ACADEMIA DA FORÇA AÉREA

# O Ciberespaço como Dimensão de Segurança

**Marcelo da Silva Aparício**

***Aspirante a Oficial-Aluno Piloto-Aviador 138261-G***

Dissertação para obtenção do Grau de Mestre em

**Aeronáutica Militar, na Especialidade de Piloto-Aviador**

**Júri**

| | |
|---|---|
| Presidente: | Major-General José Manuel dos Santos Vicêncio |
| Orientador: | Professora Doutora Sandra Maria Rodrigues Balão |
| Coorientador: | Tenente-Coronel Luís Manuel Pinto de Almeida Rocha |
| Vogal: | Professora Doutora Helena Cristina Rêgo |

**Sintra, Maio de 2017**

*(página intencionalmente em branco)*

ACADEMIA DA FORÇA AÉREA

# O Ciberespaço como Dimensão de Segurança


**Marcelo da Silva Aparício**

***Aspirante a Oficial-Aluno Piloto-Aviador 138261-G***


Dissertação para obtenção do Grau de Mestre em

**Aeronáutica Militar, na Especialidade de Piloto-Aviador**

**Júri**

| | |
|---|---|
| Presidente: | Major-General José Manuel dos Santos Vicêncio |
| Orientador: | Professora Doutora Sandra Maria Rodrigues Balão |
| Coorientador: | Tenente-Coronel Luís Manuel Pinto de Almeida Rocha |
| Vogal: | Professora Doutora Helena Cristina Rêgo |

**Sintra, Maio de 2017**

*Este trabalho foi elaborado com finalidade essencialmente escolar, durante a frequência do Curso de Pilotagem Aeronáutica cumulativamente com a atividade escolar normal. As opiniões do autor, expressas com total liberdade académica, reportam-se ao período em que foram escritas, mas podem não representar doutrina sustentada pela Academia da Força Aérea.*

# Agradecimentos

A presente dissertação de mestrado conclui o culminar de uma árdua etapa, que só foi possível realizar com a preciosa ajuda de várias pessoas e instituições.

Deste modo, em primeiro lugar quero agradecer à Sra. Professora Sandra Balão pela sua orientação, por elevar os meus parâmetros fazendo-me exigir sempre mais e melhor. Por toda a sua disponibilidade, ajuda e transmissão de conhecimentos, sem os quais não teria sido possível realizar esta dissertação.

Ao Sr. Tenente-Coronel Luís Rocha, pelo voto de confiança que me deu, exprimido na liberdade com que permitiu realizar este trabalho, e por todos os conselhos académicos que transmitiu, demonstrando-se sempre disponível.

Relativamente a todo o trabalho de pesquisa bibliográfica realizado, fica uma palavra de agradecimento à Sargento Ajudante Dulce Maria, responsável pela biblioteca da AFA, por todo o apoio e ajuda proporcionada muito para além do dever.

À Academia da Força Aérea agradeço todas as condições proporcionadas durante a realização desta dissertação, possibilitando o acesso a recursos que em muito enriqueceram e contribuíram para o sucesso do presente trabalho.

Aos Barões agradeço todo o apoio incondicional e fraternidade partilhada neste percurso que percorremos juntos.

Um agradecimento especial aos meus amigos que nunca deixaram de me apoiar e que nunca deixaram a ausência ser um motivo de distância.

À minha família agradeço toda a educação e orgulho transmitido, e por nunca deixarem de acreditar em mim.

Por último agradeço à Inês, que me acompanhou em todas as aventuras, dificuldades e sucessos, por ser o pilar da minha vida e pela vida que juntos trazemos a este mundo.

A todos os que me ajudaram e acompanharam, o meu sincero **Obrigado**!

*(página intencionalmente em branco)*

# Resumo

Num mundo cada vez mais dependente do uso tecnológico, o ciberespaço constitui um dos maiores desafios da atualidade a nível social, económico, político, cultural, tecnológico e militar, razões que justificam a sua "classificação" como um domínio de influência na esfera das Relações Internacionais.

O aumento do uso da *internet* e do número de dispositivos que a esta podem aceder veio transformar o modo de funcionar do mundo, criando inúmeras oportunidades mas permitindo, ao mesmo tempo, o aparecimento de ameaças reais e preocupantes - que afetam tanto a privacidade e segurança do cidadão comum, como as infraestruturas críticas de um Estado.

A emergência de ciberataques como o da Estónia em 2007 ou da Geórgia em 2008 vieram demonstrar a necessidade de um investimento e desenvolvimento de capacidades de ciberdefesa e cibersegurança mas, também, a carência de documentos estratégicos e políticos sobre o domínio do ciberespaço.

Organizações Internacionais como a ONU, a NATO, e a UE têm vindo a desenvolver as suas capacidades de ciberdefesa para poderem dar resposta às ameaças emergentes do ciberespaço. No entanto, realçam a importância de que este mesmo tipo de iniciativas seja levado a cabo por parte dos seus Estados Membros a título individual, além de que também é imprescindível assegurar a cooperação entre eles para que seja possível atingir o sucesso perante este desafio.

De facto, algo que o ciberataque contra a Geórgia veio revelar é a capacidade existente de coordenar o domínio "ciber" com os outros domínios de operações militares tradicionais, levando assim à possibilidade de uma ciberguerra ser despoletada ou, mesmo, de se invocar o artigo 5º do Tratado do Atlântico Norte.

Neste sentido, torna-se imperativo abordar o ciberespaço como o domínio operacional que é, promovendo medidas de ciberdefesa e cibersegurança nas principais Organizações Internacionais e nos seus Estados Membros, neste cenário atual de dependência tecnológica em que vivemos e que o Homem, graças ao saber e conhecimento, projetou para o século XXI.



**Palavras chave**: Ciberespaço; Ciberdefesa; Cibersegurança; Ciberameaças; Relações Internacionais.

## Abstract

In a world that is increasingly dependent on the use of technology, cyberspace is one of the greatest challenges in social, economic, political, cultural, technological and military terms, justifying its "status" as a sphere of influence of International Relations.

The increased use of internet and the number of devices that can access to it has transformed the way the world works, creating numerous opportunities while, at the same time, allowing the emergence of real and troubling threats - affecting the privacy and security of the ordinary citizen as well as the critical infrastructures of a State.

