ser realizado remota e anonimamente, de forma económica e sem recorrer ao manuseamento de explosivos, garantindo, contudo, "*extensive media coverage, since journalists and the public alike are fascinated by practically any kind of computer attack*.", cumprindo, desta forma, um dos intuitos do terrorismo: instigar o medo. Ainda assim, continuava Dennings (2001, p. 282), um dos problemas do ciberterrorismo, pelo menos em 2001, seria o facto de o mesmo não usar armas físicas, sendo mais difícil controlar um ataque e atingir o nível de destruição desejado (Denning, 2001, p. 282).

Por seu turno, Eddy Willems (2019, p. 51), em tempos muito mais recentes, defendeu que o terrorismo apenas existe na sua acessão tradicional, isto é, "*when it comes to bloody attacks like 9/11 or those more recently seen in London or Madrid or Paris.*", com Willems (2019, p. 51) a defender que a idealização social de terrorismo nunca foi plenamente transferível para o ciberespaço, uma vez que, ainda que consigamos encontrar "*online communication related to the implementation of such attacks, and terrorists use the Internet for recruitment and for communication, we have not yet encountered true terrorism in cyberspace.*" (Willems, 2019, p. 51).

Enquanto a conceptualização de Dennings é, invariavelmente, toldada pela época em que foi escrita, a teoria de Willems não poderá certamente ser justificada da mesma forma, razão pela qual nos vemos, manifestamente, obrigados a discordar. Terrorismo pode, efetivamente, ocorrer no ciberespaço e utilizar o mesmo em seu proveito. Para mais, veja-se que o ciberterrorismo continua a ser um ato intencional onde se encontram preenchidos os pressupostos de instigar medo e terror, atacar civis ou alvos simbólicos, provocar atitudes reativas extremas e objetivar causar morte ou destruição. A deficiência da crença de Willems centra-se no facto de utilizar exemplos de ataques terroristas, como o 11 de setembro de 2001, sem recordar que foi precisamente através do ciberespaço que os terroristas ligados à *Al-Qaeda* comunicaram enquanto preparavam este ataque. Willems não equaciona os possíveis efeitos devastadores de um

ataque análogo transposto para a atualidade. Muito provavelmente, os terroristas já não necessitariam de sequestrar as aeronaves. Teria sido, talvez, mais difícil, mas, com toda a certeza, muito mais destrutivo, invadir o sistema informático da aviação civil norte-americana, de forma a ganhar controlo dos aviões ou indicar-lhes, de forma propositada, outras rotas. O erro de Willems está em pensar que o ciberterrorismo só pode ter lugar no ciberespaço, ao invés de pensar que o ciberterrorismo é a utilização do ciberespaço para atitudes disruptivas. Ciberterrorismo não se limita à utilização da *internet* para o recrutamento de terroristas ou para a comprar de materiais a ser utilizados num ataque. Ciberterrorismo é atacar a rede informática de controlo da aviação civil e mudar a rota das aeronaves de forma a provocar acidentes; é invadir a rede informática de uma central elétrica e causar uma falha geral que deixe uma cidade 'às escuras' durante dias; é acometer a rede informática de uma barragem e provocar a inundação repentina de uma região. O potencial disruptivo do ciberterrorismo não é comparável ao do terrorismo tradicional. Um pode provocar centenas de vítimas. O outro pode provocar milhares. Resta a ideia fundamental de que será muito mais fácil afetar a infraestrutura crítica recorrendo ao ciberterrorismo do que ao terrorismo:

> A terrorist attack is most often associated with bombing, but it should be assumed that cyberspace will soon be the primary arena for terrorist attacks, and in the coming years it is expected that attacks on computer systems will be increasingly more common. It is expected that the target of such attacks will mainly be the banking infrastructure and other so called critical infrastructure. (Skórzewska-Amberg, 2017, p. 80)

Assim, quanto ao ciberterrorismo, importa pensar que existem, primordialmente, duas armas: a secundária podem ser aviões, redes elétricas ou barragens, mas a principal serão sempres os sistemas de informação, a *internet* e, globalmente, o ciberespaço.

Contudo, apesar de não se concordar com a teoria de Willems no seu todo, pode assumir-se como factual a ideia de que o ciberespaço é o principal meio de comunicação das organizações terroristas, sendo também o meio através do qual atingem uma maior audiência "*of real and potential sympathizers, publish propaganda and wage a skilful auxiliary psychological warfare campaign to amplify violence on the ground*." (Ranstorp, 2007, p. 39). Posto isto, interessará ainda salientar que, segundo refere Ulsch (2014, p. 57), os ciberataques são, a par das armas biológicas, das armas químicas, das

armas nucleares, da dispersão radiológica, dos ataques com armas de fogo e da propaganda, uma das sete armas usadas por grupos terroristas.

Desta forma, sabendo a importância que a propaganda tem para as organizações terroristas, Conway (2006, cit. por Virkar, 2016, p. 10) assumiu que o advento da *internet* tem vindo a aumentar significativamente as oportunidades "*for terrorists to pursue their activities online and has enhanced their efforts to engage in publicity, propaganda and, ultimately, in psychological warfare.*". Assim, e segundo Virkar (2016, p. 11), a *internet* fornece aos grupos terroristas um nível nunca visto de controle direto "*in the management of their organisations …; extending considerably both their legitimacy and their ability to manipulate and to shape how different target audiences perceive them and their professed opponents*.". Por esta razão, Virkar (2016, p. 19) alega ainda que os grupos terroristas do século XXI já perceberam que a sociedade não tem como permanecer isolada das redes de poder presentes neste mundo interconectado em que vivemos, razão pela qual os movimentos terroristas transnacionais estão a expandir gradualmente a sua presença *online*. Joseph Nye (2010, p. 12) corrobora esta noção da importância da *internet* para os grupos terroristas, referindo que a mesma "*has become a crucial tool that allows them to operate as networks of decentralized franchises, create a brand image, recruit adherents, raise funds, provide training manuals and manage operations*.". A este propósito, Nye (2010, pp. 12-13) dá ainda o exemplo da *Al-Qaeda* que, graças às ferramentas cibernéticas, "*has been able to move from a hierarchical organization restricted to geographically organized cells to a horizontal global network to which local volunteers can self-recruit.*". Da mesma forma, no contexto europeu, verificou-se, nos anos recentes, a forte utilização dos meios cibernéticos por parte do grupo terrorista *ISIS*, que usou amplamente o ciberespaço com objetivos de recrutamento, financiamento e disrupção.

Assim, o impacto da *internet* na expansão dos grupos terroristas foi sintetizado por Roy (2010, cit. por Nye, 2010, p. 13) ao defender que o lugar central da radicalização "*[is] neither Pakistan nor Yemen nor Afghanistan …but in a solitary experience of a virtual community: the ummah on the Web*.". Posto isto, e tendo em conta a crescente utilização da *internet* por grupos terroristas, Ulsch (2014, p. 58) referiu que a maior ameaça é que toda uma geração de terroristas "*is cyber literate, is motivated to attack, and believes strongly that such attacks are not only justified but mandatory. Not to prepare for such an attack would be negligent.*", algo que se sintetiza no facto de que "*tomorrow's terrorist may be able to do more damage with a keyboard*

than with a bomb." (National Research Council, 1991, cit. por Kremling e Parker, 2017, p. 244). Trata-se da verdadeira virtualização do terror.

Posto isto, Irving Lachow (2009, p. 450) aponta cinco características que fazem da *internet* um valor estratégico para as organizações terroristas:

> First, it enables rapid communications. … Second, using the Internet is a low-cost proposition. … Third, the ubiquity of the Internet means that small terrorist groups can have a global cyber presence that rivals that of much larger organizations. … Fourth, the growth in bandwidth combined with development of new software has enabled unsophisticated users to develop and disseminate complex information via the Internet. … Finally, modern encryption technologies allow Internet users to surf the Web, transfer funds, and communicate anonymously.

Todavia, será interessante regressar na História e analisar o surgimento do terrorismo. De acordo com Wiletts (2014, p. 327), historicamente o terrorismo foi um instrumento utilizado nos conflitos internos de uma determinada sociedade, tendo essa visão mudado quando a *Al-Qaeda* apresentou ao mundo, através das suas ações, o terrorismo transnacional. Kiras (2014, p. 360) chega mesmo a identificar o ano de 1968 como o momento do advento do terrorismo internacional, adiantando também os três fatores que levaram a este acontecimento: "*the expansion of commercial air travel, the availability of televised news coverage, and broad political and ideological interests among extremists that intersected around a common cause*". Kiras (2014, p. 358) nota ainda que, na última metade de século XX, "*terrorism has come to mean the use of violence by small groups aiming to achieve political change. Terrorism differs from criminal violence in its degree of political legitimacy.*".

