Universidade do Minho
Escola de Economia e Gestão

Hélio Samuel Farinha Campos

A Luta Contra o Cibercrime: Os Casos da União Europeia e da NATO

Dissertação de Mestrado

Mestrado em Relações Internacionais

Trabalho efetuado sob a orientação da

Professora Doutora Laura Cristina Ferreira-Pereira

Professora Doutora Alena Vysotskaya Guedes Vieira

Outubro de 2018

DECLARAÇÃO

Nome: Hélio Samuel Farinha Campos

Endereço eletrónico: heliosamuelcampos@gmail.com Telefone: 919 879 015

Cartão do Cidadão: 14184087

Título da dissertação: A Luta Contra o Cibercrime: Os Casos da União Europeia e da NATO

Orientadoras:

Professora Doutora Laura Cristina Ferreira-Pereira

Professora Doutora Alena Vysotskaya Guedes Vieira

Ano de conclusão: 2018

Mestrado em Relações Internacionais

Universidade do Minho, _____/_____/_____

Assinatura: 

AGRADECIMENTOS

Os primeiros e mais fervorosos agradecimentos são dirigidos as minhas orientadoras, a professora Doutora Laura C. Ferreira-Pereira e a professora Doutora Alena V. Guedes Vieira, que demonstraram ser não só exemplares profissionais nas suas respetivas áreas, mas também na demonstração de um inexcedível compromisso de honra na ajuda que me foi disponibilizada.

De seguida quero agradecer a minha família (dentro desta eu enumero particularmente os meus pais, os meus irmãos, os meus pais-sogros e a minha noiva) pois sem a compreensão e o constante apoio destes nunca teria almejado chegar onde cheguei em termos académicos. Foram sempre os primeiros e serão sempre os últimos a acreditar no meu potencial.

Quero também deixar um agradecimento muito especial aos meus amigos que me deram a força necessária para perseguir o meu sonho estando sempre ao meu lado - nos bons e nos maus momentos - nunca deixando de acreditar em mim.

Por último, mas definitivamente não menos importante, quero agradecer ao amor da minha vida – Ling Li – que viu esta tese nascer, crescer e ganhar asas mantendo-se ao meu lado e apoiando-me fielmente como só um grande amor o consegue fazer (**李凌永**远爱你).

Desistir?!? O sangue Lusitano é feito de perseverança, luta e fé muita fé. Que se reerga o Adamastor e se incite o Cabo das Tormentas pois ainda resta em nós Portugueses o espírito e a fibra dos descobridores. Que nunca se perca a vontade de falar e escrever em Português - língua de camões e do povo lusitano.

RESUMO

A cibersegurança e a ciberdefesa passaram a ser campos mais explorados pelos Estados e pelas Organizações Internacionais com a entrada no novo milénio. A evolução dos aparelhos eletrónicos, a globalização e as características mutáveis e transnacionais do ciberespaço tornaram o dia a dia de todos nos mais fácil, mas ao mesmo tempo mais perigoso. Com isto em mente a exploração e a evolução da cibersegurança e da ciberdefesa tornou-se parte do quotidiano de organizações como a União Europeia e NATO e a regulamentação deste espaço apareceu com naturalidade. A presente dissertação tem por objetivo examinar a evolução do papel da União Europeia e da NATO na luta contra o cibercrime. Esta análise acompanhará os acontecimentos mais relevantes ocorridos no domínio da cibersegurança no seio dos dois atores em análise e será dividida em três ciclos distintos: a entrada no século XXI, o ciberataque à Estónia em 2007 e o pós-ciberataque à Estónia, onde se procurará identificar os marcos históricos, as novas dinâmicas, as convergências e as possíveis influências de novos acontecimentos no seio destas duas organizações. Em termos de enquadramento teórico, a análise do aumento exponencial da securitização do ciberespaço no seio da agenda securitária da União Europeia e da NATO será feita com base do na teoria Neoliberalista Institucional e a Teoria dos Regimes.

Palavras-chave: União Europeia, NATO, Cibercrime, Ciberterrorismo, Ciberataques, Ciberespaço, Cibersegurança, Ciberdefesa, Neoinstitucionalismo Liberal e Teoria dos Regimes.

ABSTRACT

Cybersecurity and cyber-defence have become more explored by states and international organizations as we entered the new millennium. The evolution of electronic devices, the globalization and the changing and transnational characteristics of cyberspace have made daily life easier, but at the same time more dangerous. With this in mind, the exploitation and evolution of cyber-security and cyber-defence has become a daily part of organizations such as European Union and NATO. This dissertation aims at examining the evolution of the role of the European Union and NATO in the fight against cybercrime. This analysis will follow the most relevant events in the area of cyber-security within the two actors under examination and will be divided into three distinct cycles: the entry into the 21st century, the cyberattack in Estonia in 2007 and the aftermath of the cyberattack in Estonia, where it will be sought to identify the historical milestones, the new dynamics, the convergences and the possible influence of new events within these two organizations. In terms of the theoretical framework, the analysis of the exponential increase of the securitization of cyberspace within the security agenda of the European Union and NATO draws on the neoliberal institutional theory and the theory of regimes.

Keywords: European Union, NATO, Cybercrime, Cyberterrorism, Cyber-attacks, Cyberspace, Cybersecurity, Cyber-defence, Neoliberal Institutionalism and Regime Theory.

ÍNDICE

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS, SIGLAS E ACRÓNIMOS

ACCS	Sistema de Comando e Controlo Aéreo;
Al-Qaeda	Organização Fundamentalista Islâmica;
C4ISR	Comando, Controlo, Comunicações, Computadores, Inteligência, Vigilância e Reconhecimento;
CCDCOE	Centro Cooperativo de Defesa Cibernética de Excelência da NATO;
CE	Comissão Europeia;
CERT-UE	Equipa de Resposta a Emergências Informáticas da União Europeia;
CNCS	Centro Nacional de Cibersegurança – Portugal;
CSIRT	Equipa de Resposta a Incidentes de Segurança Informática;
EC3	Centro Europeu de Cibercriminalidade;
EDA	Agência Europeia de Defesa;
EISAS	Sistema Europeu de Partilha e Alerta de Informação;
ENISA	Agência Europeia para a Segurança das Redes e da Informação;
EUA	Estados Unidos da América;
EUISS	Instituto de Estudos de Segurança da União Europeia;
eu-LISA	Agência Europeia para a Gestão Operacional de Sistemas Informáticos de Grande Escala no Espaço da Liberdade, da Segurança e da Justiça;
EUR-Lex	Direito da União Europeia;
EUROPOL	Serviço Europeu de Polícia;
FMN	Rede de Missão Federada;
IC	Infraestruturas Críticas;
IDS	Software de Deteção de Intrusão;
ISR	Inteligência, Vigilância e Reconhecimento;
ISIS	Estado Islâmico do Iraque e do Levante;
NACMA	Agência de Gestão do ACCS da NATO;
NATO (OTAN)	Organização do Tratado do Atlântico Norte;
NC3A	Conselho de Consulta, Comando e Controlo;
NCDMA / CDMA	Autoridade para a Gestão da Defesa Cibernética da NATO;

NCIA	Agência de Comunicação e Informação da NATO;
NCIRC	Equipa de Resposta a Incidentes de Segurança Informática da NATO;
NCSA	Agência de Comunicações e Sistemas de Informação da NATO;
NIS	Serviço de Informações de Rede;
OI	Organização Internacional;
ONU	Organização das Nações Unidas
OSCE	Organização para a Segurança e Cooperação na Europa;
PCSD	Política Comum de Segurança e Defesa;
PEPIC	Programa Europeu de Proteção das Infraestruturas Críticas;
PESD	Política Europeia de Segurança e Defesa;
SRI/NIS	Segurança dos Sistemas de Rede e Informação;
TI	Tecnologias de Informação;
TIC	Tecnologias de Informação e Comunicação;
UE	União Europeia.

INTRODUÇÃO

Tema

Com os destroços e o ferro retorcido das torres gémeas nasceu uma das dinâmicas internacionais que mais preocupou e tem preocupado as Organizações Internacionais (OI) no século XXI: o terrorismo transnacional. A transnacionalidade deste fenómeno ficou clara com o 11 de setembro de 2001, o que as Organizações Internacionais, bem como os Estados, não esperavam é que globalização e a evolução tecnológica apresentassem outro perigo também ele transnacional, mas bem mais silencioso: o cibercrime.

O fenómeno da cibersegurança e da ciberdefesa, até o 11 de setembro de 2001 pouco esclarecido e aprofundado, afirmou-se com a entrada no novo milénio e surge atualmente na ordem do dia de muitos Estados e Organizações Internacionais, como é caso da União Europeia (UE) e da Organização do Tratado do Atlântico Norte (NATO), focos centrais da exploração investigativa que se pretende realizar. Tendo isto em conta o balizamento temporal desta investigação ficará compreendido entre o ano de 2000 e o ano de 2018. O ano 2000 destaca-se como o ano onde muitos dos primeiros passos relativamente ao controlo cibersecuritário tiveram lugar:

> "A reunião do G8[1] em junho de 2000 foi o início da ação para a regulamentação e controlo do ciberespaço fazendo eco no Conselho da Europa que formulou uma Convenção contra o cibercrime em 2001". (Figueiredo, 2014: 92)

Ainda durante o ano de 2000, não poderemos esquecer a afirmação que Dorothy E. Denning[2] proferiu relativamente ao ciberterrorismo no outono de 2000. O balizamento temporal final desta

[1] Grupo global com vista a discussão e resolução de problemáticas mundiais. É composto por: Estados Unidos da América, Canadá, Alemanha, Japão, França, Reino Unido, Itália e Rússia. A partir de 2014 passou a designar-se G7 com a suspensão da Rússia devido a anexação da Crimeia.

[2] Dorothy E. Denning é Professora do Departamento de Análise e Defesa da Escola de Pós-Graduação da Marinha dos EUA em Monterey. Os seus interesses na área da investigação passam pelo ciberterrorismo, ciberespaço, cibercrime, entre outras problemáticas associadas ao ciberespaço.

investigação ficará situado em julho de 2018, por permitir ainda incluir o regulamento cibersegurança da UE em junho de 2018 e a cimeira de Bruxelas da NATO em julho de 2018.

Com esta análise pretende-se compreender como se processou a regulamentação do ciberespaço tanto por parte da UE como por parte da NATO. O facto de este espaço ter a capacidade de abarcar sem controlo todas as pessoas do mundo (algo inédito e irrepetível noutra qualquer área) (Leite, 2016: 1) e de ter "colonizado e se fundido com o espaço físico" (Kissinger, 2014: 392), fez com que medidas de controlo e de defesa tivessem de ser desenvolvidas pelas duas organizações. Com o intuito primordial de fazer com que os crimes informáticos deixassem de ser só acontecimentos isolados e passassem a ser punidos como um qualquer outro crime.

Devido não só ao perigo da ameaça transnacional, que é nos tempos correntes mais real do que nunca, mas também devido a evolução tecnológica que trouxe consigo novos desafios para estes atores, as Organizações Internacionais que agora se exploram começaram então a contar com o ciberespaço, espaço onde a delimitação espacial desta dissertação se cingirá, no ambiente securitário prioritário dos seus documentos estratégicos. A UE "viria a aumentar o foco na segurança cibernética equipando-se e ajudando os Estados-membros a protegerem-se contra as ameaças cibernéticas, mantendo simultaneamente um ciberespaço aberto, livre e seguro" (Conselho da União Europeia, 2016a: 21-22)[3].

Exemplos claros destes documentos são o Relatório sobre a Implementação da Estratégia Europeia de Segurança de 2008 e Estratégia Global de 2016, no caso da UE, e o Conceito Estratégico de 2010, no caso da NATO. Um excerto do último indica claramente à vontade em abarcar o espaço cibersecuritário por parte da NATO:

> "Desenvolveremos ainda mais a nossa capacidade de prevenir, detetar, defender e recuperar de ciberataques, através do processo de planeamento da NATO para melhorar e coordenar as capacidades nacionais de defesa cibernética, colocando todos os organismos da NATO sob proteção cibernética centralizada e integrando melhor a consciência cibernética da NATO, de alerta e resposta, com as nações membros". (Conselho do Atlântico Norte, 2010: 16-17)[4]

[3] Texto original: "The EU will increase its focus on cyber security, equipping the EU and assisting Member States in protecting themselves against cyber threats while maintaining an open, free and safe cyberspace" (Conselho da União Europeia, 2016a: 21-22) (tradução do autor).

[4] Texto original: "Develop further our ability to prevent, detect, defend against and recover from cyberattacks, including by using the NATO planning process to enhance and coordinate national cyber-defence capabilities, bringing all NATO bodies under centralized cyber protection, and better integrating NATO cyber awareness, warning and response with member nations" (Conselho do Atlântico Norte, 2010: 16-17) (tradução do autor).

O surgimento e a evolução da cibersegurança continua a ser atualmente um assunto pouco abordado entre os académicos de Relações Internacionais. Em muito devido ao facto de o cibercrime ser tido como uma área pouco perigosa ou relevante (no sentido literal da palavra), algo defendido pelo Professor Doutor Henrique Santos quando afirma "que a segurança - no geral - não tem grande importância para os Estados ou para as Organizações Internacionais e isso reflete-se nos apoios financeiros disponibilizados para estes campos" (Santos, 2018). O Professor Doutor Henrique Santos argumenta mesmo que "nenhuma universidade está a assumir a cibersegurança como uma área de aplicação que mereça atenção do ponto de vista pedagógico e científico. Um projeto com uma base investigativa em cibersegurança tem uma probabilidade mínima de ser aprovado ainda que seja um projeto inovador e muito interessante do ponto de vista acadêmico. Falta consciencialização da importância da área nas pessoas, nos Estados e nas Organizações Internacionais". (Santos, 2018)

O pouco interesse nutrido pela área torna-a uma corrente esquecida e pouco delineada, razão pela qual esta dissertação fará uma retrospetiva da cibersegurança no âmago dos atores em análise, no que a segurança cibersecuritária diz respeito, para que percebamos que está esfera não surgiu só agora.

Todo este alienamento social, investigativo e académico relativamente a área[5] – em muito devido a ideia de que o cibercrime não é tão perigoso como os crimes tradicionais, conceito este indesejável e pouco racional, entenderemos o porquê em detalhe ao longo desta dissertação - denota uma necessidade urgente de aprofundamento investigativo e exploratório não só pela sua futura relevância, mas também para desmitificar várias das ideias fixas associadas à utilidade do seu estudo. No âmbito desta inquietação existiu então uma necessidade exploratória de todos os contornos que rodeiam a cibersegurança no seio das agendas da UE e da NATO, nunca descolando daquilo que é o propósito que rodeia esta investigação: a luta de ambos os atores contra a cibercriminalidade.

Os ciberataques escolhidos para figurarem o rol de protagonistas ao longo da dissertação de Mestrado foram selecionados devido a sua relevância e mediatismo, muitos outros poderiam ser integrados neste seleto grupo mas mais uma vez a limitação espacial e temporal não permitiram que esta investigação partisse para lá do que foi decidido abordar.

[5] De salientar também que a pouca importância dada a área da cibersegurança e ciberdefesa tornou está investigação exploratória ainda mais difícil. Sendo está uma investigação teórica que requere material científico factual, a impossibilidade de encontrar uma grande variedade de material traz algumas desvantagens no seio desta dissertação.

No que diz respeito à pesquisa envolvida nesta dissertação, esta ficará circunscrita ao nível político-diplomático e estratégico de ambos os atores em análise. Os níveis técnicos e práticos do ciberespaço - quer sejam relativos à programação e ao software (como por exemplo a questão da instrução em código que permite o controlo de um computador), quer sejam relativos à componente militar - não serão tidos em consideração para efeitos de exploração dissertativa. Serão tidas em conta opiniões, decretos oficiais, argumentos e noticias que digam respeito a abordagem investigativa - a exploração cibersecuritária dos atores em exploração - sem nunca descurar a fundamentação factual do que se argumenta.

Revisão Bibliográfica

Nos dias que correm estar constantemente online não é só mais um requisito fundamental, é algo necessário à nossa sobrevivência seja ela profissional ou pessoal, isto porque tudo aquilo que consideramos indispensável no nosso dia a dia é agora ligado em rede.

> "Contamos com a internet para tudo, desde a comunicação até as compras, do armazenamento de documentos até as transações e a educação. A internet tornou-se tão enraizada nas nossas vidas que está a alterar a maneira como o nosso cérebro funciona". (Rear, 2017)[6]

A internet tornou-se de tal maneira indispensável nas nossas vidas que o seu fim teria de ser encarado com um processo de reabilitação longo, demorado e possivelmente para sempre marcante. Já para não falar no consequente retrocesso económico, científico e geracional que este fim traria. Podemos então assumir que o fim da internet teria de ser encarado como algo trágico. Deste ponto de vista medidas tinham, e têm, que ser tomadas para que todos os cidadãos encontrem no ciberespaço - anárquico por natureza – alguma ordem e controlo, para que o seu fim não tenha que ser encarado ou refletido.

As vulnerabilidades do ciberespaço são mais que muitas e testam os limites das leis existentes (Tikk, 2011: 120) ainda mais se tivermos em consideração que a internet é hoje em dia "uma plataforma poderosa, barata, global e muitas vezes anônima e de difícil controlo", mas por outro lado "fácil de

[6] Texto original: "We rely on the internet for everything from communication to shopping to storing documents to transactions to education. The internet has become so ingrained in our lives that it is altering the way our brains work" (Rear, 2017) (tradução do autor).

explorar" isto "devido ao surgimento de cada vez mais infraestruturas críticas e serviços essenciais conectados online e através de plataformas de internet" (Saul e Heath, 2014: 1)[7].

Ao longo dos anos mais recentes, mais propriamente na entrada no século XXI, a UE e a NATO deram-se então conta que o ambiente de segurança de ambos iria precisar de abranger um espaço de ação diferente daquele que até então exploravam - o ciberespaço – isto para que o espaço soberano dos seus Estados-membros e o individuo na sua singularidade, não temessem o uso da internet (Estratégia Europeia de Ciberdefesa, 2013 apud Site Oficial da Agência Europeia de Defesa, 2017; Conselho do Atlântico Norte, 2016b). Algo que muitos autores argumentam só ser possível através de uma cooperação estreita no combate a cibercriminalidade visto ser este um problema transnacional com uma necessidade imediata de resolução global (Moslemzadeh et al, 2013: 207; Leite, 2016: 13).

Tendo isto em conta a cooperação com terceiros - como por exemplo os Estados Unidos através das agências de inteligência dos atores envolvidos nesta dissertação - (Segell, 2004: 81; Aldrich, 2009: 123) e a cooperação mútua a título transnacional e mundial entre a UE e a NATO (Ilves et al, 2016; Bodin et al, 2015) - exposto em várias das cimeiras realizadas ao longo do século XXI por ambas as Organizações Internacionais e parte do foco desta investigação – passaram a ser uma realidade assumida - ainda que parca em resultados práticos e desorganizada no que a liderança diz respeito.

Mas nem tudo são momentos de cooperação e de diálogo no seio da UE e da NATO. O *Brexit* e Donald Trump ameaçam abalar as estruturas de ambas as organizações em análise criando dinâmicas diferentes daquelas com que ambos os atores estavam e estão habituados a lidar (Svendsen, 2017: 111). O futuro é incerto e a capacidade de adaptação de ambos os atores será fundamental para um ciberespaço estável, controlado e seguro (Barrinha, 2018; Santos, 2018).

A cooperação está muito presente nas diversas cimeiras e declarações realizadas e prestadas por ambos os atores ao longo dos anos: cimeira de Bucareste em 2008 (Conselho do Atlântico Norte, 2008), cimeira de Chicago em 2012 (Conselho do Atlântico Norte, 2012), declaração conjunta da UE e da NATO em dezembro de 2002 no âmbito da PESD (Conselho do Atlântico Norte, 2002a) e declaração conjunta assinada pelo Presidente do Conselho Europeu, pelo Presidente da Comissão Europeia e pelo Secretário-Geral da Organização o Tratado Norte (Conselho do Atlântico Norte, 2016c), bem como em

[7] Texto original: "The Internet is a powerful, cheap, global, and often anonymous platform that is difficult to control but easy to exploit. As more critical infrastructure systems are moved online, and more essential services are delivered via an Internet platform, security vulnerabilities commensurably increase" (Saul e Heath, 2014: 1) (tradução do autor).

noticias associadas, e que nos permite assim fundamentar a escolha destes dois atores e não outros como é por exemplo o caso da OSCE.

> "O secretário-geral da Organização do Tratado do Atlântico Norte (NATO) anunciou um acordo com a União Europeia (UE) no combate ao cibercrime e outras ameaças híbridas, após a receção aos 28 ministros da Defesa da Aliança Atlântica". (Negócios, 2016)

Apesar de já existirem investigações que explanam a problemática da segurança no ciberespaço – como é o caso da tese doutoral de Tine Højsgaard Munk (2015) ou o artigo científico de Ana Ferreira Leite (2016) bem como os diversos artigos do Professor Doutor André Barrinha (2017 e 2018) - não existe uma que elucide esta problemática no seio da UE e da NATO através de uma perspetiva comparada e evolutiva. Está análise comparativa vem no seguimento da estreita cooperação entre ambos os atores no campo da cibersegurança, e na segurança no geral.

Um exemplo específico de um estudo que explora os princípios da cibersegurança e da ciberinsegurança é a tese doutoral de Tine Højsgaard Munk sob a designação de "Cyber-security in the European Region: Anticipatory Governance and Practices" produzida em 2015 sob a ótica metodológica qualitativa empossada pelo Construtivismo (Munk, 2015). A investigação de Tine Højsgaard Munk, foca-se predominantemente nas ameaças do ciberterrorismo e dos ciberataques no seio da UE, e naquilo que são as dinâmicas de direito internacional, na área da cibersegurança bem como as falhas a si associadas. A exploração este autor foca-se exclusivamente nos perigos cibernéticos da UE numa visão particular e singular sem o intuito comparativo e evolutivo que veremos ao longo desta dissertação.

Dentro desta vertente de sentido único, surge também o Professor Doutor André Barrinha com diversos trabalhos investigativos na área da cibersegurança no seio da União Europeia – "The EU as a Coherent (Cyber)Security Actor?" (Barrinha, 2017), "European Union cyber security as an emerging research and policy field, European Politics and Society" (Barinha, 2018) e "How coherent is EU cybersecurity policy?" (Barrinha, 2018). Investigações estas muito críticas daquilo que é a aplicação da cibersegurança por parte deste ator.

Ana Ferreira Leite, através do artigo científico "A Problemática da Cibersegurança e os seus Desafios" publicada em 2016, aborda também ela os perigos do ciberespaço, com um enfoque particular

nos ciberataques, no ciberterrorismo, na ciberguerra e na ciberespionagem[8], lançando também várias bases para uma cooperação internacional mais eficaz e prospera no âmbito da cibersegurança (Leite, 2016). Esta autora tem uma abordagem mais focada nos perigos cibernéticos no seio da NATO bem como a resposta aos cibercrimes (Leite, 2016) nunca se distanciando, no entanto, daquilo que é a cibersegurança no seio da UE, mas sem qualquer intuito de comparar, criticar, expor ou analisar a evolução da cibersegurança no seio dos atores que agora se passarão a analisar. Também Joe Burton, através do artigo científico "NATO's Cyber Defence: Strategic Challenges and Institutional Adaptation" (Burton, 2015), explora a capacidade adaptativa da NATO a este novo mundo, o mundo virtual.

Todos os autores referenciados anteriormente fazem análises detalhadas dos perigos relativos a cibersegurança, mas sem o foco evolutivo e cronológico que o presente autor passará a expor. Cada um deles aborda, explora, sintetiza e responde as problemáticas do seu projeto investigativo, mas mantendo-se sempre dentro do campo de um ator em particular (ainda que expondo o outro de quando em vez). Barreira esta que o autor pretende transpor comparando e analisando a evolução da cibersegurança no seio da UE e da NATO.

A presente dissertação será enquadrada no Neoliberalismo Institucional e empossada pela Teoria dos Regimes que não foi ainda aplicada ao tema escolhido. As problemáticas e as dinâmicas que se seguem nos próximos capítulos tentarão ter um carácter inovador, devido a sua característica contemporânea fruto da mutabilidade do ciberespaço. O tema escolhido para análise é por si só um fator de originalidade na sua essência, tendo sido muito pouco abordado ou explorado em qualquer área académica.

Problemática em Perspetiva

O medo da prisão, ou mesmo da morte, geralmente faz com que os chamados criminosos tradicionais assumam uma posição mais defensiva e protecionista na hora de realizar uma qualquer atividade ilegal no chamado ´mundo real´ (não querendo dizer com isto que não praticam crimes ou que se deixam influenciar por estas preocupações). Dentro do ciberespaço, no chamado mundo em rede, estes sentimentos normalmente não existem (ou pelo menos são omissos), pois entre os cibercriminosos

[8] Definição para o ato espionagem no ciberespaço.

existe a ideia de que este espaço é uma zona alienada do mundo real em que vivemos, existindo mesmo a ilusão que este não entra, nem nunca entrará, em conflito com o seu quotidiano.

> "Não há qualquer dúvida que nos dias que correm o cibercrime é um desafio quer para os legisladores quer para os investigadores. A vantagem do anonimato em conjunto com o caráter transitório e global das comunicações online dificulta grandemente a tarefa de combatê-lo ou preveni-lo". (Maciel, 2016)

A pergunta de investigação da presente dissertação é a seguinte: como tem vindo a evoluir ao longo do tempo o papel da UE e da NATO na luta contra o cibercrime e quais os aspetos em comum e as diferenças de abordagem na luta contra está ameaça?

O objetivo desta dissertação passa então por percebermos como a UE e a NATO chamaram a si a responsabilidade de proteger este espaço. Examinando aquilo que são os dados primários disponibilizados por ambos os atores em análise, as ideias e afirmações de autores consagrados na área (como vimos no subcapítulo anterior) bem como as entrevistas efetuadas a especialistas que têm investigado nestas áreas – como são os casos do Professor Doutor André Barrinha e do Professor Doutor Henrique Santos - iremos abordar à pergunta de investigação, bem como perceber como as respostas as perguntas secundárias influenciam esta questão central.

Dentro da pergunta de investigação iremos analisar, compreender e expor cronologicamente os aspetos mais relevantes e significativos respeitantes à cibersegurança no seio dos atores em análise, bem como tentar compreender as divergências e as convergências dentro desta investigação. Tudo isto explorando sempre o pressuposto de uma relação de influência da NATO para com a União Europeia.

Dentro desta questão nuclear contaremos com diversas perguntas secundárias que terão a função de suportar a primeira. Sendo estas as seguintes:

O que existe de concreto nas agendas securitárias da UE e da NATO relativamente a cibersegurança? Esta pergunta será replicada ao longo de todo o terceiro capítulo através de dois estudos de caso: a UE e da NATO. Sendo examinada através de protocolos, agendas, declarações, cimeiras, agências, e onde se procurará identificar o que existe de concreto na agenda securitária de ambos os atores no que a cibersegurança diz respeito.

Qual o papel da UE e da NATO na cibersegurança a nível mundial? Procura-se desta maneira perceber como ambos os atores estão integrados no mundo cibersecuritário e se são ou não capazes de responder a tal empreendimento.

São a UE e a NATO capazes de cooperar eficazmente neste espaço? Quando assistimos as diversas declarações e aos diversos acordos assinados entre ambos os atores percebemos que a cooperação é inerente aos dois e isso é inegável. A problemática desta cooperação é se é eficaz e se é capaz de ser eficaz neste espaço libertário.

É a regimentação[9] do ciberespaço uma solução mais eficaz que o Neoliberalismo Institucional? A conceção assumida por parte da sociedade que tudo atualmente goza e tem que gozar de uma profunda liberdade de movimentos e de expressão tornou o ciberespaço um dos locais mais perigosos do mundo. A questão central será perceber se a melhor solução para o problema é a regimentação deste espaço.

A luta contra o cibercrime continua e continuará a fazer parte de ambos os atores em análise, bem como a criminalidade neste espaço, resta saber se deixaremos o mal triunfar em função da ideologia liberal presente em nós. Esta não é mais uma área de ficção científica saída de um livro consagrado ou de um sucesso de bilheteiras de cinema, é um problema real e atual para todos e cada um de nós, sendo que o momento para lidar com esta problemática é aqui e agora. Isto porque a evolução tecnológica e a evolução ciberespaço tornará ainda mais difícil a contenção das ameaças resultantes do cibercrime.

Quadro Teórico

Desde a Sociedade das Nações[10] que a vontade de criar uma comunidade internacional responsável pela aplicação de uma Lei Internacional comum a todos era algo desejado pelos Estados. David Kennedy defende mesmo que existia já naquela altura uma reação natural que catalisou o aparecimento das Organizações Internacionais isto porque "a desorganização do mundo (sobretudo devido a destruição humana e material da I Guerra Mundial) justificava estas como uma necessidade na expetativa de ser criada uma era institucionalizada deixando de lado a era pré-institucionalizada"

[9] No sentido de controlar, reger, ter controlo sobre. Uma alusão a Teoria dos Regimes e a necessidade de controlo do ciberespaço através das 'amarras' de uma verdadeira regência.

[10] Encyclopædia Britannica - League of Nations: A primeira "organização de cooperação internacional estabelecida a 10 de janeiro de 1920, por iniciativa das potências aliadas vitoriosas no final da Primeira Guerra Mundial". Foi criada devido a "a demanda pública de que algum método fosse encontrado para impedir a continuação do sofrimento e da destruição que eram vistas como uma parte inseparável da guerra moderna" (Encyclopædia Britannica). Disponível na internet em: https://www.britannica.com/topic/League-of-Nations

(Kennedy, 1987: 845)[11]. Este não era ainda o nascimento daquilo a que hoje chamamos Neoliberalismo Institucional, mas era o começo promissor do pai deste: o Liberalismo.

Mas como a história revela apesar de toda a vontade pacifista dos Estados e da crescente ideia institucional, a II Guerra Mundial acabou mesmo por acontecer - independentemente de todos os esforços feitos em sentido contrário para que uma guerra mundial não tomasse conta do mundo de novo e só no final desta, "com a explosão do fenómeno das OI", é que se "proporcionou o desenvolvimento desta área de investigação - o estudo aprofundado sobre as potencialidades das Organizações Internacionais" (Pinto, 2007: 86).

Ainda assim segundo Maria do Céu Pinto "as OI não nascem vinculadas às questões da guerra e da paz, mas à Revolução Industrial e às suas consequências, requerendo dos Estados a cooperação para a administração conjunta de bens comuns" (Pinto, 2007: 85-86) - como é o caso da cibersegurança nesta investigação, visto tratar-se esta de uma preocupação transnacional.

A partir da Segunda Guerra Mundial "os liberais começaram a propor teorias de integração internacional à medida que a integração europeia prosseguia desde a década de 1950. Eles propuseram várias teorias, hipóteses e cenários de como restringir a soberania nacional promovendo integração do Estados-nação" (Oshiba, 2009: 261)[12].