The emergence of cyber-attacks such as Estonia's in 2007 or Georgia's in 2008 demonstrated the need for investment and the development of cyber-security and cyber-safety capabilities, but also the lack of strategic and policy documents on the domain of cyberspace.

International organizations such as the UN, NATO, and the EU have been developing their cyber-defense capabilities to address the emerging threats of cyberspace. However, they stress the importance of such individual initiatives being undertaken by individual Member States, and cooperation between them must also be ensured in order to achieve success in the face of this challenge.

Indeed, something that the cyber-attack against Georgia has revealed is the existing ability to coordinate the cyber domain with the other domains of traditional military operations, thus leading to the possibility of a Cyberwar being triggered or even the invocation of the North Atlantic Treaty's 5$^{th}$ article.

In this sense, it is imperative to approach cyberspace as the operational domain that it is, by promoting cyber-security and cyber-safety measures in the main International Organizations and in their Member States, due to the current scenario of technological dependence in which we live and thanks to the knowledge and wisdom that mankind designed for the 21$^{st}$ century.



**Key words**: Cyberspace; Cyber-defense; Cyber-safety; Cyber-threats; International Relations.

# Índice

**INTRODUÇÃO** ..... **1**

1.1. CONTEXTUALIZAÇÃO ..... 2
1.2. ÂMBITO ..... 4
1.3. OBJETO DE ESTUDO ..... 7
1.4. REVISÃO DE LITERATURA ..... 8
1.5. CONCEPTUALIZAÇÃO OPERACIONAL ..... 11
1.6. PERSPETIVAS DE ANÁLISE NO ÂMBITO DAS TEORIAS DAS RELAÇÕES INTERNACIONAIS ..... 16
1.7. MOTIVAÇÃO E PERTINÊNCIA ..... 23
1.8. PANORÂMICA ..... 25

**NOTA METODOLÓGICA** ..... **27**

*2.1. Formulação da Pergunta de Partida* ..... *30*
*2.2. Hipóteses de Trabalho* ..... *31*

**CAPÍTULO 1 - O CIBERESPAÇO COMO NOVO ESPAÇO DE CONFLITO** ..... **33**

**CAPÍTULO 2 – O *STATU QUO* DA CIBERDEFESA E CIBERSEGURANÇA NO SÉCULO XXI** **51**

2.1. ONU ..... 53
2.2. NATO ..... 54
2.3. UE ..... 59

**CAPÍTULO 3 – ESTUDO DE CASO: ATAQUE CIBERNÉTICO À GEÓRGIA** ..... **75**

**CONCLUSÃO** ..... **85**

**REFERÊNCIAS BIBLIOGRÁFICAS** ..... **91**

# Índice de Figuras

FIGURA 1 - MAPA-MUNDO COM A DISTRIBUIÇÃO DE REDE 4G, 3G E 2G (FEV 2016) ..... 38
FIGURA 2 - CUSTO DA SUBSCRIÇÃO DE SERVIÇO DE BANDA LARGA COMO PERCENTAGEM DO SALÁRIO MÉDIO ANUAL ..... 40
FIGURA 3 - ATAQUES DDOS A ACONTECER NO MUNDO A 17 MARÇO 2017 (PELAS 18:00 HORAS) ..... 41
FIGURA 4 - ATAQUES DDOS A ACONTECER EM PORTUGAL A 17 DE MARÇO DE 2017 (PELAS 18:20 HORAS) ..... 42
FIGURA 5 - DIAGRAMA DA INTERDEPENDÊNCIA DAS INFRAESTRUTURAS CRÍTICAS NACIONAIS ..... 48
FIGURA 6 - MAPA DA GEÓRGIA, COM LOCALIZAÇÃO DA ABKHAZIA E OSSÉTIA DO SUL ..... 76

# Índice de Tabelas

TABELA 1 - ESTATÍSTICAS DA POPULAÇÃO E USO DE *INTERNET* MUNDIAL (25 MAR 2017) ..... 37
TABELA 2 - ESTATÍSTICAS DA POPULAÇÃO E USO DE *INTERNET* MUNDIAL (30 NOV 2015) ..... 39

# Lista de Acrónimos

| | |
|---|---|
| 2G | 2ª Geração |
| 3G | 3ª Geração |
| 4G | 4ª Geração |
| APT | *Advanced Persistent Threat* |
| CCD COE | *Cooperative Cyber Defence Center of Excellence* |
| CDMA | *Cyber Defence Management Authority* |
| CDRA | *Cyber Defence Research Agenda* |
| CE | Conceito Estratégico |

| | |
|---|---|
| CEDN | Conceito Estratégico de Defesa Nacional |
| CERT | *Computer Emergency Response Team* |
| CERT-EU | *Computer Emergency Response Team of the Eutopean Union* |
| CIA | *Central Intelligence Agency* |
| CNO | *Computer Network Operations* |
| CSDP | *Common Security and Defence Policy* |
| CSIRT | *Computer Security Incident Response Team* |
| DDoS | *Distributed Denial of Service* |
| DoD | *Department of Defense* |
| EDA | *European Defence Agency* |
| ENISA | *European Network and Information Security Agency* |
| EUA | Estados Unidos da América |
| EUMS | *EU Military Staff* |
| Europol | *European Police Office* |
| FBI | *Federal Bureau of Investigation* |
| GGE | *Group of Governmental Experts* |
| HP | Hipótese de Trabalho |
| ICN | Infraestruturas Críticas Nacionais |
| IIG | Infraestrutura de Informação Global |
| IP | *Internet Protocol* |
| IoT | *Internet of Things* |
| J-CAT | *Joint Cybercrime Action Taskforce* |
| JSF | *Joint Strike Fighter* |
| NATO | *North Atlantic Treaty Organization* |
| NCIRC | *NATO Computer Incident Responce Capability* |
| NIS | *Network and Information Security* |
| NSA | *National Security Agency* |
| NTIC | Novas Tecnologias de Informação e Comunicação |
| NU | Nações Unidas |
| ONU | Organização das Nações Unidas |
| OSCE | *Organization for Security and Cooperation in Europe* |

| | |
|---|---|
| PD | Pergunta Derivada |
| PLA | *People's Liberation Army* |
| R&D | *Research and Development* |
| REN | Rede Elétrica Nacional |
| RI | Relações Internacionais |
| RRT | *Rapid Reaction Teams* |
| RoE | *Rules of Engagement* |
| SEA | *Syrian Electronic Army* |
| SIG | Sistema de Informações Global |
| SIS | Serviço de Informações e Segurança |
| TIC | Tecnologias de Informação e Comunicação |
| TRANSCOM | *U.S. Transportation Command* |
| UAV | *Unmanned Aerial Vehicle* |
| UE | União Europeia |
| UNIDIR | *United Nations Institute for Disarmament Research* |
| WWW | *World Wide Web* |