O impacto da globalização no terrorismo e, particularmente, no ciberterrorismo, é também de análise fundamental. De facto, nos tempos mais recentes, em que o mundo passou a viver na chamada 'aldeia global', foi notória uma mudança de paradigma no fenómeno do terrorismo. Apesar de continuar a ser um fenómeno complexo "*in which violence is used to obtain political power to redress grievances that may have become more acute through the process of globalization.*" (Kiras, 2014, p, 370), os meios usados pelas organizações terroristas foram, irremediavelmente, influenciados pela globalização. Ainda que a globalização tenha aumentado as capacidades técnicas dos grupos terroristas, permitindo-lhes ter um alcance global, não alterou "*the fundamental*

fact that terrorism represents the extreme views of a minority of the global population. In other words, globalization has changed the scope of terrorism but not its nature." (Kiras, 2014, p. 370). O domínio onde a globalização teve verdadeiro impacto foi no facto de tecnologias que lhe estão associadas terem e serem exploradas por terroristas, permitindo que diversos grupos trabalhem conjuntamente para o mesmo fim, troquem informações e consigam chegar a diferentes audiências (Kiras, 2014, p. 358). Assim, Kiras (2014, p. 359) sintetiza o seu pensamento quanto à globalização e ao terrorismo dizendo que a relação entre os dois "*is best understood as the next step in the evolution of political violence since terrorism became a transnational phenomenon in the 1960s*.".

Posto isto, de uma forma geral, pode dizer-se que a verdadeira influência da globalização no agravamento dos efeitos nefastos do terrorismo, se centra no facto de o processo de globalização, e particularmente a evolução tecnológica, facilitarem a troca e movimentação de pessoas e bens – fornecendo um maior potencial destrutivo a cada ataque –, bem como o recrutamento de novos membros, nomeadamente, através de sítios *online*, como é o caso das redes sociais. Desta forma, a globalização aliada à emergência tecnológica permite a concentração de esforços entre as organizações terroristas, potenciando um contacto permanente entre os seus membros, permitindo concatenar esforços e objetivando provocar o maior grau de destruição possível. Ainda a propósito do impacto de globalização no terrorismo, Kiras (2014, p. 366) remete, interessantemente, para o *motto* ativista '*think globaly, act locally*', defendendo que a utilização deste tipo de lemas por determinados grupos, reforça, no caso do terrorismo, as crenças de engrandecimento das causas defendidas, isto é, a perceção de poder e alcance global das organizações terroristas. Assim, de acordo com Magnus Ranstorp (2007, p. 31) – académico sueco que focou os seus estudos em movimentos terroristas islâmicos –, "*The fusion of globalization and terrorism in the twenty-first century has created a new, adaptable and complex form of 'networked' asymmetric adversary.*". Adiantando o mesmo autor (2007, p. 31) que, para a *Al-Qaeda* e outras organizações terroristas, especificamente as islâmicas, a *internet* se tornou, um santuário virtual onde todas as dimensões da *jihad* global estão a ter lugar *online*, "*In many ways cyberspace has created a virtual university of jihad with advice available anytime to any militant and it has vastly expanded the potential audience and modes of interaction*.". Ranstorp (2007, p. 31) reforça a importância do ciberespaço para a *Al-Qaeda* e organizações análogas, referindo que o mesmo constitui "*a form of central nervous system as it remains critical to its viability in terms of structure and even more as a movement*.". Já

Coll e Glasser (2005, cit. por Ranstorp, 2007, p. 31) defenderam que a *Al-Qaeda* se tornou o primeiro movimento de guerrilha a migrar do espaço físico para o ciberespaço.

Ainda que Nye (2010, p. 17) tenha afirmado que a concretização de eventos terroristas através de ciberataques não é, atualmente, a via mais atrativa, "*as groups develop their capacity to wreak great damage against infrastructure over the coming years, the temptation will grow*", torna-se evidente que o ciberespaço é, hodiernamente, uma das ferramentas mais úteis ao sucesso da causa terrorista. De facto, "*The easiest way to breed social unrest without physical presence on the ground is cyberterrorism. Cyberterrorism is cheap and leaves few traces.*" (Yeo, Birch e Bengtsson, 2016, pp. 238-239). Ideia corroborada por Ranstorp (2007, p. 39), ao referir que adotar uma abordagem cibernética multidimensional, "*combined with creative new communication technologies, allows operational agility and stealth mode far in excess of what was possible previously for terrorist organizations.*". Ranstorp (2007, p. 39) defende ainda – no capítulo "The virtual sanctuary of al-Qaeda and terrorism in an age of globalization", da obra *International Relations and Security in the Digital Age* – que a presença de organizações terroristas no ciberespaço, permite a sua sobrevivência "*through a constant virtual presence with no real or tangible physical centres of gravity and in constant stealth mode and ideological motion.*". Da mesma forma, o autor (2007, p. 39) alega que a presença destes grupos no ciberespaço lhes confere, atualmente, "*a certain degree of legitimacy which these organizations otherwise would not have.*".

Não obstante, não se pode aqui concordar com tudo o que Ranstorp defendeu na obra *International Relations and Security in the Digital Age*. A presença de uma organização terrorista no ciberespaço pode garantir a sua sobrevivência, mas nunca a sua legitimidade. Acontece que, apesar da 'infiltração' destes grupos no ciberespaço dificultar, como aponta Ranstorp, a encarceração dos seus integrantes e o desmantelamento destas organizações perniciosas, a sociedade e a atualidade em que vivemos ainda não permite que o ciberespaço, e as respetivas ações de cada um no mesmo, lhes confira qualquer tipo de legitimidade para validação da sua existência. A falácia de Ranstorp situa-se aqui. O autor usa a teoria de 'legitimidade', fornecida pela presença no ciberespaço, de forma intercambiável, não fazendo a distinção entre a legitimidade da existência e a legitimidade da ação.

De facto, a validade das organizações terroristas e de grupos radicais, comprova-se pelos atos terroristas 'físicos' que cometeram até ao momento, onde se pode incluir o 11 de setembro, os Atentados da Atocha ou os Atentados de Londres, e pelos ataques

ciberterroristas que já aconteceram – como é o caso do ciberataque à Estónia, em 2007, considerado, pela maioria, um episódio de ciberterrorismo – ou poderão vir a acontecer no, ou através, do ciberespaço. Apesar de o ciberespaço ter sido, nos últimos anos, um meio fundamental para o recrutamento de membros e difusão de crenças impregnadas em radicalismos, não podemos dizer que, no período de tempo que aqui analisamos, este tenha sido o principal meio de atuação destes grupos. Enquanto Willems (2019, p. 51) erra quando alega que terrorismo apenas existe na sua forma tradicional, visto que o ciberterrorismo não alcança inspirar o mesmo medo na sociedade, Ranstorp falha ao defender que todas as ações de uma organização terrorista são validadas tão só e apenas pela sua presença no ciberespaço. Não será necessário detonar uma bomba para que aconteça um ataque terrorista, mas será necessário mais do que o recrutamento de membros através da *internet* para legitimar uma organização terrorista ou as suas ações.

Tendo em conta o exposto, consideramos que a eventual legitimidade – se entendermos este conceito na aceção de grupo que tem força de expressão no meio em que se insere, e não de direito que assiste a estas organizações quanto à realização de ataques terroristas – que lhes possa ser dada, não partiu ainda do ciberespaço, pela tão simples razão de não se terem verificado, até ao ano de 2020, atos terroristas cujos resultados se tenham demonstrado tão danosos como nos exemplos anteriormente enumerados. Como Eriksson e Giacommello (2007b, p. 174) refeririam num capítulo posterior da obra *International Relations and Security in the Digital Age*, ainda é mais fácil e eficaz detonar uma bomba tradicional, do que escrever um código malicioso, visto que, os ciberataques podem destruir "*bits and bytes, but it is highly unlikely and extremely difficult to achieve the same effects in terms of fear and destruction produced by a bomb or a missile.*", com Lachow (2009, p. 437) a referir que "*the hype surrounding this issue [of cyberterrorism] outpaces the magnitude of the risk*.".