O final da Guerra-Fria e a globalização no geral – o livre comércio (cada vez mais em ascensão nos anos noventa), a evolução tecnológica e como não poderia deixar de ser as renovadas relações internacionais (naquilo que se passou a chamar a diplomacia internacional) – foram catalisadores importantes do Neoliberalismo Institucional, que em conjugação com a paz necessária e prometida pelos Estados, e ansiada pelo mundo no geral, fizeram desta corrente filosófica a mais influente nos finais do século XX e inícios do século XXI (para um melhor entendimento destas correntes filosóficas ver anexo I).

A possibilidade do compartilhamento de conhecimentos e de forças no combate a um inimigo comum fez também com que a área da cibersegurança e da ciberdefesa passasse não só a ser real,

[11] Texto original: "(...) international institutions were necessary and desirable reactions to a disorganized world, distinguishing a preinstitutional from an institutionalized international order" (Kennedy, 1987: 845) (tradução do autor).

[12] Texto original: "Liberals proposed theories of international integration as European integration went on since the 1950s. They proposed several theoretical hypotheses and scenarios of how to restrict national sovereignty by promoting integration of nation-states" (Oshiba, 2009: 261) (tradução do autor).

mas também evoluísse com o tempo (isto porque este é um campo com uma grande prospeção transnacional onde os Estados necessitam obrigatoriamente de trabalhar em conjunto).

A perda de poder central do Estado - que com o final do comunismo da União Soviética fez ainda mais dissipar as qualidades deste como líder e sentenciador inquestionável - fez com que as Organizações Internacionais ganhassem novo fôlego na tomada de decisão a nível mundial (Freire, 2012) os Estados passaram a olhar para estas literalmente como as possíveis 'salvadoras da pátria' - visto serem as OI as principais impulsionadoras da cooperação e do bem-estar entre os povos.

Ainda assim "o Estado manteve-se na categoria de ator principal na arena internacional sem deixar para segundo plano a sua descentralização e a emergência dos novos atores" (Camargo e Junqueira, 2013: 21) tendo como principais propagadoras dos princípios neoliberais no mundo a "Margareth Thatcher (a dama de ferro)[13] na Inglaterra e Ronald Reagan[14] nos Estados Unidos" (Freire, 2012).

Tudo isto pressupõe desde logo o Neoliberalismo Institucional como enquadramento teórico e a escola da Teoria dos Regimes como possível vertente a explorar, isto porque, a cooperação e o palco transnacional serão base onde assentará a dissertação de Mestrado e consequentemente os dois estudos de caso – com normas, regras e leis comuns aos intervenientes que compõem os Estados membros de ambas as Organizações Internacionais (Robert Keohane, 1989).

Os defensores do Neoliberalismo Institucional defendem, entre outras as seguintes dinâmicas: "total liberdade relativamente às leis do mercado, limitação da intervenção do Estado na economia, privatização das empresas estatais, melhor adequação às políticas internacionais de comércio, liberdade dos capitais internacionais e a diminuição ou eliminação da proteção ou incentivos às empresas nacionais" (Freire, 2012) desde logo se percebe que o Estado, aos olhos destes teóricos, tem que ter a mínima intervenção em tudo aquilo que são as novas características da globalização. A verdade é que para muitos teóricos está utopia não é perfeita:

[13] Primeira Ministra do Reino Unido entre 1979 e 1990. A governação de Margareth Thatcher valeu a definição de Tchaterismo as suas políticas. "O thatcherismo representava uma crença desta conservadora nos mercados livres e na ideia de pequeno estado. Em vez deste planear e regular os negócios e a vida das pessoas, o trabalho do governo era sair do caminho – valores familiares acima de tudo" (BBC, 2013).

[14] 40º Presidente Norte-Americano entre 1981 e 1989. O foco das políticas de Reagan era idêntico ao de Thatcher: sincronização com o capitalismo e a defesa da democracia liberal.

> "Para Jervis os neoliberais institucionalistas olham para a política mundial como sendo mais cooperativa do que na realidade acontece (...) os neoliberais mesmo não negando os profundos conflitos existentes no palco internacional, acham que estes conflitos não são representativos daquilo que é a política mundial (...) acabando por acreditar sempre que os Estados são capazes de trabalhar juntos mitigando os efeitos nocivos da anarquia e produzindo dessa maneira ganhos mútuos, evitando riscos". (Jervis, 1999 apud Regis, 2007: 56)

Segundo Iro pode dar-se mesmo o caso de "cessarem cooperar devido à falta de informação no que a colaboração diz respeito, sendo que dessa maneira às verdadeiras intenções dos parceiros no âmbito deste entrosamento de ideias não é algo claro (visto que através disto podem ser explorados ou induzidos em erro)". Também os "custos e os riscos associados - quando desconhecidos ou excedem os benefícios da parceria - podem tornar-se um problema" (Iro, 2015)[15]. Tendo em conta todas estas dinâmicas que podem interferir no entrosamento cooperativo entre atores, alguns defensores do Neoliberalismo Institucional acabam mesmo por concluir que "a cooperação entre os Estados pode ser difícil de alcançar quando os ganhos são desproporcionais" (Iro, 2015)[16].

A cooperação no combate a um inimigo comum – e no caso particular desta exploração dissertativa: o cibercrime – tem tudo para ser algo exequível e atingível, mas na prática ainda não é bem assim: "Os Estados não estão ainda dispostos a cooperar intensamente; é por isso que ainda não existe uma Lei Internacional de cibersegurança ou ciberdefesa. Existe apenas uma convenção do Conselho da Europa de 2001, especificamente relacionada com a luta contra a pornografia infantil" (Arpagian, 2015 apud Euronews, 2015)[17].

Sendo a UE assumidamente responsável pelo bem-estar e pela proteção dos Estados-membros o facto de estes atores serem ainda os responsáveis pela sua própria segurança, é uma falha basilar da política de cooperação da UE.

---

[15] Texto original: "States may fail to cooperate due to lack of information and true intentions of partners or when one might take advantage or cheat. Other factors that hinder cooperation include where the costs, or associated risks are unknown or outweigh benefits of partnership" (Iro, 2015) (tradução do autor).

[16] Texto original: "Neoliberalism argues that state cooperation can be difficult to achieve where the gains are disproportionate (Iro, 2015) (tradução do autor).

[17] Texto Original: "States are still unwilling to co-operate intensively enough; that's why we don't yet have an international cybersecurity or cyberdefence law. There is only a 2001 Council of Europe convention linked specifically to the fight against child pornography" (Arpagian, 2015 apud Euronews, 2015) (tradução do autor).

> "(...) continua a existir uma falta de coesão na política de segurança cibernética da UE onde as principais responsabilidades inerentes a segurança cibernética, continuam a permanecer a cargo dos Estados-membros". (Barrinha e Farrand-Carrapico, 2018)[18]

A NATO não é também ela alheia a este problema nas dinâmicas cooperativas, mas numa matriz diferente. A cooperação é ainda vista para esta como um desafio e não como algo completamente positivo ou alcançável.

> "Embora a NATO tenha trabalhado para uma política de segurança cibernética mais abrangente, há dois grandes desafios na sua estratégia atual. O plano atual coloca os ciberataques no âmbito do artigo 5° do Tratado do Atlântico Norte e a existência de um conceito de defesa coletiva – gerando consequentemente a cooperação. Além disso, permite medidas principalmente defensivas e reativas deixando menos espaço para operações preventivas ou ofensivas". (Roggeveen, 2017 apud Conselho do Atlântico Norte, 2017)[19]

Tudo isto remete para um tipo de resolução diferente daquela que é utilizada atualmente. As falhas cooperativas de ambos os atores em estudo, mas também as problemáticas de significância do próprio enquadramento teórico (o Neoliberalismo pressupõe a liberdade de ação seja para os Estados e organizações, seja para os cidadãos e grupos de indivíduos) - a restrição da liberdade de uma parte para com a outra é ir contra o próprio propósito do enquadramento teórico que decidimos abordar.

Se pensarmos que "alcançar a cooperação na política mundial é difícil visto que não há um governo comum para fazer cumprir as regras" e se "tivermos em conta que os padrões da sociedade interna ditam que as instituições internacionais são fracas" (Axelrod e Keohane, 1985: 226)[20], a escolha

[18] Texto original: "there remains a lack of cohesion in EU cybersecurity policy, with the main responsibilities in cybersecurity governance remaining with the member states" (Barrinha e Farrand-Carrapico, 2018) (tradução do autor).

[19] Texto original: "Although NATO has been working toward a more comprehensive cybersecurity policy, there are two major challenges with its current strategy. The current plan places cyberattacks within the scope of Article 5 of the North Atlantic Treaty and the concept of collective defence, thus, creating high thresholds for engagement. In addition, it allows for mainly defensive and reactive measures, leaving less room for preventive or offensive operations" (Roggeveen, 2017 apud Conselho do Atlântico Norte, 2017) (tradução do autor).

[20] Texto original: "ACHIEVING cooperation is difficult in world politics. There is no common government to enforce rules, and by the standards of domestic society, international institutions are weak" (Axelrod e Keohane, 1985: 226) (tradução do autor).

de uma escola como a Teoria dos Regimes tornou-se necessária para circundar a exploração com a devida propriedade.

Dentro do Neoliberalismo Institucional, a abordagem que mais se enquadra nesta exploração dissertativa, é a Teoria dos Regimes, isto porque "os Estados (ou outros atores políticos) existem dentro de um ambiente anárquico[21] e agem dentro deste de forma bastante racional[22] e calculada no que toca a tomada de decisões" (Moravcsik, 2010: 2)[23] necessitando da influência e do *know-how*[24] das OI.

Estes Regimes internacionais são primeiramente desejados por três razões em especifico: em primeiro lugar porque evitam que as negociações internacionais de qualquer tipo sejam debilitadas, em segundo lugar porque permitem controlar o comportamento de outros Estados através de um sistema de regras previamente acordados e por último e em terceiro lugar porque permitem evitar a despesa de contactos bilaterais múltiplos e providenciam informações relevantes sobre o Estado do mercado e as respetivas ações interventivas. (Aggarwal, 1985: 4)[25].

Para Krasner, pioneiramente em 1983, os jogos de bastidores das OI tinham em consideração um "conjunto de princípios, normas, regras e procedimentos, implícitos ou explícitos, focados na tomada de decisão e em torno dos quais as expectativas dos atores convergiam numa determinada área das relações internacionais" (Krasner, 1983: 2)[26].

---

[21] "A suposição da anarquia significa que os atores políticos existem dentro de um ambiente distintivo da política internacional (..) onde a autoajuda passa a ser a melhor opção" (Moravcsik, 2010: 2) (tradução do autor) = Texto original: "The anarchy assumption means that political actors exist in the distinctive environment of international politics, without a world government or any other authority with a monopoly on the legitimate use of force" (Moravcsik, 2010: 2).

[22] "Dentro da dinâmica racional os Estados passam a envolver-se na política externa com o propósito de garantir benefícios proporcionados por atores fora das suas fronteiras (acordos na exportação) almejando sempre aquilo que lhes interessa mais individualmente em termos de custo-benefício" (Moravcsik, 2010: 2) (tradução do autor) = Texto original: "The rationality assumption means that state leaders and their domestic supporters engage in foreign policy for the instrumental purpose of securing benefits provided by (or avoiding costs imposed by) actors outside of their borders, and in making such calculations, states seek to deploy the most cost-effective means to achieve whatever their ends (preferences) may be" (Moravcsik, 2010: 2).

[23] Texto original: "(...) states (or other political actors) exist in an anarchic environment and they generally act in a broadly rational way in making decisions" (Moravcsik, 2010: 2) (tradução do autor).

[24] Conhecimento prático e domínio relativamente a uma série de informações privilegiadas.

[25] Texto original: "Briefly, I argue that international regimes are desired by actors for three reasons. First, they may prevent broader international arrangements from being undermined, a constraint I label "nesting". Second, regimes provide a way to control the behavior of other countries through a system of rules. Third, regimes minimize the organizational costs of conducting multiple negotiations and provide participants with information about the market and interventionist actions (Aggarwal, 1985: 4) (tradução do autor).

[26] Texto original: "Regimes can be defined as sets of implicit or explicit principles, norms, rules and decision-making procedures around which actors expectations converge in a given area of international relations" (Krasner, 1983: 2) (tradução do autor).

Vemos então que estas normas, regras, princípios e procedimentos no seio das instituições internacionais são ainda atualmente "marcadas pela ausência de uma ordem política hierárquica e mecanismos de implementação de sanções" (Herz, 1997). Isto porque, e tendo em conta a UE e a NATO, num conjunto de Estados-membros, onde cada um vale o mesmo independentemente do seu poder, seja ele económico ou territorial, não existe um líder ou um Estado que domine (o que normalmente faz com que existam retificações e atrasos na tomada de decisão (Santos, 2018) e onde é necessário uma atenção e um esforço redobrado).

Esta cooperação multilateral entre os regimes é então baseada, e como Young esclarece, em torno de uma forma de negociação onde todos têm um poder de decisão igual a dos restantes Estados-membros (Young, 1982: 277-297) isto porque existem "padrões reconhecidos de práticas em torno das quais há uma convergência de expectativas o que pode ou não ser acompanhado por arranjos organizacionais explícitos" (Young, 1980: 332-333)[27]. A confiança e a transparência afetas a estes atores é então baseada na sua completa legitimidade para atuar para lá do espectro dos Estados (mas tendo sempre em conta estes como seus integrantes), fornecendo ferramentas díspares aos seus afiliados:

> "As OI podem funcionar como o culminar de um processo de definição e adoção de um dado regime. Noutros casos, as OI são o mecanismo através do qual os regimes são criados ou adaptados". (Pinto, 2007: 92)

Apesar de todas estas características de poder implícito, assumido pelas Organizações Internacionais, as leis, decisões e os pressupostos base assumidos por estas não têm o peso de leis ou de normas internacionais oficiais - como se estivéssemos a falar de um Estado – isto porque estas leis/decisões/acordos são vistos/as como *'soft laws'*[28] não tendo sido criadas para vingaram naturalmente sem o peso de normas oficiais implícitas[29]. Estas regras, e estando nós a falar de um

[27] Texto original: "Regimes are social institutions governing the actions of those interested in specifiable activities (or meaningful sets of activities). As such, they are recognized patterns of practice around which expectations converge (...) like other structures, regimes may be more or less formally articulated, and they may or may not be accompanied by explicit organizational arrangements (Young, 1980: 332-333) (tradução do autor).

[28] Dicionário jurídico - Soft Law: "Expressão utilizada no âmbito do Direito Internacional Público que designa o texto internacional, sob diversas denominações, que são desprovidos de caráter jurídico em relação aos signatários. São, portanto, facultativas, ao contrário do que ocorre com o *jus cogens* (normas imperativas). São também conhecidas como leis *droit doux* (direito flexível) ou mesmo *soft norms*". Disponível na Internet em: https://www.direitonet.com.br/dicionario/exibir/1042/Soft-law

[29] O principal motivo pelo qual muitas vezes os protocolos, regulamentos, estratégias, et al não são acatados ou respeitados pelos Estados Membros. Existe uma necessidade real de se tornar estas *soft laws* em leis reais e objetivas.

conjunto de Estados, são muitas vezes definidas pelos governos de cada país – tendo em conta setores específicos - e posteriormente, acatadas por estas organizações (Keohane, 1989) no seio da cooperação multilateral que é o pilar destes atores.

Tendo em conta estes princípios, e explorando a Teoria dos Regimes nas Organizações Internacionais, vemos que estes atores "têm um importante papel a desempenhar (se assim lhes for permitido) no que diz respeito à criação e implementação de regimes internacionais devido à legitimidade que é necessária para a credibilização de um regime, à transparência exigida no comportamento dos participantes e ao elevado custo decorrente da violação desses mesmos regimes" (Pinto, 2007: 92-93). Percebemos então que estes atores internacionais além do respeito retido a nível internacional têm também a capacidade de fazer valer aquilo que são os seus ideais e aquilo que defendem (em muito devido a imagem de atores íntegros que foram passando ao longo dos anos).

Esta conceção subentendida de poder partilhado é a base que define as Organizações Internacionais na atualidade, isto porque, estas têm o poder 'não-oficial' de defender políticas, acordos ou mesmo de aplicar sanções num processo já por si só naturalizado e reconhecido pela comunidade internacional - mas ainda com muito caminho pela frente no que toca as vantagens da real aplicação do mesmo.

A capacidade de estes atores abarcarem esta desejada 'governança[30] subentendida' – fruto em grande parte da globalização e fazerem desta uma governança oficial com poderes legais será fundamental para um ciberespaço seguro e controlado.

> "Os regimes podem facilitar a cooperação fornecendo informações, reduzindo custos de transação, facilitando vínculos e alongando a sombra do futuro[31]". (Axelrod, 1984: 124 apud Brahm, 2005)[32]

Comprovando isto, Krasner em 1983, afirmou que as dinâmicas em torno das Organizações Internacionais eram, e são ainda atualmente, uma combinação natural "de princípios, normas, regras e procedimentos de tomada de decisão, implícitos ou explícitos, em torno dos quais as expectativas dos

[30] Governança: "Forma de governar baseada no equilíbrio entre o Estado, a sociedade civil e o mercado, ao nível local, nacional e internacional". Disponível na internet em: https://www.infopedia.pt/dicionarios/lingua-portuguesa/governança

[31] A continuação da cooperação futura entre atores através de punições ou incentivos.

[32] Texto original: "Regimes can facilitate cooperation by providing information, reducing transaction costs, facilitating linkages, and lengthening "the shadow of the future" (Axelrod, 1984: 124 apud Brahm, 2005) (tradução do autor).

atores convergem numa determinada área das relações internacionais" (Krasner, 1983: 2)[33] o que válida e torna ainda mais possível a escolha da Teoria dos Regimes como escola a aplicar neste enquadramento teórico[34] dentro do objetivo secundário desta investigação: encontrar factos para a regimentação do ciberespaço.

Metodologia de Investigação

A dissertação de Mestrado que agora se inicia será fortemente delineada por uma abordagem qualitativa. O método de pesquisa contará com dois estudos de caso e a análise de documentos primários e secundários (vf. Vromen, 2010: 258). E o método de desenvolvimento será fortemente delineado por um método de análise comparativo (Collier, 1993: 105).

Os dois estudos de caso – UE e NATO - que se irão realizar na presente dissertação, foram escolhidos em detrimento de outros estudos de caso, tal como por exemplo a OSCE, devido ao nível de cooperação nas áreas securitárias, seja entre ambos ou mesmo com outros atores, na área da cibersegurança. Um dos primeiros sinais desta cooperação é a declaração conjunta da EU e da NATO datada de dezembro de 2002 no âmbito da Política Europeia de Segurança e Defesa (PESD) (Conselho do Atlântico Norte, 2002a) (como foi falado anteriormente) sendo que daí para a frente foram inúmeras as cimeiras, declarações, relatórios e comunicados que exaltaram as boas relações entre ambas as Organizações Internacionais. A vantagem de utilizar duas Organizações Internacionais como a UE e a NATO é a possibilidade comparativa de dinâmicas convergentes no ramo da cibersegurança e ciberdefesa - isto em grande parte devido ao nível de influência da NATO para com a UE no campo securitário, bem como as características evolutivas similares deste espaço no seio destes atores.

A análise de documentos contará na sua base com fontes primárias fontes secundárias. De entre as fontes primárias encontram-se os conceitos estratégicos, tratados, discursos, declarações, relatórios, fichas informativas e comunicados de imprensa das respetivas Organizações Internacionais. Quanto as fontes secundárias serão utilizados artigos científicos, livros e capítulos de livros e webgrafia (na sua

[33] Texto original: "Regimes can be defined as sets of implicit or explicit principles, norms, rules and decision-making procedures around which actors expectations converge in a given area of international relations" (Krasner, 1983: 2) (tradução do autor).

[34] O uso do neorrealismo torna-se então de difícil, ou mesmo impossível, aplicação devido a sua centralização no Estado e não na cooperação entre Estados. Tendo em conta as dinâmicas globais e transnacionais da atualidade isto é ainda menos uma possibilidade.

maioria sites oficiais e de agências ligadas a ambos os atores em estudo bem como jornais online de destaque (nacionais e internacionais).

Por último foram também realizadas duas entrevistas ao Professor Doutor André Barrinha e ao Professor Doutor Henrique Santos. Estas focaram-se sobretudo no atual Estado securitário de ambas as organizações em estudo.

Se nos focarmos naquilo que é a ideia geral anárquica do ciberespaço e a ideologia liberal e democrática da UE e da NATO, compreenderemos a escolha do Neoliberalismo Institucional como quadro teórico a explorar nesta investigação. Isto porque "o Neoliberalismo Institucional levanta questões sobre os efeitos das instituições nas dinâmicas do Estado e quais as causas desta mudança institucional; isto pressupõe desde logo que os Estados sejam agentes importantes nestas dinâmicas, examinando as forças materiais da política mundial e o conhecimento de si mesmos que os seres humanos têm". (Keohane, 1989: 2)[35].

Quando olhamos para os princípios basilares tanto da UE como da NATO - os dois estudos de caso em exploração nesta dissertação de Mestrado - vemos que a cooperação e a responsabilização através da ideia 'um por todos e todos por um' define ambas as agendas destes mesmos atores (ainda que com dinâmicas diferentes i.e. (global e regional). Confirmando isto, e olhando para o site oficial da UE e da NATO, vemos que os princípios capitais de ambos os atores são a cooperação. Começando pela NATO, vemos que o seu princípio de suporte é "garantir a segurança dos seus Estados-membros através de meios políticos e militares" (Organização do Atlântico Norte Website Oficial[36]), enquanto os princípios fundamentais - mais do que valores - da UE são regidos pelos direitos humanos, a solidariedade, a integração, o respeito e acima de tudo a prevalência do direito comunitário (União Europeia Website Oficial[37]). Mas estes princípios nem sempre são aplicados como veremos ao longo desta investigação.

Estrutura da Dissertação

Sendo difícil dissociar quer a cibercriminalidade da criminalidade comum quer o ciberterrorismo do terrorismo clássico, a dissertação que agora se inicia realizará uma análise daquilo que é a

[35] Texto original: "Neoliberal institutionalism asks questions about the impact of institutions on state action and about the causes of institutional change; it assumes that states are key actors and examines both the material forces of world politics and the subjective self-understandings of human beings" (Keohane, 1989: 2) (tradução do autor).
[36] NATO: disponível na internet em: https://www.nato.int/nato-welcome/index.html
[37] União Europeia: disponível na internet em: https://europa.eu/european-union/about-eu/eu-in-brief_pt

cibercriminalidade/criminalidade informática como ameaça a combater por parte da UE e da NATO, quer a nível individual quer num quadro de cooperação interinstitucional. A inserção da cibersegurança na agenda estratégica de ambos os atores é parte de uma evolução que tem vindo a acontecer desde o início dos anos 90 tendo o seu apogeu na entrada do novo milénio com um maior investimento na ciberdefesa e na cibersegurança por parte de ambos os atores.

As bases desta dissertação, assim como o seu contributo, passam, em primeiro lugar, por percebermos o funcionamento do ciberespaço e a evolução do cibercrime, bem como a subsequente insegurança face a este espaço por parte das pessoas no seu quotidiano, divididas em 4 subcapítulos onde acompanharemos três períodos distintos cada um destes com a sua particularidade: o pós ataque terrorista as torres gémeas a 11 de setembro de 2001, o ciberataque a Estónia em abril de 2007 - um dos maiores marcos históricos no que ao cibercrime diz respeito - e a caminhada até ao presente (no caso concreto desta investigação julho de 2018).

O segundo capítulo realizará um enquadramento teórico e conceptual que circundará a problemática e a exploração investigativa. Será dividida num capítulo principal e numa subsecção onde figurarão respetivamente o Neoliberalismo Institucional – tendo em conta a segurança no pós-Guerra-Fria e as mudanças registadas nestes dois atores – e a escola da Teoria dos Regimes onde analisaremos os benefícios desta segunda em função da primeira.

Findo o segundo capítulo, e entrando no terceiro capítulo, analisaremos a cibersegurança no ambiente estratégico da UE e da NATO. Faremos um acompanhamento cronológico e detalhado de todas as dinâmicas cibersecuritárias que surgiram e foram surgindo no seio de ambos os atores.

Na primeira secção do quarto capítulo, faremos uma análise comparativa de todas as dinâmicas que conectam a UE e a NATO no ciberespaço. Já na segunda secção do quarto capítulo iremos aflorar recentes desenvolvimentos – como são os casos do processo de saída do Reino Unido da União Europeia e a Eleição de Donald Trump - onde iremos analisar os possíveis contratempos na área da cibersegurança e da ciberdefesa explorando estes exemplos específicos.

Através desta análise detalhada da luta contra o cibercrime por parte da UE e da NATO concluiremos que ambos os atores em análise contam com uma política pensada e detalhada relativamente aquilo que é a cibersegurança e a ciberdefesa. A verdade é que também perceberemos que esta não tem sido eficaz na sua plenitude e a missão colossal a qual a UE e a NATO escolheram responder tem-se tornado diariamente ainda mais monstruosa. Resta esperar e acreditar que o regulamento geral sobre a proteção de dados (RGPD) imposto pela UE durante o ano corrente de 2018

tenha sido um passo importante no que a implementação real das normas cibersecuritárias por parte dos Estados diz respeito.

1. A Emergência da Cibercriminalidade como Ameaça para a União Europeia e para a NATO

Sendo o mundo cibernético um dos espaços mais complexos do mundo algumas definições básicas terão de ser explicadas antes de começarmos este estudo no combate ao cibercrime por parte da UE e da NATO. Explorando com isto o ciberterrorismo e os ciberataques (também conhecidos como ataques cibernéticos), bem como o espaço onde estes se propagam o ciberespaço, em três momentos distintos: o pós-11 de setembro de 2001, o ciberataque ou ato de ciberterrorismo na Estónia em 2007 e o pós-ciberataque ou ato de ciberterrorismo na Estónia em 2007.

1.1 Ciberterrorismo, Ciberataques e Ciberespaço

O ciberespaço obteve um crescimento avassalador ao longo dos últimos anos e globalmente falando está presente no dia-a-dia de todos os cidadãos – algo que nos primórdios da existência da internet ninguém alguém poderia antever ou sonhar um dia acontecer (Choucri et al, 2014: 96). Isto deu asas a que todas as pessoas do mundo conseguissem executar a mais pequena tarefa de maneira mais eficiente e mais rápida, mas ao mesmo tempo também deixou todos e cada um de nós expostos a novos perigos e ameaças.

A UE e a NATO passaram a designar o ciberespaço como o ambiente circundante onde a informação e a comunicação são processadas e transmitidas (Site Oficial do CCDCOE, 2008-2018; Site Oficial da ENISA, 2004-2018). Tal como refere Leite, "pode-se então afirmar então que o ciberespaço é um espaço sem dimensões e um universo de informações navegável de forma instantânea e reversível, caracterizando-se sobretudo pela ubiquidade, pelo tempo real e pelo espaço não físico" (Leite, 2016: 4).

Este espaço virtual contém uma parte física que é composta por "várias camadas diferentes, quer políticas, quer económicas e quer mesmo judiciais" já a parte virtual conta "com práticas económicas crescentes que tornam o controlo judicial (por parte) de qualquer governo neste espaço

quase impossível" (Nye, 2014: 1)[38] E é precisamente destas dinâmicas que o ciberterrorismo se aproveita para criar o caos.

No dicionário da Porto Editora ciberterrorismo é descrito como uma "atividade terrorista praticada com computadores, com o objetivo de sabotar ou controlar sistemas informáticos" (Porto Editora, 2003-2018b) algo que no sentido literal da palavra constitui uma atividade criminosa e que tem como único intuito infligir dano a algo ou alguém.

Já a estratégia de segurança nacional dos Estados Unidos da América define o ciberterrorismo como "um ato criminoso perpetrado através de computadores que resulta em violência, morte/ou destruição e que gera o terror com o objetivo de coagir um governo a alterar as suas políticas" (NSSC, 2003 apub Paulo Nunes, 2004: 4) definição esta que não mudou muito ao longo dos anos como podemos comprovar no site oficial do centro de excelência da NATO:

> "Ciberterrorismo USA: O uso politicamente motivado de computadores e tecnologias de informação para causar perturbações severas ou medo generalizado na sociedade". (Estados Unidos da América apud Site Oficial do CCDCOE, 2008-2018)[39]

Relativamente aos perpetradores deste cibercrime, Paulo Santos, Ricardo Bessa e Carlos Pimentel argumentam que existe uma nova "guerra tecnológica" proporcionada pelos ciberterroristas com o objetivo de "paralisar, ganhar o controlo ou destruir sistemas de informação inimigos por meio de TI" (Santos et al, 2008: 85-86) algo também associado aos ciberataques.

Dentro da categoria de ciberterroristas cabem terroristas e simpatizantes de terroristas que utilizam ciberataques para fazer valer a sua causa e Estados que utilizem o mundo cibernético como arma (ciberguerra[40]) (Weimann, 2005: 141). De fora, e apesar de poderem causar danos tão graves

---

[38] Texto original: "Cyberspace is a unique combination of physical and virtual properties. The physical infrastructure layer largely follows the economic laws of rival resources and increasing marginal costs, and the political laws of sovereign governmental jurisdiction and control. The virtual or informational layers have economic network characteristics of increasing returns to scale, and political practices that make government jurisdictional control difficult (Nye, 2014: 1) (tradução do autor).

[39] Texto original: "The politically motivated use of computers and information technology to cause severe disruption or widespread fear in society" (Estados Unidos da América apud Site Oficial do CCDCOE, 2008-2018) (tradução do autor).

[40] A definição de ciberguerra é ainda nos dias de hoje dúbia na sua significância, isto sobretudo devido a sua inovação. Ainda assim a definição mais recorrente e convencional, segundo José Pedro Fernandes, é que esta é "uma guerra conduzida substancialmente no ciberespaço ou no domínio virtual" (Fernandes, 2012: 59). A "nova guerra" de hoje em dia – a ciberguerra - "pode processar-se de forma irregular e assimétrica, com a possibilidade de ser conduzida sem frentes, sem campanhas, sem bases, com escassos efetivos, sem lastro logístico significativo, sem pontos de apoio, não sendo confinada a limites territoriais e detendo objetivos fluidos de largo espectro estratégico" (Santos et al, 2008: 99-101).

como os acima mencionados, ficam os *hackers*[41] que procuram apenas a adrenalina da ilegalidade ou os potenciais ganhos através de ciberataques (Weimann, 2005: 141). A geração que cresce agora no mundo digital e em constante mutação começa a compreender que o *hacking*[42] é uma arma muito poderosa e os terroristas não são exceção a esta perceção (Weimann, 2005: 146).

Dentro do mundo dos cibercrimes existem também os ciberataques que, apesar de serem menos incapacitantes são, mais comuns e mais problemáticos devido à sua regularidade. Estes são designados pelo centro de excelência de Tallinn (CCDCOE) como um "ato ou ação iniciada no ciberespaço com o intuito de causar danos e comprometer a comunicação, a informação ou outros sistemas eletrônicos, ou as informações armazenadas, processadas e transmitidas por estes sistemas" (Conselho do Atlântico Norte, 2014)[43] afetando dessa maneira direta ou indiretamente "um sistema de comunicação e informação" e consequentemente comprometendo "a confidencialidade, a integridade e a disponibilidade do sistema e qualquer informação trocada ou armazenada por este" (Veenendaal e Brangetto, 2016: 117).