# Glossário

***Botnet*** - são computadores com ligação à *internet*, controlados sem o conhecimento dos seus donos, que fazem transmissões (como vírus e *spam*) para outros computadores através da *internet*. São conhecidos por exército *zombie* e os computadores que a este estão associados são geralmente aqueles que têm uma fraca *firewall* ou serviços de proteção e antivírus (Rouse, 2012).

**DDoS** - é um ataque feito a partir de vários computadores, a um sistema ou rede, que impede o acesso dos seus utilizadores, causando tipicamente uma perda

de conexão aos serviços disponíveis na rede, devido ao consumo da largura de banda da rede ou pela sobrecarga dos recursos computacionais do sistema ou rede afetado (APDSI, 2007).

***Hackers*** - são indivíduos dotados de um nível elevado de conhecimentos sobre redes e sistemas de acesso a computadores, e que utilizam estes conhecimentos para entrar em sistemas alheios, encontrando e explorando os seus pontos fracos (APDSI, 2007).

**Hacktivismo** - é o conceito referente ao *hacking* levado a cabo em função de motivações políticas (Oxford LD, [s.d.]).

***Host*** - *Host* ou o *Computer Host* é o computador principal num sistema de dois ou mais computadores, sendo este o que desempenha as funções de controlo (APDSI, 2007).

**Largura de banda** - é a capacidade de transmissão de dados, expressa pela quantidade máxima de informação transmitida por unidade de tempo (APDSI, 2007).

***Malware*** - é um programa informático, desenvolvido com o intuito de alterar, perturbar ou mesmo destruir todas ou parte das unidades necessárias para o correto funcionamento de um determinado sistema informático (APDSI, 2007).

*(página intencionalmente em branco)*

# Introdução

O ciberespaço constitui um dos mais marcantes desafios do século XXI nas sociedades humanas, num âmbito social, político, económico, tecnológico e cultural, sendo deste modo uma temática influente nas Relações Internacionais.

Atualmente, é difícil imaginar um mundo sem *internet* e, por isso, sem ciberespaço. A nossa sociedade está dependente do seu uso, quer sejam as plataformas no universo do ensino, os motores de busca, o uso da "cloud", as infraestruturas críticas de qualquer Estado e ou, mesmo, uma simples ida ao nosso banco - a um "clique de distância".

De facto, a realidade em que vivemos é bastante diferente da do século passado, devido à grande evolução e desenvolvimento do sector tecnológico. Com ela surgiram inúmeras oportunidades mas, também, potenciais ameaças (Balão, 2010).

A dependência da sociedade face ao uso do ciberespaço é atualmente um fator crítico da nossa economia e segurança, quer em termos individuais, quer coletivos pois muita informação crítica acaba por estar acessível, de forma mais ou menos direta e ou imediata, *online*. Nos dias de hoje podemos aceder não só à nossa informação pessoal em redes sociais como à da nossa conta bancária, por exemplo. E esta pode ser acedida não só por nós como por pessoas ou programas que passam pelas nossas medidas de cibersegurança e ciberdefesa, podendo colocar em perigo não apenas a nós próprios como todos aqueles aos quais estamos ligados em rede (Martins, 2012).

Numa perspectiva mais global, um potencial ciberataque a um Estado ou a uma Organização Internacional, assume uma dimensão de efeitos, também eles, potencialmente devastadores. Neste contexto, é importante ter presente que nos últimos anos foram registados diversos ciberataques, não só a Estados como a organizações privadas e mesmo a infraestruturas militares (como foi o exemplo da

Estónia em 2007, cenário no âmbito do qual tanto o governo como os setores públicos e privados foram alvo de uma série de ciberataques coordenados) (Rehman, 2013). Estes ataques estão a tornar-se mais frequentes e organizados, ameaçando não só a segurança e estabilidade, como a prosperidade de cada Estado em geral e da comunidade Euro-Atlântica, em particular (NATO, 2010).

No entanto, devido à sua natureza, é extremamente difícil determinar a origem de um ciberataque, assim como a posterior reação perante o mesmo. Isto é, como irá reagir um Estado ou uma Organização Internacional em face de um ataque cuja origem não consegue identificar? Como pode ser declarada guerra a uma ofensiva de origem não identificada?

Em face das considerações apresentadas, constitui objetivo deste trabalho académico analisar não só o ciberespaço como um (novo) espaço de conflito mas, também, refletir sobre as medidas atuais de ciberdefesa e cibersegurança, apresentadas no quadro da North Atlantic Treaty Organization (NATO) e União Europeia (UE). Deste modo, considera-se evidenciada a pertinência deste objeto no quadro das preocupações que se perfilam, simultaneamente, no contexto das Relações Internacionais em geral e da vertente dos estudos securitários em particular.

## 1.1. Contextualização

O conceito de ciberespaço surgiu com uma história de 1982 de William Gibson intitulada de *"Burning Chrome*", sendo mais tarde popularizada no romance "Neuromancer" de 1984. Neste, Gibson refere-se ao ciberespaço como uma representação gráfica do conjunto de dados computacionais existentes, retirados de computadores do sistema humano (Gibson, 1984).

Embora a obra de Gibson fosse ficção, o ciberespaço desenvolveu-se ao longo dos anos chegando aos dias de hoje como uma vasta dimensão de uso diário e massivo.

O ciberespaço é atualmente reconhecido como uma rede global que liga entre si infraestruturas de tecnologias e informação, com destaque para as redes de telecomunicações e para os sistemas de processamento dos computadores, estando maioritariamente associado à *internet* (Fernandes, 2012).