Todavia, por todas as razões anteriormente enumeradas, é notório que, apesar de ainda não terem existido, na Europa, episódios ciberterroristas com baixas equivalentes ao terrorismo tradicional, impera que os Estados-nação e os seus cidadãos validem o risco e a ameaça do ciberterrorismo, tal como validam, diariamente, o risco e a ameaça do terrorismo 'físico'. Após os ataques terroristas ocorridos a 11 de setembro de 2001, ocorreu um despertar de consciência global relativamente à proteção das nações e dos seus cidadãos contra organizações terroristas. Enquanto a Guerra ao Terror, ou Guerra ao Terrorismo, se iniciou, por ordem da administração Bush, a partir dos Estados Unidos – contra o que George W. Bush denominou, no Discurso sobre o Estado da

União, a 29 de janeiro de 2002, como o 'eixo do mal' –, sendo também posta em prática a chamada Doutrina Bush[29], a preocupação para com o flagelo do terrorismo estendeu-se gradualmente a outros países. Por essa razão e, até maioritariamente, devido ao Artigo 5.º da *Organização do Tratado do Atlântico Norte*, foi desenvolvida uma cooperação internacional contra o terrorismo que levou diversas nações europeias, a apoiar os Estados Unidos da América em missões internacionais que tinham em vista erradicar diversas organizações terroristas. Mas aplicar a Guerra ao Terror apenas ao terrorismo tradicional não basta. É necessário que esta vontade de assegurar a defesa nacional e segurança comum se estenda ao ciberespaço. Assegurar, desde já, a defesa do ciberespaço face ao ciberterrorismo, diferenciará esforços de prevenção de controle de danos. Assegurar, desde já, a defesa do ciberespaço face ao ciberterrorismo, é impedir que este se torne uma ameaça transnacional tão preponderante quanto o cibercrime. Assegurar, desde já, a defesa do ciberespaço face ao ciberterrorismo, é garantir que as vítimas dos atentados de 11 de setembro de 2001, dos atentados da Atocha, dos atentados de Londres ou dos de Paris, não o terão sido em vão. Significará que as nações retiraram ilações destas tragédias e que consideraram, por fim, a cooperação internacional e a antecipação como a única hipótese possível para o combate ao terrorismo e, futuramente, ao ciberterrorismo. E tal é possível.

A propósito da cooperação, Bosco (2013, cit. por Virkar, 2016, p. 13) referiu que, após os ataques de 11 de setembro de 2001, "*a number of civil society groups and organisations have undertaken initiatives to disrupt terrorist use of the Internet and its associated platforms and applications*". Se grupos de civis mostraram este nível de capacidade de cooperação, será impossível crer que os Estados não conseguirão mimetizar estas ações. Como referiu Kiras (2014, p. 358), quanto ao terrorismo, a comunidade global não é impotente face a tamanha violência, "*In order to succeed, the global community must utilize the resources at its disposal collaboratively, in a way that is consistent with international law and human rights*". Da mesma forma, Gabriel Weimann (2015, cit. por Marsili, 2019, p. 175) disse que "*the War on Terror (WoT) has not been won, as it continues on in the cyberdomain*.".

Por estas razões, a troca de informações, particularmente no caso do continente europeu, entre o *Sistema de Informação Schengen*, os *Gabinetes Nacionais SIRENE*, a

[29] Tratou-se de um conjunto de medidas de política externa, instituídos durante a presidência de George W. Bush, que tinham como principal característica a permissão para tratar como terroristas as nações onde se encontram situadas organizações terroristas ou que apoiam estes grupos.

Europol, as polícias nacionais e o *Sistema Echelon*, torna-se uma parte vital da luta global e europeia contra o terrorismo (Mathiesen, 2006, cit. por Aas, 2007, pp. 146-147). O continente europeu poderia ainda usufruir, no combate ao ciberterrorismo, da Convenção de Budapeste e do seu Protocolo Adicional à Convenção sobre o Cibercrime Relativo à Incriminação de Atos de Natureza Racista e Xenófoba Praticados através de Sistemas Informáticos, contudo, como referiu Marsili (2019, p. 180) nenhum destes tratados inclui "*cyberterrorism among proscribed acts*". A Convenção sobre o Cibercrime não teve os resultados necessários. As suas deficiências, levaram a tentativas de criar uma Convenção Internacional sobre o Cibercrime. Contudo, e apesar de em 2015, o 13º Congresso das Nações Unidas sobre a Prevenção ao Crime e Justiça Criminal ter debatido se seria realmente necessária uma nova convenção, desta feita internacional, "*The Congress addressed cybercrime jointly with terrorism, without making a distinction and without considering them as a unicum*." (Organização das Nações Unidas, 2015, cit. por Marsili, 2019, p. 180).

2.4. Ciberguerras: A transmutação do campo de batalha

Tal como vimos, os tempos atuais são não só acompanhados da globalização, mas também de uma mudança de paradigma das ameaças como as conhecíamos até há poucos anos. O crime está diferente. O terrorismo está diferente. E as guerras também o estão. Suscetíveis, agora, também elas, de ocorrer no ciberespaço, lugar que alguns autores identificam como um novo campo de batalha.

Apesar de as guerras serem, normalmente, "*fought over land, and typically on the land countries are fighting for … in cyber space the traditional boundaries disappear*" (Winterfeld e Andress, 2013, p. 8). Assim, o campo de batalha cibernético, "*the information space of focus during wartime, and it consists of everything in both the physical environment as well as the cyberspace environment*" (Johnson, 2015a, p. 159). Devido a esta transmutação do campo de batalha tradicional onde ocorriam as guerras – disputas "*between two or more states through their armed forces, for the purpose of overpowering each other and imposing such conditions of peace as the victor pleases*" (Oppenheim, 1952, cit. por Marsili, 2019, pp. 189-190) – esta aceção deixou de ser a mais correta, tendo o conceito de conflito armado substituído, amplamente, o conceito de guerra (Use of Force Committee, 2010, cit. por Marsili, 2019, p. 190).

Posto isto, e por, tal como no cibercrime ou no ciberterrorismo, não haver um conceito de ciberguerra uno, tomamos por definição a cunhada por Clarke (2010, cit.

por Khan, 2011, p. 93) que disse tratar-se de "*actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption*.". De facto, "*Once governments began using cyber weapons for espionage and covert operations, using cyber weapons in conjunction with actual war naturally followed*.", diz-nos Preciado (2012, p. 117).

Mas, o ponto comum relativamente ao fenómeno bélico, baseia-se na conceção Clausewitziana de que a guerra é um comportamento social e político, ainda que a natureza política da guerra tenha sofrido mudanças "*in recent decades under the impact of globalization, which has increasingly eroded the economic, political, and cultural autonomy of the state*." (Sheenan, 2014, p. 218). O que não mudou relativamente às guerras foi a sua assimetria, uma vez que, como referiu Martins (2019, p. 102), "*[cyberspace] is inherently asymmetrical … and this characteristic is a critical point in understanding the cyberwars of the future*", ideia corroborada por Wesley Clark (2009, cit. por Martins, 2017, p. 102) quando diz que não há combate militar mais assimétrico que um ciberataque, uma vez que este é extremamente acessível e rápido, pode ser concretizado anonimamente e pode corromper serviços críticos nos momentos de risco máximo. Naím (2017, p. 86) defende também que as ciberguerras são assimétricas, visto que as democracias liberais estão em desvantagem contra os regimes autoritários, numa desigualdade que não é tecnológica, mas antes devida ao facto "*that its authoritarian rivals do not have the legal, institutional, and political constraints or the checks and balances of a democracy.*". Torna-se, assim, visível a utilidade da força como um instrumento político (Sheenan, 2014, p. 216). Por fim, Martins (2017, p. 102) relembra que, apesar de os ciberataques serem rápidos, frequentes e, eventualmente, persistentes, também são incapazes de replicar os efeitos cinéticos do combate tradicional, o que leva a que quase todos os conflitos sejam de baixa intensidade.

Mas a questão que se coloca é a seguinte: *Existem realmente guerras assimétricas?* Para que haja assimetria, é preciso observar a simetria, e em que momento se verificou um fenómeno bélico simétrico? Nunca. A guerra, como supramencionado, pressupõe, na sua conceção original, um fenómeno de violência extrema que não pode, por isso, ser simétrico. E apesar de, como referiu Clausewitz, cada época ter a sua forma característica de guerra (Sheenan, 2014, p, 219), evolutiva consoante os tempos, o facto de as guerras se poderem, agora, fixar no ciberespaço, não significa que possam ser simétricas ou assimétricas. Nas guerras, não há lutas entre

iguais. Trata-se de um fenómeno onde haverá sempre assimetria de meios e, consequentemente, de esforços e resultados.