Durante o ano de 2017 a UE acabou também ela por explicitar aquilo que pensa sobre os ciberataques acabando por definir estes como um ato de guerra, propondo no seguimento destas declarações uma série de medidas que visam o combate a este crime (Conselho da União Europeia, 2017), tal como veremos com mais detalhe no 2º Capítulo: A luta contra a cibercriminalidade - Estudo de caso I - União Europeia. Isto coloca, desde logo, a premissa do ciberterrorismo no mesmo reduto do terrorismo clássico - o que pode levar a uma resposta idêntica por parte de Estados que sintam que foram vítimas de um 'atentado terrorista' que tenha posto em causa as suas infraestruturas críticas (IC)

[41] As definições de *hacker* variaram com o tempo não só nos termos que definem o fenómeno, mas também no que diz respeito a legalidade do mesmo. Os primeiros *hackers*, eram assim chamados devido ao nível profissionalização das suas áreas de investigação tecnológica – um sinal de reconhecimento (de maneira geral era aplicado aos investigadores/estudantes do MIT (Instituto de Tecnologia de Massachusetts), a segunda geração de *hackers* contribuí ativamente no desenvolvimento de computadores pessoais e de sistemas tecnológicos que acabaram por mudar para sempre as nossas vidas (p. ex. Steve Jobs - um inventor e empresário que ficou mundialmente conhecido por cocriar a companhia Apple inc. tendo falecido em outubro de 2011) a última geração, e a atual, trouxe o desprestigio e a ilicitude a este termo – esta diz respeito aos piratas e sabotadores informáticos, aos cibercriminosos, aos ciberterroristas, et al. Estes através de um computador com ligação a internet tentam obter lucros, roubar informações ou simplesmente disseminar o terror a nível global sem que para isso tenham que se deslocar do conforto da sua casa (Santos et al, 2008: 51-53).

[42] *Hacking/Hackear* - Utilização de técnicas de software (muitas vezes de maneira ilegal) para explorar as TI (Santos et al, 2008: 81).

[43] Texto original: "An act or action initiated in cyberspace to cause harm by compromising communication, information or other electronic systems, or the information that is stored, processed or transmitted in these systems" (Conselho do Atlântico Norte, 2014) (tradução do autor).

e a sua soberania - e os ciberataques comuns no mesmo reduto dos crimes tradicionais. Mas qual então a real diferença entre um ato de ciberterrorismo e um ciberataque?

1.2 Distinção entre Ciberterrorismo e Ciberataques no Pós-11 de Setembro de 2001

"(...) cada vez mais somos reféns da tecnologia e já não nos imaginamos sem ela. É isto que torna o ciberterrorismo e os ciberataques métodos tão perniciosos e poderosos. Estes podem fazer colapsar as infraestruturas de um Estado ou divulgar informações erróneas às massas (...) tratando-se está de uma ameaça silenciosa, invisível, que não se cinge apenas ao ciberespaço tendo, desta forma, efeitos na vida real"

(Leite, 2016: 17).

Tanto a UE como a NATO foram intrinsecamente transformadas pelo terrorismo transnacional que se fez notar com o 11 de setembro de 2001. Esta nova ameaça fez com que ambos os atores tivessem de adaptar os seus conceitos estratégicos de maneira a que estes abarcassem esta nova "radicalização" que entrava assim de rompante na vida de todos nós - isto tudo enquanto consolidavam a sua adaptação ao fim da bipolaridade da Guerra-Fria.

Juntando a esta dinâmica a globalização, a evolução tecnológica e a característica transnacional e sem fronteiras do ciberespaço, que se fez notar com mais força que nunca com a entrada no novo milénio, podemos então perceber o porquê de este espaço se ter tornado tão apetecível para os pioneiros na arte do cibercrime no geral.

Para os autores da época (e sendo ainda algo muito atual), a problemática da cibercriminalidade informática residia então na dicotomia de separação de definições no cibercrime - visto que nem todos os crimes informáticos são ciberterrorismo e nem só o aclamado 'puro ciberterrorismo' é a verdadeira ameaça no ciberespaço. O que nos transporta para a separação do ciberterrorismo dos comuns crimes informáticos (i.e. os ciberataques), que para alguns autores teria e deveria ser separada convenientemente devido as suas características díspares (Gordon e Ford, 2002: 13) mas que ao mesmo tempo era ainda muito complexa para tal abordagem como explicitam Gordon e Ford:

> "Se decidirmos perguntar a 10 pessoas o que é o ciberterrorismo receberemos pelo menos nove respostas diferentes. Quando estas 10 pessoas são especialistas em segurança informática, cuja tarefa é criar várias formas de proteção contra o ciberterrorismo (e os ciberataques), essa discrepância muda de anedótico para algo bastante preocupante". (Gordon e Ford, 2002: 3)[44]

Ainda antes do ataque ás torres gémeas a 21 de setembro de 2001, Dorothy E. Denning deixava explicito, num discurso efetuado no outono de 2000, no comité de forças armadas dos Estados Unidos, o que na sua opinião seria o ciberterrorismo, e que consistia na "convergência do terrorismo e do ciberespaço" através de "ataques ilegais e ameaças de ataques contra computadores, redes e informações armazenadas neles", tudo isto "quando feito para intimidar ou coagir um governo ou as suas pessoas em adiantamento de objetivos políticos ou sociais" (Denning, 2000: 1)[45].

Muitos autores acabaram por 'beber' da inspiração de Denning e acabaram por definir ciberterrorismo como "o uso de ferramentas de rede informática para prejudicar ou mesmo fechar infraestruturas críticas nacionais (como a energia, os transportes e as operações governamentais)" (Weimann, 2005: 130)[46] concordando também eles com a definição geral de Denning.

> "(...) para se qualificar como ciberterrorismo, um ataque deve resultar em violência contra pessoas ou propriedades, ou pelo menos causar danos suficientes para gerar medo. Os ataques que levam à morte ou lesões corporais, explosões ou perdas econômicas severas seriam exemplos. Os ataques sérios contra infraestruturas críticas podem ser atos de ciberterrorismo, dependendo do seu impacto. Os ataques que perturbam os serviços não essenciais de um Estado ou que são principalmente um incômodo dispendioso, não são exemplos de ciberterrorismo". (Denning, 2000: 1)[47]

---

[44] Texto original: "If you ask 10 people what 'cyberterrorism' is, you will get at least nine different answers! When those 10 people are computer security experts, whose task it is to create various forms of protection against 'cyberterrorism', this discrepancy moves from comedic to rather worrisome (Gordon e Ford, 2002: 3) (tradução do autor).

[45] Texto original: "Cyberterrorism is the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives" (Denning, 2000: 1) (tradução do autor).

[46] Texto original: "Cyberterrorism is the use of computer network tools to harm or shut down critical national infrastructures (such as energy, transportation, government operations)" (Weimann, 2005: 130) (tradução do autor).

[47] Texto original: "Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not" (Denning, 2000: 1) (tradução do autor).

Apesar da definição pioneira de ciberterrorismo, e segundo Weimann, o medo do desconhecido, os meios de comunicação social (através de filmes, séries e programas), a ignorância das pessoas, a agenda dos políticos e o facto do combate ao ciberterrorismo se ter tornado algo economicamente apetecível para os Estados (devido aos poucos recursos necessários) foram os principais fatores que estiveram na origem das definições díspares e pouco conclusivas do ciberterrorismo na época (Weimann, 2005: 131-132-133-134). "O ciberterrorismo, tem como maior condicionante o facto de apresentar um impacto menor na opinião pública que as tradicionais formas de terrorismo clássico. Um ciberataque poderá assim ser lançado para criar as condições ideais e para maximizar os efeitos de um ataque terrorista tradicional" (Paulo Nunes, 2004: 13).

O Professor Doutor Henrique Santos discorda de todas estas ideias fornecidas pelos autores relativamente ao ciberterrorismo e afirma mesmo que "os terroristas não têm nem nunca tiveram muito a ganhar com um ataque silencioso e sem projeção mediática, como são o caso dos ciberataques com motivações políticas (ou o ciberterrorismo), têm sim mais a ganhar se estes ataques tiverem uma visão monetária e de capitalização da organização que defendem" (Santos, 2018). Algo que também contraria a visão de Dennnig em 2000 quando afirmava que "o ciberterrorismo se iria tornar ainda mais atraente (para os terroristas) no futuro à medida que o mundo real e o mundo virtual se tornavam mais estreitamente conectados um com o outro - com um maior número de dispositivos físicos conectados à Internet" (Denning, 2000: 10)[48]. Ainda assim, e segundo o Professor Doutor Henrique Santos, "apesar do ciberterrorismo não ser almejado por terroristas como o ISIS ou a Al-qaeda, os comuns ciberataques são tão perigosos como um ato ciberterrorista" este afirma ainda que é preciso perceber que um ato de ciberterrorismo não necessariamente parte só de uma organização fundamentalista, mas pode partir também de um Estado (Santos, 2018).

Apesar de a literatura ter já separado convenientemente os conceitos ciberterrorismo e ciberataques - "o terrorismo pode ser muitas vezes distinguível do comum crime organizado transnacional, focado no lucro privado, devido a causa política envolvida[49] ou por outro qualquer motivo

[48] Texto original: "Cyberterrorism could also become more attractive as the real and virtual worlds become more closely coupled, with a greater number of physical devices attached to the Internet" (Denning, 2000: 10) (tradução do autor).

[49] Algo que pode causar algum desalinho com a definição de *Hacktivismo* (os *hackers* ativistas exploram através das técnicas de *hacking* a visibilidade e a capacidade de influência para as causas que defendem – muitas vezes políticas – podendo dessa maneira publicitar e chamar a atenção sobre os seus ideais (Santos et al, 2008: 81)) visto ser esta não só uma prática politicamente motivada, mas também por muitas vezes existir o uso de *hackers* por parte dos terroristas. No entanto em 2005 Weimann acabou por clarificar que "os ativistas querem protestar e perturbar não querem matar, mutilar ou aterrorizar"

público subjacente ao terrorismo" - aquilo que Ben Saul e Kathleen Heath nos explicam é que tudo isto dependerá sempre "de como o terrorismo é definido" visto que "algumas leis nacionais não requerem um motivo político para definirem o terrorismo" podendo assim "existir sobreposições na categoria de crime organizado particularmente devido às características estruturadas e organizadas de muitos grupos terroristas" isto é ainda mais preocupante se tivermos em conta "que certos grupos terroristas, com motivos políticos, podem também eles agir, em certos contextos, focados no lucro, em particular se existir uma visão estreita da intenção imediata de lucro por trás das suas atividades de angariação de fundos (seja roubando bancos, extorquindo negócios ou traficando drogas)" (Saul e Heath, 2014: 4)[50].

No geral, e de acordo com estas definições, "para que um ciberataque possa ser considerado como ciberterrorismo, este terá de satisfazer dois critérios: apresentar uma motivação política e um resultado destrutivo fisicamente visível. No entanto, ainda que alguns destes ataques apresentem uma forte motivação política, não existem registos conhecidos de que os ciberataques lançados através de computadores tenham, por si só, destruído infraestruturas ou originado a perda de vidas humanas" (Paulo Nunes, 2004: 4). A data os ciberataques existentes tinham pouca (ou nenhuma) capacidade de chegarem ao atributo de ciberterrorismo, visto que o "seu impacto tinha sido primariamente projetado para causar a interrupção de serviços (ou os ganhos monetários provenientes desta interrupção) não tendo dessa maneira um impacto sério em serviços críticos ou infraestruturas" dos Estados (Weimann, 2005: 130). Weimann afirma mesmo que "a grande maioria destes ciberataques eram lançados por hackers com poucos ou nenhuns objetivos políticos e sem nenhum desejo de causarem o caos e a carnificina com o qual os terroristas sonhavam (e sonham hoje em dia)" (Weimann, 2005: 130)[51].

Exercendo um pouco de futurismo Weimann reiterou em 2005 que um ciberterrorista iria acabar por um dia "perturbar os bancos, as transações financeiras internacionais ou a bolsa de valores" de um qualquer Estado, com a intenção de que os cidadãos deste mesmo país perdessem "toda a confiança

---

(Weimann, 2005: 136). No lado oposto do *hacktivismo* temos o *ativismo* que se foca no uso considerado legal do ciberespaço para a transmissão de uma mensagem, ideal ou crença para um grande número de pessoas (Leite, 2016: 6).

[50] Texto original: "Terrorism is often distinguishable from 'ordinary' transnational organised crime for private profit because of the political or other 'public' motive underlying terrorism. But it depends on how terrorism is defined, and quite a few national laws do not define terrorism to require a political motive. It can thus overlap with the category of organised crime, particularly given the structured and organised characteristics of many terrorist groups. More importantly, even terrorist groups with political motives may still act for profit in certain contexts, particularly if a narrow view is taken of the immediate intention behind their fundraising activities (whether robbing banks, extorting businesses, or trafficking drugs)" (Saul e Heath, 2014: 4) (tradução do autor).

[51] Texto original: "Its impact was primarily designed to cause disruption and did not have a serious impact on critical services or infrastructure. The vast majority of cyberattacks are launched by hackers with few if any political goals and no desire to cause the mayhem and carnage of which terrorists dream" (Weimann, 2005: 130) (tradução do autor).

no sistema econômico". Sendo que o ciberterrorista iria "estar sentado noutro continente enquanto os sistemas econômicos de uma nação paralisavam. A desestabilização seria assim alcançada" (Weimann, 2005: 137)[52].

Sarah Gordon e Richard Ford, também eles de alguma forma tentaram antecipar em 2002, aquilo que poderia ser o perigo do ciberespaço nas mãos de ciberterroristas quando afirmaram que "o perigo emergente do termo terrorismo cibernético é que o ciberterrorismo irá de alguma forma ser tratado separadamente do terrorismo regular", o que fará com exista uma "fragmentação artificial das nossas defesas, suscetível de proporcionar aos terroristas uma vantagem significativa em qualquer campanha contra um Estado" que na opinião dos autores "deveria ser evitada a todo custo" (Gordon e Ford, 2002: 13)[53].

O ciberataque na Estónia em 2007 veio trazer à tona a verdade por trás destes pensamentos e estes tornaram-se mais reais do que aquilo que os autores desejariam. Tenha sido um ato de ciberterrorismo ou um comum ciberataque, um Estado e as IC deste país no Báltico sofreram um ciberataque sem precedentes, um marco histórico neste campo. Apesar de presentemente os ciberataques já terem destruído as IC's de Estados ou mesmo paralisado estes por completo, como iremos ver no capítulo seguinte, as motivações políticas nunca são conhecidas e muito dificilmente os atores destes ataques alguma vez o serão.

1.3 Estónia 2007

"... foi um ataque com motivações políticas contra o nosso governo"

(Priisalu, 2015 apud Cyberwar 1.0 – chasing my digital self)[54].

---

[52] Texto original: "A cyberterrorist will disrupt the banks, the international financial transactions, the stock exchanges. The key: the people of a country will lose all confidence in the economic system. Would a cyberterrorist attempt to gain entry to the Federal Reserve building or equivalent? Unlikely, since arrest would be immediate. Furthermore, a large truck pulling along side the building would be noticed. However, in the case of the cyberterrorist, the perpetrator is sitting on another continent while a nation's economic systems grind to a halt. Destabilization will be achieved" (Weimann, 2005: 137) (tradução do autor).

[53] Texto original: "The nascent danger in the term cyberterrorism is that cyberterrorism will somehow be dealt with separately to regular terrorism. This artificial fragmentation of our defences is likely to provide the terrorist with a significant advantage in any campaign against a nation state, and is to be avoided at all costs" (Gordon e Ford, 2002: 13) (tradução do autor).

[54] Discurso original: "(...) it was a political and motivated attack against our government" (Priisalu, 2015 apud Cyberwar 1.0 – chasing my digital self) (tradução do autor).

"Ground Zero[55] da Ciberguerra: Estónia 2007"

(Hambsch, 2015)[56].

Antes do ciberataque a Estónia em 2007, as Organizações Internacionais tinham tendência para tratar deste tipo de assuntos cibernéticos solitariamente e em segredo "tendo apenas em consideração a contingência individual, não se preocupando com os riscos mais sistémicos" (Tikk, 2011: 119)[57].

Apesar de já existir uma extensa literatura dedicada à temática aqui abordada a partir da entrada no novo milénio, como já tivemos a oportunidade de mencionar, só em 2007 o ciberterrorismo, a ciberinsegurança e os ciberataques deixaram de ser efetivamente parte do imaginário de todos nós e passaram a fazer parte do nosso dia a dia, catalisados pelos ciberataques que se realizaram na Estónia neste mesmo ano.

> "Ataques realizados com o uso da Internet (ciberataques) contra informações-chave de infraestruturas críticas de Estados tem o melhor exemplo no ataque de 2007 contra a Estónia". (Joanna Kulesza, 2010: 3)[58]

Muitas das versões oficiais e semioficiais dizem que o ciberataque a Estónia em 2007 foi provocado pela mera mudança de uma estatua comemorativa da libertação da Estónia Nazi por parte da União Soviética (Herzog, 2011: 50/51; Burton, 2015: 306). Esta movimentação da estatua causou tumultos e muita contestação por parte da minoria de falantes russos na região (Herzog, 2011: 50/51; Burton, 2015: 306), o que causou desde logo uma tensão latente entre a Rússia e a Estónia.

A NATO no seguimento desta desordem, tanto na Rússia (com o clima de tensão vivido na embaixada da Estónia em Moscovo), como neste país, emitiu uma declaração oficial tendo em vista a estabilização do conflito.

---

[55] Ponto de partida para algo.

[56] Texto original: "Ground zero cyberwar: Estonia 2007" (Hambsch, 2015) (tradução do autor).

[57] Texto original: "Cyber security was merely the sum of individual contingency plans having little to do with more systemic risks" (Tikk, 2011: 119) (tradução do autor).

[58] Texto original: "Attacks conducted with the use of the Internet (cyber-attacks) onto key information infrastructures of sovereign states are best represented by the 2007 attack on Estonia" (Joanna Kulesza, 2010: 3) (tradução do autor).

"A NATO está profundamente preocupada com as ameaças à segurança física do pessoal diplomático estónio, incluindo o Embaixador, em Moscovo, bem como a intimidação na Embaixada da Estónia. Estas ações são inaceitáveis e devem ser interrompidas imediatamente; as tensões sobre o memorial soviético de guerra e as sepulturas na Estónia devem ser resolvidas diplomaticamente entre os dois países. A NATO exorta as autoridades russas a cumprirem as suas obrigações decorrentes da Convenção de Viena sobre relações diplomáticas". (NATO Press Release, 2007)[59]

No seguimento de todos estes protestos e guerras de palavras aconteceu algo que mudou a maneira como os países e as Organizações Internacionais olhavam para o ciberespaço – um ciberataque contra um Estado. Este ataque à Estónia, pioneiro em todas as frentes[60], foi concretizado através de um *DDoS* (ou um ataque de negação de serviço)[61] conjugado com a utilização de *Botnets*[62] que fizeram com que o efeito do ataque fosse ainda mais devastador (Burton, 2015: 299). Os *hackers* responsáveis por este ataque foram capazes de desabilitar, como se sabe, o normal funcionamento deste Estado do Báltico através de pedidos incessantes de acesso a sites governamentais e a sites privados até estes entrarem em colapso, causando dessa maneira problemas em sistemas centrais de órgãos tão diversos como os sites do sistema governamental, os bancos nacionais estónios e os meios de comunicação social deste mesmo país. No seguimento do ataque, todos estes serviços tiveram que ser encerrados completamente, o que resultou no fecho temporário de toda a estrutura informática do país devido ao desconhecimento do tipo de ataque com o qual se estava a lidar. Tendo em conta que em 2007 80% dos cidadãos estónios estavam constantemente ligados a internet, dá para imaginar o caos vivido neste Estado no pós-ataque

[59] Texto original: "NATO is deeply concerned by threats to the physical safety of Estonian diplomatic staff, including the Ambassador, in Moscow, as well as intimidation at the Estonian Embassy. These actions are unacceptable, and must be stopped immediately; tensions over the Soviet war memorial and graves in Estonia must be resolved diplomatically between the two countries. NATO urges the Russian authorities to implement their obligations under the Vienna Convention on diplomatic relations" (NATO, 2007) (tradução do autor).

[60] A desenvoltura com que foi praticado, as consequências que provocou bem como a magnitude do mesmo espantam ainda hoje os especialistas.

[61] DoS (ou ataque de negação de serviço) é um ataque informático que visa desabilitar ou controlar uma série de computadores de maneira a que seja impossível aceder aos mesmos ou controlá-los livremente. Existem várias técnicas para desabilitar este tipo de equipamentos a mais comum (e a que foi usada no ataque a Estónia em 2007) é a 'Flood'. Está consiste numa infinidade de pedidos de acesso ao servidor central - através do envio de pacotes de dados - até que este entra em saturação e se desligue ou reinicie, impedido dessa maneira o normal funcionamento do processo – vulgarmente conhecido como DDoS (ou ataque distribuído de negação de serviço) (Santos, Bessa e Pimentel, 2008: 169/170).

[62] É um programa malicioso que permite a um qualquer *hacker*/pirata informático que perpetra um crime informático controlar o(s) computador(es) infetado(s) remotamente através deste *malware* (*software* malicioso) (Site Oficial da ENISA, 2004-2018). O Botnet é muitas vezes usado em conjunto com o DDoS fazendo com que este atue com mais facilidade e eficácia, e dessa maneira com consequências ainda mais devastadoras (como se viu no caso da Estónia).

(Hambsch, 2015). A verdade é que "quanto mais tecnologicamente desenvolvido um país é, mais vulnerável se torna a um ataque cibernético contra as suas infraestruturas (Weimann, 2005: 130)[63] e a Estónia é a prova viva disso.

Sistemas informáticos de instituições financeiras foram inutilizados tal como o acesso a informação da midia (O'Neill, 2016), deixando a população sem dinheiro, sem notícias e sem acesso a informação governamental durante semanas.

Ainda assim segundo o ex-diretor de segurança Estónio, Jaan Priisalu, através do Documentário *Cyber War 1.0 - Chasing My Digital Self*, este ataque poderia ter resultado em problemas ainda mais graves se não tivessem sido tomadas as medidas necessárias para o controlo do mesmo. Entre outros problemas, ele refere que o impedimento de abastecimento de água e de alimentos a população bem como problemas com as telecomunicações poderiam ter sido uma realidade "e com isto o tipo de sociedade que tínhamos iria parar" (Jaan Priisalu, 2015)[64].

No seguimento deste ataque, a Estónia como membro da NATO pediu a aplicação do artigo 5º aos restantes membros desta organização internacional como resposta a subversão de que foi vítima. Os membros da NATO, no seguimento deste pedido, sentiram imediatamente dificuldades no tipo de resposta a efetuar no seguimento do ciberataque, devido não só a magnitude, mas também a complexidade do assunto com o qual estavam a lidar. Isto porque não só não tinham normas pré-definidas para reagirem a um ataque desta natureza (devido ao carácter inédito do ataque), mas também porque não sabiam concretamente quem perpetrou o ataque. Isso resultou na negação do pedido efetuado pela Estónia (Hansen e Nissenbaum, 2009: 1169). Ainda assim a NATO ultimou todos os preparativos para ser conferida a segurança necessária a Estónia.

É percetível e expectável que no pós-ataque de 2007, a Estónia pretendesse responder e defender-se deste ataque sem precedentes e escolheu fazê-lo focando-se num paradigma feito para responder a conflitos clássicos – o artigo 5º - devido não só a insensatez e à possível premeditação do ataque, mas também pela característica pioneira do mesmo.

Tudo isto vai de encontro as declarações feitas pelo ex-Ministro da Defesa Nacional, José Alberto Azeredo Lopes, que em abril de 2017 na Universidade do Minho, quando afirmou que os Estados Unidos da América tinham decidido utilizar uma "resolução clássica para um problema moderno" no seguimento

[63] Texto original: "The more technologically developed a country is, the more vulnerable it becomes to cyberattacks against its infrastructure" (Weimann, 2005: 130) (tradução do autor).
[64] Texto original: "So this kind of normal society would stop" (Jaan Priisalu, 2015) (tradução do autor).

dos ataques as torres gémeas a 11 de setembro de 2001 (II Seminário IDN Jovem, 2017). Apesar do contexto ser completamente diferente do que foi vivido em 2001, a dificuldade em responder a um problema contemporâneo (como o que foi vivido na Estónia em 2007) foi idêntico.

Jaan Priisalu mais uma vez através do Documentário *Cyber War 1.0 - Chasing My Digital Self*, diz claramente e abertamente que este ciberataque foi perpetrado por hackers russos apoiados pelo governo deste país (Priisalu, 2015). No entanto, entre os suspeitos encontram-se também a China, bem como hackers deste território, e hackers sem qualquer ligação estatal - como é o caso de um grupo de ativistas pró-Kremlim que numa entrevista a agência Reuters, em março de 2009, garantiram ter invadido o sistema informático da Estónia "por sua própria iniciativa" (Lowe, 2009).

Em abril de 2017 o Coronel Nuno Lemos Pires, numa palestra efetuada na Universidade do Minho, referiu-se a este tipo de ataques perenes (como o que aconteceu na Estónia) como "ataques de disrupção massiva capazes de indiretamente afetar tudo num país" este deu ainda um exemplo fictício de um ataque as centrais elétricas de um país onde estas poderiam indiretamente afetar toda a estrutura de um Estado (II Seminário IDN Jovem, 2017). O que aconteceu na Estónia em 2007 não foi muito diferente do que foi ficcionado pelo Coronel Nuno Lemos Pires a diferença é que este ataque atingiu diretamente o coração deste país do Báltico.

As questões fulcrais que ficam por responder neste ataque é não só a responsabilidade do ataque em si[65], mas também as premissas básicas que envolveram o ataque: será este um comum ciberataque ou um ato de ciberterrorismo? Como se percebe são sempre mais as perguntas que as respostas, uma característica que começa a ser um hábito em torno dos crimes informáticos.

A incapacidade de uma resposta eficaz conferira então uma necessidade de mudança no que ao paradigma do ciberespaço diz respeito por parte da UE e da NATO, que tendo no seu seio uma agenda global se tornava efetivamente uma prioridade.

1.4 Ciber(In)segurança no Pós-Estónia 2007

[65] Até a data de conclusão desta dissertação de Mestrado o responsável por este ataque era omisso e muitas são as teorias conspiratórias em torno deste crime.

"(...) este novo mundo acarreta perigos e dá azos a ações perniciosas, por parte de quem se esconde no anonimato que o ciberespaço proporciona, pois este coloca à sua disposição novos meios e ferramentas, antes inalcançáveis, uma vez que desafia a territorialidade, a soberania e a autonomia dos Estados".

(Leite, 2016: 16).

Como vimos anteriormente nem sempre um comum ciberataque pode ser descartado como um ato de ciberterrorismo e nem sempre um ato que à primeira vista aparenta ser um ataque ciberterrorista pode ser considerado inequivocamente um ato de terror. Apesar das diferenças enumeradas e explanadas anteriormente os quatro próximos crimes informáticos, tal como a Estónia em 2007 o foi (e sem descartar a Geórgia em 2008[66]), são a prova clara de que tudo pode ter duas ou mais interpretações no mundo cibernético.

Em novembro de 2014, um ciberataque "expôs informação confidencial e sensível da Sony[67], como as remunerações de funcionários de topo da companhia, trocas de emails entre executivos ou a disponibilização para download de filmes inéditos". "A tese inicial sugeria que teriam sido *hackers* ligados ao regime da Coreia do Norte a levar a cabo o ciberataque"[68] – levando Barack Obama a responsabilizar diretamente Kim Jong-un (líder Norte-Coreano) pelo incidente. Uma outra tese sugere que "ex-empregados da empresa *sony* se tenham aliado a grupos pró-pirataria online na Europa, EUA e Ásia para coordenar os ataques" (Almeida, 2014).

Em abril de 2015 a TV5 Monde, uma estação televisiva francesa, sofreu um ataque inédito na história da televisão mundial. Este ciberataque resultou na inacessibilidade dos doze canais por parte dos telespetadores, que ficaram sem emissão durante um largo período. Deste ciberataque resultaram também a usurpação da página de internet e as respetivas redes sociais da TV5 Monde – tudo isto provocou milhões de euros em prejuízo. Este ataque foi desde logo reivindicado por hackers ligados ao

[66] "Semanas antes das bombas russas começarem a cair na Geórgia na mais recente ofensiva russa contra a independência da Ossétia do Sul, outra guerra já mobilizava os dois países e os Estados Unidos, uma ciberguerra. Há mais acusações do que provas, mas o fato é que as nações duelam desde o dia 20 de julho pela internet – os servidores são autênticas arenas de combate na tentativa de controlar as infraestruturas de rede e até os sites governamentais. É a primeira vez na história que ataques *hackers* coincidem com uma guerra real" (Markoff, 2008).

[67] Multinacional Japonesa fabricante de produtos eletrónicos (telemóveis, computadores, consolas de videojogos, et al) – sobejamente conhecida por ser a fabricante da playstation.

[68] Um ato de represália contra o filme "The Interview" (em português "Uma Entrevista de Loucos") uma paródia a Kim Jong-un - distribuído e produzido pela sony pictures entertainment inc. (uma sucursal da empresa mãe, a sony).

cibercalifado[69] do ISIS, o que denota desde logo a capacidade multifacetada que inclusive grupos terroristas têm para aceder e cometer crimes no ciberespaço. Posteriormente, também foi levantada a hipótese de este ciberataque ter sido causado por hackers russos ligados ao Kremlim (JeanMartial Lefranc, 2015).

Entre 2015 e 2016 também a *DNC* (*Democratic National Committee*), uma plataforma informática de apoio ao Partido democrata Norte-Americano, sofreu um ciberataque que abalou as eleições presidenciais americanas de 2016. Este ataque visou o roubo de informação sigilosa (financiadores, estratégias de campanha e os famosos emails de Hillary Clinton) que posteriormente foram disponibilizados no *Wikileaks*[70]. Mais uma vez os responsáveis por este ataque variam, mas desde a primeira hora os serviços de informação americanos garantiram que este ataque foi perpetrado pela Rússia, levando inclusive a que Barack Obama tenha expulsasse 35 diplomatas russos de território norte-americano (Evan Perez e Daniella Diaz, 2016). Também *hackers* isolados reclamam a autoria deste ataque como é o caso de *Guccifer 2.0*[71]. Este último afirmou que "até pode ter sido o primeiro que penetrou nos servidores de correspondência da Hillary Clinton e outros democratas, mas ele certamente não será o último. Não é de admirar que qualquer outro *hacker* possa facilmente acessar os servidores da DNC" (Guccifer2, 2016)[72].

Dois dos ciberataques mais recentes aconteceram durante o ano transato de 2017 e deixaram os utilizadores do sistema operativo[73] *Windows* da *Microsoft*[74] a mercê de *hackers* que infetaram e manipularam os computadores de milhares de utilizadores deste sistema operativo da Microsoft com um

---

[69] *Hackers* ligados ao grupo terrorista ISIS.