A sua importância tem vindo a aumentar gradualmente ao longo dos anos, pois tem acompanhado os avanços e as necessidades tecnológicas da sociedade, assumindo diversas formas: redes sociais, plataformas de serviços públicos *online*, de natureza privada e ou comercial, procurando incessantemente soluções para os problemas do quotidiano. Verifica-se, assim, uma transferência da atividade humana para o universo digital (Barrinha e Carrapiço, 2016).

Em 2007 verificou-se que mais de 50% dos agregados familiares na UE-28 tinham acesso à *internet* (55%), tendo essa percentagem continuado a aumentar atingindo os 81% em 2014. No Luxemburgo e nos Países Baixos verificou-se a maior percentagem, chegando a uns impressionantes 96% no ano de 2014 (Eurostat, 2016).

Hoje em dia, um cidadão pode usufruir de uma vasta gama de serviços *online*, não só a partir do seu computador ou telemóvel mas também através de relógios, televisões ou mesmo eletrodomésticos. Relevante é destacar que estes serviços não só permitem socializar, como aprender, trabalhar, fazer compras e até gerir contas bancárias ou regularizar situações fiscais (Barrinha e Carrapiço, 2016).

Deste modo, as ameaças inerentes do ciberespaço e da implementação do acesso aos mais variados serviços através da *internet*, apresentam-se não só apenas ao nível do cidadão comum (como a invasão de privacidade), mas também numa perspetiva mais global e alarmante, como por exemplo a espionagem, a propagação de vírus e mesmo o roubo de informação sensível numa esfera governamental (Martins, 2012).

A cibersegurança surge, então, como uma necessidade, e atualmente é reconhecida a sua importância pelos Estados e principais Organizações Internacionais (NATO, 2010). Duas das maiores potências mundiais a nível

tecnológico identificam a influência que a cibersegurança representa, sendo que para o governo dos Estados Unidos da América (EUA), a cibersegurança é atualmente uma prioridade estratégica, pelo aumento de ataques cibernéticos ao Estado, enquanto que para o governo Chinês, é um ponto crucial numa esfera de segurança mas também ao nível do desenvolvimento económico e tecnológico (Barrinha e Carrapiço, 2016).

## 1.2. Âmbito

A presente dissertação de mestrado constitui um trabalho académico realizado no âmbito da área científica de Relações Internacionais (RI), sendo este decorrente da frequência do curso de Mestrado Integrado em Ciências Militares e Aeronáuticas, lecionado na Academia da Força Aérea, na especialidade de Piloto-Aviador.

A liberdade académica e isenção política foram os valores que regeram toda a investigação científica e posterior análise e tratamento de informação levada a cabo no âmbito desta dissertação.

É necessário também dar importância ao facto da presente dissertação ter sido realizada numa instituição militar de ensino superior público, e como tal, a ela estão subjacentes valores e princípios que constituem pressuposto incontornável na formação de um futuro Oficial das Forças Armadas.

Tendo como área de investigação as Relações Internacionais, é imprescindível ter presente tanto o conceito como a abrangência desta área científica de conhecimento, de modo a ser possível garantir a melhor contextualização possível do objeto de estudo a desenvolver.

Assim, e na linha daquilo que é defendido pelo Professor Adriano Moreira, consideramos que o domínio das Relações Internacionais é “o conjunto de relações entre entidades que não reconhecem um poder político superior, ainda que não

sejam estatais, somando-se as relações diretas entre entidades formalmente dependentes de poderes políticos autónomos" (Moreira, 2014, p.54). Como tal, nas Relações Internacionais são considerados diversos atores, como os Estados, as organizações internacionais, os poderes erráticos, as instituições espirituais, e por fim os indivíduos.

As Relações Internacionais constituem, em si mesmas, um ambiente que nos rodeia, fazendo parte do nosso quotidiano, mesmo sem que, muitas vezes, nos apercebamos da sua vasta dimensão e abrangência. Sendo assim, a complexidade do seu estudo justifica a necessidade de se apoiar em várias disciplinas, "que, genericamente, podem ser indicadas como sendo aquelas cujo campo classicamente definido vem a ser interceptado por esta nova perspectiva." (Moreira, 2014).

Deste modo, devido à abrangência do âmbito de estudo das Relações Internacionais e ao seu carácter interdisciplinar, torna-se necessário um estudo multidisciplinar e amplo nas mais diversas áreas da ciência contemporânea (Dougherty e Pfaltzgraft Jr., 2003), tais como, o direito internacional, a geografia, a economia, a política, de entre outras.

O estudo elaborado para esta dissertação de mestrado tem como foco o ciberespaço como dimensão de segurança, e como tal, é necessário equacionar as ameaças que aquele espaço representa ou engloba, assim como o consequente reconhecimento (ou não) das mesmas, enquanto tal, pelos Estados e Organizações Internacionais (NATO e UE).

O Conceito Estratégico de Defesa Nacional (CEDN) português, por exemplo, identifica a cibercriminalidade e o ciberterrorismo não só como ameaças ou risco no domínio da Segurança Nacional, mas também na esfera global (MDN, 2013).

Nos dias de hoje verifica-se uma grande facilidade de acesso ao ciberespaço, e aos resultados do rápido e complexo desenvolvimento tecnológico, que engloba tanto redes sociais e informação pessoal, como o desenvolvimento de

empresas e a própria economia dos estados. No mesmo sentido, é também importante estar consciente da automatização resultante da introdução das Tecnologias de Informação e Comunicação (TIC) em praticamente todos os setores da nossa sociedade, inclusivamente aqueles reconhecidos pela Comissão Europeia como infraestruturas críticas nacionais (ICN), como por exemplo os transportes, a energia ou a água (Escravana, Lima e Ribeiro, 2012). Deste modo, parece fazer cada vez mais sentido considerar que: "A cibercriminalidade, porquanto os ciberataques são uma ameaça crescente a infraestruturas críticas, em que potenciais agressores (terroristas, criminalidade organizada, Estados ou indivíduos isolados) podem fazer colapsar a estrutura tecnológica de uma organização social moderna" (MDN, 2013, p.22).