Contudo, torna-se evidente que o ciberespaço mudou permanentemente o paradigma do fenómeno bélico, com a tendência a ser para que o uso de ciberataques "*in modern warfare [increases] because of its low costs*." (Brenner e Clarke, 2009, cit. por Preciado, 2012, p. 146). O ciberataque tornou-se, numa era pós-Guerra Fria onde o ciberespaço se transformou num campo de batalha crucial para a atualidade (Sheenan, 2014, p. 217), "*[a] low-cost option of warfare*" (Mahmoud, 2013, p. 1).

Será precisamente o período pós-Guerra Fria aquele que muitos autores consideram ser um ponto de viragem no que era, até então, a tipologia bélica. Acredita-se que o advento da Guerra Fria, associado a uma crescente globalização e internacionalização de informações e recursos, tenha levado a que imergissem novas tipologias de guerras, muitas vezes extrapoladas dos seus limites devido à emergência "*of an embryonic global society*" (Baylis, 2014, p. 231). Contudo, Kaldor tem outra perceção. A autora (2012, p. 3) considera que "*the 'new war' argument does reflect a new reality – a reality that was emerging before the end of the Cold War*.", partilhando ainda da ideia de que a globalização "*is a convenient catch-all to describe the various changes that characterize the contemporary period and have influenced the character of war*" (Duffield, 1998, cit. por Kaldor, 2012, p. 3). Assim, Kaldor (2012, p. 2), à semelhança de Martins, entende que as ciberguerras, ou guerras virtuais, como lhes chama, são conflitos de baixa intensidade, que incluem elementos de pré-modernidade e modernidade, que se inserem no âmbito das 'novas guerras', distinguíveis, pela sua intensidade, das guerras características da modernidade clássica. Kaldor (2012, p. 4) refere, igualmente, que as 'novas guerras' têm de ser consideradas no contexto da globalização – para a autora (2012, p. 4) explicável como uma consequência da revolução tecnológica e comunicacional das décadas de 80 e 90 do século XX –, ou seja, "*the intensification of global interconnectedness – political, economic, military and cultural – and the changing character of political authority.*". A este propósito, a autora referiu-se ainda às palavras de Frank Hoffman (2011, cit. por Kaldor, 2012, p. 2), que recordou o conceito 'guerras híbridas', afirmando que o termo "*nicely captures the blurring of public and private, state or non-state, formal and informal that is characteristic of new wars*" (Kaldor, 2012, p. 02).

Contudo, há autores, como Valeriano e Maness (2015), que não observam as guerras híbridas como uma verdadeira ameaça, preferindo a defesa da conceção de que

uma guerra cibernética é, apenas, aquela que, ainda que provoque reações iniciais no ciberespaço, extrapola os meios cibernéticos provocando reações violentas numa realidade e contexto físico. Por outro lado, creem que empolar a perceção de ameaça de uma guerra cibernética, "*is dangerous because the response could then end up being the actual cause of more conflict.*" (Valeriano e Maness, 2015, p. 3). Assim, os autores (2015, p. 7) deixam um alerta: "*While there is a real danger of cyber combat, one must remain prudent in relation to the actual threat, not the inflated threat presented by the imagination.*". Outra caracterização importante das ciberguerras, por oposição às guerras tradicionais, será o facto de serem, ou não, cinéticas. Enquanto nas guerras cinéticas (tradicionais), o armamento usado são as armas e seus elementos análogos, nas guerras não-cinéticas (no caso, ciberguerras), o armamento usado é o existente no ciberespaço (Winterfeld e Andress, 2013, p. 3).

Todavia, apesar de ser observável o grau de perniciosidade das ciberguerras, existem autores que não acreditam verdadeiramente no mesmo. É o caso de Thomas Rid, autor da obra *Cyber War Will Not Take Place*, e de Marsili (2019, p. 191) que, apesar de aceitar a existência, tanto das ciberguerras, como do ciberterrorismo, diz que estes não são comparáveis aos conflitos tradicionais, isto porque, mesmo considerando as ciberguerras como um conflito armado tradicional, "*we must keep in mind that a war should have a temporal, physical space: a territory where the clash occurs and beginning and end of hostilities*.". Na desvalorização das ciberguerras, Willems (2019, p. 47) – que já tinha assumido não acreditar em ciberterrorismo – junta-se a Marsili e fundamenta a sua opinião no facto de uma guerra tradicional ter sempre "*at least two identifiable nations or regions involved (or ideologies, or religious, or even classes)*", referindo que, contrastivamente, os ciberataques "*are usually attacks made by or on behalf of a party that cannot even be identified with absolute certainty*." (Willems, 2019, p. 47).

Contudo, apesar de ser notório que, até ao momento não se verificou, verdadeiramente, nenhuma ciberguerra, é preciso analisar este evento à luz da hodiernidade e da globalização. Será, antes de mais, necessário recordar que devemos sempre retirar ensinamentos da História, razão pela qual, quando se decide uma ciberestratégia, "*we must not throw out hundreds of years' worth of doctrine and tactics but rather understand how to modify it based on the new paradigm we are facing*." (Winterfeld e Andress, 2013, p. 19). Depois, é preciso recuarmos a 2007, à Estónia. Apesar de este episódio ter sido largamente identificado com ciberterrorismo,

Winterfeld e Andress (2013, pp. 21-22), referem que este ciberataque teve contornos de ciberguerra, tendo integrado disputas entre Estados e ação militar (visto que a Estónia pediu apoio à NATO), pensamento corroborado por Johnson (2015a, p. 177) que apontou ainda que este poderá ter sido "*the first real cyber war*". Para alicerçar esta ideia, Johnson (2015a, p. 193) refere que o propósito base do Manual de Tallin, documento ímpar resultante destes ciberataques, "*is to focus on cyber warfare*.", tratando a forma como a lei internacional "*governs the resort to force by states as an instrument of their national policy, as well as the international law that regulates the conduct of armed conflict or the law of war*." (Schmitt, 2013 cit. Por Johnson, 2015a, p. 193). Hayward (2017, p. 409) relembra-nos ainda que "*[the] destruction of data may have compounding scale and real-world effects severe enough to constitute an "armed attack"*". Assim, não tendo havido até ao momento uma (verdadeira) ciberguerra, não existindo uma definição universal para o conceito, e tendo apenas como instrumento de ajuda o Manual de Tallin, de que forma pode ser regulado o uso de força no ciberespaço? Como se poderá disputar uma ciberguerra?

Importa, primeiramente, valorizar devidamente o ciberespaço, sendo necessário tomar a consciência de que se a invenção da pólvora mudou o paradigma da guerra, então obter o controlo "*of the modern technological state could paralyze major nations and bring them to their knees without firing a single bullet*." (Jurji, 2013, cit. por Mahmoud, 2013, p. 11). Assim, tal como as forças militarizadas adaptaram a sua forma de 'combate' face à utilização da pólvora, também o terão de fazer face à transmutação do seu campo de batalha, pelo que, segundo Mahmoud (2013, p. 11), terão de se formar 'exércitos inteligentes', isto é, "*based on quality not size, or, to be more precise, based on advanced technology and the ability to achieve the highest gains with the fewest resources.*". Tendo em conta esta mudança do paradigma bélico, Bruce Schneier (2008, cit. por Johnson, 2015a, p. 158), especialista de cibersegurança norte-americano, refere que, no século XXI, a guerra irá, inevitalvelmente, incluir as ciberguerras, "*as war moved into space with the development of satellites and ballistic missiles, and war will move into cyberspace with the development of specialized weapons, software, electronics, tactics, and defenses.*". Por esta razão, não só a definição de 'armamento' passou a ser inconclusiva no que respeita ao ciberespaço (Yeo, Birch e Bengtsson, 2016, p. 224), como o impacto das ciberguerras transcende barreiras geográficas e políticas (Mahmoud, 2013, p. 24).

Posto isto, e sendo notório que o fenómeno das ciberguerras ainda não chegou ao seu apogeu, Winterfeld e Andress (2013, p. 67) definiram a *Computer Network Exploitation* "*[as] the phase of cyber warfare that we are experiencing globally at this point*.", isto é, apesar de ainda não termos assistido a ciberguerras, já se verificam inúmeras ocorrências de ciberespionagem, uma espécie de fase embrionária do fenómeno bélico. Contudo, este embrião crescerá, indubitavelmente, para se tornar uma guerra que, não só se tornará uma das maiores ameaças do futuro (Bernik, 2014, p. 56), como será disputada por "*various groups and organizations, ... [and] individual countries, which play an offensive role to maintain or take leadership*." (Bernik, 2014, p. 56). Mas atentemos, agora, nos possíveis atores das ciberguerras. Bernik (2014, p. 56), não só inclui grupos e organizações nesta disputa, como nomeia os Estados-nação em último, dando quase a entender que estes não serão os principais atores deste renovado conflito. Terá sido este pensamento que levou Johnson (2015a, p. 158) a alertar para o facto de os ciberataques não terem, contrariamente a outros tipos de guerra, uma origem óbvia – referindo que "*there is something very terrifying not knowing your adversary*" – e Mahmoud (2013, p. 7) a descrever o grupo *Anonymous* como "*An Army Stationed in Cyberspace*", aludindo à noção de ciberexército. Tendo em conta esta diversidade de possíveis atores, que em muito diferem dos tradicionais, percebemos que o confronto de que aqui falámos, seja físico ou cibernético, poderá vir a apresentar-se com uma 'faceta encoberta', isto é, com uma aura de secretismo e de rivalidade não declarada que dificultará a identificação imediata do inimigo.