[70] "*WikiLeaks* é uma organização multinacional de media e biblioteca associada. Foi fundada por Julian Assange (um dos primeiros piratas informáticos do mundo (vulgarmente conhecidos como *hackers*) - encontra-se neste momento confinado a embaixada do Equador em Londres onde permanece em asilo político (pedido este baseado numa possível extradição para os Estados Unidos e consequente prisão ou homicídio devido ao que expos sobre este mesmo estado no site que fundou: o *Wikileaks)* em 2006. O *WikiLeaks* é especialista em análise e publicação de grandes conjuntos de dados de materiais oficiais, censurados ou restritos de guerra, espionagem e corrupção" (Wikileaks, 2006-2018) (tradução do autor) = texto original: "WikiLeaks is a multi-national media organization and associated library. It was founded by its publisher Julian Assange in 2006. WikiLeaks specializes in the analysis and publication of large datasets of censored or otherwise restricted official materials involving war, spying and corruption (Wikileaks, 2006-2018).

[71] *Hacker*. Disponível na internet em: https://guccifer2.wordpress.com/

[72] Texto original: "Guccifer may have been the first one who penetrated Hillary Clinton's and other Democrats' mail servers. But he certainly wasn't the last. No wonder any other hacker could easily get access to the DNC's servers" (Guccifer2, 2016) (tradução do autor).

[73] Gestor de recursos do computador – ponte entre o utilizador e o *software* da máquina.

[74] "Líder mundial em serviços de software" (Microsoft). Disponível na internet em: https://news.microsoft.com/facts-about-microsoft/

Ransomware[75]. Ambos os ciberataques foram similares na sua essência e tinham por base a encriptação[76] de ficheiros de um qualquer computador pessoal com um sistema operativo *Windows.* A isto, seguia-se um pedido de resgate e aquando do pagamento do mesmo, o computador era desencriptado[77] e devolvido ao utilizador. O primeiro ciberataque foi apelidado de *WannaCry* e o segundo de *NotPetya* (Site Oficial do CCDCOE, 2008-2018). Tanto a UE – através da ENISA (Agência Europeia para a Segurança das Redes e da Informação) – como a NATO – através do CCDCOE – reagiram a estes ciberataques declarando que poderiam existir retaliações severas, se a iniciativa dos ataques fosse de proporções extremas, sendo dessa maneira acionado o artigo 5º da NATO[78] (Site Oficial do CCDCOE, 2008-2018).

A opacidade destes crimes faz com que presentemente ainda não se saiba quem foram os verdadeiros responsáveis por todos os ataques enumerados e explanados anteriormente. Podemos então a partir desta análise compreender o quão difícil é investigar um ataque realizado no ciberespaço, seja quanto ao culpado – que como vimos é incógnito sempre que queira – quer através das básicas definições de ciberataque comum e ciberterrorismo.

Até onde podemos compreender não sabendo quem é responsável de um ciberataque não se sabe as reais motivações por trás deste, não se sabendo as reais motivações por trás deste pode-se partir do pressuposto que este pode automaticamente ser um ciberataque comum ou um ato de ciberterrorismo – tendo obviamente em conta que o ataque afetou as IC do Estado visado e não passou de um ataque isolado.

Confirmando esta incapacidade de controlo, Tobias Feakin dizia já em 2015 que "os Estados/governantes vão continuar despreparados para responder adequadamente aos ciberataques,

---

[75] O Ransomware é segundo a ENISA um "malware (vírus, Trojan ("um malware que se disfarça de peça legitima de software do computador para o seu proprietário a instalar") (Site Oficial da ENISA, 2004-2018) (tradução do autor = texto original: "A Trojan (Trojan Horse) is a type of malware that disguises itself as a legitimate piece of software in order to convince a victim to install it") (Site Oficial da ENISA, 2004-2018) que infecta os sistemas informáticos dos utilizadores e manipula o sistema de forma a que a vítima não consiga utilizar, parcial ou totalmente, os dados armazenados" (Site Oficial da ENISA, 2004-2018) (tradução do autor) = texto original "(...) malware (like Viruses, Trojans, etc.) that infect the computer systems of users and manipulates the infected system in a way, that the victim cannot (partially or fully) use it and the data stored on it" (Site Oficial da ENISA, 2004-2018).

[76] Dicionário da Porto Editora – Encriptar: "converter (dados informáticos e mensagens) com um código especial, tornando-os incompreensíveis para quem não tem acesso a esse código" (Porto Editora, 2003-2018c).

[77] Descodificado.

[78] A base que sustenta o princípio da NATO é a defesa coletiva e desde logo o artigo 5º explana esta conceção dizendo que "Collective defence means that an attack against one Ally is considered as an attack against all Allies" (NATO, 2017). Disponível na internet em https://www.nato.int/cps/ic/natohq/topics_110496.htm

mesmo com este tipo de ataques destrutivos e disruptivos a crescer" (Feakin, 2015: 2)[79]. Isto faz com que com que "governos ou agentes não estatais sintam a necessidade de fazer uma de duas coisas para se protegerem, cooperar ou competir pelo poder nesta arena complexa" e anárquica (Nye, 2014: 1)[80] sendo muitas vezes chamadas a intervir as duas OI que constituem os estudos de caso desta dissertação – a UE e a NATO.

Além destes ciberataques um grande número de ataques individuais continua a subir aos milhares todos os dias. Isto é demonstrado pelo site da empresa *Kaspersky Lab*[81] e pelo site da empresa *Norse Corp*[82] que diariamente e em tempo real mostram toda a atividade maliciosa no ciberespaço[83].

Reforçando esta ideia o senador John McCain disse em abril de 2017, numa entrevista ao canal *National Geographic*, afirmou que "um ciberataque bem-sucedido por si só é capaz de nos deixar profundamente preocupados" (McCain, 2017 apud National Geographic, 2017)[84]. Também Leon Panetta tem uma posição semelhante declarando que "um ataque cibernético perpetrado por Estados ou grupos extremistas violentos pode ser tão destrutivo quanto os ataques terroristas de 11 de setembro de 2001" (Panetta,2012 apud Departamento de Defesa Norte-Americano, 2012)[85].

Tendo isto em conta, muitos defendem que "chegou a hora de os governos considerarem uma resposta coordenada aquilo que é o constante risco cibernético" (Kopp et al, 2017)[86] isto porque as leis locais deixaram de ser eficazes contra esta ameaça transnacional" (Tehrani et al, 2013: 207)[87] .

A realidade é que "os ciberataques podem criar um sentimento geral de insegurança nas organizações que maioritariamente dependem de computadores para funcionarem - desde os transportes até aos sistemas bancários passando pelos processos industriais e mesmo nas nossas vidas pessoais e profissionais – e isto pode fazer com que sejam criados graves problemas nestes serviços se

---

[79] Texto original: "Even as the number of highly disruptive and destructive cyberattacks grows, governments remain unprepared to respond adequately" (Feakin, 2015: 2) (tradução do autor).

[80] Texto original: "Governments and non-state actors cooperate and compete for power in this complex arena" (Nye, 2014: 1) (tradução do autor).

[81] Companhia de antivírus Russa.

[82] Companhia focada na deteção e no combate de ameaças cibernéticas.

[83] <https://cybermap.kaspersky.com/> <http://map.norsecorp.com/#/>

[84] Discurso original: "When you see the potential of what a successful cyberattack can achieve, it's enough to make you deeply concerned" (McCain, 2017 apud National Geographic, 2017) (tradução do autor).

[85] Discurso original: "A cyber-attack perpetrated by nation states are violent extremists groups could be as destructive as the terrorist attack on 9/11" (Panetta, 2012 apud Departamento de Defesa Norte-Americano, 2012).

[86] Texto original: "Ha llegado el momento de que los gobiernos se planteen una respuesta coordinada al ciberriesgo sistémico" (Kopp et al, 2017) (tradução do autor).

[87] Texto original: "Since cyber terrorism is an international crime, local regulations alone are not able to defend against such attacks; they require a transnational response (Tehrani et al, 2013: 207) (tradução do autor).

um ataque cibernético acontecer" (Arpagian, 2015 apud Euronews, 2015)[88]. Partindo deste pressuposto desde a entrada no novo milénio tanto a UE como a NATO chamaram a si a responsabilidade de proteger o ciberespaço.

1.5 A Luta Contra a Cibercriminalidade

Tomando por base os dois estudos casos da presente dissertação testemunharemos aquilo que foi o nascimento, a evolução e a afirmação da cibersegurança e da ciberdefesa, respetivamente, na agenda da UE e na NATO. Analisaremos de maneira detalhada os eventos mais relevantes que surgiram ao longo do século XXI (acompanhando também um pouco do final do século XX), no seio de ambos os atores em análise. Desde cimeiras a agências passando também pelos mais diversos protocolos e promulgações, olharemos com redobrada atenção para a luta contra a ciberinsegurança por parte de ambas as Organizações Internacionais.

[88] Texto original: "The very principle of terrorism is to install a climate of fear in its enemy. Cyber-attacks can create a general feeling of insecurity as so many organisations are computer-reliant, from transport to banking systems to industrial processes and even into our personal and professional lives, that major malfunctions can be created" (Arpagian, 2015 apud Euronews, 2015) (tradução do autor).

2. UNIÃO EUROPEIA[89]

"Os esforços da cibersegurança por parte da UE também envolvem a dimensão da defesa cibernética"

(Estratégia Europeia de Ciberdefesa, 2013 apud Site Oficial da Agência Europeia de Defesa, 2017)[90].

"O ciberespaço é tido como o quinto domínio da guerra[91], igualmente crítico para as operações militares como a terra, o mar, o ar e o espaço. O sucesso das operações militares nos domínios físicos depende cada vez mais da disponibilidade e do acesso ao ciberespaço. As forças armadas dependem do ciberespaço tanto como usuário, como domínio para realizar missões de defesa e segurança"

(Agência Europeia de Defesa, 2017: 1)[92].

Quando falamos em cibersegurança na UE temos de recuar até 2001[93] para contemplarmos os primeiros indícios desta matéria nas dinâmicas de segurança deste ator. "Com a entrada no século XXI os ataques informáticos passaram a ser entendidos como cibercrimes" (Barrinha, 2018)[94], mais

[89] Mais informações em Anexo II.

[90] Texto original: "Cyber security efforts in the EU also involve the cyber defence dimension" (Estratégia Europeia de Ciberdefesa, 2013 apud Site Oficial da Agência Europeia de Defesa, 2017).

[91] "Depois da terra, do mar, do ar e do espaço, a guerra entrou no quinto domínio: o ciberespaço" (The Economist, 2010) (tradução do autor) = Texto original: "After land, sea, air and space, warfare has entered the fifth domain: cyberspace" (The Economist, 2010) (tradução do autor).

[92] Texto original: "Cyberspace is understood as the fifth domain of warfare equally critical to military operations as land, sea, air, and space. Success of military operations in the physical domains is increasingly dependent on the availability of, and access to, cyberspace. The armed forces are reliant on cyberspace both as a user and as a domain to achieve defence and security missions" (Agência Europeia de Defesa, 2017: 1) (tradução do autor).

[93] É importante salientar "a diretiva 1999/93/CE do Parlamento Europeu e do Conselho, de 13 de dezembro de 1999" - que estabeleceu um quadro legal comunitário e jurídico para as assinaturas eletrónicas a nível europeu e o reconhecimento dos prestadores de serviços de certificação (com o objetivo de tornar as assinaturas eletrônicas mais fáceis de usar e ajudá-las a ser legalmente reconhecidas em todos os países da UE) (Conselho da União Europeia e Parlamento Europeu, 1999) – e o regulamento que veio a substituir esta o "Regulamento (UE) No. 910/2014 do Parlamento Europeu e do Conselho de 23 de julho de 2014 relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno e que revoga a Diretiva 1999/93/CE" – através deste regulamento foi colocado em prática um conjunto único de regras sobre serviços de confiança eletrônica (assinaturas, marcações horárias e selos eletrônicas(os) e serviços de entrega e de autenticação) e de identificação eletrônica diretamente aplicável em toda a Europa (Conselho da União Europeia e Parlamento Europeu, 2014). Não sendo diretamente enquadrada na área de pesquisa é ainda assim importante reconhecer a sua existência.

[94] Quando André Barrinha olha para o papel cibersecuritário da União Europeia a nível mundial defende que "este assenta em dois vetores: 1° a consciência por parte da União Europeia relativamente aos cibercrimes (com a entrada no novo século)" (Barrinha, 2018) (continua).

concretamente na "Convenção Europeia do Cibercrime em Budapeste" (Conselho da União Europeia, 2001: 2). A UE entendeu que "a dependência da sociedade em relação à tecnologia, e os riscos securitários que isto acarretava, teriam de ser adequadamente resolvidos" servindo esta convenção como marco inicial para as dinâmicas da cibersegurança nesta união de Estados (Barrinha e Carrapico, 2018: 1)[95].

"A Convenção de Budapeste (também conhecida como a convenção sobre o cibercrime)[96] foi necessária na dissuasão de ações contra a confidencialidade, a integridade e a disponibilidade de sistemas informáticos, redes e dados bem como o mau uso de tais sistemas, redes e dados antecipando a criminalização de tal conduta. Conforme descrito nesta convenção serão adotados poderes suficientes para combater eficazmente tais delitos, facilitando dessa maneira a sua deteção, a sua investigação e a sua perseguição nos níveis doméstico e internacional sendo providenciados mecanismos de cooperação internacional rápidos e confiáveis" (Conselho da União Europeia, 2001: 2)[97].

Nesta Convenção vários dos Estados-membros à data acordaram em reprimir o cibercrime de uma maneira eficaz e com base nos princípios de coordenação. Estes alcançaram um acordo multilateral sobre a legislação do cibercrime através de protocolos estabelecidos. A convenção foi também alvo de críticas devido às particularidades das medidas tomadas, isto porque estas não tinham em vista a proteção dos direitos dos indivíduos ou dos Estados. Em geral, a convenção também não conseguiu garantir medidas especificas para cessar com a atividade criminosa no ciberespaço (Direção Geral da Política de Justiça (DGPJ), 2008).

Depois das várias ratificações relativamente à convenção sobre o cibercrime em Budapeste, e depois da UE ter percebido que o "ciberespaço e os cibercriminosos não são limitados pelas fronteiras

[95] Texto original: "(...) the EU discourse slowly started to reflect the idea that societal reliance on technology constituted a rapidly growing security risk that had to be adequately addressed" (Barrinha e Carrapico, 2018: 1) (tradução do autor).

[96] "Convenção aberta à assinatura a 23 de novembro de 2001, em Budapeste, com entrada em vigor na ordem jurídica internacional a 1 de julho de 2004, após as cinco ratificações exigidas" (DGPJ - Direção-Geral da Política de Justiça, 2008). Disponível na internet em: http://www.dgpj.mj.pt/sections/relacoes-internacionais/copy_of_anexos/convencao-sobre-o/

[97] Texto original: "Convinced that the present Convention is necessary to deter action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalisation of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating their detection, investigation and prosecution at both the domestic and international levels and by providing arrangements for fast and reliable international co-operation" (Conselho da União Europeia, 2001: 2) (tradução do autor).

nacionais" (Barrinha e Carrapico, 2018: 1)[98], surgiu a ENISA indagada pelo "Regulamento (CE) n.º 460/2004 do Parlamento Europeu e do Conselho Europeu a 10 de março de 2004" (Conselho da União Europeia e Parlamento Europeu, 2004 apud EUR-Lex, 2004).

> "A Agência Europeia para a Segurança das Redes e da Informação (ENISA) é um centro especializado na segurança cibernética na Europa. A Agência está localizada na Grécia, com sede em Heraklion Crete, contando também com um escritório operacional em Atenas. A ENISA contribui para um alto nível de segurança das redes e informação dentro da União Europeia desde que foi criada em 2004, sempre na procura do desenvolvimento da cultura de segurança das redes e informação na sociedade Europeia e na procura de um aumento de consciencialização sobre esta prática, contribuindo assim para o correto funcionamento do mercado interno". (Site Oficial da ENISA, 2004-2018)[99]

Como ato prioritário, a ENISA estabeleceu algumas primazias relativamente aquilo que passaria a ser a sua visão de futuro: Experiência, perícia e antecipação por parte daqueles que fazem parte desta agência no combate ao cibercrime, "promoção da segurança das redes e da informação como uma prioridade política da UE", o acompanhamento da evolução tecnológica, o reforço da cooperação entre os Estados-membros e a UE e o fortalecimento da contribuição da ENISA no seio da UE (Site Oficial da ENISA, 2004-2018)[100].

De entre os muitos programas, missões, protocolos e estudos sob a alçada da ENISA de salientar o Sistema Europeu de Partilha e Alerta de Informação (EISAS) que foi encomendado pela Comissão Europeia em 2006. O EISAS era "um estudo de viabilidade sobre um possível sistema de partilha de informações relacionadas com o NIS. Este era destinado a utilizadores finais, cidadãos e pequenas e médias empresas, na expetativa de assim ser aumentada a sensibilização relativamente a segurança

[98] Texto original: "Given that cyberspace and cyber criminals are not limited by national boundaries, the EU presented itself as the logic and efficient solution to Member States' challenge of how best to tackle cyber security threats" (Barrinha e Carrapico, 2018: 1) (tradução do autor).

[99] Texto original: "The European Union Agency for Network and Information Security (ENISA) is a centre of expertise for cyber security in Europe. The Agency is located in Greece with its seat in Heraklion Crete and an operational office in Athens. ENISA is actively contributing to a high level of network and information security (NIS) within the Union, since it was set up in 2004, to the development of a culture of NIS in society and in order to raise awareness of NIS, thus contributing to proper functioning of the internal market" (Site Oficial da ENISA, 2004-2018) (tradução do autor).

[100] Texto original: "Promote network and information security as an EU policy priority" (Site Oficial da ENISA, 2004-2018) (tradução do autor).

informática e eliminar lacunas na cobertura de tais informações" (Site Oficial da ENISA, 2004-2018)[101]. Em 2007, foram apresentados os primeiros relatórios aos Estados-membros (Site Oficial da ENISA, 2004-2018).

No seguimento da criação da ENISA, mais concretamente durante o ano de 2005 e 2006, o Conselho Europeu e a Comissão Europeia tomaram medidas oficiais relativamente ao impedimento de ataques contra os sistemas de informação, lançando com este intuito uma diretiva contra ciberataques sob a denominação de "Decisão-Quadro 2005/222/JAI do Conselho, de 24 de Fevereiro de 2005, relativa a ataques contra os sistemas de informação" (Comissão Europeia, 2005 apud EUR-Lex, 2005) com várias indicações para os Estados-membros relativamente a interferência ou acesso ilegal a sistemas de informação e consequentes punições e competências por parte destes, um protocolo adicional a convenção europeia do cibercrime e dando seguimento a um projeto idealizado pelos Estados-membros em 2004, a criação de um programa de proteção das infraestruturas críticas sob a diretiva "Comunicação da Comissão relativa a um Programa Europeu de Proteção das Infraestruturas Críticas /* COM/2006/0786 final */" - PEPIC (Comissão Europeia, 2006 apud EUR-Lex, 2006)[102].

Tudo isto não foi, no entanto, o suficiente para impedir o ciberataque a Estónia ocorrido durante o ano de 2007. "É um ponto relativamente pacífico, na literatura de segurança internacional, que a crise na Estônia em 2007 constitui um marco nos estudos sobre guerra cibernética" (W. M. Teixeira et al, 2017: 41). Não só nos estudos de segurança internacional, mas também no seio das Organizações Internacionais:

> "As economias modernas são largamente dependentes de infraestruturas críticas, nomeadamente de transportes, de comunicações e de fornecimento de energia, mas também da Internet. A Estratégia da UE para uma sociedade de informação segura, adotada em 2006, visa combater a

[101] Texto original: "EISAS stands for European Information Sharing and Alert System. ENISA has been asked by the European Commission to deliver a feasibility study on a Europe-wide sharing system for NIS related information to end-users/citizens and SMEs, to raise IT security awareness and close gaps in the coverage with such information" (Site Oficial da ENISA, 2004-2018) (tradução do autor).

[102] "Objetivo do PEPIC - O objetivo geral do PEPIC é melhorar a proteção das infraestruturas críticas na UE. Este objetivo será alcançado através da criação de um enquadramento da UE em relação à proteção das infraestruturas críticas, que é estabelecido na presente comunicação. Tipos de ameaças abrangidas pelo PEPIC - embora se reconheça que a ameaça do terrorismo constitui uma prioridade, a proteção das infraestruturas críticas basear-se-á numa abordagem de todos os riscos. Se as medidas de proteção de um dado sector das infraestruturas críticas forem consideradas adequadas, as partes interessadas devem centrar a sua atenção nas ameaças em relação às quais se encontram vulneráveis (o programa expirou em 06/07/2016)." (Conselho da União Europeia, 2006 apud EUR-Lex, 2006).

> cibercriminalidade. No entanto, os atentados contra sistemas informáticos tanto privados como governamentais que ocorreram nos Estados-membros, vieram conferir a este tipo de criminalidade uma nova dimensão, revelando o seu potencial como nova arma económica, política e militar. É necessário um maior esforço neste domínio, com vista a uma abordagem global europeia, a uma maior sensibilização e ao reforço da cooperação internacional". (Conceito Estratégico EU, 2008: 5)

De maneira clara, percebemos que a o ciberataque a Estónia em 2007 catalisou a UE para uma redobrada preocupação com a cibersegurança. A consciência que a cibercriminalidade era efetivamente um perigo real (apesar de já ser compreendido como um desde 2001) foi grande parte daquilo que ficou exposto no documento estratégico da União Europeia de 2008.

Enquanto a Estratégia Europeia de Segurança de 2003 não fazia qualquer referência ao ciberespaço ou a maneira como este deve ser protegido, o Relatório sobre a Implementação da Estratégia Europeia de Segurança de 2008, um ano após o ciberataque a Estónia em 2007, lançou a UE no ciberespaço e na cibersegurança de maneira efetiva. A partir deste momento, a UE chamou também si a responsabilidade de proteger este espaço em virtude daqueles que compõem esta União de Estados.

Em 2010 a UE lançou a Estratégia de Segurança Interna da União Europeia com o intuito de reforçar o Relatório sobre a Implementação da Estratégia Europeia de Segurança de 2008, e nesta espelhou a cibersegurança como ponto prioritário nos seguintes termos: "A cibercriminalidade representa uma ameaça global, técnica, transfronteiriça e anônima aos nossos sistemas de informação representando dessa maneira um desafio adicional para as forças de segurança" (Conselho da União Europeia, 2010: 14)[103].

A Cibersegurança era um dos objetivos cruciais desta estratégia de segurança interna. Esta definia que todos os Estados-membros "teriam de possuir uma equipa de resposta a emergências cibernéticas até ao ano de 2012" e além disso era também crucial que estas equipas fossem inseridas numa "plataforma de redes de contato bem como realizassem exercícios em conjugação com a ENISA periodicamente" (Conselho da União Europeia e Parlamento Europeu, 2010: 11-12). Em consonância com esta vontade, em 2012 surge no seio da UE a CERT-EU - Equipa de resposta a emergências informáticas da União Europeia. Trata-se de uma equipa focada na resposta a emergências cibernéticas

[103] Texto original: "Cybercrime represents a global, technical, cross-border, anonymous threat to our information systems and, because of that, it poses many additional challenges for law-enforcement agencies" (Conselho da União Europeia, 2010: 14) (tradução do autor).

com a capacidade e com o intuito de "responder a incidentes relacionados com a segurança da informação e ameaças cibernéticas" (Site Oficial da CERT-UE, 2012-2018)[104].

A par da ENISA, em 2004, a UE criou mais duas instituições entre os anos 2012 e 2013. Em 2012 surgiu a eu-LISA - Agência Europeia para a gestão operacional de sistemas informáticos de grande escala na área da liberdade, da segurança e da justiça. "A eu-LISA, agência Europeia para a gestão operacional de sistemas informáticos de grande escala no espaço de liberdade, da segurança e da justiça, nasceu na expetativa de aumentar a consciência, por parte dos cidadãos da UE, sobre as Tecnologias de Informação e Comunicação (TIC) e através disto facilitar e proactivamente contribuir para o sucesso das políticas desta união de Estados na área da justiça e dos assuntos internos, amparando com isto os Estados-membros nos seus esforços para uma Europa mais segura" (Garkov, 2012-2018 apud eu-LISA Website Oficial, 2012-2018)[105].

Em 2013, através da Europol surge o EC3 - o Centro Europeu de Cibercriminalidade – com sede em Haia tal como a Europol. "A Europol criou o Centro Europeu da Cibercriminalidade (EC3) em 2013 com o intuito de reforçar a aplicação da lei no âmbito da cibercriminalidade no seio da UE, e assim, ajudar a proteger os cidadãos, as empresas e os governos europeus dos crimes no ciberespaço. Desde a sua criação, a EC3, contribuiu significativamente na luta contra a cibercriminalidade: esteve envolvida em dezenas de operações de alto nível e em centenas de missões de apoio operacional, analisando centenas de milhares de arquivos - a grande maioria dos quais evidenciaram ser maliciosos - e culminando em centenas de prisões" (EUROPOL Website Oficial, 1999-2018)[106].

Ainda em 2013 "o Parlamento Europeu exortou para a luta contra a cibercriminalidade e adiu para a prevenção contra a mesma, impelindo mesmo os Estados-membros a retificarem a convenção de

---

[104] Texto original: "In recent years, CERTs have been developed in both private and public sectors as small teams of cyber-experts connected to the internet that can effectively and efficiently respond to information security incidents and cyber threats, often on a 24 hours a day-7days a week basis" (Site Oficial da CERT-UE, 2012-2018) (tradução do autor).

[105] Texto original: "eu-LISA, the European Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice, is called to increase the added value of ICT technology to the citizens of EU and through it to facilitate and proactively contribute to the success of the EU policies in the area of justice and home affairs and to support the Member States (MS) in their efforts for safer Europe" (Garkov , 2012-2018 apud eu-LISA Website Oficial, 2012-2018) (tradução do autor).

[106] Texto original: "Europol set up the European Cybercrime Centre (EC3) in 2013 to strengthen the law enforcement response to cybercrime in the EU and thus to help protect European citizens, businesses and governments from online crime. Since its establishment, EC3 has made a significant contribution to the fight against cybercrime: it has been involved in tens of high-profile operations and hundreds on-the-spot operational-support deployments resulting in hundreds of arrests, and has analysed hundreds of thousands of files, the vast majority of which have proven to be malicious" (EUROPOL Website Oficial, 2013-2018) (tradução do autor).

Budapeste e incutindo a UE na mudança do escopo do PEPIC" (Comissão Europeia, 2013: 7-9). Afirmando mesmo que "a União Europeia deveria desempenhar um papel de liderança no desenvolvimento de normas e de comportamento no ciberespaço" (Comissão Europeia, 2013: 11), não sendo de estranhar, portanto, as várias mudanças no panorama securitário do ciberespaço que advieram no seguimento dessa sugestão.

Durante este mesmo ano, 2013, a União Europeia lançou uma diretriz com o intuito de substituir a diretiva (decisão-quadro) de 2005, com a nomenclatura "Diretiva 2013/40/UE do Parlamento Europeu e do Conselho, de 12 de agosto de 2013, relativa a ataques contra os sistemas de informação e que substitui a Decisão-Quadro 2005/222/JAI do Conselho" (Conselho da União Europeia e Parlamento Europeu, 2013 apud EUR-Lex, 2013). "Esta diretiva introduzia novas regras destinadas a harmonizar a criminalização e as sanções por várias infrações contra os sistemas de informação. Estas regras incluem a proibição da utilização dos chamados *botnets* - software maligno concebido para estabelecer o controlo à distância de uma rede de computadores. Apela, além disso, aos Estados-membros da UE para que utilizem os mesmos pontos de contacto utilizados pelo Conselho da Europa e pelo G8 para reagir rapidamente a ameaças que envolvam tecnologias avançadas" (Conselho da União Europeia e Parlamento Europeu, 2013: 1-3 apud EUR-Lex, 2013).

Durante este mesmo ano, lançou uma estratégia relativamente a cibersegurança denominada "Comunicação Conjunta do Parlamento Europeu, do Conselho Europeu, do Comité Económico e Social Europeu e do Comité das Regiões: Estratégia da União Europeia para a cibersegurança - Um ciberespaço aberto, seguro e protegido" (Comissão Europeia, 2013) com o seguinte intuito:

> "A presente proposta de estratégia da União Europeia para a cibersegurança, apresentada pela Comissão e pela Alta Representante da União para os Negócios Estrangeiros e a Política de Segurança, define a visão da UE e as ações necessárias, fundadas numa proteção e numa promoção eficazes dos direitos dos cidadãos, para tornar o ambiente em linha na UE o mais seguro do mundo. Esta visão apenas pode ser concretizada através de uma verdadeira parceria entre os numerosos intervenientes de assumir a responsabilidade e responder aos desafios que se perfilam". (Comissão Europeia, 2013: 3 e 19)[107]

[107] Texto original: "This proposal for a Cybersecurity strategy of the European Union, put forward by the Commission and the High Representative of the Union for Foreign Affairs and Security Policy (High Representative), outlines the EU's vision in this domain, clarifies roles and responsibilities and sets out the actions required based on strong and effective protection and promotion of citizens' rights to make the EU's online environment the safest in the world (...) this vision can only be realised

Entrando em anos mais recentes, mais concretamente em 2015, é lançada pela UE a estratégia digital de mercado único com o intuito de tornar a Europa líder global no campo das TIC's - com o objetivo claro de proteger os cidadãos europeus nos níveis domésticos: sociais e económicos das agruras do ciberterrorismo. Ainda durante este ano a agenda europeia de segurança passou a englobar o cibercrime como uma das três maiores prioridades ao nível da segurança (lado a lado com o crime organizado e o terrorismo).