Esta ameaça é real e necessita da devida atenção por parte de todos nós enquanto cidadãos, bem como do Estado pois, como escreve Marco Martins: "Assiste-se na arena internacional a novas formas emergentes de ameaças que cada vez mais se posicionam na rede cibernética, provocando a deslocação do campo de batalha para o ciberespaço" (Martins, 2012, p.32).

Deste modo, considerando-se a evolução dos ataques cibernéticos tal como o seu atual reconhecimento como uma ameaça global, justifica-se a importância de uma pesquisa e análise do ciberespaço como espaço de conflito, bem como do *statu quo* da ciberdefesa e cibersegurança no século XXI.

Neste contexto, e assumindo que o ciberespaço cada vez mais se apresenta como tendo evoluído (ou estando a fazê-lo) para uma dimensão de "campo de batalha", torna-se necessária uma análise (sistemática primeiro, e crítica depois) aos principais documentos que definem a forma de atuação de um Estado membro da NATO ou UE perante um ciberataque, nomeadamente – e assumindo, a nosso ver, particular interesse - a questão da possibilidade e consequente legitimidade de invocar, ou não, o artigo 5º do Tratado do Atlântico Norte, também conhecido por Tratado de Washington (NATO, 1949). Esta questão assume particular relevância, tanto na estrita perspectiva das Relações Internacionais como

no âmbito mais amplo dos atuais desafios que a comunidade internacional enfrenta em pleno século XXI.

## 1.3. Objeto de Estudo

Face ao que tem vindo a ser exposto, é extremamente importante definir o objeto de estudo da dissertação pois é este que vai definir os limites da análise que se pretende efetuar. Deste modo, procura-se garantir uma base sólida e objetiva da análise enquanto, simultaneamente, se busca reduzir a possibilidade de sermos confrontados com imprecisões ou ambiguidades, o que é essencial para que este trabalho possa assumir o carácter científico esperado (Quivy e Campenhoudt, 2008).

Como tal, é de extrema importância limitar a análise empírica no espaço, tanto geográfico como social, e no tempo (ibidem).

No que diz respeito à delimitação geográfica do ciberespaço, é necessário perceber que o ciberespaço, não tendo uma dimensão física, é melhor compreendido através de uma análise geográfica (Nunes, 2015).

Sendo assim, a *internet* é a principal rede no âmbito da qual se acede ao ciberespaço, e o seu desenvolvimento e crescimento geográfico é bastante importante no que diz respeito às esferas culturais, políticas e económicas (ibidem).

No que diz respeito à limitação social, o ator em questão é o Estado, e a análise será efetuada a um nível estratégico nacional e supranacional (multilevel analysis) (Balão, 2014), culminando num caso de estudo sobre o ataque cibernético à Geórgia em 2008.

Relativamente à limitação temporal, o período da análise será o século XXI, por se considerar que é neste que se verifica a grande evolução da dimensão do ciberespaço (associada ao aprofundamento do uso da *internet*), e

consequentemente, da sua evolução como um espaço de conflito e “facilitador” de disseminação de potenciais ameaças.

Neste contexto, será considerado um caso de estudo de modo a buscar fundamentar a análise, recorrendo a factos documentados e analisados em situações reais.

## 1.4. Revisão de Literatura

O ciberespaço pode ter começado como um assunto de ficção científica, mas faz atualmente parte das nossas vidas, constituindo uma dimensão paralela à “tradicional” dimensão física e à qual tem vindo a ser dada e reconhecida crescente relevância, em vários domínios e por várias razões, tendo vindo a ser estudada cada vez mais extensiva e intensivamente, por vários autores de referência tanto na cena internacional como nacional.

Em 1998 Rob Kitchin publicou um livro importante sobre o ciberespaço. Nele, o autor debate as mudanças sociais verificadas nas sociedades humanas, a maneira como comunicamos ou fazemos negócios, e também a importância do ciberespaço na nossa economia, assim como na forma como as tecnologias estão a mudar as nossas vidas (Kitchin, 1998).

Em “Deciphering Cyberspace” da autoria de Leonard C. Shyles, é examinado o ciberespaço a partir de três perspetivas: tecnologia, mercado financeiro, e política. Ao estudar o ciberespaço nestas perspetivas, o autor transmite uma visão abrangente, mas clara, em como o ciberespaço está a criar um impacto, não só no aspeto social das nossas vidas, mas também no legal (Shyles, 2002).

Seymour Goodman e Herbert Lin escreveram um livro intitulado “Toward a Safer and More Secure Cyberspace”, sendo este de referência no que diz respeito a ciberataques e cibersegurança, pois mostra o quão importante é para as nossas vidas ter acesso a um ciberespaço seguro e o quão vulneráveis são os nossos

sistemas de segurança a ele associados face às (novas) ameaças que nele pululam (Lin e Goodman, 2007).

A professora Sandra Balão, do Instituto Superior de Ciências Sociais e Políticas da Universidade Técnica de Lisboa, publicou em 2010 um artigo sobre a Geopolítica e Geoestratégia do Ciberespaço, nele apresentando uma importante reflexão sobre a necessidade da existência de uma Estratégia da Informação Nacional em articulação com a assumida importância e emergência do ciberespaço como chave nos sistemas de informação e comunicação (Balão, 2010).

Em 2012, o Tenente-Coronel Viegas Nunes, publica a obra: "Definição de uma Estratégia Nacional de Cibersegurança". Nesta, Nunes refere a importância de "reduzir o risco social e potenciar a utilização do ciberespaço" e também a necessidade do "levantamento de novas capacidades, à revisão dos seus modelos de governação e à geração de competências, cada vez mais associadas à exploração das TIC, ao acesso à *internet* e à utilização do ciberespaço" (Nunes, 2012, p.113).

Segundo o professor da Universidade de Évora, Marco Martins, "*A internet representa uma realidade incontornável das relações internacionais no quadro político e da segurança internacional*.", e também que "*as novas tecnologias revolucionaram o mundo como também provocaram um sentimento negativo em torno do fator de segurança, nomeadamente em questões de privacidade e garantia dos sistemas de informação do Estado.*" (Martins, 2012, p.32). Assim, este autor procura demonstrar que é muito difícil afirmar que um sistema de informação é totalmente seguro e invulnerável, pelo que se verifica existirem vários problemas no que diz respeito à segurança internacional.