Por todos estes fatores, e por não existirem ainda, naturalmente e ao contrário dos restantes ciberataques aqui enumerados, legislação, tratados ou convenções que definam e regulem efetivamente as ciberguerras, também não se poderá apontar falhas na cooperação para dirimir as mesmas. Objetivamente, esta nunca existirá. São guerras, no fim de contas. A palavra que as acompanhará, seja no ciberespaço, no espaço, no ar, no mar ou terra firme, será sempre *oposição*.

III. Ciberdefesa na modernidade líquida: Estratégias para uma Europa ciberresiliente

De tudo o que se disse nas páginas anteriores, onde se descreveu os ciberataques e a sua perniciosidade nas suas principais vertentes, fica uma noção fundamental. Apesar de já muito ter sido feito pela cibersegurança e ciberresiliência europeia, o muito foi pouco. E o muito será sempre pouco. Os ciberataques são cada vez mais frequentes e

destrutivos. A cooperação europeia contra os ataques cibernéticos evoluiu muito, é certo, mas nunca será suficiente. Num mundo cada dia mais avançado, global e tecnologicamente, a tendência será para que os 'crimes tradicionais' venham, num futuro próximo ou a médio-longo prazo, a alforriar-se do mundo real, passando a habitar no ciberespaço.

2007 foi o aviso de que os decisores políticos europeus precisavam. Cibercrime, ciberterrorismo ou ciberguerra? Nunca existiu uma definição conclusiva e universal. Ficou a certeza de se ter tratado de um ciberataque altamente disruptivo que mudou profundamente a forma como a Europa – e, em última instância, parte do mundo, uma vez que foi necessária a intervenção da *NATO* – pensava o ciberespaço. Todavia, o facto de ainda não estar, como se viu, concretamente definido o que se passou na Estónia – com académicos a apontar entre cibercrime, ciberterrorismo ou ciberguerra – demonstra que a inexistência de definições estanques destes três conceitos, promove uma falta de identificação coerente e universal, abrindo espaço para que eventos semelhantes continuem a ter lugar e prossigam – tal como se passou na Estónia e em muitos outros ciberataques ao longo dos anos – sem culpados condenados, isto é, sem a necessária imputação[30]. O tradicional caso em que a 'culpa morre solteira'. E continuará, em grande parte, a morrer. Se a comunidade internacional, nomeadamente a europeia, nada melhorar, o sentimento de impunidade aumentará gradualmente e estes ataques serão cada vez mais disruptivos. Os ciberataques enumerados nesta dissertação devem ser entendidos como um 'grito de alerta' para a segurança nacional e internacional. O cibercrime, o ciberterrorismo e a ciberguerra do futuro já não serão avisos, mas antes acontecimentos concretos. E o maior culpado nunca será quem os cometeu. Enquanto atacantes cibernéticos continuam a conseguir, diariamente, ultrapassar fronteiras para lançar o caos, os Estados-Nação continuam a não conseguir – ou talvez a não querer – igualar esta ação para unir esforços contra esse caos. E enquanto assim permanecerem, serão sempre os decisores políticos, as organizações e as instituições, isto é, os que não conseguiram ultrapassar as fronteiras, os reais responsáveis pelos danos dos ciberataques. Enquanto os governantes europeus, e mundiais, não conseguirem

[30] Foram raros os casos em que ciberataques tiveram a devida imputação, sendo que, apenas em julho de 2020, a União Europeia, enquanto organismo, impôs, pela primeira vez na História, sanções decorrentes de ciberataques. Para mais informações sobre estas sanções, *vide*: https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/.

coadjuvar esforços para proteger o seu povo, não sofre uma nação, sofre a comunidade internacional.

Ainda que o verdadeiro ciberataque da atualidade seja o cibercrime – que se tornou tão pernicioso na virtualidade como o era, e é, na realidade – o mesmo não aconteceu com o ciberterrorismo e as ciberguerras. Mas isso não significa que não venha a acontecer. O contexto mundial apenas ainda não o proporcionou. Nunca será exequível acabar totalmente com os ciberataques. Esse pensamento não passará de uma utopia. Mas é possível fazer mais e melhor do que atualmente. Não sendo exequível travar a evolução tecnológica ou a globalização, será necessário promover a literacia digital entre a sociedade europeia, especialmente, nas nações da Europa de Leste, que se verificou serem, sucessivamente, as mais atacadas do continente. Tornou-se também notório que, apesar dos esforços, a coordenação entre as autoridades nacionais e supranacionais melhorou substancialmente no decorrer dos anos, visto que, apesar de os ciberataques terem aumentado em frequência, não se observou novamente um desafio análogo ao de 2007. Apesar de ser verificável a eficiência dos programas, estratégias e gabinetes para a ciberdefesa europeia, tendo em vista a prevenção de futuros ciberataques, bem como a diminuição das suas consequências, é notório que é preciso fazer mais e melhor. Não serão necessárias mais instituições, nacionais ou europeias, mas antes fazer uso, efetivo, das Convenções já assinadas – como a do Cibercrime. Será preciso, naturalmente, atualizar as mesmas, mas não elaborar outras. Para dirimir o cibercrime e acautelar o ciberterrorismo e as ciberguerras, será necessário melhorar os resultados da cooperação. Será necessário que as agências europeias continuem a notificar as agências nacionais. Será necessário robustecer o sistema de ciberdefesa europeu.

A globalização, promotora da revolução tecnológica que se vive, teve, indubitavelmente, entre 2000 e 2020, no continente europeu, influência no aumento gradual, e por vezes exponencial, dos ciberataques. O registo cronológico das ocorrências mostrou-o. A crescente gravidade dos ciberataques, também. Nos Estudos de Estratégia, não raras vezes associados aos Estudos de Segurança, a ordem é ‘preparar contra o provável, precaver contra o pior’. A Europa precisa de continuar o seu caminho de ciber-resiliência com estas palavras em mente.

Conclusão

Elaborar uma apreciação final de um relatório de estágio, contrastivamente a uma dissertação, será sempre mais árduo. Não podemos colocar em evidência conclusões retiradas de pesquisas ou análises, mas antes aprendizagens constantes e concretas. De facto, a ideia fulcral é que este estágio curricular proporcionou, fundamentalmente, uma imersão completa no que é o mercado de trabalho e, em particular, a experiência laboral numa Missão diplomática.

Posto isto, considero que este estágio acarretou vários benefícios, uma vez que tive oportunidade de utilizar, para além da teoria, os ensinamentos do Mestrado em Ciência Política e Relações Internacionais, particularmente das Relações Internacionais. A componente teórica desta área de estudos, acompanhada da sua respetiva aplicação, são fundamentais, mas a aplicação dos ensinamentos das Relações Internacionais num contexto laboral que não esteja acompanhado de internacionalidade, nunca será tão enriquecedor como foi um estágio curricular realizado no estrangeiro. De facto, considero que a oportunidade de imersão numa cultura diametralmente diferente da portuguesa foi, indubitavelmente, o elemento decisivo desta experiência. A necessária ambientação a um ambiente multicultural, o contacto com novas práticas culturais, políticas e sociais – num país que vive, e pensa, a Europa e a União Europeia, distintamente dos portugueses – e o contacto com diferentes formas de pensar, trabalhar e aplicar conhecimentos, foram decisivas para a correta vivência do que é o âmago das Relações Internacionais. Tratou-se, fundamentalmente, de uma aquisição de perspetivas e saberes que teriam ficado manifestamente inexploradas no caso de o estágio curricular ter ocorrido em território nacional. Para o desenvolvimento profissional, em muito contou a autonomia recebida desde o primeiro momento, experiência incomum para um estagiário, mas que permitiu, por um lado, desenvolver habilidades, até ao momento, inexploradas, e, por outro, aplicar e aprofundar capacidades já existentes. Por fim, os diversos momentos, ao longo de seis meses, em que tive oportunidade de comparecer a reuniões e encontros de alto nível, bem como de estar em contacto com missões congéneres, provaram ser altamente educativos, permitindo perceber a realidade política e diplomática, muito para além da teoria.