Durante o ano de 2016, por iniciativa da alta representante da UE Federica Mogherini, surge um novo documento estratégico intitulado 'Visão partilhada, ação comum: uma Europa mais forte - Estratégia Global para a política externa e de segurança da União Europeia'. A cibersegurança não faltou no ambiente securitário e prioritário deste documento e ficou retratada num tópico específico de seu nome 'cibersegurança' onde assumiu:

> "Aumentar o seu foco na segurança cibernética equipando-se e ajudando os Estados-membros a protegerem-se contra as ameaças cibernéticas, mantendo simultaneamente um ciberespaço aberto, livre e seguro. Isso implicará o fortalecimento das capacidades tecnológicas, voltadas não só para à mitigação das ameaças cibernéticas e à resiliência das infraestruturas críticas, redes e serviços, mas também na redução do cibercrime no geral. Isto significa que existirá uma fomentação de tecnologias inovadoras de informação e comunicação (TIC) sendo garantida dessa maneira a disponibilidade e a integridade dos dados bem como a segurança do espaço digital europeu através de políticas de localização relativamente ao armazenamento de dados e a certificação de produtos e serviços. Tudo isto requer que sejam levantadas questões cibernéticas em todas as políticas bem como o reforço de todos os componentes cibernéticos nas missões e operações da PCSD bem como o desenvolvimento de plataformas de cooperação. A União Europeia, em termos cibernéticos, apoiará a cooperação política, operacional e técnica entre os Estados-membros, nomeadamente na análise e na gestão de consequências e nas avaliações partilhadas entre as estruturas da UE e as instituições relevantes dos Estados-membros. A UE melhorará também a sua cooperação cibersecuritária com os parceiros, como são o caso dos Estados Unidos e da NATO, bem como a incorporação, no seu seio, de fortes parcerias público-privadas. Cooperação e partilha de informação entre os Estados-membros, as instituições, o sector privado e a sociedade civil podem fomentar uma cultura comum de segurança cibernética e

---

through a true partnership, between many actors, to take responsibility and meet the challenges ahead" (Comissão Europeia, 2013: 3 e 19) (tradução do autor).

aumentar, dessa maneira, a preparação para possíveis interrupções e ciberataques". (Conselho da União Europeia, 2016a: 21-22)[108]

A regulamentação deste espaço deixou de ser só uma preocupação a nível regional, devido às características transnacionais e mutáveis deste espaço, passando a ser encarada como uma preocupação global e real por parte da UE. Neste mais recente documento estratégico da UE, também a cooperação público-privada foi mencionada como essencial no processo de securitização deste espaço, bem como a já habitual conceção de uma maior cooperação entre os Estados-membros. O desenvolvimento deste ator, bem como a evolução do mesmo, no ciberespaço, já referido no Relatório sobre a Implementação da Estratégia Europeia de Segurança de 2008, ganhou neste conceito estratégico de 2016 um tópico específico sob a definição de 'a desenvolver':

"A UE será um ator cibernético voltado para o futuro protegendo os ativos e os valores críticos, no mundo digital, daqueles que compõem esta união de Estados, promovendo uma Internet global livre e segura. Vamos envolver-nos em diplomacia cibernética e trabalhar na capacitação junto dos nossos parceiros na procura de acordos focados no comportamento responsável por parte dos Estados no ciberespaço - com base no direito internacional existente. Apoiaremos a governança digital multilateral e uma estrutura global de cooperação em segurança cibernética, respeitando o livre fluxo de informações. No ciberespaço, a governança global depende de uma aliança progressiva entre Estados, Organizações Internacionais, indústria, sociedade civil e especialistas técnicos". (Conselho da União Europeia, 2016a: 42-43)[109]

---

[108] Texto original: "The EU will increase its focus on cyber security, equipping the EU and assisting Member States in protecting themselves against cyber threats while maintaining an open, free and safe cyberspace. This entails strengthening the technological capabilities aimed at mitigating threats and the resilience of critical infrastructure, networks and services, and reducing cybercrime. It means fostering innovative information and communication technology (ICT) systems which guarantee the availability and integrity of data, while ensuring security within the European digital space through appropriate policies on the location of data storage and the certification of digital products and services. It requires weaving cyber issues across all policy areas, reinforcing the cyber elements in CSDP missions and operations, and further developing platforms for cooperation. The EU will support political, operational and technical cyber cooperation between Member States, notably on analysis and consequence management, and foster shared assessments between EU structures and the relevant institutions in Member States. It will enhance its cyber security cooperation with core partners such as the US and NATO. The EU's response will also be embedded in strong public-private partnerships. Cooperation and information-sharing between Member States, institutions, the private sector and civil society can foster a common cyber security culture, and raise preparedness for possible cyber disruptions and attacks" (Conselho da União Europeia, 2016a: 21-22) (tradução do autor).

[109] Texto original: "The EU will be a forward-looking cyber player, protecting our critical assets and values in the digital world, notably by promoting a free and secure global Internet. We will engage in cyber diplomacy and capacity building with our partners, and seek agreements on responsible state behaviour in cyberspace based on existing international law. We will support multilateral digital governance and a global cooperation framework on cybersecurity, respecting the free flow of

Em julho de 2016, surge também a proposta para a implementação de um regulamento e de uma diretiva. O regulamento RGPD contava com a demarcação da EUR-Lex - Direito da União Europeia - de "Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados" (Conselho da União Europeia e Parlamento Europeu, 2016 apud EUR-Lex, 2016a) e tem o objetivo explicito de proteger os dados dos cidadãos desta união de Estados de uma maneira regulada e oficial. A diretiva SRI/NIS foi nomeada sob a listagem de "Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União" (Conselho da União Europeia e Parlamento Europeu, 2016 apud EUR-Lex, 2016b). Tem como intuito primário "a obrigação de os Estados-membros adotarem uma estratégia nacional de segurança das redes e dos sistemas de informação, a criação de um grupo de cooperação a fim de apoiar e facilitar a cooperação estratégica e o intercâmbio de informações entre os Estados-membros" (CNCS, 2016).

A evolução da ideologia cibersecuritária no seio da UE em conjugação com os perigos recorrentes do ciberterrorismo e dos ciberataques fizeram com que "a cibersegurança se tornasse um elemento central na infraestrutura digital da Europa e do próprio mercado único digital" (Katainen e Limnell, 2018)[110], com tendência para evoluir cada vez mais com o tempo para o "bom funcionamento do mercado único ser mantido" (Barrinha, 2018)[111]. Isto porque "sem uma indústria europeia de cibersegurança credível e autossuficiente a Europa não terá competitividade digital" algo fundamental para "que as empresas europeias cresçam e se tornem intervenientes no mercado mundial e dessa maneira permaneçam na Europa" (Katainen e Limnell, 2018)[112].

Tendo isto em conta, em junho de 2017 a UE definiu que os atos maliciosos na internet – os ciberataques – seriam a partir daquela data retorquidos de acordo com "o objetivo, a escala, a duração,

information. (...) On cyber, global governance hinges on a progressive alliance between states, international organisations, industry, civil society and technical experts" (Conselho da União Europeia, 2016a: 42-43) (tradução do autor).

[110] Texto original: "Cybersecurity is a core element of Europe's whole digital infrastructure and of the Digital Single Market itself" (Katainen e Limnell, 2018) (tradução do autor).

[111] (continuação) 2º vetor: "económico - bom funcionamento do mercado único" (Barrinha, 2018).

[112] Texto original: "Without a credible and self-sufficient European cybersecurity industry, Europe will lack digital competitiveness. (...) a more developed and dynamic venture capital market and a true single market are key elements to ensure that European companies grow to become global market players - and stay in Europe" (Katainen e Limnell, 2018) (tradução do autor).

a intensidade, a complexidade, a sofisticação e o impacto da atividade cibernética"[113] com a qual teriam de lidar, defendendo e proporcionando dessa maneira a segurança que os Estados-membros mereciam e precisavam (Conselho da União Europeia, 2017)[114]. Ainda em 2017, mais concretamente em setembro, no Discurso sobre o Estado da União Europeia, Jean-Claude Juncker, defendeu a criação de uma agência europeia de segurança cibernética (Juncker, 2017) com o objetivo claro de lidar com a ameaça incessante do ciberterrorismo[115].

No final deste mesmo ano, 2017, o Conselho Europeu solicitou que fosse aplicada uma "abordagem comum para a cibersegurança na UE após a proposta de um pacote de reforma pela Comissão Europeia em setembro" com o intuito de "implementar com celeridade a Diretiva SRI/NIS, abrir portas a inclusão de um sistema de certificação de cibersegurança na UE e criar uma agência de cibersegurança mais forte no seio desta união de Estados" isto porque se "prevê que os ataques informáticos tenham um custo de 400 mil milhões de euros por ano acabando por minar dessa maneira a confiança dos consumidores" (Conselho da União Europeia, 2018) e também dos investidores.

Com isto em mente, durante o dia 8 de junho de 2018 "o Conselho definiu a sua orientação geral sobre o chamado Regulamento Cibersegurança". Esta proposta tem o intuito de "reforçar a ciber-resiliência criando assim um quadro de certificação à escala da UE para os produtos, serviços e processos TIC, tendo também o intento de reforçar a atual Agência da UE para a Segurança das Redes e da Informação (ENISA)" (Conselho da União Europeia, 2018). Ainda durante o ano de 2018, mais concretamente a 25 de maio, o Regulamento Geral sobre a Proteção de Dados (RGPD) foi imposto pela EU e passou a ser implementado por todos os Estados-membros.

A evolução do ciberespaço e os perigos que este acarretou fez com que a preocupação da EU deixa-se de ser exclusivamente focada no futuro, e nos possíveis contratempos deste espaço, passando a ser parte do dia-a-dia deste ator. Ao longo de todos estes anos o investimento foi notório, real e percetível e a verdadeira preocupação ficou espelhada em todos as medidas tomadas neste sentido. Isto

---

[113] Reconhecendo não só desta maneira criminalmente estes crimes e aproximando-se ainda mais da visão da NATO neste espaço, mas também contrariando a visão de Gordon e Ford em 2002 quando disseram que "o ciberterrorismo iria de alguma forma ser tratado separadamente do terrorismo regular" (Gordon e Ford, 2002: 13) (tradução do autor) = Texto original: "The nascent danger in the term cyberterrorism is that cyberterrorism will somehow be dealt with separately to regular terrorismo" (Gordon e Ford, 2002: 13).

[114] Texto original: "The EU diplomatic response to malicious cyber activities will make full use of measures within the Common Foreign and Security Policy, including, if necessary, restrictive measures. A joint EU response to malicious cyber activities would be proportionate to the scope, scale, duration, intensity, complexity, sophistication and impact of the cyber activity" (Conselho da União Europeia, 2017) (tradução do autor).

[115] Até a data de entrega desta dissertação este plano mantinha-se com novas declarações nesse sentido.

reflete também a passagem para uma preocupação global por parte deste ator isto devido a característica transnacional e mutável que esta dinâmica exigia.

3. NATO[116]

"As ameaças e os ciberataques estão a tornar-se mais comuns, mais sofisticados e mais prejudiciais com o passar dos anos. A Aliança enfrenta por isso um complexo ambiente de ameaças e precisa de estar preparada para defender as suas redes e as suas operações contra a crescente sofisticação das ameaças e dos ataques cibernéticos que enfrenta. A NATO e os seus aliados confiam em defesas cibernéticas fortes e flexíveis para cumprir as tarefas de defesa coletiva, de gestão de crises e de segurança cooperativa"

(Conselho do Atlântico Norte, 2018a)[117].

"Os ciberataques representam um claro desafio à segurança da aliança e podem ser tão prejudiciais para as sociedades modernas quanto um ataque convencional"

(Conselho do Atlântico Norte, 2016b)[118].

Duas cimeiras marcaram o início dos trabalhos relativamente à cibersegurança no seio da NATO.[119] A primeira das quais foi a cimeira de Washington, em 1999[120], onde foram "aprovadas duas decisões sobre o levantamento de capacidades de defesa relacionadas com a necessidade de garantir a segurança das comunicações e dos sistemas de informação e com a análise de vulnerabilidades desses sistemas" (IDN, 2013: 59). A segunda foi a cimeira Praga, em 2002, onde foi incluída a segurança da informação como um dos pontos da agenda:

[116] Mais informações em Anexo III.

[117] Texto original: "Cyber threats and attacks are becoming more common, sophisticated and damaging. The Alliance is faced with an evolving complex threat environment. In recent events, cyber-attacks have been part of hybrid warfare. NATO and its Allies rely on strong and resilient cyber defences to fulfil the Alliance's core tasks of collective defence, crisis management and cooperative security" (Conselho do Atlântico Norte, 2018a) (tradução do autor).

[118] Texto original: "Cyber-attacks present a clear challenge to the security of the Alliance and could be as harmful to modern societies as a conventional attack" (Conselho do Atlântico Norte, 2016b) (tradução do autor).

[119] Para uma correta análise do estudo de caso em causa é necessário referir a agência de comunicações e sistemas de informação da NATO (NCSA) que surgiu durante a década de 70 com o objetivo de providenciar um apoio técnico de inteligência, comunicação, vigilância e reconhecimento detalhado a aliança

[120] Os conceitos estratégicos da NATO de 1991 e de 1999 não fazem qualquer referência a ciberdefesa ou ao ciberespaço.

> "Ressaltamos que os nossos esforços para transformar e adaptar a NATO não devem ser compreendidos como uma ameaça por qualquer país ou organização internacional, mas sim como uma demonstração da nossa determinação em proteger as populações, os territórios e as nossas forças de qualquer ataque armado - incluindo qualquer ataque terrorista dirigido do exterior. Estamos determinados em impedir, interromper, defender e proteger ataques dirigidos contra a nossa aliança de acordo com o Tratado de Washington[121] e a Carta das Nações Unidas[122]". (Conselho do Atlântico Norte, 2002b: 2-4)[123]

Cinco anos após a cimeira de Washington, mais concretamente durante o ano de 2004, surge a equipa de resposta a incidentes de segurança informática da NATO (NCIRC) com o objetivo de "dar apoio técnico e legislativo no combate a incidentes de segurança informática da NATO" (Anil, 2004: 4)[124] e onde estavam reunidas serviços tão diversos como: "medidas preventivas (boletins, atualizações de software e equipas de resposta rápida), medidas de resposta (incidentes, suporte e resposta por parte do IDS) e suporte legislativo (forense, investigações e atualização de políticas)". (Anil, 2004: 4)[125]

Enquadrado no NCIRC, durante o ano de 2005 foi proposto que as infraestruturas críticas fizessem parte da agenda contraterrorista da NATO e durante o ano de 2006 foi publicado um "guia para o estabelecimento de prioridades relativas às capacidades de planeamento e informações da NATO" (IDN, 2013: 59) sob o desígnio de orientação política global, levantando um pouco mais o véu sobre a

---

[121] "No dia 4 de abril de 1949, o Tratado do Atlântico Norte é assinado em Washington e a Guerra-Fria entra na sua fase institucional. O artigo 5º determinava que todos os signatários se auxiliassem militarmente caso houvesse um ataque externo a um membro do grupo (...) este organismo internacional nasceu assim através do tratado de Washington e ficou encarregado de coordenar as ações militares dos seus membros. Dizia-se uma aliança defensiva, apesar do termo defesa não constar na sua nomenclatura (Altman, 2012). Disponível na internet em: http://operamundi.uol.com.br/conteudo/noticias/20946/hoje+na+historia+1949+-+e+assinado+em+washington+o+tratado+do+atlantico+norte.shtml

[122] Dicionário da Porto Editora - "A organização das Nações Unidas, constituída em 1945, em substituição da Sociedade das Nações criada pelo Tratado de Versalhes de 1919, foi instituída pelos Estados que acordaram os princípios enunciados na carta das Nações Unidas, discutidos em S. Francisco, a 26 de junho de 1945. Os objetivos primordiais desta organização internacional eram a manutenção da paz e a cooperação social, económica e cultural entre todas as nações que assinaram este compromisso" (Porto Editora, 2003-2018a).

[123] Texto original: "We underscore that our efforts to transform and adapt NATO should not be perceived as a threat by any country or organisation, but rather as a demonstration of our determination to protect our populations, territory and forces from any armed attack, including terrorist attack, directed from abroad. We are determined to deter, disrupt, defend and protect against any attacks on us, in accordance with the Washington Treaty and the Charter of the United Nations" (Conselho do Atlântico Norte, 2002b: 2-4) (tradução do autor).

[124] Texto original: "Technical and Legislative support services to respond to Technical and Legislative support services to respond to computer security incidents within NATO" (Anil, 2004: 4) (tradução do autor).

[125] Texto original: "Centralized Services for: Preventive Measures (bulletins, software updates, VA Teams, etc.), Responsive Measures (Incident & IDS Support and Response) Legislative Support (Forensic, Investigations, Policy Updates)" (Anil, 2004: 4) (tradução do autor).

agenda de cibersegurança da aliança. Durante este mesmo ano, realizou-se mais uma cimeira – a cimeira de Riga – onde as problemáticas do corrente século fizeram parte do leque da agenda a discutir, e onde a cibersegurança não faltou. A "adaptação das forças da NATO" (Conselho do Atlântico Norte, 2006b)[126], no sentido de combaterem o problema que era o cibercrime, foi grande parte do que marcou está cimeira, mas não só: "trabalharemos para desenvolver uma rede confiável, segura e rápida com a capacidade para serem partilhadas informações, dados e inteligência em rede das operações da aliança, melhorando dessa maneira e simultaneamente a proteção dos nossos principais sistemas de informação contra ciberataques". (Conselho do Atlântico Norte, 2006b)[127]

Como vimos anteriormente 2007 foi o ano do ataque à Estónia e devido a esta investida os anos que se seguiram foram prósperos em mudanças no seio da aliança (da mesma maneira que o foi na União Europeia como vimos anteriormente). No pós-ataque a Estónia em 2007 muitos começavam já a considerar esta investida "como a primeira guerra no ciberespaço" (O'Neill, 2016) [128], outros interpretavam-no apenas como um ato de uma magnitude cibernética muito elevada e "um ato relevante mas não determinante, mas definitivamente algo com o qual a NATO não podia brincar" (Santos, 2018). Devido a esta conceção de ideias a NATO, chegou-se a frente e decidiu então que os sistemas digitais e tecnológicos deveriam entrar no seio da segurança coletiva desta instituição (Lene Hansen e Helen Nissenbaum, 2009: 1156).

Ainda durante o ano de 2007, foi estabelecido o conselho de consulta, comando e controlo (NC3B) por parte da NATO. O NC3B ficou responsável pelo "desenvolvimento da política de ciberdefesa e pelo aconselhamento na constante melhoria da ciberdefesa, garantindo também desta forma o apoio ao desenvolvimento do conceito de ciberdefesa da NATO (IDN, 2013: 60).

Em 2008, com a cimeira de Bucareste, "não só a política de ciberdefesa da NATO foi aprovada juntamente com a definição do conceito de ciberdefesa" (IDN, 2013: 60)

---

[126] Texto original: "The adaptation of our forces must continue. We have endorsed a set of initiatives to increase the capacity of our forces to address contemporary threats and challenges (...) work to develop a NATO Network Enabled Capability to share information, data and intelligence reliably, securely and without delay in Alliance operations, while improving protection of our key information systems against cyber-attack" (Conselho do Atlântico Norte, 2006b) (tradução do autor).

[127] Texto original: "The adaptation of our forces must continue. We have endorsed a set of initiatives to increase the capacity of our forces to address contemporary threats and challenges (...) work to develop a NATO Network Enabled Capability to share information, data and intelligence reliably, securely and without delay in Alliance operations, while improving protection of our key information systems against cyber-attack" (Conselho do Atlântico Norte, 2006b) (tradução do autor).

[128] Texto/Discurso original: "When you hear of the worst-case scenarios when it comes to the future of cyberwar, experts are imagining Estonia first when they imagine the future" (O'Neill, 2016) (tradução do autor).

> "A aliança aprovou a sua primeira política de ciberdefesa em janeiro de 2008, logo após os ciberataques contra a Estônia, adaptando-se desta maneira aos desafios e a evolução nesta arena". (Conselho do Atlântico Norte, 2016a: 23)[129]

Como também foi estabelecido um centro de ciberdefesa em Bruxelas - autoridade para a gestão da defesa cibernética da NATO (NCDMA). Este tinha como "objetivo coordenar as respostas aos ciberataques, se assim fosse a vontade das autoridades nacionais de ciberdefesa. Também tinha o objetivo de desenvolver e de sugerir padrões e procedimentos para que as organizações nacionais e as equipas de ciberdefesa da NATO pudessem prevenir, detetar e impedir ataques cibernéticos" (Grant, 2008)[130].

Com a política de ciberdefesa e com o NCDMA surge também o centro de excelência da NATO (CCDCOE), situado em Tallinn. Este surge como o "quartel general" para a ciberdefesa em finais de 2008 (depois de anos de discussão entre os Estados-membros) (Herzog, 2011: 55)[131]. Com este centro surge também o *cyber coalition* - exército focado na ciberdefesa da NATO, dos seus integrantes e dos seus aliados. Tem também o intuito de preparar exercícios e treinos conjuntos com os Estados para dessa maneira estarem preparados para eventuais atividades cibercriminosas.

O CCDCOE "foca-se particularmente na pesquisa e no desenvolvimento de contramedidas para a defesa atempada e eficaz contra ciberataques e no fornecimento de treino as equipas responsáveis pela defesa cibernética" (Grant, 2008)[132]. Tem como missão principal "melhorar constantemente a capacidade, a cooperação e a partilha de informações entre a NATO, as nações integrantes da NATO e os parceiros - no que a ciberdefesa diz respeito - através da educação, da pesquisa e do desenvolvimento nas diversas áreas a esta anexada. O seu objetivo primário é ser a principal fonte de conhecimento no campo de defesa cibernética cooperativa, acumulando, criando e disseminando conhecimento em diferentes temáticas dentro da NATO, nas nações integrantes da NATO e nos parceiros associados a

[129] Texto original: "The Alliance approved its first cyber defence policy in January 2008, shortly after major cyber-attacks against Estonia, and has adapted to the evolving challenges in this arena" (Conselho do Atlântico Norte, 2016a: 23) (tradução do autor).

[130] Texto original: "The CDMA will co-ordinate responses to attacks if invited by national cyberdefence authorities. It will also develop and propose standards and procedures for national and Nato cyberdefence organisations to prevent, detect and deter attacks" (Grant, 2008) (tradução do autor).

[131] Texto original: "NATO Cooperative Cyber Defence Centre of Excellence (CCD CoE), the Atlantic Alliance's cyber-security headquarters headquarters" (Herzog, 2011: 55) (tradução do autor).

[132] Texto original: "The Estonia centre of excellence will research and develop counters to cyberattacks, and provide training to cyberdefence staff" (Grant, 2008) (tradução do autor).

esta". (Site Oficial do CCDCOE, 2008-2018)[133]. Este foi estrategicamente colocado no local onde o maior ataque cibernético da história aconteceu, o que desde logo denota o simbolismo e a importância do local para a NATO, mas também a completa confiança nas suas capacidades não temendo o local ou o que aconteceu no mesmo.

Na cimeira de Lisboa em 2010 foi aprovado o novo Conceito Estratégico da NATO e com este a assimilação da "ciberdefesa como uma capacidade prioritária da Aliança" bem como a "revisão da política de ciberdefesa da NATO"[134] (IDN, 2013: 60). Este espaço ganhou então lugar no conceito estratégico de 2010 onde foi um dos novos temas na agenda desta organização internacional. No ponto 12 referente ao ambiente securitário da NATO está exposto o seguinte:

> "Os ciberataques estão a tornar-se mais frequentes, mais organizados e mais dispendiosos relativamente aos danos que infligem às administrações governamentais, as empresas, as economias e potencialmente também às redes de transporte e de fornecimento, bem como a outras infraestruturas críticas; podem atingir um limiar que ameaça a prosperidade, a segurança e a estabilidade nacional e euro-atlântica. As forças armadas e os serviços de inteligência estrangeiros, os grupos organizados, os grupos terroristas e/ou extremistas podem ser, cada um deles, a fonte de tais ataques". (Conselho do Atlântico Norte, 2010: 11)[135]

É notória também neste conceito estratégico a preocupação em prevenir e defender qualquer ciberataque no espaço regional de todos os membros da NATO, para que nunca mais se viva algo parecido como o que foi vivido na Estónia.[136] Como explicito em um dos pontos da secção 19 deste Conceito Estratégico:

---

[133] Texto original: "Our mission is to enhance the capability, cooperation and information sharing among NATO, NATO nations and partners in cyber defence by virtue of education, research and development, lessons learned and consultation. Our vision is to be the main source of expertise in the field of cooperative cyber defence by accumulating, creating, and disseminating knowledge in related matters within NATO, NATO nations and partners" (Site Oficial do CCDCOE, 2008-2018) (tradução do autor).

[134] Em 2011 surgiu a "revisão da política de ciberdefesa da NATO e o plano de ação para a sua implementação" (IDN, 2013: 60).

[135] Texto original: "Cyber-attacks are becoming more frequent, more organised and more costly in the damage that they inflict on government administrations, businesses, economies and potentially also transportation and supply networks and other critical infrastructure; they can reach a threshold that threatens national and Euro-Atlantic prosperity, security and stability. Foreign militaries and intelligence services, organised criminals, terrorist and/or extremist groups can each be the source of such attacks" (Conselho do Atlântico Norte, 2010: 11) (tradução do autor).

[136] Esta preocupação com a correta proteção e securitização dos Estados-membros da aliança é clara isto porque, a NATO tem a necessidade de referir, num dos pontos da secção 19 deste mesmo conceito estratégico, que todos os esforços serão

> "Desenvolveremos ainda mais a nossa capacidade de prevenir, detetar, defender e recuperar de ciberataques, através do processo de planeamento da NATO para melhorar e coordenar as capacidades nacionais de defesa cibernética, colocando todos os organismos da NATO sob proteção cibernética centralizada e integrando melhor a consciência cibernética da NATO, de alerta e resposta, com as nações membros". (Conselho do Atlântico Norte, 2010: 16-17)[137]

Durante o ano de 2012, e com a cimeira de Chicago, a NATO "iniciou a revisão da sua política de segurança da informação que agora também passou a incluir a ciberdefesa"[138] (IDN, 2013: 60) alargando assim o leque das prioridades defensivas da aliança e reafirmando a cooperação com a UE. Além da estabilização da NCIRC[139], surge também no seio desta OI a agência de comunicação e informação da NATO (NCIA), convergindo em si 3 agências (agência de gestão do sistema de comando e controlo aéreo da NATO (NACMA), o conselho de consulta, comando e controlo (NC3A) e a agência de comunicações e sistemas de informação da NATO (NCSA)) (Site Oficial da NCIA, 2012-2018) tinha como função principal, "vinte e quatro horas por dia, conectar a aliança, defender as suas redes, fornecer apoio rápido às operações e missões da NATO, fornecer apoio em áreas críticas como: a tecnologia de comando e controlo para a defesa antimísseis balísticos da NATO, o sistema de comando e controlo aéreo (ACCS), apoio à iniciativa de ISR conjunto da NATO e as redes de missões federadas (FMN), assistir a aliança e as nações parceiras nos projetos bilaterais e multinacionais no desenvolvimento das capacidades interoperáveis e de custo efetivo na área do C4ISR, dar apoio as nações na certificação dos seus elementos das forças de reação - reutilizando as soluções experimentadas e testadas no Afeganistão" (Site Oficial da NCIA, 2012-2018)[140].

---

feitos para que a sua capacidade tecnológica evolua de acordo com este mesmo espaço, para que assim este espaço não se torne o local perfeito para o crime perfeito.

[137] Texto original: "Develop further our ability to prevent, detect, defend against and recover from cyberattacks, including by using the NATO planning process to enhance and coordinate national cyber-defence capabilities, bringing all NATO bodies under centralized cyber protection, and better integrating NATO cyber awareness, warning and response with member nations" (Conselho do Atlântico Norte, 2010: 16-17) (tradução do autor).

[138] Processo este que se iniciou um ano antes, em 2011, com a um plano para a "revisão da ciberdefesa e a sua implementação" (IDN, 2013: 60).

[139] Em 2014 a NCIRC atingiu o seu potencial máximo sendo capaz de proteger mais e melhor a rede da NATO e das respetivas nações integrantes, bem como a dos aliados.

[140] Texto original: "The Agency has a 24/7 mission to: Connect the Alliance, defend its networks, provide rapid support to NATO operations and missions, deliver critical capabilities, including: the command and control technology for NATO's ballistic missile defence, the Air Command and Control System (ACCS), support to NATO's Joint ISR Initiative and Federated Mission Networking (FMN), through bilateral and multinational projects assist NATO and Partner Nations in developing interoperable

Durante a cimeira de Gales em 2014 os Ministros da Defesa dos países integrantes da NATO "endossaram uma nova política de defesa cibernética e um plano de ação que, juntamente com a política, contribui para o cumprimento das principais tarefas da Aliança" (NATO, 2018)[141] para que exista dessa maneira uma maior clarividência sobre as tarefas e as responsabilidades dos aliados no que a ciberdefesa diz respeito. Durante essa mesma cimeira os aliados "reconheceram as leis internacionais como parte do ciberespaço, visto serem os ciberataques tão perigosos quanto os ataques convencionais" (Conselho do Atlântico Norte, 2018b)[142].

Dois anos depois, durante a cimeira de Varsóvia em 2016, os Ministros da Defesa dos países integrantes da aliança "aprovaram a atualização relativamente a ciberdefesa (requisitada durante a cimeira de Gales), bem como um guia técnico para a implementação do ciberespaço como um domínio operacional" na expetativa de assim "aumentarem a sua capacidade de trabalho em equipa e desenvolverem, dessa maneira, as suas capacidades técnicas bem como a partilha constante de formação" (Conselho do Atlântico Norte, 2016b)[143].

Nesta mesma cimeira, vários acordos cooperativos entre a NATO e a UE foram estabelecidos em várias das áreas ligadas a ciberdefesa, "numa procura de apoiar e ajudar ambas as organizações a prevenir e a responder melhor aos ciberataques. O acordo técnico entre o NCIRC e a equipa de resposta a emergências da UE (a CERT-UE) fornece um quadro para a troca de informações e partilha de práticas entre as equipas de resposta a emergências cibernéticas" (Conselho do Atlântico Norte, 2016d)[144].

---

and cost-effective capabilities in the area of C4ISR and support nations in cost-effective certification of their NATO Response Force elements by re-using solutions tried and tested in Afghanistan" (Site Oficial da NCIA, 2012-2018) (tradução do autor).

[141] Texto original: "At the Wales Summit in September 2014, Allies endorsed a new cyber defence policy and approved an action plan which, along with the policy, contributes to the fulfilment of the Alliance's core tasks. The policy and its implementation is under close review at both the political and technical levels within the Alliance and will be refined and updated in line with the evolving cyber threat" (NATO, 2018) (tradução do autor).

[142] Texto original: "At the 2014 NATO Summit in Wales, Allies recognised that international law applies in cyberspace, and that the impact of cyber-attacks could be as harmful to our societies as a conventional attack" (Conselho do Atlântico Norte, 2018b) (tradução do autor).

[143] Texto original: "Now, in Warsaw, we reaffirm NATO's defensive mandate, and recognise cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea (...) Interoperability of our armed forces is fundamental to our success and an important added value of our Alliance. Through training and exercises, the development of NATO standards and common technical solutions" Conselho do Atlântico Norte, 2016b) (tradução do autor).

[144] Texto original: "NATO and the European Union face similar challenges in protecting their networks against the growing threat of cyber-attacks. To help both organisations better meet this challenge, today a Technical Arrangement on Cyber Defence was concluded between the NATO Computer Incident Response Capability (NCIRC) and the Computer Emergency Response Team of the European Union (CERT-EU). The Technical Arrangement provides a framework for exchanging information and sharing best practices between emergency response teams" (Conselho do Atlântico Norte, 2016d) (tradução do autor).

Entre as várias medidas acordadas, encontram-se "o combate as ameaças híbridas, a defesa cibernética e a capacidade para tornar o espaço comum mais estável e seguro". "No que a defesa cibernética diz respeito, a NATO e a UE fortaleceram a sua participação mútua em exercícios conjuntos promovendo também a pesquisa, os treinos e a partilha de informações" (Conselho do Atlântico Norte, 2016c)[145].

> "Os aliados aprovaram o ciberespaço como um domínio para as operações da NATO (além disto também elogiaram os esforços para a normatização e a estabilização deste espaço). Estes também se comprometeram a aprimorar as defesas cibernéticas das suas redes nacionais e infraestruturas como uma questão de prioritária" (Conselho do Atlântico Norte, 2016b)[146].