Um dos mais importantes estudos e reflexões conhecidos acerca da história dos conflitos do ciberespaço foi desenvolvido por Jason Healy. Este escreveu um livro no qual acompanha eventos de 1986 a 2012, que apresentam o ciberespaço como um instrumento dotado de uma dimensão punitiva, repleta de disputas para se atingir superioridade entre nações, e também as lições que os líderes políticos e militares devem reter (Healey, 2013).

Cybersecurity and Cyberwar: What Everyone Needs to Know é o título do livro escrito por Singer e Friedman. Neste, é demonstrada não só a importância da relação entre ciberespaço e cibersegurança, como as ações que nós como cidadãos podemos tomar no nosso dia-a-dia para que estejamos mais seguros e também para não comprometermos a segurança daqueles que a nós estão ligados (Singer e Friedman, 2014).

Outro autor importante no estudo de conflitos do ciberespaço é William D. Bryant. Este escreveu sobre como é importante, no âmbito do estudo dos conflitos internacionais, compreender a superioridade do ciberespaço, para perceber as batalhas entre nações nesta dimensão. São analisados e explicados oito conflitos ao longo da sua obra e é demonstrada a importância da superioridade no ciberespaço para as operações militares (Bryant, 2016).

No contexto da análise necessária para a elaboração do estudo de caso - o ataque cibernético à Geórgia -, é relevante referir a importância de obras como, Cyberwar Case Study: Georgia 2008 por David Hollis. Nesta, é feita não só uma análise ao ataque contra a Geórgia em 2008, como aos seus antecedentes, e ainda que lições se podem tirar das operações realizadas (Hollis, 2011).

Outra importante obra sobre o ataque cibernético à Geórgia é o artigo escrito pelo capitão do exército dos EUA Paulo Shakarian intitulado “Análise da Capanha Cibernética da Rússia Contra a Geórgia, em 2008” onde o autor analisa o desenvolvimento dos eventos na Geórgia, dando ênfase à coordenação entre as operações no domínio do ciberespaço e as levadas a cabo pelas forças convencionais. Este autor examina, ainda, os pormenores da participação russa nos ataques efetuados (Shakarian, 2011).

O professor Armando Marques Guedes escreveu, por seu lado, um livro intitulado “A Guerra dos Cinco Dias: A invasão da Geórgia pela Federação Russa”. Esta obra é extremamente importante para o desenvolvimento do estudo de caso, pois explica a história e os contornos dos conflitos que têm envolvido a Geórgia e a Rússia nos últimos séculos, para além de fazer uma análise da invasão à Geórgia

em 2008, tecendo considerações sobre interesses políticos, estratégicos e económicos sobre a costa leste da região do Mar Negro (Guedes, 2009).

A temática do ciberespaço tem, assim, sido explorada no decorrer dos anos, sob diferentes perspetivas, principalmente devido à importância que tem vindo a assumir na sociedade dos dias de hoje. Desde as mudanças sociais e culturais que estão a decorrer, ao poder politico e militar que está em jogo, o ciberespaço é uma temática que tem sido foco de numerosos e importantes estudos. Dito isto, a investigação elaborada na presente dissertação de mestrado pretende possibilitar um ponto de vista sobre em que cenário se pode considerar uma ciberguerra, e ainda em que situações é legítimo, ou não, apelar à defesa coletiva pela invocação do artigo 5º do Tratado do Atlântico Norte, contribuindo deste modo para o conhecimento científico relativo ao ciberespaço numa ótica de segurança.

## 1.5. Conceptualização Operacional

Este subponto tem como propósito definir os conceitos-chave desta investigação, de modo a clarificar e proporcionar um melhor entendimento sobre o objeto de estudo, assim como a articulação que se estabelece entre aqueles e este.

### Ameaça

Ameaça é qualquer acontecimento ou ação, de variada natureza, que contraria a consecução de um objetivo e que, normalmente, é causador de danos, materiais ou morais, sendo que no âmbito da estratégia consideram-se principalmente as ameaças provenientes de uma vontade consciente, analisando a relação entre possibilidades e intenções (Couto, 1988). Como tal, pode-se afirmar que só é considerada uma ameaça se não apenas o agente que a representa tiver a capacidade para a concretizar, mas também a necessária intenção de a provocar.

O conceito alargado de ameaça está presente no "*discurso emergente de securitização de fenómenos que ameacem a paz e a segurança internacionais*" (Kowalski, 2014, p.23). Este discurso pode verificar-se estar a ser aplicado não só a um nível estatal, como ao nível de organizações internacionais como a UE e a NATO (Kowalski, 2014).

Uma ameaça pode ser, também, considerada como um acontecimento ou um processo que leve a um número de mortes em larga escala, que reduza a esperança de vida ou que ponha em causa a soberania e segurança do Estado. Esta abordagem define como ameaças o terrorismo, as armas nucleares ou o crime organizado transnacional, de entre outros (UN, 2004).

## Cibersegurança

*"A Cibersegurança são o conjunto de medidas que procuram garantir o bem-estar e o regular funcionamento da ação de um Estado e das suas populações no ciberespaço e fora dele, desde que derivado de ações diretamente a ele acometidas."* (Militão, 2014, p.26).

A proteção dos interesses gerais dos cidadãos, que somos todos e cada um de nós, incluindo o uso particular do ciberespaço é o que define a cibersegurança. Esta começa em cada um de nós individual ou coletivamente - pois somos o elo mais fraco de todas as cadeias de ligações do ciberespaço. Ao falharmos ou violarmos as regras de segurança comprometemos todos aos quais estamos ligados, pessoal e profissionalmente (US DHS, 2016).

A cibersegurança pode, ainda, ser considerada como a tomada contínua de medidas políticas, jurídicas, económicas e educativas, de sensibilização para os riscos do ciberespaço, transformando assim este espaço digital num ambiente seguro para as interações sociais e económicas que nele decorrem (GH, 2013).

## Ciberdefesa

A ciberdefesa tem a função de garantir a realização de missões de segurança e defesa nacional, e de garantir e salvaguardar a soberania do Estado no ciberespaço global, ou seja, “assegurar a defesa do Estado contra ciberataques que, pela sua natureza e potencial disruptivo e destrutivo, coloquem em risco a soberania nacional ou sejam lançados por outros Estados” (Nunes, 2012, p.124).