Não obstante, verificaram-se parâmetros suscetíveis de melhoria por parte da Embaixada de Portugal em Praga, mormente do orientador de estágio nesta instituição. Primeiramente, acredito que teria sido interessante permitir aos estagiários exercer funções em todos os setores da Embaixada – consular, político-diplomático e

secretariado –, objetivando, através do contacto com diferentes realidades, complementar a sua formação e aprendizagem, possibilitando, concomitantemente, enriquecer, qualitativa e quantitativamente, os seus relatórios de estágio. Depois, observou-se alguma falta de apoio na integração dos estagiários no país – nomeadamente, na falta de auxílio quanto à procura de alojamento –, uma certa desadequação entre as funções atribuídas aos estagiários e os seus conhecimentos/estudos académicos, uma discrepância entre a descrição das funções a desempenhar – apresentada pelo Ministério dos Negócios Estrangeiros e pela Embaixada – e as atividades efetivamente realizadas e, ainda, a inexistência, por parte do orientador de estágio, de uma concreta explicação bem como exemplificação, das funções incumbidas aos estagiários, tendo essa tarefa ficado a cargo de outros formandos sem vínculo permanente àquela Embaixada. Assim, apesar de se ter observado uma positiva exposição ao contexto profissional e a atividades ligadas ao mesmo, que não teria sido possível sem a realização deste estágio curricular, acredito que não existiu por parte da instituição de acolhimento, particularmente por parte do orientador de estágio, elemento que, para este efeito, representa a mesma, um desempenho adequado do seu papel, nomeadamente na mentoria contínua que se pede nesta função, o que por vezes causou entropias nas ações a desempenhar, bem como dificuldades no desenvolvimento do relatório de estágio.

Bibliografia

Aas, KF, 2007. *Globalization & Crime*. London: Sage Publications

Bajovic, V, 2017. 'Criminal Proceedings in Cyberspace: The Challenge of Digital Era'. In: E. C. Viano, 2017. *Cybercrime, Organized Crime and Societal Responses. International Approache*s. Cham: Springer. Cap. 5

Baylis, J, 2014. 'International and global security'. In: J. Baylis, S. Smith e P. Owens, ed., 2014. *The Globalization of World Politics. An introduction to international relations*. Oxford: Oxford University Press. Cap. 15

Baylis, J, Smith, S e Owens, P, 2014. *The Globalization of World Politics. An introduction to international relations*. Oxford: Oxford University Press.

Bernik, I, 2014. *Cybercrime and Cyberwarfare*. Londres: ISTE

Bîzgă, A, 2020. *Mysterious cyberattack cripples Czech hospital amid Covid-19 outbreak*. [Em linha] Bucareste: Bitdefender. Disponível em: https://www.bitdefender.com/blog/hotforsecurity/mysterious-cyberattack-cripples-czech-hospital-amid-covid-19-outbreak, [Consult. 11 Jun. 2022]

Booth, K, 2014. 'Global Security'. In: M. Kaldor e I. Rangelov, 2014. *The Handbook of Global Security Policy*. West Sussex: Wiley Blackwell. Cap. 1

Brenner, SW, 2006. 'Cybercrime, Cyberterrorism and Cyberwarfare'. *Revue Internationale de Droit Pénal*, 77:3, 453-471

Câmara de Comércio Checo-Portuguesa, s.d., *Sobre Nós*. [em linha] Praga: Câmara de Comércio Checo-Portuguesa. Disponível em: http://www.czptchamber.eu/pt/sobre-nos/, [Consult. 30 Mai. 2022]

Center for Strategic & International Studies, s.d.. *Significant Cyber Incidents Since 2006*. [Em linha] Washington, DC: CSIS. Disponível em: [Consult. 11 Jan. 2022]

Centro Nacional de Cibersegurança, 2021. *Quadro Nacional de Referência para a Cibersegurança*. [Em linha] Lisboa: CNCS. Disponível em: https://www.cncs.gov.pt/pt/quadro-nacional/, [Consult. 13 Jan. 2022]

Computer Security Resource Center, s.d.. *Cyber Attack*. [Em linha] Maryland: National Institute of Standards and Technology. Disponível em: https://csrc.nist.gov/glossary/term/cyber_attack, [Consult. 15 Out. 2021]

Consulado Geral de Portugal em Nova Iorque, s.d.. *Consulados Honorários*. [em linha] Nova Iorque: Ministério dos Negócios Estrangeiros. Disponível em:

https://novaiorque.consuladoportugal.mne.gov.pt/pt/o-consulado/jurisdicao/consulados-honor%C3%A1rios, [Consult. 26 Mai. 2022]

Council of Europe Portal, s.d.. *Protocol negotiations: The Drafting Group assists the T-CY Plenary in the preparation of a draft Second Additional Protocol to the Convention on Cybercrime (ETS 185)*. [Em linha] Estrasburgo: COE. Disponível em: https://www.coe.int/en/web/cybercrime/t-cy-drafting-group, [Consult. 13 Jan. 2022]

Denning, DE, 2001. 'Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy'. In: Arquilla, J e Ronfeldt, D, 2001. *Networks and Netwars: The Future of Terror, Crime, and Militancy*. Santa Monica: RAND Corporation. Cap. 8

Ducaru, S, 2016. 'Is Cyber Defense Possible?'. Journal of International Affairs, 70:1, 182-189

Elias, L, 2016. Criminalidade Transnacional Organizada. Paradoxos Conceptuais e Desafios Políticos e Operacionais. In: Borges JV e Rodrigues TF, ed., 2016. *Ameaças e Riscos Transnacionais no Novo Mundo Global*. Porto: Fronteira do Caos Editores. Cap. 5

Eriksson, J e Giacomello, G, 2007a. 'Introduction: Closing the gap between international relations theory and studies of digital-age security'. In: J. Eriksson e G. Giacomello, 2007. *International Relations and Security in the Digital Age*. Oxon: Routledge. Cap. 1

Eriksson, J, e Giacomello, G, 2007b. 'Conclusion: Digital-age security in theory and practice'. In: J. Eriksson e G. Giacomello, 2007. *International Relations and Security in the Digital Age*. Oxon: Routledge. Cap. 8

Euronews, 2021. *Czech officials in Prague 'hit by massive cyber attack'*. [Em linha] Lyon: Euronews. Disponível em: https://www.euronews.com/2021/03/05/czech-officials-in-prague-hit-by-massive-cyber-attack, [Consult. 11 Jun. 2022]

European Comission, 2019. *Questions and Answers: Mandate for the Second Additional Protocol to the Budapest Convention*. [Em linha] Bruxelas: EC. Disponível em: Questions and Answers: Mandate for the Second Additional Protocol to the Budapest Convention (europa.eu), [Consult. 13 Jan. 2022]

European Cybercrime Training and Education Group, s. d.. *European Cybercrime Training and Education Group*. [Em linha] Bruxelas: ECTEG. Disponível em: https://www.ecteg.eu/, [Consult. 09 Jan. 2022]

Europol, 2011. *Threat Assessment (Abridged) Internet Facilitated Organised Crime (IOCTA)*. The Hague: Europol

Europol, 2014. *The Internet Organised Crime Threat Assessment (IOCTA)*. The Hague: Europol

Europol, 2015. *Internet Organised Crime Threat Assessment (IOCTA)*. The Hague: Europol

Europol, 2016. *Internet Organised Crime Threat Assessment (IOCTA)*. The Hague: Europol

Europol, 2017. *Internet Organised Crime Threat Assessment (IOCTA)*. The Hague: Europol

Europol, 2018. *Internet Organised Crime Threat Assessment (IOCTA)*. The Hague: Europol

Europol, 2019. *Internet Organised Crime Threat Assessment (IOCTA)*. The Hague: Europol

Europol, 2020. *Internet Organised Crime Threat Assessment (IOCTA)*. The Hague: Europol

Europol, 2021. *European Cybercrime Centre - EC3*. [Em linha] Haia: Europol. Disponível em: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3, [Consult. 05 Jan. 2022]

Gabinete Coordenador de Segurança, 2006. *Relatório Anual de Segurança Interna*. Lisboa: Ministério da Administração Interna

Gabinete Coordenador de Segurança, 2007. *Relatório Anual de Segurança Interna*. Lisboa: Ministério da Administração Interna