Durante o ano de 2017, foi aprovada a criação de um novo centro de operações cibernéticas (NCIRC) em Bruxelas na Bélgica (além do já existente em Haia na Holanda) por parte dos Estados-membros. Este tem o intuito de:

> "Partilhar informações em tempo real sobre ameaças cibersecuritárias através de uma plataforma dedicada a repartição de informações sobre *malware*, bem como melhores práticas no tratamento de ameaças cibernéticas; gerir as equipas cibersecuritárias de reação rápida (que podem ser enviadas para ajudar os aliados no tratamento de ciberataques); desenvolver metas para facilitar uma abordagem comum às capacidades de defesa cibernética dos aliados; investir em educação, treino e exercícios". (Conselho do Atlântico Norte, 2018b)[147]

---

[145] Texto original: "The overall goal of NATO and EU remains the same: maintain peace and stability and promote security for our citizens (...) acting on the decisions adopted by our Heads of State and Government at our Summit in Warsaw, while fully preserving the foundation of the cooperation between our two organisations established almost two decades ago, we have decided, as a first step, to strengthen our strategic partnership in concrete areas including countering hybrid threats; operational cooperation including maritime issues; cyber security and defence; defence capabilities; defence industry and research; exercises; and defence and security capacity building" (Conselho do Atlântico Norte, 2016c) (tradução do autor).

[146] Texto original: "In July 2016, Allies reaffirmed NATO's defensive mandate and recognised cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land and at sea. Allies also made a Cyber Defence Pledge in July 2016 to enhance their cyber defences, as a matter of priority" (Conselho do Atlântico Norte, 2016b) (tradução do autor).

[147] Texto original: "Sharing real-time information about threats through a dedicated malware information sharing platform, as well as best practices on handling cyber threats; Maintaining rapid-reaction cyber defence teams that can be sent to help Allies in handling cyber challenges; Developing targets for Allies to facilitate a common approach to their cyber defence capabilities; Investing in education, training and exercises, such as Cyber Coalition, one of the largest cyber defence exercises in the world" (Conselho do Atlântico Norte, 2018b) (tradução do autor).

Em março de 2017, a NATO declarou que irá fazer um investimento de 2,6 biliões de libras em satélites, segurança cibernética e drones (Mortimer, 2017) e tendo isto em conta o ano de 2017, este promete ser um ano ainda mais atarefado para a NATO, no que a ciberdefesa diz respeito. O comprometimento com a ciberdefesa é uma vontade real da aliança e os esforços passam mesmo pelo treino e pelo desenvolvimento operacional como demonstra o *cyber range* da NATO.

> "Sediado em Tartu, na Estónia, o *cyber range* é utilizado por especialistas ligados a área cibernética com o intuito de desenvolver as suas capacidades através de exercícios realistas. O *cyber range* facilita o exercício anual de defesa cibernética do *cyber coalition* da NATO". (Conselho do Atlântico Norte, 2018b)[148]

Durante o ano vigente de 2018, não só foi aprovada a construção de uma academia de comunicação e informação em Oeiras, Portugal[149] (Conselho do Atlântico Norte, 2018b), como também foi realizada, durante o mês de julho, a cimeira da NATO em Bruxelas. Mais uma vez esta cimeira contou com uma declaração conjunta da UE e da NATO onde foi reiterada a cooperação em áreas diversas, como é o caso da cibersegurança, e a "a investigação na indústria de defesa, a cibersegurança e o apoio aos parceiros de Leste e Sul são pontos também em destaque" (Diário de Notícias, 2018).

A interpretação do cibercrime como uma ameaça é grande parte daquilo que fica explicito ao longo dos anos no seio da NATO e dos seus protocolos, conferências e agências. Fica também explanada na maneira de se exprimir, atuar, defender e desenvolver as suas atividades e defesas neste espaço. O cibercrime é claramente visto como uma ameaça e algo a aniquilar por parte desta OI.

---

[148] Texto original: "The NATO Cyber Range in Tartu, Estonia, is used by cyber experts to develop their capabilities through realistic exercises. The Cyber Range facilitates NATO's flagship annual cyber defence exercise 'Cyber Coalition'" (Conselho do Atlântico Norte, 2018b) (tradução do autor).

[149] "Uma vez concluída e a funcionar (em 2019), a Academia vai treinar milhares de civis e militares por ano e contribuir assim para as defesas cibernéticas da NATO. A Escola da NATO em Oberammergau, Alemanha, também realiza formação e treino na mesma área cibernética, com o objetivo de apoiar as operações, a estratégia, a política, a doutrina e os procedimentos da Aliança" (Conselho do Atlântico Norte, 2018b) (tradução do autor) = Texto original: "The NATO Communications and Information Academy is being built in Oeiras, Portugal. Once up and running in 2019, the Academy will train thousands of civilian and military personnel a year, and make a major contribution to NATO's cyber defences. The NATO School in Oberammergau, Germany also conducts cyber-related education and training to support Alliance operations, strategy, policy, doctrine and procedures" (Conselho do Atlântico Norte, 2018b).

4. As Estratégias Contra Ataques Cibernéticos da União Europeia e da NATO

Neste último capítulo iremos comparar ambos os atores em análise, tendo em conta tudo aquilo que os conecta neste campo tecnológico, bem como cravar bandeiras no presente e analisar os possíveis contratempos que podem surgir nesta jornada cibersecuritária.

4.1 Perspetiva Comparada

"A cooperação UE-NATO neste período de crise global é cada vez mais importante. No campo da cibersegurança, e da defesa no geral, os últimos anos foram fundamentais no que a este campo em particular diz respeito. Estas questões fazem parte da UE e da NATO há muito tempo, mas só recentemente se mudaram para o topo das suas agendas"

(Lété e Pernik, 2017: 1)[150].

Cronologicamente falando a NATO chegou primeiro a conclusão que os sistemas de informação e comunicação precisariam de segurança. Isto sucedeu na cimeira de Washington em 1999, enquanto que a União Europeia só abordou o problema em 2001 na Convenção Europeia do Cibercrime em Budapeste. Porém ao longo da análise dos documentos estratégicos das duas organizações é visível a vontade de ambos em se responsabilizarem por este espaço anárquico, transnacional e global, tornando-se mesmo este o principal foco dos respetivos documentos estratégicos. O esforço de ambas as Organizações Internacionais, e dos seus Estados-membros, em sugerir a aplicação de normas e regras neste espaço anárquico é notório e percetível.

A motivação inconstante dos *hackers* é considerada e absorvida de forma similar por parte de ambos os atores. Isto porque esta pode variar dentro da dinâmica de destruição gratuita e fortuita de

[150] Texto original: "EU–NATO cooperation in this time of global crisis is increasingly important. In the field of cybersecurity and defence the past years have indeed been pivotal. These issues have long been part of EU and NATO calculus but have only recently moved to the top of their agendas" (Lété e Pernik, 2017: 1) (tradução do autor).

instituições fundamentais para os Estados-membros, tendo dois possíveis e bem diferenciados intuitos em mente por parte destes. O primeiro dos quais será obterem algum tipo de fim lucrativo, e a consequente perca monetária por parte do visado (ou mesmo, e só, pela adrenalina do ato em si) – comum ciberataque focado no benefício próprio (ato privado) (Barrinha, 2018). O segundo é mais focado na transmissão de uma mensagem política – ciberterrorismo (Barrinha, 2018).

É percetível então o porquê de ambos os atores serem forçados a garantir que são capazes de lidar com este problema díspar e que mediante este será feito um investimento para isto continue assim no futuro. Grande parte daquilo que é o discurso promovido nos Documentos Estratégicos destes dois atores resulta numa apreensão com as perdas monetárias e intelectuais resultantes de um ciberataque - ou através de um ato de ciberterrorismo em si - tanto para com as empresas públicas como para com as privadas.

> "Nos últimos dois anos o custo com os cibercrimes cresceu e é agora 23% maior do que no ano de 2016. Isto esta a custar as às organizações, em média, 11,7 milhões de dólares anualmente". (Ponemon Institute LCC e Accenture, 2017: 3)[151]

O foco na cooperação também é muito visado por ambos os atores e revela desde logo a impossibilidade - tanto da UE como da NATO - em lidarem com um problema desta magnitude sozinhos - fechados na sua própria jurisdição - devido sobretudo a característica mutável, irreverente, contemporânea e transnacional do ciberespaço.

Dentro destas duas categorias principais algumas ideias base são inerentes a ambos os atores, a proteção e a vontade de se responsabilizarem por este espaço transnacional e global e a aplicação de normas a nível transnacional - com o objetivo de controlarem e defenderem o ciberespaço (um fenómeno sem fronteiras).

Dentro desta ideia Bruno Lété e Piret Pernik afirmam que o "desenvolvimento de uma legislação baseada na confiança por parte da UE e da NATO não seria uma ideia tão descabida de ser almejada" criando assim dessa maneira condições para a "aplicação do direito internacional e com este o desenvolvimento de normas globais em torno do comportamento dos Estados no ciberespaço" (Lété e

[151] Texto original: "Over the last two years, the accelerating cost of cybercrime means that it is now 23 percent more than last year and is costing organizations, on average, US$11.7 million" (Ponemon Institute LCC e Accenture, 2017: 3) (tradução do autor).

Pernik, 2017: 7)[152] algo que a data é apenas um sonho mas que muitos ser uma prioridade em todos os aspetos (Euronews, 2018).

Existe uma latente convergência de ideias, dinâmicas e vontades entre ambos os atores aqui analisados, não só porque ambos se intercetam em muitos pontos que definem as suas agendas cibersecuritárias, mas também devido ao facto de ambos contarem com muitos dos mesmos associados.

> "Ao nível nacional, os governos dos Estados membros europeus, tiveram de tomar medidas para desenvolver as suas políticas de segurança cibernética, ao mesmo tempo que faziam valer a sua soberania através da NATO e da União Europeia – tudo isto com o intuito de reforçar as suas defesas individualmente e coletivamente". (Ilves et al, 2016: 127)[153]

Para muitos dos interessados na matéria, a "União Europeia continua a crescer geminada e ligada a NATO desde a sua criação" (Goulão, 2017), o que implica uma atuação idêntica a esta em todas as áreas em que estas se intercetam, a cibersegurança não é exceção, e os exemplos partem desde os mais pequenos pontos da agenda até a criação de uma estrutura completa em torno da problemática.

É percetível uma maior organização, simplicidade e foco na problemática da ciberinsegurança por parte da NATO, com uma agenda operacional sem bloqueios, enquanto a agenda da UE sofre muito com a resistência dos Estados-membros e com a falta de organização destes (Barrinha, 2018) - percetível pelas muitas retificações, atrasos e críticas na tomada de decisão (Santos, 2018).

Apesar de contarem com um núcleo central focado nas mesmas problemáticas no combate a ciberinsegurança, existe uma clara separação de práticas por parte de ambos os atores em análise, bem presente e bem esclarecida por parte da UE e da NATO (apesar de serem parcos em explicações mais concisas relativamente as mesmas):

> Ciberdefesa - NATO: "Esta é uma medida proativa para detetar ou obter informações sobre invasões no ciberespaço, ciberataques ou operações cibernéticas iminentes ou uma tentativa de determinar a

[152] Texto original: "In this light, the development of a Joint EU–NATO Cyber Trust fund may not be such a far-fetched idea (...) lead application of international law and development of global norms around state behavior in cyberspace" (Lété e Pernik, 2017: 7) (tradução do autor).

[153] Texto original: "European governments have had to take steps to develop cybersecurity policies at the national level while simultaneously pooling their sovereignty through the North Atlantic Treaty Organization (NATO) and the European Union (EU) to bolster their defences" (Ilves et al, 2016: 127) (tradução do autor).

origem de uma operação através de manobras preventivas, antecipatórias ou de contra-ataque cibernético contra um ou vários alvos". (Site Oficial do CCDCOE, 2008-2018)[154]

Cibersegurança - União Europeia: "A cibersegurança geralmente refere-se às salvaguardas e as ações utilizadas para proteger o domínio do ciberespaço de ameaças associadas ou que possam prejudicar as redes e infraestruturas de informações interdependentes, tanto no campo civil quanto no campo militar. A cibersegurança esforça-se para preservar a disponibilidade e a integridade das redes e das infraestruturas, bem como a confidencialidade das informações nelas contidas". (Comissão Europeia, 2013: 3)[155]

A exclusiva preocupação da NATO no ciberespaço é com a ciberdefesa e com a perda de soberania de um Estado as mãos de um ataque cibernético ou de um ato de ciberterrorismo (forças armadas) (Santos, 2018). A União Europeia preocupa-se mais com a cibersegurança, o bem-estar e a liberdade de cada um de nós – indivíduo - no ciberespaço (policiamento) (Santos, 2018), não descurando também ela a ciberdefesa.

Enquanto que a União Europeia, num intuito mais proativo em relação a cibersegurança, conta com a Europol - e com o centro por esta criado a EC3 - e com a ENISA para proteger os seus cidadãos, empresas e respetivos Estados-membros destes criminosos sem rosto (EUROPOL Website Oficial, 2013-2018), a NATO, como organização internacional focada na defesa, foca-se quase exclusivamente na ciberdefesa e conta para isso com um exército – o Cyber Coalition – focado exclusivamente na luta contra o ciberterrorismo e contra os ciberataques (Leite, 2016: 14) e com o CCDCOE, a NCDMA, a NCIA e a NCIRC.

Está claro o foco de ambos os atores nesta área bem como a vontade destes em tentarem controlar e combater o cibercrime no presente, mas o que é expetável quanto ao futuro nesta área? Isso é algo muito difícil de antecipar (devido sobretudo a mutabilidade e a inconsistência deste espaço) mas algo parece certo, tanto a UE como a NATO parecem ter-se mentalizado que não só os cibercrimes irão

[154] Texto original: "A proactive measure for detecting or obtaining information as to a cyber intrusion, cyber-attack, or impending cyber operation or for determining the origin of an operation that involves launching a preemptive, preventive, or cyber counter-operation against the source" (CCDCOE, 2008-2018) (tradução do autor).

[155] Texto original: "Cyber-security commonly refers to the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cyber-security strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein" (Comissão Europeia, 2013: 3) (tradução do autor).

continuar a ser uma ameaça no futuro, mas também será neste campo que as guerras se desenrolarão nos próximos anos (Agência Europeia de Defesa, 2017: 1; Conselho do Atlântico Norte, 2018a). Algo que o Professor Doutor Henrique Santos afirma inclusive já ter acontecido no passado - "como são os casos da Geórgia em 2008 ou mesmo das várias tentativas de atacar o Irão neste espaço ao longo dos anos. Isto porque não importa se foi um drone[156] que carregou uma bomba ou uma pen[157] que transportou um vírus se o objetivo final for o mesmo, fazer guerra" (Santos, 2018).

Segundo Dan Smith, em entrevista ao instituto internacional de pesquisas sobre a paz de Estocolmo (SIPRI), "todas as tecnologias e inovações do presente tornar-se-ão antiquadas em poucos anos e devido a isso o momento certo para todos nós nos sentarmos e conversarmos sobre todas estas problemáticas que rodeiam o ciberespaço é agora, antes de nos apercebermos que é tarde demais" (Dan Smith, 2018 apud SIPRI, 2018). O Coronel Nuno Lemos Pires corrobora com esta ideia quando afirma que existe uma aceleração tecnológica que não sabemos acompanhar, devido sobretudo a época em que vivemos onde os aparelhos digitais se tornam obsoletos em poucos minutos (Pires, 2017 apud II Seminário IDN Jovem, 2017). O que torna ainda mais proeminente e urgente uma solução eficaz para a problemática sendo que uma cooperação sólida e eficaz entre a União Europeia e a NATO ajudaria em todos os aspetos.

É compreensível que no futuro as ameaças poderão não só partir de elementos sem rosto escondidos atrás de um monitor, mas talvez mesmo de Estados ou organizações outrora regidos/as pelo Neoliberalismo económico e pela globalização. Algo que pode mudar a maneira como compreendemos o mundo e transportar-nos para uma nova era: a era da ciberguerra.

> "Não posso deixar de dar grande destaque à necessidade absoluta da criação de mecanismos de cooperação estreitos, ágeis e operacionais entre todas as entidades com responsabilidades nesta matéria que atravessa fronteiras nacionais, mas também transpõe fronteiras institucionais e de competências[158] (Monteiro[159], 2017 apud Público, 2017).

---

[156] Veículo aéreo não tripulado.

[157] Dispositivo de memória com o objetivo de armazenar conteúdos digitais.

[158] "(O tema da cibersegurança foi debatido no dia 9 de janeiro de 2018 numa audiência pública que decorreu em Bruxelas e que faz parte do processo de consultas relativo a esta questão) A conclusão deste relatório é que temos de cooperar com certos países e identificar melhor os parceiros no ocidente, aumentando a cooperação com os Estados Unidos, o Japão, a Índia, Israel e outros países - desenvolver significa defendermo-nos melhor num contexto de conflito digital" (Mazzola , 2018 apud Euronews, 2018).

[159] Artur Neves Pina Monteiro: ex-chefe do Estado-Maior General das Forças Armadas entre 2014 e 2018.

O presente e possivelmente o futuro da cibersegurança, podem ver-se ainda moldados por aquilo que são as novas dinâmicas no mundo atual: o processo de saída do Reino Unido da UE e a eleição Donald Trump.

4.2 Processo de Saída do Reino Unido da União Europeia e a Eleição de Donald Trump

"O Brexit pode ter duas abordagens distintas - uma negativa: a União Europeia deixará de poder contar com o know-how do Reino Unido, e uma positiva: esta união de Estados ver-se-á obrigada a integrar novos países e atores nesta área da cibersegurança"

(Barrinha, 2018).

"Quando estamos a pagar, mas mais ninguém o faz, a exceção de alguns países, sentimo-nos maltratados e ofendidos"

(Trump, 2016 apud Hardt, 2017: 121)[160].

Tanto a União Europeia como a NATO podem sofrer mudanças políticas e estratégicas devido a dois fatores em particular: o processo de saída do Reino Unido da União Europeia e a eleição de Donald Trump. No dia 23 de junho de 2016, a população britânica, e no seguimento de um referendo acerca da permanência deste ator na União Europeia, confirmou a intenção do Reino Unido deixar de integrar esta União de Estados e seguir um caminho independente da UE (comumente conhecido como *Brexit*) deixando de integrar esta em todas as áreas comuns inclusive na área da cibersegurança. No dia 8 de novembro de 2016 Donald Trump foi eleito o 45º presidente do EUA prometendo ao longo da sua campanha cortar com as subvenções e as despesas avolumadas que os Estados Unidos da América tinham para com a NATO, afirmando mesmo que "os membros da aliança deveriam começar a contribuir com a sua quota parte nas despesas da segurança deste ator e cumprir assim dessa maneira com as

[160] Discurso original: "When we're paying and nobody else is really paying, a couple of other countries are but nobody else is really paying, you feel like the jerk" (Trump, 2016 apud Hardt, 2017: 121) (tradução do autor).

suas obrigações financeiras" isto porque segundo este "23 dos 28 países membros ainda não pagam o que deveriam pagar pela sua defesa" (Trump, 2017 apud The New York Times, 2017)[161]. Ainda durante o ano corrente de 2018 Donald Trump voltou a criticar a aliança transatlântica na cimeira do G7[162], no Quebec Canadá, afirmando que está era "tão má quanto o NAFTA[163]" (Expresso, 2018).

De maneira clara percebemos que ambas as dinâmicas influenciarão os atores em análise. No entanto ao passo que o *Brexit* poderá acabar por afetar mais a União Europeia, a presidência de Donald Trump poderá acabar por influenciar mais a abordagem da NATO. O que não sabemos é a intensidade com que esta se manifestará nem de que maneira afetará (positiva ou negativamente), o que sabemos é que tanto uma problemática como a outra poderão tornar o ciberespaço ainda mais um território sem lei.

Para o Professor Doutor Henrique Santos, tanto o *Brexit* como Donald Trump irão ter uma influência mínima nas dinâmicas da UE e da NATO isto porque, e segundo este, é verdade que "a questão da cibersegurança não pode ser interrompida por fronteiras terrestres e o Reino Unido não o pode fazer saindo desta união de Estados" mas ainda assim "ambas as dinâmicas são questões meramente políticas e apesar de existir um decréscimo nos apoios financeiros neste campo, este sempre recebeu um apoio muito reduzido e a partir daí a influência do *Brexit* e da presidência de Donald Trump não é muito limitadora neste aspeto" (Santos, 2018).

Já para o Professor Doutor André Barrinha esta problemática pode ser vista de duas maneiras: uma negativa e outra positiva (como vimos no início) isto porque, e focando-nos no lado positivo, "o Reino Unido serviu muitas vezes de travão nas matérias de segurança e defesa o que vai possibilitar, agora com a sua saída, a integração de novos Estados membros e de novas ideias neste campo e nesta matéria" já em contrapartida "o Reino Unido tinha (e continua a ter) um papel muito importante em muitas áreas, a segurança é uma delas, e o seu conhecimento e as sua competências farão muita falta a União Europeia"[164] (Barrinha, 2018).

---

[161] Discurso original: "NATO members must finally contribute their fair share and meet their financial obligations, for 23 of the 28 member nations are still not paying what they should be paying and what they're supposed to be paying for their defense" (Trump, 2017 apud The New York Times, 2017) (tradução do autor).

[162] "É um grupo informal composto por sete países, entre estes estão as maiores e as mais industrializadas economias do mundo. Estes países também possuem uma grande influência estratégica, política e militar no mundo. Fazem parte do G7 os seguintes países: Estados Unidos da América, Canadá, Alemanha, Japão, França, Reino Unido e Itália" (Mariz, 2008 apud Sua Pesquisa.com, 2004-2018).

[163] "Acordo de comércio livre entre os EUA, o Canadá e o México" (Expresso, 2018).

[164] Relativamente a Donald Trump não foram tecidos quaisquer comentários.

Sven Biscop, de maneira muito similar ao Professor Doutor André Barrinha, enumera os possíveis benefícios e contratempos desta saída do Reino Unido da União Europeia. Para este a parte positiva desta problemática é o facto de "Londres não ter mais, nem os argumentos nem a importância para poder impedir os restantes Estados-membros de utilizarem as instituições e as disposições desta união de Estados em toda a sua extensão, competindo agora as outras capitais o aceleramento do processo de cooperação para que possam provar que não se estavam a esconder convenientemente atrás das objeções britânicas, sendo sérios em relação a defesa europeia" (Biscop, 2016: 432)[165]. Este autor não esquece também os possíveis contratempos do *Brexit* e "sendo o Reino Unido um dos mais importantes atores em termos militares, a arquitetura de segurança europeia pode vir a sofrer com a sua saída causando dessa maneira uma assimetria (no que a segurança e defesa diz respeito) entre a União Europeia e a NATO" (Biscop, 2016: 443)[166].

Tudo isto não indica claramente que a União Europeia e o Reino Unido irão deixar de cooperar. Muito pelo contrário possivelmente irão ter mesmo que colaborar em várias matérias e mesmo em algumas áreas (através de contactos bilaterais entre o Reino Unido e os Estados-membros que a compõem) (Barrinha, 2018; Moran, 2017: 68)

Também não é claro que que Donald Trump mudará o seio da NATO com os cortes anunciados e com as constantes críticas. Isto porque "é importante lembrar que a aliança resistiu a crises e a divisões antes e sobreviveu, continuando a operar devido a sua capacidade em se adaptar às realidades em mudança" (Kaufman, 2017: 266)[167].

A verdade é que também não sabemos muito bem se os cenários negativos antecipados não serão também eles uma triste e futura realidade, neste momento "resta-nos negociar e esperar que as coisas aconteçam para se saber os desafios que nos podem esperar" (Svendsen, 2017: 111). Para já apenas é percetível que as coisas irão deixar de ser iguais, tanto na União Europeia como na NATO, não sabemos muito bem ainda é em que sentido irá ser diferente.

---

[165] Texto original: "London will no longer be in a position to block the remaining Member States from using EU institutions and Treaty provisions to the full. It is now up to the other capitals to accelerate cooperation and prove that they were not conveniently hiding behind the British objections but are serious about European defence" (Biscop, 2016: 432) (tradução do autor).

[166] Texto original: "The Brexit will certainly not make it any easier to make this architecture work, as one of the most important military actors voluntarily withdraws from a key part of the architecture, increasing the asymmetry in EU and NATO membership" (Biscop, 2016: 443) (tradução do autor).

[167] Texto original: "it is also important to remember that the alliance has weathered crises and divisions before and has survived and continued to operate because of its ability to adapt to changing realities" (Kaufman, 2017: 266) (tradução do autor).

CONCLUSÃO

Iniciando aqui as considerações finais desta exploração cibersecuritária, é manifesta a ideia de que para ambos os atores o medo da incerteza passou de exclusivamente físico e palpável, ganhando uma complementação virtual. Isto fez com que os cibercrimes, e dentro destes os ciberataques e o ciberterrorismo, em particular, ganhassem relevância e se impusessem como algo real no seio de ambos os atores, continuando ainda assim e ao mesmo tempo remotos em termos práticos (devido sobretudo a sua complexidade teórica e prática).

Apesar de ser possível compreender que ambas as OI têm um papel importante nas questões cibersecuritárias a nível mundial e que irão continuar a tentar desempenhar da melhor maneira este papel, é sobretudo a falta de capacidade no combate ao fenómeno do cibercrime que salta a vista. Isto é ainda mais preocupante se tivermos em conta "que a tecnologia está a evoluir a passos largos e de maneira igual para as aplicações ilícitas como para a cibersegurança o que torna premente a necessidade de proteção de infraestruturas sem as quais a vida não teria a existência tal qual a conhecemos" como são exemplo "o setor energético, financeiro, da banca, água, serviços de emergência, comunicações, entre outros" (Leite, 2016: 9).

Os hackers são agora capazes de transmitirem e obterem mais informação que um Estado ou uma OI inteira, algo que era impossível de vislumbrar acontecer há uns anos atrás, e que coloca as aspirações do mundo literalmente na palma das mãos de qualquer um destes criminosos. Se a isto associarmos a percentagem elevadíssima de aparelhos conectados a internet diariamente – calcula-se que serão 50 milhões até 2020 (Kissinger, 2014: 313) - com a capacidade de serem remotamente controlados por um *hacker* que tenha o engenho e a arte suficiente para o fazer, perceberemos a magnitude do fenómeno no qual a União Europeia e a NATO estão agora inseridas: a cibersegurança. Atualmente estamos a chegar a um ponto onde os dividendos retirados da utilização diária da internet estão a ser menores que as consequências desta prática.

> "Um ator solitário munido de um computador eficaz pode aceder ao ciberespaço para incapacitar e destruir infraestruturas fundamentais a partir de uma posição de quase total anonimato. Se pensarmos bem um computador portátil pode ter repercussões mundiais". (Kissinger, 2014: 395)

Esta evolução digital bem como os perigos a si associados são notórios no nosso dia-a-dia, sendo que ambos os atores em análise garantem ter a capacidade para lhe fazer frente através das várias medidas e contramedidas tomadas em conformidade[168]. Mas será a evolução do ciberespaço restringida por estas medidas?

Diariamente estamos apenas a tocar um pouco da superfície do ciberespaço quando utilizamos internet (ver anexo IV), isto torna a cibersegurança um assunto sério e possivelmente assustador. O facto da internet profunda e da internet obscura[169] (*Deep Web e Dark Web*) serem potencialmente quinhentas vezes maiores que a internet que utilizamos diariamente – já para não falar de ocultas e anónimas para quem decidir utilizá-las - (para muitos apenas 4% da totalidade do ciberespaço) (Harada, 2015) far-nos-á questionar a capacidade real e objetiva que estes atores podem ter contra colossal empreendimento, deixando ao mesmo tempo antever muito espaço para que esta nova dimensão possa evoluir e tornar ainda mais difícil a vida daqueles que tem a função de nos proteger.

É então o ciberespaço um espaço seguro e transparente para todos nós? Mais uma pergunta que se torna cada vez mais existencial no panorama mundial da cibersegurança, este espaço complexo e enigmático é tudo o que nos liga presentemente a atualidade e a modernidade e no qual todos nós já percebemos não estarmos 100% seguros. O controlo sobre este mesmo espaço é que é o cerne da questão aqui, se já é difícil para os atores em estudo controlarem e pacificarem a internet superficial, imaginemos estas duas camadas ocultas do ciberespaço.

Não se quer com isto dizer que o problema está no espaço, mas sim no utilizador do mesmo pois nem só de criminosos vive a internet profunda e a internet obscura sendo lar de muitos bem feitores e comuns utilizadores da internet.

Voltando ao início e à base que rodeia esta investigação importa salientar que ambos os atores têm uma agenda cibersecuritária estabelecida com objetivos, dinâmicas, estratégias, protocolos, regulamentos, medidas e principalmente ideias para tornarem o ciberespaço um local seguro para todos nós, sendo que a evolução destas tem sido notória e positiva ao longo dos últimos anos. A cooperação é também ela uma vontade firmada e clara entre ambos os atores (e não só) sendo claro também o papel de exemplo a seguir que a NATO tem para com a UE.

---

[168] Sendo estas mais ou menos eficazes no combate a estas ciberameaças – partindo do entendimento pessoal e particular de cada um de nos relativamente ao assunto em questão.

[169] Designação utilizada pelo autor para nomear as camadas Deep Web e Dark Web.

O que falta, e segundo o Professor Doutor André Barrinha e o Professor Doutor Henrique Santos, é a aplicação estratégica e operacional destes princípios (Barrinha, 2018 e Santos, 2018). Na opinião destes dois entrevistados ambos os atores em análise criaram as oportunidades para que a cibersegurança surgisse no seio da sua agenda securitária, e consequentemente no seio da agenda securitária dos Estados membros que as compõem, mas continuam a ser as empresas privadas a tratar dos assuntos cibersecuritários - o que desde logo transforma esta problemática numa incoerência estratégica (Barrinha, 2018 e Santos, 2018) e também numa oportunidade de negócio para estas companhias (mostrando o quão pouca influência ambos os atores tem neste campo) (Santos, 2018). Algo que fica espelhado ao longo desta análise à luz do enquadramento teórico - o neoliberalismo institucional complacente e perdulário dos atores em análise.

O caos torna-se ainda mais uma realidade visto que no momento em que a dissertação é finalizada "a ideia de ordem internacional é inconcebível" isto porque "a área onde estão a ser decididos o progresso e a sobrevivência dos Estados continua privada de padrões internacionais de conduta e entregues a decisões unilaterais" (Kissinger, 2014: 397). E desde logo em resposta a pergunta "qual o papel da União Europeia e da NATO na cibersegurança a nível mundial?" seremos obrigados a concordar que este é papel é quase nulo ou inexistente visto ser ainda muito parco e limitado o trabalho de ambos os atores neste campo.

A cibersegurança é o que se pode chamar de uma "área residual: tem menos gente associada a mesma, a sociedade tradicional não vê esta como uma área prioritária (sendo que o próprio Estado não dá o exemplo), a comunidade europeia cria regulamentos e protocolos, mas não passa disso. Isto revela uma clara falta de visão e uma clara falta de vontade em resolver o problema" (Santos, 2018).