Numa outra perspetiva, a ciberdefesa é o termo associado a todas as medidas de defesa no domínio do ciberespaço, que utilizam meios militares apropriados, de modo a alcançar objetivos estratégico-militares. É também um sistema integrado que compromete a implementação de todas as medidas relacionadas com a segurança de TIC, com as capacidades das *Computer Network Operations* (CNO) e ainda com o apoio às capacidades físicas das forças armadas (FCRA, 2013).

## Ciberguerra

A ciberguerra é o ato de guerra dentro e associado ao espaço virtual, ao ciberespaço, estando associada predominantemente às TIC. Para que se possa considerar estarmos perante uma situação de ciberguerra e não apenas perante um ciberataque, é necessária a existência de uma campanha militar associada (que decorre nos domínios operacionais tradicionais) e articulada com medidas tomadas no ciberespaço. De um modo geral, este termo surge associado à utilização de tecnologia de guerra extraordinariamente sofisticada que caracteriza a era informacional que a sociedade contemporânea vive, tendo por base a profunda computorização e digitalização dos setores militares (Maurer e Morgus, 2014) suscetível de articulação com os tradicionais campos de operações.

Num sentido mais simples, a ciberguerra é considerada como o uso de tecnologia computacional para perturbar as atividades de um Estado ou Organização, num ataque deliberado aos seus sistemas de comunicação, conduzido por outro Estado ou Organização (Oxford LD, [s.d.]).

## Cibercrime

É o ato que tem como alvo as redes e sistemas de informação, ou que a elas recorre para cometer um crime, violando a legislação nacional e internacional (ANSSI, 2011).

O termo cibercrime é também utilizado para nos referirmos a atividades ilegais com objetivos de ganhos financeiros. Estas atividades exploram as vulnerabilidades decorrentes do uso da *internet* e de outros sistemas eletrónicos para aceder, ilicitamente, a informação ou serviços utilizados por cidadãos, empresas ou pelo governo. Este tipo de crime pode ser levado a cabo tanto por organizações criminosas como por indivíduos oportunistas, que possuam o conhecimento técnico para os por em prática (Deltica e OCSIA, 2011).

## Ciberataque

O ciberataque é uma ação ofensiva levada a cabo no domínio do ciberespaço e resulta de uma sequência de atos perpetrados com o propósito de prejudicar inadvertidamente a confidencialidade, integridade ou a disponibilidade de um serviço ou produto. A maioria dos ciberataques são considerados atos ilícitos, estando a sua classificação e regulação integrados na legislação nacional e internacional, podendo deste modo ser feita a identificação e julgamento dos perpretores (Santos, Bravo e Nunes, 2012).

Este termo é utilizado para o tipo de ataques que são levados a cabo através de tecnologias de informação no ciberespaço, e são direcionados contra um, ou vários, sistemas de informação. Estes têm como objetivo impossibilitar total, ou parcialmente, a proteção e segurança das TIC, podendo depois ser tirados dividendos do seu funcionamento desprotegido (FCRA, 2013).

A ciber-estratégia de segurança canadiana afirma que os ciberataques incluem o acesso, o uso, a manipulação, a interrupção ou mesmo a destruição, com carácter não autorizado, de informação eletrónica, e também de infraestruturas

físicas usadas para processar ou guardar informação. Deste modo, a gravidade do ciberataque irá determinar as medidas de resposta adequadas pelas entidades competentes (MPSC, 2010).

## Ciberterrorismo

No sentido mais simples, o ciberterrorismo é o uso do ciberespaço para propósitos terroristas de acordo com o definido na lei nacional e internacional (Godwin III *et al.*, 2014).

Segundo a premissa segundo a qual os Estados e as suas Infraestruturas críticas estão cada vez mais dependentes de redes computacionais e de informação para a sua operacionalidade, o ciberterrorismo é considerado o uso de ferramentas de redes computacionais para prejudicar ou incapacitar infraestruturas críticas nacionais (como, por exemplo, as infraestruturas responsáveis pelos sistemas de energia, transportes, saúde ou distribuição de água) colocando, assim, em causa a segurança e o bem-estar da sociedade (Weimann, 2005).

A *Organization for Security and Cooperation in Europe* (OSCE) define o ciberterrorismo como o terrorismo ciber-relacionado, ou seja, os ataques terroristas realizados contra ciber-infraestruturas, particularmente os sistemas de controlo de infraestruturas críticas responsáveis pela energia não nuclear (OSCE, 2013).

## Globalização

A globalização é um longo processo histórico relativo à tendência crescente da interconectividade mundial, que se tornou num objeto de estudo constante para a política mundial (McGrew, 2011).

O fenómeno da globalização foi fortemente impulsionado pelo avanço tecnológico que teve um grande desenvolvimento nas últimas décadas, e veio criar grandes oportunidades mas também enormes riscos. Uma maior comunicação,

interligação e interdependência entre estados, aumentou exponencialmente o potencial do efeito de bola de neve, e consequentemente os danos causados por ataques.

Segundo a professora Sandra Balão, ainda não existe um consenso sobre o significado da palavra Globalização, ou mesmo a sua operacionalização. No entanto pode ser designada como *"a crescente amplitude, profundidade e celeridade das interações mundiais em todos os aspetos da vida social contemporânea, desde o âmbito cultural ao criminal, do financeiro ao espiritual ou, ainda, o aumento contínuo das interações económicas, sociais e culturais transnacionais que ultrapassam as fronteiras dos Estados do mundo, com a ajuda dos avanços tecnológicos."* (Balão, 2014).

## 1.6. Perspetivas de Análise no âmbito das Teorias das Relações Internacionais

De modo a enquadrar o objeto de estudo no âmbito das Teorias das Relações Internacionais, é importante referenciar o problema do subjectivismo e objectivismo referidos pelo Professor Adriano Moreira. Este, afirma que a principal questão que envolve esta problemática surge articulada com o ponto de vista criado pelas circunstâncias pessoais e condicionantes que marcam o observador de modo a que aquele tenha uma visão própria do mundo, a sua visão do mundo. Deste modo, assume-se a complexidade de que se reveste, para o investigador, a capacidade de se separar das suas relações com os fatos a observar e a avaliar (Moreira, 2014).