Gabinete do Secretário-Geral do Sistema de Segurança Interna, 2008. *Relatório Anual de Segurança Interna*. Lisboa: Ministério da Administração Interna

Garon, JM, 2018. 'Cyber-World War III Origins'. *Journal of Law & Cyber Warfare*, 7:1, 1-60

Gelernter, L e Regev, M, 2010. 'Internet and globalization'. In: B.S. Turner, ed., 2010. *The Routledge International Handbook of Globalization Studies*. Oxon: Routledge. Cap. 4

Geraldes, SM, 2019. A Estratégia de Cibersegurança da União Europeia: Catastrofista, Realista e/ou Otimista?. *Nação e Defesa*, [Em linha] 154. Disponível em: https://comum.rcaap.pt/bitstream/10400.26/33162/1/GERALDESSofiaMartins_A

estrat%C3%A9giadeciberseguran%C3%A7adaUni%C3%A3oEuropeia_Na%C3%A7%C3%A3oDefesa_N_154_p_91_108.pdf, [Consult. 5 Dez. 2021]

Ghosh, S, 2010. 'Nature of Cyberattacks in the Future'. In: S. Ghosh e E. Turrini. *Cybercrimes: A Multidisciplinaty Analysis*. Heidelberg: Springer. Cap. 20

Giddens, A, 1991. *The Consequences of Modernity*. Reino Unido: Polity Press

Giovannelli, D, s. d.. *Proposal of United Nations Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes: Comment on the first draft text of the Convention*. [Em linha] Tallinn: NATO Cooperative Cyber Defence Centre of Excellence. Disponível em: https://www.ccdcoe.org/library/publications/proposal-of-united-nations-convention-on-countering-the-use-of-information-and-communications-technologies-for-criminal-purposes-comment-on-the-first-draft-text-of-the-convention/, [Consult. 04 Jan. 2022]

Goldsmith, J, 2011. 'Cybersecurity Treaties: A Skeptical View'. *Future Challenges Essay*. [Em linha] Hoover Institution. Disponível em: https://media.hoover.org/sites/default/files/documents/FutureChallenges_Goldsmith.pdf, [Consult. 07 Jan. 2022]

Goodman, M, 2010. 'International Dimensions of Cybercrime'. In: S. Ghosh e E. Turrini. *Cybercrimes: A Multidisciplinaty Analysis*. Heidelberg: Springer. Cap. 17

Hayward, RJ, 2017. 'Evaluating the "Imminence" of a Cyber Attack for Purposes of Anticipatory Self-Defense'. *Columbia Law Review*, 117:2, 399-434

Herzog, S, 2011. Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. *Journal of Strategic Security*, 4, 49-60

Instituto Camões, s.d. *República Checa*. [Em linha] Lisboa: Ministério dos Negócios Estrangeiros. Disponível em: https://www.instituto-camoes.pt/activity/o-que-fazemos/investigacao/centros-de-lingua-portuguesa/republica-checa, [Consult. 26 Mai. 2022]

International Trade Administration, 2021. *The Czech government approved its National Cybersecurity Strategy for 2021 – 2025*. [Em linha] Washington, DC: ITA. Disponível em: https://www.trade.gov/market-intelligence/czech-republic-cybersecurity, [Consult. 11 Jun. 2022]

Johnson, TA, 2015a. 'Cyber Intelligence, Cyber Conflicts, and Cyber Warfare'. In: T. A. Johnson, 2015. *Cyber-Security. Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare*. Boca Raton: CRC Press. Cap. 4

Johnson, TA, 2015b. ‘Cybersecurity. Threat Landscape and Future Trends’. In: T. A. Johnson, 2015. *Cyber-Security. Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare*. Boca Raton: CRC Press. Cap. 7

Jones, DM, 2016. ‘Surveillance and Resistance: Online Radicalization and the Political Response’. In: Silva, E, 2016. *National Security and Counterintelligence in the Era of Cyber Espionage*. Hershey: IGI Global. Cap. 7

Kaldor, M, 2012. *New and Old Wars. Organised Violence in a Global Era*. Cambridge: Polity Press

Keating, J, 2010. *Who was behind the Estonia cyber attacks?*. [Em linha] Washington D.C.: Foreign Policy. Disponível em: https://foreignpolicy.com/2010/12/07/who-was-behind-the-estonia-cyber-attacks/ [Consult. 23 Jan 2022]

Khan, FU, 2011. ‘States rather than criminals pose a greater threat to global cyber security’. *Strategic Studies*, 31:3, 91-108.

Kiras, JD, 2014. ‘Terrorism and globalization’. In: J. Baylis, S. Smith e P. Owens, ed., 2014. *The Globalization of World Politics. An introduction to international relations*. Oxford: Oxford University Press. Cap. 23

Kremling, J e Parker, AMS, 2017. *Cyberspace, cybersecurity, and cybercrime*. Thousand Oaks: Sage Publications.

Lachow, I, 2009. ‘Cyber Terrorism: Menace or Myth?’. In: F. D. Kramer, S. H. Starr e L. K. Wentz, 2009. *Cyberpower and National Security*. Lincoln: University of Nebraska Press. Cap. 19

Lopatka, J e Muller, R, 2020. *Czech hospitals report cyberattacks day after national watchdog’s warning.* [Em linha] Londres: Reuters. Disponível em: https://www.reuters.com/article/us-czech-cyber-ostrava-idUSKBN21Z1OH, [Consult. 11 Jun. 2022]

Mahmoud, KW, 2013. *Cyber Attacks: The Electronic Battlefield*. Arab Center for Research & Policy Studies, [Em linha]. Disponível em: http://www.jstor.com/stable/resrep12651, [Consult. 03 Set. 2021]

Marsili, M, 2019. ‘The War on Cyberterrorism’. *Democracy and Security*, [Em linha] 15:2, 172-199

Martins, R, 2017. ‘Anonymous' Cyberwar Against ISIS and the Asymmetrical Nature of Cyber Conflicts’. *The Cyber Defense Review*, 2-3, pp. 95-106

Matusitz, J, 2005. ‘Cyberterrorism: How Can American Foreign Policy Be Strengthned in the Information Age?’. *American Foreign Policy Interests*, 27, 137-147

McCormick, T, 2013. ‘Anthropology of an Idea: Hacktivism’. *Foreign Policy*, 200, pp. 24-25

Naím, M, 2017. ‘Why Democracies Are at a Disadvantage in Cyber Wars’. *Journal of International Affairs*, Special 70th Anniversary Issue, 85-91

Národní Úřad pro Kybernetickou a Informační Bezpečnost, s. d.. *About NÚKIB*. [Em linha] Praga: NÚKIB. Disponível em: https://www.nukib.cz/en/about-nukib/, [Consult. 11 Jun. 2022]

Noble, W, 2017. ‘Cyber Armies - The Growth of the Cyber Defence Industry’. In: T. Owen, W. Noble e F. C. Speed, ed., 2017. *New Perspectives on Cybercrime*. Suíça: Palgrave McMillan

Nunes, PFV, 2016. Ciberameaças e Quadro Legal dos Conflitos no Ciberespaço. In: Borges JV e Rodrigues TF, ed., 2016. *Ameaças e Riscos Transnacionais no Novo Mundo Global*. Porto: Fronteira do Caos Editores. Cap. 9

Nye, JS, 2010. ‘Cyber Power. Belfer Center for Science and International Affairs’. [Em linha] Harvard Kennedy School. Disponível em: https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf, [Consult. 22 Dez. 2021]

Olesen, N, 2016. ‘European Public-Private Partnerships on Cybersecurity - An Instrument to Support the Fight Against Cybercrime and Cyberterrorism’. In: B. Akhgar e B. Brewster, 2016. *Combatting Cybercrime and Cyberterrorism: Challenges, Trends and Priorities*. Suíça: Springer. Parte III

Organização das Nações Unidas, 1995. ‘Ninth United Nations Congress on the Prevention of Crime and the Treatment of Offenders’. Cairo, 29 de Abril a 8 de Maio de 1995. Cairo: ONU

Park, D, Summers, J e Walstrom, M. 2017. *Cyberattack on Critical Infrstructure: Russia and the Ukrainian Power Grid Attacks*. [Em linha] Seattle: s.n.. Disponível em: https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/, [Consult. 20 Dez. 2021]

Peters, A e Jordan, A, 2019. ‘Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime’. *Third Way*, [Em linha]. Disponível em: http://www.jstor.com/stable/resrep20150, [Consult. 03 Set. 2021]

Picarelli, JT, 2008. ‘Transnational Organized Crime’. In: P.D. Williams, 2008. *Security Studies: An Introduction*. Oxon: Routledge. Cap. 30