Perante esta condensação de ideias a pergunta (filosófica) que se levanta é, será o conceito Neoinstitucionalista Liberal o principal responsável por está incapacidade? Na opinião do autor sim. A capacidade de estes dois atores regimentarem as suas agendas e os seus modos de agir será fundamental para um ciberespaço seguro e controlado, isto porque se continuarmos a fazer o mesmo e a esperar fins diferentes corremos o risco de cairmos na conceção de insanidade (pelo menos para Rita Mae Brown) (Brown, 1983: 68). O apregoado enquadramento filosófico raiz – Neoinstitucionalismo Liberal - e onde mais se enraízam os padrões morais da nossa sociedade, cria não só um paradoxo no que a cooperação diz respeito, mas cria também dificuldades na simples tomada de decisão.

Concluindo a temática do Neoliberalismo Institucional e a visão mais que necessária da Teoria dos Regimes, seria necessária uma mudança muito profunda no seio dos Estados membros que

compõem ambos os atores analisados para que esta surtisse efeito. E aqui não falamos só de acordos, agendas ou protocolos, falamos de ideologias e de maneiras de pensar tanto políticas como sociais para que algo como a regimentação do ciberespaço surtisse efeito, algo se não impossível muito difícil de acontecer no seio de tantos Estados-membros com visões próprias e individuais sobre o problema em análise.

A verdade é que ventos em sentido contrário também já começam a soprar e "um regime internacional para o ciberespaço já está no escopo de interesse algumas Organizações Internacionais, incluindo o Fórum de Governança da Internet[170]" (Kulesza, 2010: 14)[171]. Sendo apenas um sonho ou não, a ideia está presente.

Sendo ou não a regimentação do ciberespaço algo possível de se concretizar, a cooperação entre a UE e a NATO continua a ser algo fundamental. Outra pergunta que se levanta uma vez analisados ambos os atores é se é possível uma cooperação 'real' e 'sólida' entre a União Europeia e a NATO?

Com todas as problemáticas do Neoliberalismo Institucional associadas ao surgimento de outras como o processo de saída do Reinou Unido da UE e a eleição de Donald Trump isto torna-se efetivamente, mais difícil (mas não impossível) sendo necessário um esforço redobrado não só de ambas as organizações, mas também dos Estados membros que os compõem. Ainda que seja possível observar os dois lados da moeda relativamente aos dois casos enumerados (como vimos no último capítulo desta dissertação: visões positivas e negativas), problemáticas como estas deixarão sempre marcas em ambos os atores e será sempre preciso tempo para que ambas recuperem dos possíveis 'traumas' sofridos. Tempo este escasso, diminuto e essencial no que a uma proteção eficaz do ciberespaço diz respeito.

A questão proeminente de futuro é perceber se as relações União Europeia-NATO passarão a ser pautadas por um clima de instabilidade resultado não só da ineficiência na luta contra o cibercrime, mas também devido a estas duas dinâmicas: *Brexit* e Donald Trump. A tudo isto temos ainda que juntar

[170] "O Fórum de Governança da Internet (IGF) serve para reunir pessoas de vários grupos de partes interessadas como um, em discussões sobre questões de políticas públicas relacionadas com à Internet" (Fórum de Governança da Internet Website Oficial, 2006-2018) (tradução do autor) = Texto original: "The Internet Governance Forum (IGF) serves to bring people together from various stakeholder groups as equals, in discussions on public policy issues relating to the Internet" (Fórum de Governança da Internet Website Oficial, 2006-2018).

[171] Texto original: "An international regime for cyberspace is already in the scope of interest of some international organizations, including the Internet Governance Forum" (Kulesza, 2010: 14) (tradução do autor).

"a falta de coordenação interinstitucional" entre ambos os atores e a "batalha contínua para determinar qual agência (organização) está na liderança" (Marazis, 2018)[172].

Se a tecnologia evolui a um ritmo que não conseguimos acompanhar, se o ciberespaço superficial é ainda uma pequena parte do que realmente conhecemos, se o papel da UE e da NATO na cibersegurança a nível mundial é quase inexistente, se a liberalização do ciberespaço é um fardo e se a cooperação parece também ela ser, serão estes atores capazes de nos proteger e capazes de combater o cibercrime? A resposta partindo da análise efetuada é não. Nem a União Europeia nem a NATO são neste momento capazes de nos proteger no ciberespaço, "o papel limitado de ambos os atores nesta área" (Barrinha, 2018) "bem como a sua incapacidade face aos problemas cibernéticos" (Santos, 2018) são um problema latente e preocupante que nos impede de ter uma resposta mais positiva face a esta questão. Algo que não invalida, no entanto, a sua evolução ritmada nesta área ao longo do tempo por parte de ambos os atores, bem como a sua cooperação em diversas áreas como é o caso da cibersegurança.

Futuras explorações nesta área devem ter em conta o carácter mutável do tema explorado e aconselha-se a assimilação da ideia de que ambos os atores em exploração, apesar de todas as medidas, regulamentos, declarações oficiais e posições de defesa e segurança assumidos, ainda não são capazes de nos proteger de maneira eficaz no ciberespaço. Um futuro ponto de trabalho a partir desta dissertação seria perceber como os Estados na sua individualidade adotam as leis cibersecuritárias da UE e da NATO ou como as empresas privadas nos protegem neste campo.

Um projeto a longo prazo – possivelmente o projeto de uma vida - por parte do autor desta investigação será comparar a capacidade cibersecuritária da China com a da União Europeia e da NATO, tentando ao mesmo tempo perceber qual a mais eficaz neste campo. Tudo isto tendo em conta as limitações de estarmos a comparar um Estado e duas Organizações Internacionais, o que representará sempre dois pesos e duas medidas em todas as decisões tomadas por parte de ambas as entidades. Projeto este que dependerá sempre de uma aprendizagem eficaz e fluente do mandarim por parte do investigador, visto serem as referências primárias uma fonte importante para a investigação.

[172] Texto original: "They lack, however, inter-agency coordination. There is an ongoing battle just to determine which agency is in the lead" (Marazis, 2018) (tradução do autor).

BIBLIOGRAFIA

Entrevistas Realizadas no Âmbito Desta Dissertação

Barrinha, André. (2018). *Cibersegurança: União Europeia.* Entrevistado pessoalmente a 9 de maio de 2018 pelo autor (Hélio Samuel Farinha Campos). Braga – Universidade do Minho - O Professor Doutor André Barrinha leciona a cadeira de Segurança Internacional na Universidade de Bath, no Reino Unido e é também ele Investigador do Centro de Estudos Sociais da Universidade de Coimbra (ORCID, 2012-2018a)

Santos, Henrique. (2018). *Cibersegurança: União Europeia e NATO*. Entrevistado pessoalmente a 29 de maio de 2018 pelo autor (Hélio Samuel Farinha Campos). Braga - O Professor Doutor Henrique Santos é professor da Universidade do Minho e leciona cadeiras tão diversas como a Segurança em Sistemas de Informação, a Segurança em Redes de Computadores, a Arquitetura de Computadores e a Programação de Computadores. É também membro do centro Algoritmi (ORCID, 2012-2018b).

Fontes Primárias

Documentos Primários

Agência Europeia de Defesa. (2017). *Cyber defence.* Bruxelas: "Ficha informativa". Disponível na internet em: https://www.eda.europa.eu/docs/default-source/eda-factsheets/2017-09-06-factsheet_cyber-defence.pdf

Anil, Suleyman. (2004). *NCIRC (NATO Computer Incident Response Capability): 11th TF-CSIRT Meeting*. Madrid: "Seminário". Disponível na internet em: https://www.terena.org/activities/tf-csirt/meeting11/NCIRC-Anil.pdf

- Suleyman Anil: Ex-chefe da defesa cibernética Europeia (entre 2010 e 2016) atualmente aposentado.

C. Carey III, Casimir. (2013). *NATO's Options for Defensive Cyber Against Non-State Actors.* Pensilvânia: "Army War College Class of 2013". Disponível na internet em: https://www.hsdl.org/?view&did=793826

Conselho da União Europeia e Parlamento Europeu. (1999). *Diretiva 1999/93/CE do Parlamento Europeu e do Conselho, de 13 de dezembro de 1999, relativa a um quadro legal comunitário para as assinaturas eletrónicas.* Bruxelas: "Diretiva". Disponível na internet em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31999L0093

Conselho da União Europeia. (2001). *Convenção sobre o Cibercrime*. Budapeste: "Tratado da União Europeia nº 185". Disponível na internet em: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561

Conselho da União Europeia. (2003a). *Protocolo Adicional a Convenção sobre o Cibercrime.* Estrasburgo: "Tratado da União Europeia nº 185". Disponível na internet em: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/090000168008160f

Conselho da União Europeia. (2003b). *Estratégia Europeia de Segurança*. Bruxelas: "Conceito Estratégico". Disponível na internet em: http://consilium.europa.eu/uedocs/cmsUpload/031208ESSIIP.pdf

Conselho da União Europeia e Parlamento Europeu. (2004). *Regulamento (CE) n.º 460/2004 do Parlamento Europeu e do Conselho, de 10 de março de 2004, que cria a Agência Europeia para a Segurança das Redes e da Informação.* Bruxelas: "Regulamento". Disponível na Internet em: http://eur-lex.europa.eu/legal-content/PT/ALL/?uri=celex:32004R0460

Conselho da União Europeia. (2008). *Relatório sobre a Implementação da Estratégia Europeia de Segurança.* Bruxelas: "Conceito Estratégico". Disponível na internet em: http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressdata/PT/reports/104638.pdf

Conselho da União Europeia. (2010). *Estratégia de segurança interna para a União Europeia: Rumo a um modelo de segurança europeu.* Bruxelas: "Conselho Justiça e Assuntos Internos". Disponível na internet em: http://www.consilium.europa.eu/media/30754/qc3010313ptc.pdf

Conselho da União Europeia e Parlamento Europeu. (2010). *Estratégia de Segurança Interna da UE em Acção: cinco etapas para uma Europa mais segura.* Bruxelas: "Comunicação conjunta". Disponível na internet em: http://eur-lex.europa.eu/legal-content/GA/TXT/?uri=celex%3A52010DC0673

Conselho da União Europeia e Parlamento Europeu. (2013). *Diretiva 2013/40/UE do Parlamento Europeu e do Conselho, de 12 de agosto de 2013, relativa a ataques contra os sistemas de informação e que substitui a Decisão-Quadro 2005/222/JAI do Conselho.* Bruxelas: "Diretiva". Disponível na internet em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32013L0040

Conselho da União Europeia. (2014a). *Regulação eIDAS (Serviços eletrônicos de identificação e fidedignidade).* Bruxelas: "Regulamento da União Europeia nº 910/2014". Disponível na internet em: https://ec.europa.eu/futurium/en/system/files/ged/eidas_regulation.pdf

Conselho da União Europeia e Parlamento Europeu. (2014b). *Agenda Digital para a Europa*. Luxemburgo: "Serviço das Publicações da União Europeia". Disponível na internet em: http://www.eurocid.pt/pls/wsd/wsdwcot0.detalhe?p_cot_id=6280#contexto

Conselho da União Europeia. (2016a). *Estratégia Global para a Política Externa e de Segurança da União Europeia*. Bruxelas: "Conceito Estratégico". Disponível na internet em: http://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf

Conselho da União Europeia. (2016b). *Cimeira da OTAN, em Varsóvia, na Polónia, 08-09/07/2016.* Varsóvia: "Reunião". Disponível na internet em: http://www.consilium.europa.eu/pt/meetings/international-summit/2016/07/08-09/

Conselho da União Europeia e Parlamento Europeu. (2016a). *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE.* Bruxelas: "Regulamento". Disponível na internet em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679

Conselho da União Europeia e Parlamento Europeu. (2016b). *Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União.* Bruxelas: "Diretiva". Disponível na Internet em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016L1148

Conselho do Atlântico Norte. (1991). *Conceito Estratégico para a Defesa e Segurança dos Membros da Organização do Tratado do Atlântico Norte.* Londres: Conceito Estratégico. Disponível na internet em: http://www.nato.int/cps/sl/natohq/official_texts_23847.htm

Conselho do Atlântico Norte. (1999). *Conceito Estratégico para a Defesa e Segurança dos Membros da Organização do Tratado do Atlântico Norte*. Washington D.C.: Conceito Estratégico. Disponível na internet em: http://www.nato.int/cps/en/natohq/official_texts_27433.htm

Conselho do Atlântico Norte. (2002a). *Declaração UE-NATO sobre a PESD*. Bruxelas: "Declaração". Disponível na internet em: http://www.nato.int/cps/en/natolive/official_texts_19544.htm

Conselho do Atlântico Norte. (2002b). *Declaração sobre a Cimeira de Praga*. Praga: Declaração NATO. Praga: "Declaração". Disponível na internet em: http://www.nato.int/cps/po/natohq/official_texts_19552.htm

Conselho do Atlântico Norte. (2006a). *Guia político*. Bruxelas: "Declaração". Disponível na internet em: http://www.nato.int/cps/en/natohq/official_texts_56425.htm?selectedLocale=en

Conselho do Atlântico Norte. (2006b). *Declaração sobre a Cimeira de Riga*. Riga: Declaração NATO. Riga: "Declaração". Disponível na internet em: http://www.nato.int/docu/pr/2006/p06-150e.htm

Conselho do Atlântico Norte. (2008). *Declaração sobre a Cimeira de Bucareste*. Bucareste: "Declaração". Disponível na internet em: http://www.nato.int/cps/in/natohq/official_texts_8443.htm

Conselho do Atlântico Norte. (2010). *Conceito Estratégico para a Defesa e Segurança dos Membros da Organização do Tratado do Atlântico Norte*. Lisboa: "Conceito Estratégico". Disponível na internet em: http://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf

Conselho do Atlântico Norte. (2012). *Declaração sobre a Cimeira de Chicago*. Chicago: Declaração NATO. Chicago: "Declaração". Disponível na internet em: http://www.nato.int/cps/en/natohq/official_texts_87593.htm?mode=pressrelease

Conselho do Atlântico Norte. (2013). *Parcerias: uma abordagem cooperativa da segurança*. Bruxelas: "Informações". Disponível na internet em: http://www.nato.int/nato_static/assets/pdf/pdf_2013_12/20131127_131201-MediaBackgrounder-Partnerships_en.pdf

Conselho do Atlântico Norte. (2014). *Declaração sobre a Cimeira de Gales*. Gales: Declaração NATO. Gales: "Declaração". Disponível na internet em: http://www.nato.int/cps/ic/natohq/official_texts_112964.htm

Conselho do Atlântico Norte. (2016a). *Relatório Anual do Secretário Geral*. Bruxelas: "Relatório". Disponível na internet em: http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_01/20160128_SG_AnnualReport_2015_en.pdf

Conselho do Atlântico Norte. (2016b). *Declaração sobre a Cimeira de Varsóvia*. Varsóvia: Declaração NATO. Varsóvia: "Declaração". Disponível na internet em: http://www.nato.int/cps/en/natohq/official_texts_133169.htm

Conselho do Atlântico Norte. (2016c). *Declaração Conjunta assinada pelo Presidente do Conselho Europeu, pelo Presidente da Comissão Europeia e pelo Secretário-Geral da Organização do Tratado Norte.* Bruxelas: "Declaração". Disponível na internet em: http://www.nato.int/cps/on/natohq/official_texts_138829.htm

Conselho do Atlântico Norte. (2016d). *NATO and the European Union enhance cyber defence cooperation.* Bruxelas: "Comunicação Conjunta". Disponível na internet em: https://www.nato.int/cps/en/natohq/news_127836.htm

Conselho do Atlântico Norte. (2016e). *Cyber Defence Pledge.* Bruxelas: "Documento de Comprometimento". Disponível na internet em: https://www.nato.int/cps/su/natohq/official_texts_133177.htm

Conselho do Atlântico Norte. (2017). *Relatório Anual do Secretário Geral*. Bruxelas: "Relatório". Disponível na internet em: http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_03/20170313_SG_AnnualReport_2016_en.pdf#page=7

Conselho do Atlântico Norte. (2017). *Ciberdefesa NATO.* Bruxelas: "Ficha Informativa". Disponível na internet em: http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_201_03/20170331_1704-factsheet-cyber-defence-en.pdf

Conselho Atlântico Norte. (2018a). *Cyber defence.* Bruxelas: "Tópico". Disponível na internet em: https://www.nato.int/cps/en/natohq/topics_78170.htm

Conselho do Atlântico Norte. (2018b). *NATO Cyber Defence.* Bruxelas: "Ficha informativa". Disponível na internet em: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_02/20180213_1802-factsheet-cyber-defence-en.pdf

Comissão Europeia. (2005). *Decisão-Quadro 2005/222/JAI do Conselho, de 24 de fevereiro de 2005, relativa a ataques contra os sistemas de informação.* Bruxelas: "Decisão-quadro". Disponível na internet em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32005F0222

Comissão Europeia. (2006). *Comunicação da Comissão relativa a um Programa Europeu de Proteção das Infraestruturas Críticas /* COM/2006/0786 final */.* Bruxelas: "Comunicado". Disponível na internet em: http://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A52013PC0048

Comissão Europeia. (2013). *Estratégia da União Europeia para a Cibersegurança: um ciberespaço aberto e seguro.* Bruxelas: Comunicação Conjunta do Parlamento Europeu, do Conselho Europeu, do Comité Económico e Social Europeu e do Comité das Regiões. Pp: 1-20 Disponível na internet em: https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

Comissão Europeia. (2015a). *Estratégia Digital de Mercado Único.* Bruxelas: Comunicado de imprensa. Disponível na internet em: http://europa.eu/rapid/press-release_IP-15-4919_pt.htm

Comissão Europeia. (2015b). *Agenda Europeia para a Segurança Rumo a uma União de segurança.* Bruxelas: Comunicado de imprensa. Disponível na internet em: http://europa.eu/rapid/press-release_IP-16-1445_pt.htm

Comissão Europeia. (2016). *Scientific Advice Mechanism.* Scoping Paper: Cybersecurity. Bruxelas: "Documento Avaliativo". Disponível na internet em: https://ec.europa.eu/research/sam/pdf/meetings/hlg_sam_012016_scoping_paper_cybersecurity.pdf

Denning, D. (2000). *Cyberterrorism*. Washington D.C.: "Testimony before the Special Oversight Panel of Terrorism Committee on Armed Services - US House of Representatives"

ENISA. (2015). *Definition of Cybersecurity: Gaps and overlaps in standardisation.* Creta: "ENISA" Vol. 1.0

Jean-Claude Juncker. (2017). *State of the Union Address 2017.* Bruxelas: "Comissão Europeia – Discurso". Disponível na internet em: http://europa.eu/rapid/press-release_SPEECH-17-3165_en.htm

- Jean-Claude Juncker: Presidente da comissão Europeia.
NSSC. (2003). *National Strategy to Secure Cyberspace*. Washington: "White House Office of Homeland Security". Disponível na internet em: https://www.nitrd.gov/cybersecurity/documents/NationalStrategytoSecureCyberspace2003.pdf

Conferências

II Seminário IDN Jovem. (2017). *Política Externa e Defesa Nacional*. Comparência pessoal do autor (Hélio Samuel Farinha Campos) entre os dias 4 e 5 de abril de 2017. Universidade do Minho – Braga
- José Alberto Azeredo Lopes: Doutorado pela Universidade Católica Portuguesa na área das Ciências Jurídico-Políticas e ex-Ministro da defesa Nacional (entre 2015-2018).
- Coronel Nuno Lemos Pires: Doutorado em História, Defesa e Relações Internacionais em 2013 pelo Instituto Universitário de Lisboa, é atualmente investigador no Centro de Estudos Internacionais do Instituto Universitário de Lisboa e Professor na Academia Militar.
XXXIX Colóquios de Relações Internacionais. (2018). *(in)Governabilidade no Século XXI.* Comparência pessoal do autor (Hélio Samuel Farinha Campos) entre os dias 8 e 9 de maio de 2018. Universidade do Minho - Braga

Fontes Secundárias

Livros, Capítulos de Livros e Monografias

Aggarwal, V. K. (1985). *Liberal protectionism: The international politics of organized textile trade*. Berkeley: "University of California Press"
Axelrod, Robert. (1984). *The Evolution of Cooperation*. New York: "Basic Books"
Brown, Rita Mae. (1983). *Sudden Death.* New York: "Bantam".
David Collier. (1993). *The Comparative Method.* In: Ada W. Finifter. (1993). "Political Science: The State of Discipline II". Washington, DC: "American Political Science Association". Pp: 105-119
IDN Cadernos. (2013). *Estratégia da informação e segurança no ciberespaço: investigação conjunta IDN-CESEDEN.* Lisboa: "Instituto da Defesa Nacional" nº 12
Kissinger, H. (2014). *Capítulo 9 – Tecnologia, Equilíbrio e Consciência Humana*. In: *Ordem Mundial*. (2014). Alfragide: "Dom Quixote". Pp: 391-398
Krasner, Stephen D. (1983). *International Regimes*. Ithaca e Londres: "Cornell University Press"
Nunes, Paulo Fernando Viegas. (2012). *A Definição de uma Estratégia Nacional de Cibersegurança*. In: Rodrigues Viana, Vitor. (2012). "Cibersegurança". Lisboa: "Instituto da Defesa Nacional" nº 133, Pp: 113-127
O. Keohane, Robert. (1989). *International Institutions and State Power: Essays in International Relations Theory*. Boulder: "CO: Westview Press"
Oshiba, Ryo. (2010). *International Regimes.* in: Sekiguchi, Masashi. (2010). "Government and Politics Vol. II". Oxford: "Encyclopedia of Life Support Systems (EOLSS)", Pp: 260-268

Purser Steve. (2014). *Standards for Cyber Security.* In: Hathaway, Melissa E.. (2014). "Best Practices in Computer Network Defence: Incident Detection and Response". Amsterdam-Berlin-Tokyo-Washington D.C.: "IOS Press", Pp: 97-106.

Santos, Paulo. Bessa, Ricardo. Pimentel, Carlos. (2008). *Cyberwar – O fenómeno, as Tecnologias e os Atores*. Lisboa: "FCA - Editora de Informática, Lda"

Teixeira Fernandes, José Pedro. (2014). *Ciberguerra: Quando a Utopia se Transforma em Realidade.* Lisboa: "Quidnovi Ensaio"

Vromen, Ariadne. (2010). *Debating Methods: Rediscovering Qualitative Approaches.* In: David Marsh, Gerry Stoker. (2010). "Theory and Methods in Political Science 3º Edition". Nova Iorque: "Palgrave Macmillan" Pp: 249-266

Artigos Científicos e Relatórios

A. Veenendaal, Matthijs. Brangetto, Pascal. (2016). *Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations*. Tallinn: "NATO CCDCOE Publications"

Axelrod, Robert and Borzutzky, Silvia. (2006). *NATO and the war on terror: The organizational challenges of the post 9/11 world.* In: "The Review of International Organizations" Vol. 1, Pp: 293-307

Axelrod, Robert. O. Keohane, Robert. (1985). *Achieving cooperation under anarchy: Strategies and institutions*. In: "World Politics a Quarterly Journal of International Relations" Vol. 38, nº. 1, Pp: 226-254

Bachmann, Sascha-Dominik. (2011). *Hybrid threats, cyber warfare and NATO's comprehensive approach for countering 21st century threats – mapping the new frontier of global risk and security management.* In: "Amicus Curiae" Vol. 88, Pp: 14-17

Barrinha, André. Carrapico, Helena. (2017). *The EU as a Coherent (Cyber)Security Actor?*. "JCMS: Journal of Common Market Studies" Vol. 55 nº 6, Pp: 1–19

Barrinha, André. Carrapico, Helena. (2018). *European Union cyber security as an emerging research and policy field, European Politics and Society.* "European Politics and Society" Vol. 19, Pp: 1-6

Biscop, Sven. (2016). *All or nothing? The EU Global Strategy and defence policy after the Brexit*. "Contemporary Security Policy" Vol. 37, Pp: 431-445

Blank, Stephen. (2008). *Web War I: Is Europe's First Information War a New Kind of War?*. "Comparative Strategy" Vol. 27, Pp: 227-247

Bodin, Sylvia. Echilley, Marc. Quinard-Thibault, Odile. (2015). *International cooperation in the face of cyber-terrorism: current responses and future issues.* "Themis competition 2015 edition – French Team", Semi-Final A – International Cooperation in Criminal Matters

Burton, Joe. (2015). *NATO's cyber defence: strategic challenges and institutional adaptation*. "Defence Studies" Vol. 15, Pp: 297-319

Centre of Excellence Defence Against Terrorism. (2010). *Defence against terrorism review: DATR*. Turkey: Centre of Excellence - Defence Against Terrorism Vol. 3, nº 2. Disponível na internet em: http://www.coedat.nato.int/publication/datr/volumes/datr5.pdf

Choucri, Nazli. Madnick, Stuart. Ferwerda, Jeremy. (2014). *Institutions for Cyber Security: International Responses and Global Imperatives*. In: "Information Technology for Development" Vol. 20:2, Pp: 96-121

Conselho do Atlântico Norte. (2014). *NATO Cyber Defence Taxonomy and Definitions*. Norfolk: "Organização do Tratado do Atlântico Norte"

Den Boer, Monica. (2003). *9/11 and the Europeanisation of anti-terrorism policy: A critical assessment.* "Groupement d'études et de recherches – Notre Europe" Policy Paper nº 6

de Vos, Luc. (2009). *Towards a Global and Transformed NATO via a better EU?.* Universidade Católica do Sagrado Coração - Milão: "Simpósio Internacional"

Dogrul, Murat. Aslan, Adil. Celik, Eyyup. (2011). *Developing an international cooperation on cyber defence and deterrence against Cyber terrorism.* Tallinn: "3ª conferência internacional sobre conflitos cibernéticos", Pp: 1-15

E. Mix, Derek. (2013). *The European Union: Foreign and Security Policy.* Washington D.C.: "Congressional Research Service" 7-5700

Feikes, Allison. (2014). *Transatlantic Cooperation on Cyber Security: Data Privacy and Cybercrime*. New Brunswick: "Honors College Capstone Experience/Thesis Projects", Paper 459

Ferreira Leite, Ana. (2016). *A Problemática da Cibersegurança e os seus Desafios.* Faculdade de Direito da Universidade Nova de Lisboa - Lisboa: "Cedis Working Papers - Direito, Segurança e Democracia" nº49

Figueiredo, Herivelton Rezende de. (2014). *Cibercrime*. Mato Grosso do Sul: "Revista Jurídica UNIGRAN" Vol. 16 nº 32, Pp: 89-103

Gabriel Camargo, Alan. Gabriel Borges Junqueira, Cairo. (2013). *A Teoria Neoliberal nas Relações Internacionais: O Tripé Institucional e o Papel do Estado.* Pp: 20-24 in: "O Debatedouro" Edição nº 83

Gordon, Sarah and Ford, Richard. (2002). *Cyberterrorism?.* In: "Computers and Security" Vol. 21 nº 7, Pp: 636-647

Hansen, Lene. Nissenbaum, Helen. (2009). *Digital Disaster, Cyber Security, and the Copenhagen School*. "International Studies Quarterly" nº 53, Pp. 1155–1175

Hardt, Heidi. (2017). *How NATO remembers: explaining institutional memory in NATO crisis management*.. In: "European Security" Vol. 26, Pp: 120-148

Healey, Jason. Jordan, Klara Tothova. (2014). *NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow.* Washington D.C.. "Brent Scowcroft Center on International Security". Disponível na internet em: http://www.atlanticcouncil.org/images/publications/NATOs_Cyber_Capabilities.pdf

Heisbourg, François. (2017). *The Emperor vs the Adults: Donald Trump and Wilhelm II*. In: "Survival" Vol. 59, Pp: 7-12

Herz, Mônica. (1997). *Teoria das Relações Internacionais no Pós-Guerra Fria*. Rio de Janeiro: "Dados - Revista de Ciências Sociais" Vol. 40 nº 2

Herzog, Stephen. 2011. *Revisiting the Estonian Cyber-Attacks: Digital Threats and Multinational Responses*. "Journal of Strategic Security Vol. 4 nº 2", Pp. 49-60

J. Aldrich, Richard. (2009). *US–European Intelligence Co-operation on Counter-Terrorism: Low Politics and Compulsion*. "The British Journal of Politics & International Relations" Vol. 11, Pp: 122-139

Jervis, Robert. (1999). *Realism, neoliberalism, and cooperation.* Pp: 42-63. In: "International Security" Vol. 24 nº1. Massachusetts: "The MIT Press"

K. Ilves, Luukas. J. Evans, Timothy. J. Cilluffo, Frank. A. Nadeau, Alec. (2016). *European Union and NATO Global Cybersecurity Challenges: A Way Forward.* Washington D.C.: "PRISM" Vol. 6, nº 2, Pp: 127-141

Krasner, Stephen D. (2012). *Causas Estruturais e Consequências dos Regimes Internacionais: Regimes como Variáveis Intervenientes*. Curitiba: "Revista de Sociologia e Política" Vol. 20, Pp: 93-110

Krzysztof, Sliwisnki. (2014). *European Union-Cyber Power in the Making*. "Asia-Pacific Journal of EU Studies" Vol. 12, Pp: 1-23

Kulesza, Joanna. (2010). *State responsibility for acts of cyber-terrorism.* Faculty of Law and Administration University of Lodz - Lodz: "Simpósio Anual"

Lété, Bruno. Pernik, Piret. (2017). *EU–NATO Cybersecurity and Defence Cooperation: From Common Threats to Common Solutions.* "German Marshall Fund of the United States – Policy Brief" nº 38, Pp: 1-9

L. Konstantopoulos, Ioannis. M. Nomikos, John. (2017). *Brexit and intelligence: connecting the dots*. "Journal of Intelligence History" Vol. 16, Pp: 100-107

M. Archer, Emerald. (2014). *Crossing the Rubicon: Understanding Cyber Terrorism in the European Context*. In: "The European Legacy" Vol. 19, Pp: 606-621

Martins, Marco. (2017). *A União Europeia num Mundo em Mudança: Era Trump 2.0?.* Lisboa: "Análise Europeia - Revista da Associação Portuguesa de Estudos Europeus" Vol. 2, Pp: 93-117

Moran, Christopher. (2017). *A JIH special forum on Brexit: implications for UK and European intelligence agencies*. "Journal of Intelligence History" Vol. 16, Pp: 67-69

Moravcsik, Andrew. (2010). *Liberal Theories of International Relations: A Primer.* Princeton: "Princeton University Press", Pp: 1-15

Moslemzadeh Tehrani, Pardis. Abdul Manap, Nazura. Hossein Taji. (2013). *Cyber terrorism challenges: The need for a global response to a multi-jurisdictional crime.* Faculty of Law –The National University of Malaysia - Selangor: "Computer Law & Security Report" Vol. 29 nº 3

M. Segell, Glen. (2004). *Intelligence Agency Relations Between the European Union and the U.S.* "International Journal of Intelligence and Counter Intelligence", Pp: 81-96

Munk, Tine Højsgaard. (2015). *Cyber-security in the European Region: Anticipatory Governance and Practices.* "Doctoral Thesis - University of Manchester"

Nunes, Paulo Fernando Viegas. (2004). *Ciberterrorismo: Aspetos de Segurança.* "Revista Militar" nº 2433, Pp: 1-19

Pinto, Maria do Céu. (2007). *Contributos das teorias das RI para o estudo das Organizações Internacionais e da integração regional.* Lisboa: "Revista de Imprensa Internacional" nº 16

P. Kaufman, Joyce. (2017). *The US perspective on NATO under Trump: lessons of the past and prospects for the future*. In: "International Affairs" Vol. 93, nº 2, Pp: 251-266

Regis, André. (2007). *Intervenções Humanitárias: O Problema da cooperação Internacional.* In: Pessoa, João. "Prim@ facie Revista da Pós-graduação em Ciências Jurídicas". Universidade Federal da Paraíba – Paraíba: "Prim@ facie" Vol. 6 nº11, Pp: 53-63.