Portal Diplomático, s.d.a. *O que é a Rede Diplomática?*. [Em linha] Lisboa: Ministério dos Negócios Estrangeiros. Disponível em: https://portaldiplomatico.mne.gov.pt/rede-diplomatica/o-que-e-a-rede-diplomatica, [Consult. 26 Mai. 2022]

Portal Diplomático, s.d.b. *Países*. [em linha] Lisboa: Ministério dos Negócios Estrangeiros. Disponível em: https://portaldiplomatico.mne.gov.pt/relacoesbilaterais/paises-geral/republica-checa, [Consult. 30 Mai. 2022]

Preciado, M, 2012. 'If You Wish Cyber Peace, Prepare for Cyber War. The Need for the Federal Government to Protect Critical Infrastructure From Cyber Warfare'. *Journal of Law & Cyber Warfare*, 1:1, 99-154

Ranstorp, M, 2007. 'The virtual sanctuary of al-Qaeda and terrorism in an age of globalization'. In: J. Eriksson e G. Giacomello, 2007. *International Relations and Security in the Digital Age*. Oxon: Routledge. Cap. 2

Rogers, P, 2008. 'Terrorism'. In: P.D. Williams, 2008. *Security Studies: An Introduction*. Oxon: Routledge. Cap. 12

Security Magazine, 2020. *Brno University Hospital in Czech Republic Suffers Cyberattack During COVID-19 Outbreak*. [Em linha] Canadá: Security Magazine. Disponível em: https://www.securitymagazine.com/articles/91921-brno-university-hospital-in-czech-republic-suffers-cyberattack-during-covid-19-outbreak, [Consult. 11 Jun. 2022]

Sheenan, M, 2014. 'The changing character of war'. In: J. Baylis, S. Smith e P. Owens, ed., 2014. *The Globalization of World Politics. An introduction to international relations*. Oxford: Oxford University Press. Cap. 14

Shorer-Zeltser, M, e Ben-Israel, GM, 2016. 'Developing Discourse and Tools for Alternative Content to Prevent Terror'. In: Silva, E, 2016. *National Security and Counterintelligence in the Era of Cyber Espionage*. Hershey: IGI Global. Cap. 8

Sistema de Segurança Interna, 2009. *Relatório Anual de Segurança Interna*. Lisboa: Ministério da Administração Interna

Sistema de Segurança Interna, 2010. *Relatório Anual de Segurança Interna*. Lisboa: Ministério da Administração Interna

Sistema de Segurança Interna, 2011. *Relatório Anual de Segurança Interna*. Lisboa: Ministério da Administração Interna

Sistema de Segurança Interna, 2012. *Relatório Anual de Segurança Interna*. Lisboa: Ministério da Administração Interna

Sistema de Segurança Interna, 2013. *Relatório Anual de Segurança Interna*. Lisboa: Ministério da Administração Interna

Sistema de Segurança Interna, 2014. *Relatório Anual de Segurança Interna*. Lisboa: Ministério da Administração Interna

Sistema de Segurança Interna, 2015. *Relatório Anual de Segurança Interna*. Lisboa: Ministério da Administração Interna

Sistema de Segurança Interna, 2016. *Relatório Anual de Segurança Interna*. Lisboa: Ministério da Administração Interna

Sistema de Segurança Interna, 2017. *Relatório Anual de Segurança Interna*. Lisboa: Ministério da Administração Interna

Sistema de Segurança Interna, 2018. *Relatório Anual de Segurança Interna*. Lisboa: Ministério da Administração Interna

Sistema de Segurança Interna, 2019. *Relatório Anual de Segurança Interna*. Lisboa: Ministério da Administração Interna

Sistema de Segurança Interna, 2020. *Relatório Anual de Segurança Interna*. Lisboa: Ministério da Administração Interna

Skopik, F, Settanni, G e Fiedler, R, 2018. 'The Importance of Information Sharing and Its Numerous Dimensions to Circumvent Incidents and Mitigate Cyber Threats'. In: F. Skopik, 2018. *Collaborative Cyber Threat Intelligence: Detecting and Responding to Advanced Cyber Attacks at the National Level*. Flórida: CRC Press. Cap. 4

Skórzewska-Amberg, M, 2017. 'Global Threats But National Legislations - How to Adapt to the New Cyberspace Society'. In: E. C. Viano, 2017. *Cybercrime, Organized Crime and Societal Responses. International Approache*s. Cham: Springer. Cap. 4

Socor, V, 2008. *NATO Creates Cyber Defense Center in Estonia*. [Em linha] Washington DC: The Jamestown Foundation. Disponível em: https://jamestown.org/program/nato-creates-cyber-defense-center-in-estonia/, [Consult. 05 Jan. 2022]

Sullivan, JP, 2014. 'Transnational Crime'. In: M. Kaldor e I. Rangelov, 2014. *The Handbook of Global Security Policy*. West Sussex: Wiley Blackwell. Cap. 9

Turner, BS, 2010. ‘Theories of Globalization: issues and origins’. In: B.S. Turner, ed., 2010. *The Routledge International Handbook of Globalization Studies*. Oxon: Routledge. Cap. 1

Turrini, E e Ghosh, S, 2010. ‘A Pragmatic, Experiential Definition of Computer Crimes’. In: S. Ghosh e E. Turrini. *Cybercrimes: A Multidisciplinaty Analysis*. Heidelberg: Springer. Cap. 1

Ulsch, NM, 2014. *Cyber Threat! How to Manage the Growing Risk of Cyber Attacks*. Nova Jersey: Wiley

United Nations Office on Drugs and Crime, s. d.. *Transnational Organized Crime*. [Em linha] Central America and the Caribbean: UNODC. Disponível em: https://www.unodc.org/ropan/en/organized-crime.html, [Consult. 16 Jan 2022]

Valeriano, B, e Maness, RC, 2015. *Cyber War vs. Cyber Realities. Cyber Conflict in the International System*. Oxford: Oxford University Press

Viano, EC, 2017. ‘Cybercrime: Definition, Typology, and Criminalization’. In: E. C. Viano, 2017. *Cybercrime, Organized Crime and Societal Responses. International Approache*s. Cham: Springer. Cap. 1

Vincent, NA, 2017. ‘Victims of cybercrime: Definitions and challenges’. In: E. Martellozzo e E. A. Jane, 2017. *Cybercrime and its Victims*. Oxon: Routledge. Cap. 1

Virkar, S, 2016. ‘The Mirror Has Two Faces: Terrorist Use of the Internet and the Challenges of Governing Cyberspace’. In: Silva, E, 2016. *National Security and Counterintelligence in the Era of Cyber Espionage*. Hershey: IGI Global. Cap. 1

Wiletts, P, 2014. ‘Transnational actors and international organizations in global politics’. In: J. Baylis, S. Smith e P. Owens, ed., 2014. *The Globalization of World Politics. An introduction to international relations*. Oxford: Oxford University Press. Cap. 21

Willems, E, 2019. ‘From Cyberwar to Hacktivism’. In: E. Willems, 2019. Cyberdanger. Understanding and Guarding Against Cybercrime. Cham: Springer. Cap. 4

Williams, PD, 2008. ‘Security Studies: An Introduction’. In: P.D. Williams, 2008. *Security Studies: An Introduction*. Oxon: Routledge. Cap. 1

Winslow, R, e Winslow, V, 2010. ‘The globalization of crime’. In: B.S. Turner, ed., 2010. *The Routledge International Handbook of Globalization Studies*. Oxon: Routledge. Cap. 13

Winterfeld, S, e Andress, J, 2013. *The Basics of Cyber Warfare. Understanding the Fundamentals of Cyber Warfare in Theory and Practice*. Waltham: Elsevier.

Wong, WH e Brown, PA, 2013. 'E-Bandits in Global Activism: WikiLeaks, Anoonymous, and the Politics of No One'. *Perspectives on Politics*, 11-4, pp. 1015-1033

XXI Governo - República Portuguesa, 2016. *Portugal é fundador do grupo europeu de formação para combate ao cibercrime*. [Em linha] Lisboa: XXI Governo. Disponível em: https://www.portugal.gov.pt/pt/gc21/comunicacao/noticia?i=20161125-mj-cibercrime, [Consult. 09 Jan. 2022]

Yeo, S, Birch, AS e Bengtsson, HIJ, 2016. 'The Role of State Actors in Cybersecurity: Can State Actors Find Their Role in Cyberspace?'. In: Silva, E, 2016. *National Security and Counterintelligence in the Era of Cyber Espionage*. Hershey: IGI Global. Cap. 13