Saul, Ben. Heath, Kathleen. (2014). *Cyber Terrorism.* Law School - Sydney: "Legal Studies Research Paper" nº 14/11

Shaffer, Tony. (2017). *Hard Brexit on defence: how the UK can lead Europe in global security*. "Journal of Intelligence History" Vol. 16, Pp: 76-78

Sliwinski, Krzysztof Feliks. (2014). *Moving beyond the European Union's Weakness as a Cyber-Security Agent*. "Contemporary Security Policy" Vol. 35, Pp: 468-486

S. Nye, Joseph. (2014). *The Regime Complex for Managing Global Cyber Activities.* Harvard University - Cambridge: "Centre for International Governance Innovation and the Royal Institute for International Affairs" nº 1, Pp: 1-16

Svendsen, Adam D. M.. (2017). *Brexit: an agent of 'disruptive change' for UK and European intelligence?*. "Journal of Intelligence History" Vol. 16, Pp: 108-111

Tasheva, Iva. (2017). *European cybersecurity policy – Trends and prospects.* European Policy Centre – Bruxelas: "Policy Brief"

Teixeira Fernandes, José Pedro. (2012). *A ciberguerra como nova dimensão dos conflitos do século XXI*. Lisboa: In: "Relações Internacionais" nº 33, Pp: 53-69

Tikk, Eneken. (2011). *Ten Rules for Cyber Security*. In: "Survival" Vol. 53, Pp: 119-132

Weimann, Gabriel. (2005). *Cyber-terrorism: The Sum of All Fears?* In: "Studies in Conflict & Terrorism" Vol. 28, Pp:129–149

W. Kennedy, David. (1987). *The Move to Institutions.* Cambridge - "Cardozo Law Review" Vol. 8, Pp: 841-988

W. M. Teixeira Júnior, Augusto. Vilar-Lopes, Gills. Túlio Delgobbo Freitas, Marco. (2017). *As três tendências da guerra cibernética: novo domínio, arma combinada e arma estratégica.* In: "Carta Internacional – Publicação da Associação Brasileira de Relações Internacionais", Belo Horizonte: "Carta Internacional" Vol. 12 nº 3, Pp: 30-53

Young, Oran R. (1980). International regimes: problems of concept formation. In: "World Politics" Vol. 32, Pp: 331-356. Cambridge: "Cambridge University Press"

Young, Oran R. (1982). Regime dynamics: The rise and fall of international regimes. In: "International Organization - JSTOR" Vol. 36, Pp: 277-297

Documentários e Entrevistas

Hambsch, Mathew. (2015). *Cyber war 1.0 - chasing my digital self.* Berlim: "Weltenangler Berlin/Little Kingfisher Entertainment"

- Jaan Priisalu: Ex-diretor do departamento de segurança e informação estónio (entre 2011-2015), é atualmente um colaborador no Centro Cooperativo de Ciberdefesa e Excelência da NATO em Tallinn. Palavras proferidas no documentário "Cyber war 1.0 – chasing my digital self".
- Mathew Hambsch: diretor/jornalista/protagonista do documentário "Cyber war 1.0 - chasing my digital self".

Lefranc, JeanMartial. (2015). *Hack me If You Can - Tales from the Digital Battlefield*. Paris: "Narratio Films, Media Res, RTBF"

National Geographic. (2017). *The Future of Cyberwarfare - Origins: The Journey of Humankind.* "Website – Youtube". Publicado a 6 de abril de 2017. Disponível na internet em: https://www.youtube.com/watch?v=L78r7YD-kNw

- John McCain: Ex-chefe do comitê das forças armadas do Senado Norte-americano.

SIPRI. (2018). *Peace Points: Arms control in cyberspace?*. "Website – Youtube". Publicado a 31 de maio de 2018. Disponível na internet em: https://www.youtube.com/watch?v=1w_JstA9vl8

Webgrafia

Notícias e Artigos Online

Almeida, Markus. (2014). *Ciberataque à Sony com novas pistas.* "Website - Revista Sábado Online". Publicado a 30 de dezembro de 2014. Disponível na internet em: http://www.sabado.pt/gps/palco-plateia/cinema/detalhe/ciberataque-a-sony-com-novas-pistas

Altman, Max. (2012). *Hoje na História: 1949 - É assinado em Washington o Tratado do Atlântico Norte.* São Paulo: "Website - Opera Mundi". Publicado a 4 de abril de 2012. Disponível na internet

em: http://operamundi.uol.com.br/conteudo/noticias/20946/hoje+na+historia+1949+-+e+assinado+em+washington+o+tratado+do+atlantico+norte.shtml

Barrinha, André. Farrand-Carrapico, Helena. (2018). *How coherent is EU cybersecurity policy?.* "Website - The London School of Economics and Political Science/ EUROPP European Politics and Policy". Publicado a 16 de janeiro de 2018. Disponível na internet em: http://blogs.lse.ac.uk/europpblog/2018/01/16/how-coherent-is-eu-cybersecurity-policy/

BBC. (2013). *What is Thatcherism?*. Publicado a 10 de abril de 2013. Disponível na internet em: http://www.bbc.com/news/uk-politics-22079683

Brahm, Eric. (2005). *International Regimes.* "Website – Beyond Intractability". Publicado em setembro de 2005. Disponível na internet em: https://www.beyondintractability.org/essay/international_regimes

CNCS. (2016). *Transposição da Diretiva SRI/NIS.* "Website – Centro Nacional de Cibersegurança Portugal". Disponível na internet em: https://www.cncs.gov.pt/transposicao-da-diretiva-nissri/

Conselho da União Europeia. (2016c). *Cimeira da OTAN, em Varsóvia, na Polónia, 08-09/07/2016.* "Website - Conselho da União Europeia". Publicado a 9 de julho de 2016. Disponível na internet em: http://www.consilium.europa.eu/pt/meetings/international-summit/2016/07/08-09/

Conselho da União Europeia. (2017). *Cyber-attacks: EU ready to respond with a range of measures, including sanctions.* "Website - Conselho da União Europeia". Publicado a 19 de junho de 2017. Disponível na internet em: http://www.consilium.europa.eu/en/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/

Conselho da União Europeia. (2018). *Reforma da cibersegurança na Europa*. "Website - Conselho da União Europeia". Disponível na Internet em: http://www.consilium.europa.eu/pt/policies/cyber-security/

Conselho do Atlântico Norte. (2017). *NATO Needs an Offensive Cybersecurity Policy by Barbara Roggeveen.* "Website - Conselho do Atlântico Norte". Publicado a 8 de agosto de 2017. Disponível na internet em: http://www.atlanticcouncil.org/blogs/new-atlanticist/nato-needs-an-offensive-cybersecurity-policy

Departamento de Defesa Norte-Americano. (2012). *Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City.* "Website – U. S. Department of Defense". Publicado a 11 de outubro de 2012. Disponível na internet em: http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136

- Leon Panetta: Ex-secretário da defesa dos Estados Unidos da América. Reportagem efetuada por Gopal Ratnam, disponível na internet em: https://www.bloomberg.com/news/articles/2012-10-12/cyberattacks-could-become-as-destructive-as-9-11-panetta

DGPJ – Direção-Geral da Política de Justiça. (2008). *Convenção sobre o cibercrime, de 23 de novembro de 2001 (STE 185).* "Website - Direção-Geral da Política de Justiça". Publicado a 23 de novembro de 2001. Disponível na internet: http://www.dgpj.mj.pt/sections/relacoes-internacionais/copy_of_anexos/convencao-sobre-o/

Diário de Notícias. (2018). *Migrações: UE e NATO concordam em aprofundar resposta à crise migratória.* "Website: Diário de Notícias". Publicado a 10 de julho de 2018. Disponível na internet em: https://www.dn.pt/lusa/interior/migracoes-ue-e-nato-concordam-em-aprofundar-resposta-a-crise-migratoria-9572179.html

Euronews. (2015). *Cyberterrorism: is there a European response?.* "Website - Euronews". Publicado a 17 de abril de 2015. Disponível na internet em: http://www.euronews.com/2015/04/17/cyberterrorism-is-there-a-european-response

Euronews. (2018). *União Europeia debate cibersegurança.* "Website - Euronews". Publicado a 9 de janeiro de 2018. Disponível na internet em: http://pt.euronews.com/2018/01/09/uniao-europeia-debate-ciberseguranca

Expresso. (2018). *Trump diz que NATO "é tão má" quanto acordo comercial com Canadá e México.* "Website - Expresso". Publicado a 29 de junho de 2018. Disponível na internet em: http://expresso.sapo.pt/internacional/2018-06-28-Trump-diz-que-NATO-e-tao-ma-quanto-acordo-comercial-com-Canada-e-Mexico#gs.59nKnNc

Gardezi, Saadia. (2010). *International Relations, Political Theory: The Political Spectrum.* Diagrama de Love Venn. "Website – Dashbored". Publicado a 26 de setembro de 2010. Disponível na Internet em: https://dashbored.wordpress.com/2010/09/26/the-political-spectrum/

Goulão, José. (2017). *NATO e União Europeia: a óbvia e velha geminação.* "Website - AbrilAbril". Publicado a 23 de março de 2017. Disponível na internet em: https://www.abrilabril.pt/nato-e-uniao-europeia-obvia-e-velha-geminacao

Grant, Ian. (2008). *Nato sets up Cyber Defence Management Authority in Brussels.* "Website - ComputerWeekly.com". Publicado a 4 de abril de 2008. Disponível na internet em: https://www.computerweekly.com/news/2240085580/Nato-sets-up-Cyber-Defence-Management-Authority-in-Brussels

Harada, Eduardo. (2015). *TecMundo Explica: o que é essa tal de "Deep Web"?.* "Website - TecMundo". Publicado a 10 de março de 2015. Disponível na internet em: https://www.tecmundo.com.br/tecmundo-explica/74998-tecmundo-explica-tal-deep-web.htm

Howell O'Neill, Patrick. (2016). *The cyberattack that changed the world*. "Website – The Daily Dot". Publicado a 20 de maio de 2016. Disponível na Internet em: https://www.dailydot.com/layer8/web-war-cyberattack-russia-estonia/

Iro, Cecilia. (2015). *Why International Cooperation is difficult to achieve - Neolibralism theory.* "Website – Linkedin". Publicado a 21 de outubro de 2015. Disponível na internet em: https://www.linkedin.com/pulse/why-international-cooperation-difficult-achieve-cunningham-ph-d-

Katainen, Jyrki. Limnell, Jarno. (2018). *Cybersecurity and defence for the future of Europe.* "Website - euobserver". Disponível na internet em: https://euobserver.com/opinion/141556

Kopp, Emanuel. Kaffenberger, Lincoln. Wilson, Christopher. (2017). *La ciberdefensa debe ser mundial.* "Website - Diálogo a Fondo". Publicado a 26 de outubro de 2017. Disponível na internet em https://blog-dialogoafondo.imf.org/?p=8448

Lowe, Christian. (2009). *Kremlin loyalist says launched Estonia cyber-attack.* "Website – Reuters". Publicado a 13 de março de 2009. Disponível na Internet em: http://www.reuters.com/article/us-russia-estonia-cyberspace-idUSTRE52B4D820090313

Maciel, Elisabete. (2016). *Cibercrime: um rosto anónimo.* "Website – Revista Visão Online". Publicado a 11 de agosto de 2016. Disponível na internet em: http://visao.sapo.pt/opiniao/silnciodafraude/2016-08-11-Cibercrime-um-rosto-anonimo

Marazis, Andreas. (2018). *The untapped potential of EU-NATO cooperation.* "Website - Euractiv". Publicado a 10 de julho de 2018. Disponível na internet em: https://www.euractiv.com/section/defence-and-security/opinion/the-untapped-potential-of-eu-nato-cooperation/

Mariz, Vasco. (2008). *Temas da Política Internacional - ensaios, palestras e recordações diplomáticas.* In: Sua Pesquisa.com. (2004-2018). "G7". "Website – Sua Pesquisa.com". Publicado em 2008. Disponível na internet em: https://www.suapesquisa.com/economia/g7.htm

Markoff, John. (2008). *Geórgia inaugura era da ciberguerra.* "Website - Estadão". Publicado a 18 de agosto de 2008. Disponível na internet em: http://www.estadao.com.br/noticias/geral,georgia-inaugura-era-da-ciberguerra,1298

Mortimer, Caroline. (2017). *NATO to spend £2.6 billion on satellites, cyber security and drones.* "Website - Independent". Publicado a 27 de março de 2017. Disponível na internet em: http://www.independent.co.uk/news/world/politics/nato-to-spend-three-billion-euros-on-satellites-cyber-security-and-drones-a7651966.html

NATO. (2007). *NATO statement on Estonia.* "Website – Conselho do Atlântico Norte". Publicado a 3 de maio de 2007. Disponível na internet em: https://www.nato.int/docu/pr/2007/p07-044e.html

NATO. (2018). *Cyber defence.* "Website – Conselho do Atlântico Norte". Publicado a 16 de julho de 2018. Disponível na internet em: https://www.nato.int/cps/en/natohq/topics_78170.htm

Negócios. (2016). *NATO e União Europeia juntas contra o cibercrime.* "Website - Jornal de Negócios Online". Publicado a 10 de fevereiro de 2016. Disponível na internet em: http://www.jornaldenegocios.pt/empresas/detalhe/nato_e_uniao_europeia__juntas_contra_o_cibercrime

Nuwer, Rachel. (2017). *What if the internet stopped working for a day?.* "Website - BBC". Publicado a 7 de fevereiro de 2017. Disponível na internet em: http://www.bbc.com/future/story/20170207-what-if-the-internet-stopped-for-a-day

Perez, Evan. Diaz, Daniella. (2016). *White House announces retaliation against Russia: Sanctions, ejecting diplomats*. "Website – CNN". Publicado a 29 de dezembro de 2016. Disponível na Internet em: http://edition.cnn.com/2016/12/29/politics/russia-sanctions-announced-by-white-house/index.html

Ponemon Institute LCC e Accenture. (2017). *2017: Cost of Cybercrime Study.* "Website - Accenture". Pp: 1-56. Disponível na internet em: https://www.accenture.com/us-en/insight-cost-of-cybercrime-2017?src=SOMS

Público. (2017). *Trump critica dívidas à NATO, cortes na defesa e alerta aliados para novos atentados*. "Website – Jornal Público Online". Publicado a 25 de maio de 2017. Disponível na internet em: https://www.publico.pt/2017/05/25/mundo/noticia/trump-diz-que-pode-haver-mais-ataques-como-o-de-manchester-se-nao-forem-tomadas-medidas-1773484

Rear, Jack. (2017). *International Internet Day — what would happen if the internet shut down?.* "Website - Verdict". Publicado a 27 de outubro de 2017. Disponível na internet em: https://www.verdict.co.uk/international-internet-day-happen-internet-stopped/

Rodrigo Candido Freire, Antonio. (2012). *O Neoliberalismo e a Teoria da Interdependência Complexa.* "Website – Juris Way: Sistema Educacional Online". Publicado a 3 de abril de 2012. Disponível na internet em: https://www.jurisway.org.br/v2/dhall.asp?id_dh=7410

Segal, Adam. (2017). *EU Creates a Diplomatic Toolbox to Deter Cyberattacks*. "Website - Council on Foreign Relations". Publicado a 20 de junho de 2017. Disponível na internet em: https://www.cfr.org/blog-post/eu-creates-diplomatic-toolbox-deter-cyberattacks

SGMAI. (2015). *Agenda Europeia para a Segurança.* "Website - Secretaria Geral da Administração Interna". Publicado a 25 de agosto de 2015. Disponível na internet em: http://www.sg.mai.gov.pt/Noticias/Paginas/Agenda-Europeia-para-a-Seguran%C3%A7a–.aspx

The Economist. (2010). *War in the fifth domain.* "Wrbsite – The Economist". Publicado a 1 de julho de 2010. Disponível na internet em: https://www.economist.com/node/16478792

The New York Times. (2017). *Trump Says NATO Allies Don't Pay Their Share. Is That True?.* "Website – The New York Times". Publicado a 26 de maio de 2017. Disponível na internet em: https://www.nytimes.com/2017/05/26/world/europe/nato-trump-spending.html

Tomkiw, Lydia. (2016). *Quotes from Donald Trump on NATO: what republican candidate said about North Atlantic Treaty Organization and US obligations*. "Website - International Business Times". Publicado a 21 de julho de 2016. Disponível na internet em: http://www.ibtimes.com/quotes-donald-trump-nato-what-republican-candidate-said-about-north-atlantic-treaty-2393661

Páginas Web Oficiais

Agência de comunicação e informação da NATO - website oficial. (2012-2018). Página Web oficial: https://www.ncia.nato.int/Pages/homepage.aspx

Agência Europeia de Defesa - website oficial. (2004-2018). Página Web oficial: https://www.eda.europa.eu/what-we-do/activities/activities-search/cyber-defence

Agência Europeia para a gestão operacional de sistemas informáticos de grande escala no espaço de liberdade, da segurança e da justiça (eu-LISA) - website oficial. (2012-2018). Página Web oficial: http://www.eulisa.europa.eu/Pages/default.aspx

- Krum Garkov é o Diretor Executivo da eu-LISA desde 1 de novembro de 2012. Este conta no seu currículo com mais de 15 anos de experiência entre os setores públicos e privados complementados por dois mestrados na área da tecnologia e da informação e um MBA.

Agência Europeia para a Segurança das Redes e da Informação - website oficial. (2004-2018). Página Web oficial: https://www.enisa.europa.eu/

Centro Cooperativo de Defesa Cibernética de Excelência da NATO - website oficial. (2008-2018). Página Web oficial: https://ccdcoe.org/

CERT-EU – Equipa de resposta a emergências cibernéticas da União Europeia - website oficial. (2012-2018). Página Web oficial: https://cert.europa.eu/cert/filteredition/en/CERT-LatestNews.html

Chatham House the Royal Institute of International Affairs - website oficial. Ano de fundação 1920. Página Web oficial: https://www.chathamhouse.org/

Conta oficial de Twitter da Agência Europeia para a Segurança das Redes e da Informação. (2012-2018). Página Web oficial: https://twitter.com/enisa_eu

Comissão Europeia - website oficial. (1995-2018). Página Web oficial: https://ec.europa.eu/commission/index_pt

Council on Foreign Relations - website oficial. Ano de fundação 1921. Página Web oficial: https://www.cfr.org/

EUR-Lex - website oficial. (1997-2018). Página Web oficial: http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex:32004R0460

EUROPOL – website oficial. (1999-2018). Página Web oficial: https://www.europol.europa.eu/

Fórum de Governança da Internet – website oficial. (2006-2018). Página Web oficial: https://www.intgovforum.org/multilingual/

Guccifer 2.0. (2016 - 2018). Página Web oficial: https://guccifer2.wordpress.com/

Instituto de Estudos de Segurança da União Europeia - website oficial. (2002 – 2018). Página Web oficial: https://www.iss.europa.eu/

Organização do Atlântico Norte - website oficial. (1997-2018). Página Web oficial: http://www.nato.int/

União Europeia - website oficial. (1995-2018). Página Web oficial: https://europa.eu/european-union/index_pt

Wikileaks. (2006-2018). Página Web oficial: https://wikileaks.org/

Informações Complementares

Kaspersky lab. (1997-2018). *Cyberthreat real-time map.* Página Web oficial: https://cybermap.kaspersky.com/

Norse Corp. (2016-2018). *Live Attacks.* Página Web oficial: http://map.norsecorp.com/#/

ORCID. (2012-2018a). *Biografia André Barrinha*. "Website – ORCID". Disponível na internet em: https://orcid.org/0000-0002-6650-3730

ORCID. (2012-2018b). *Biografia Henrique Santos*. "Website – ORCID". Disponível na internet em: http://orcid.org/0000-0001-5389-3285

Porto Editora. (2003-2018a). *Carta das Nações Unidas.* "Website – Infopédia". Disponível na Internet em: https://www.infopedia.pt/apoio/artigos/$carta-das-nacoes-unidas

Porto Editora. (2003-2018b). *Ciberterrorismo.* "Website – Infopédia". Disponível na internet em: https://www.infopedia.pt/dicionarios/lingua-portuguesa/ciberterrorismo

Porto Editora. (2003-2018c). *Encriptar.* "Website – Infopédia". Disponível na internet em: https://www.infopedia.pt/dicionarios/lingua-portuguesa/encriptar

ANEXOS

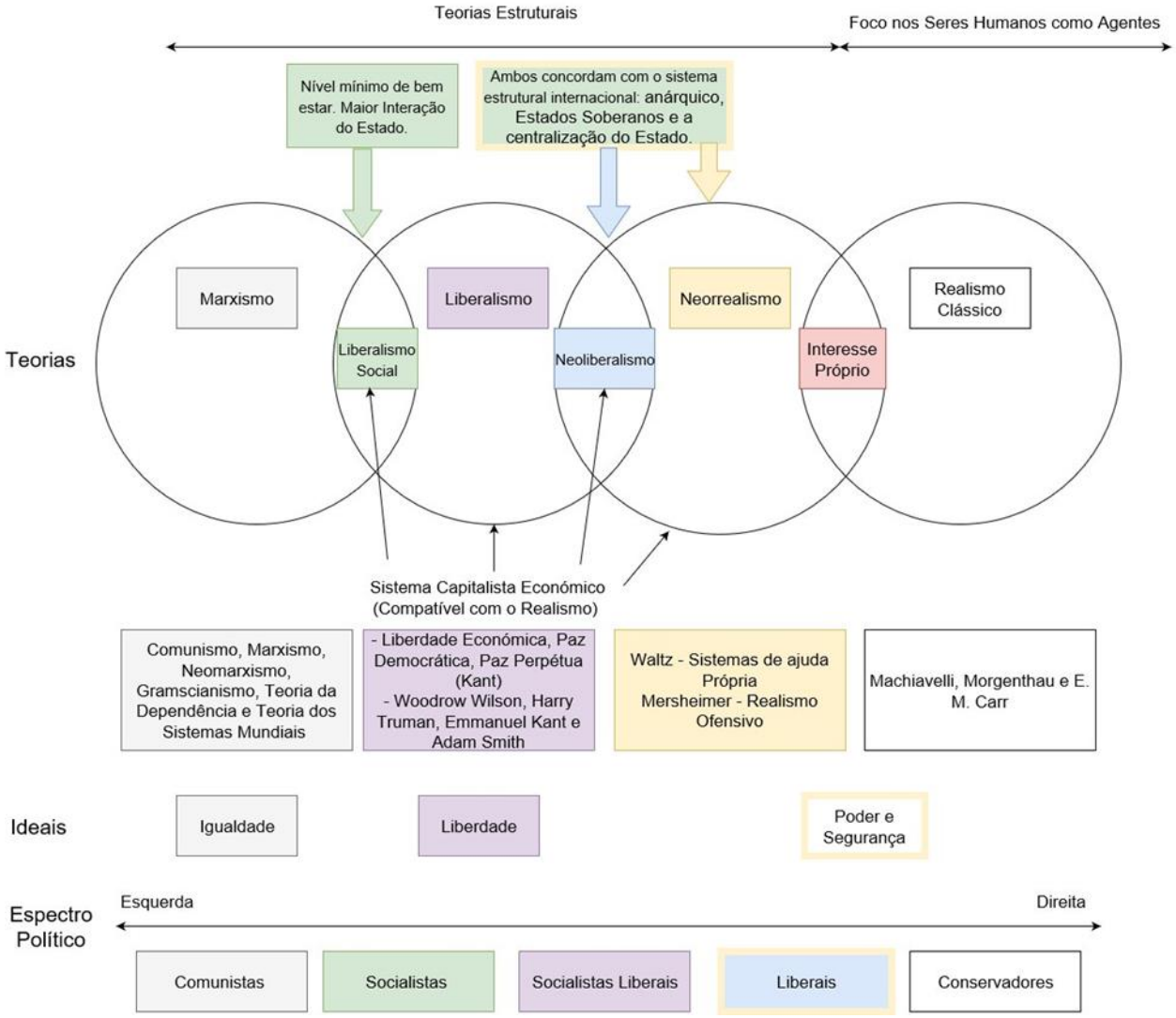


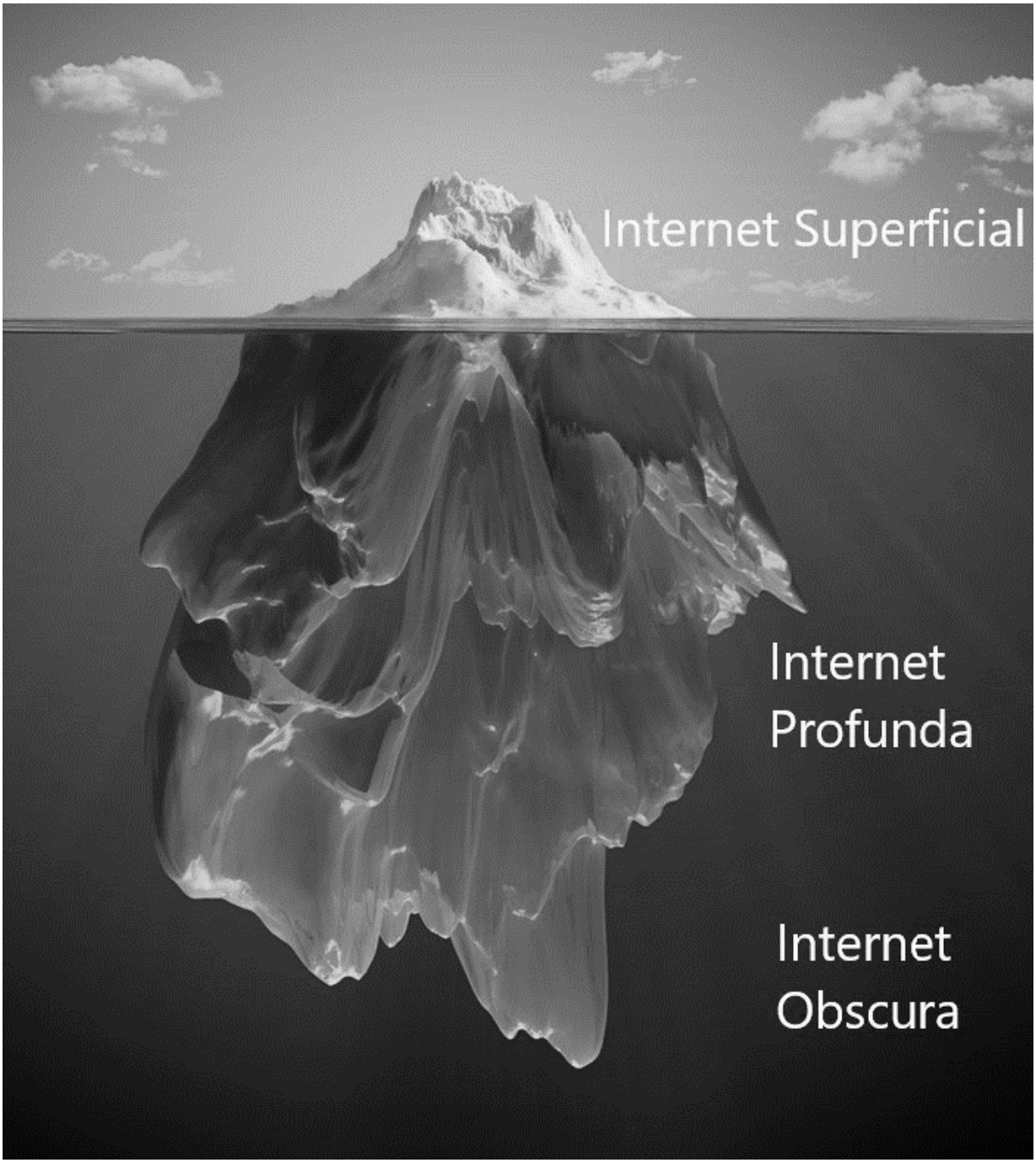
Tabela 1 – Teorias das Relações Internacionais (Gardezi, 2010).

União Europeia	
2001	Convenção Europeia do cibercrime em Budapeste/ (Plano de ação antiterrorista);
2003	Sugestão de um protocolo adicional a convenção Europeia do cibercrime;
2004	ENISA;
2005	Decisão do conselho Europeu relativa ao impedimento de ataques contra os sistemas de informação;
2006	Protocolo adicional a convenção Europeia do cibercrime/ EISAS;
2007	Ataque a Estónia;
2008	EPCIP/ Relatório sobre a execução da estratégia Europeia de segurança;
2009	O surgimento de um plano detalhado para a aplicação do EPCIP;
2010	Estratégia de segurança interna da União Europeia
2012	eu-LISA/ CERT-UE;
2013	EC3/ Estratégia da União Europeia para a cibersegurança/ Diretiva sobre ataques contra sistemas de informação;
2014	Regulação eIDAS;
2015	Estratégia digital de mercado único/ Agenda Europeia de segurança;
2016	Estratégia global/Regulamento RGPD/ Diretiva SRI/NIS;
2017	Retificação do protocolo adicional a convenção Europeia do cibercrime/ Ciberataques = guerra/ Reforma da cibersegurança.
2018	Regulamento Cibersegurança/Implementação do RGPD

Tabela 2 – Ordem cronológica dos eventos cibersecuritários no seio da União Europeia.

NATO	
1999	Cimeira de Washington;
2002	Cimeira de Praga;
2004	NCIRC I (fundação);
2005	Proposta para que infraestruturas críticas fizessem parte da agenda contraterrorista;
2006	Cimeira de Riga/ Publicação do documento orientação política global;
2007	Ataque a Estónia/ NC3B;
2008	Cimeira de Bucareste/ Ciberdefesa/ CCDCOE/ NCDMA;
2010	Cimeira de Lisboa/ Conceito estratégico;
2011	"Revisão da ciberdefesa e plano de ação para a sua implementação" (IDN, 2013: 60);
2012	Cimeira de Chicago/ NCIA/ NCIRC I (estabilização);
2014	Cimeira de Gales/ Ministros da defesa/ NCIRC I (capacidade máxima);
2016	Cimeira de Varsóvia/ NATO-UE;
2017	NCIRC II (aprovação)
2018	Cimeira de Bruxelas
2019	Academia de comunicação e informação de Oeiras (prazo estabelecido para a conclusão)

Tabela 3 – Ordem cronológica dos eventos cibersecuritários no seio da NATO.



Anexo IV – As diferentes camadas do ciberespaço (Harada, 2015).