Relativamente ao problema identificado no parágrafo anterior, o Professor Victor Marques dos Santos acrescenta que o observador está *"condicionado pelo seu enquadramento espácio-temporal, sócio-cultural e epistemológico, bem como pelo contexto científico mais alargado em que se insere a sua investigação, pelos instrumentos de análise e pelos métodos adoptados"* (Santos, 2007, p.118).

Por seu lado, e segundo o Professor Luís Pereira Coutinho, as teorias das RI correspondem a uma conceção da realidade internacional, e que devido a um "*âmbito disciplinar marcado pela pluralidade, senão mesmo pela conflitualidade",* não poderia haver apenas uma teoria mas sim várias (Coutinho, 2014, p.506).

As teorias das RI não só são importantes, como necessárias por constituírem o meio através do qual é garantida a ordem necessária ao estudo científico dos objetos sobre os quais se debruçam os estudos na respetiva área científica. Estas são, portanto, essenciais para conceptualizar eventos históricos e contemporâneos (Burchill e Linklater, 2009). Considerando que a presente dissertação de mestrado tem como objetivo estudar o ciberespaço como dimensão de segurança, torna-se relevante enquadrá-lo no âmbito das teorias das RI que, a nosso ver, mais se adequem ao estudo e à análise de questões no domínio securitário.

O Liberalismo é a teoria que tem como fundamentos o raciocínio científico, valores como a liberdade, o individualismo e a inevitabilidade do progresso humanos. Nesse sentido, valoriza uma governança baseada nos direitos individuais, no constitucionalismo, na democracia e na limitação dos poderes do Estado. É, no entanto, uma teoria considerada utópica na medida em que defende a prossecução de ideais praticamente impossíveis de alcançar na sua plenitude (Burchill, 2009).

Por sua vez, o Liberalismo Internacional surge com o Presidente dos Estados Unidos da América, Woodrow Wilson, em 1918, num discurso ao Congresso. Neste, Wilson - que era considerado um ator principal no pensamento idealista liberal - apresenta os seus catorze (14) pontos ou princípios que, na sua perspetiva, era necessário prosseguir para garantir um mundo mais seguro e atingir a paz internacional, introduzindo o princípio da racionalidade nas relações entre os Estados (Ferreira, 2014). O 14º ponto do seu discurso diz que: *"A general association of nations must be formed under specific covenants for the purpose of affording mutual guarantees of political independence and territorial integrity to great and small states alike."* (Wilson, [n.d.]).

Este discurso surge no contexto de uma conjuntura afetada pelo ambiente pós-Primeira Guerra Mundial, sendo que esta teve repercussões a nível social, político e económico. A Grande Guerra mostrou que o anterior equilíbrio de potências que se tinha verificado nos Estados Europeus do século XVII ao XX, o período pós-vestfaliano, não podia continuar a ser considerado como uma solução para a manutenção da paz global. Neste sentido, é proposto um novo princípio de ordem global, apoiado na formação de organizações internacionais intergovernamentais (Ferreira, 2014).

O Liberalismo Internacional apresentava uma análise em duas partes, mostrando o que correra mal em 1914, e a respetiva solução para evitar acontecimentos semelhantes no futuro. A primeira parte identificava que o povo não queria a guerra que lhes tinha sido imposta por militaristas ou autocratas, ou por sistemas antidemocráticos, multinacionais ou imperiais que desrespeitavam as suas aspirações à nacionalidade, pelo que apresentava como solução a promoção de sistemas políticos democráticos e o princípio da autodeterminação nacional, procurando assegurar, deste modo, que a guerra seria evitada. A segunda parte refere-se a uma crítica às estruturas institucionais prévias a 1914, considerando que o sistema de relações internacionais anárquico sabotava as perspetivas de paz, pois a diplomacia secreta levava a sistemas de alianças não regulamentadas por Assembleias ou Parlamentos. Não existia nenhum mecanismo para evitar a guerra, sem ser o equilíbrio de poder verificando-se, portanto, a necessidade de se criar uma nova estrutura internacional para as relações internacionais (Brown e Ainley, 2012).

Com o fim da Primeira Guerra Mundial e com o Tratado de Versalhes de 1919, é criada a Sociedade das Nações. Esta resulta da necessidade de regular a paz mundial, e foi o resultado do acordo estabelecido entre os Estados vencedores, tendo na base estatutária os ideais contidos nos “14 pontos de Wilson”. Com o objetivo de salvaguardar a paz, aquela organização baseou-se nos princípios da autodeterminação e da segurança coletiva, para buscar prevenir um novo conflito mundial (Vieira, 2014).

Numa ótica de segurança, o liberalismo é um desafio global colocado à nossa civilização, e que se mantém pertinente nos dias de hoje. Tentando passar de um exercício individual para uma comunidade particular e, mais tarde, com um horizonte mais vasto em perspetiva, para uma comunidade plural, como por exemplo uma organização internacional, esta abordagem requer não só esforço e compromisso mas, também, confiança entre os Estados para que se possa atingir a paz (Dias e Samões, 2016).

Nos dias de hoje é difícil alcançar um estado de confiança e de compromisso entre atores internacionais para alcançar a paz liberal, mesmo sabendo que parte do sucesso para combater as ciber-ameaças e os ciberataques, passa pela cooperação entre os Estados e agentes internacionais, de modo a facultar informação essencial para combater esta ameaça emergente (Nunes, 2012), pois nenhum Estado quer pôr em causa os seus interesses, sobretudo os mais poderosos e tecnologicamente mais avançados.

O liberalismo foi, entretanto, considerado irrealista e utópico, sendo até intitulado de idealismo por autores como o Professor Adriano Moreira (Moreira, 2014), surgindo em oposição aos seus ideais, o Realismo. Esta teoria afirmava, por sua vez, que os Estados não apresentam uma harmonia de interesses em prol de uma paz perpétua. Antes pelo contrário: o sistema internacional é anárquico e é marcado pelo conflito de interesses entre Estados (Donnelly, 2009).

Na perspetiva Realista, os Estados *"são os atores principais das RI, cuja acção se subordina aos imperativos do interesse nacional"* (Santos, 2014, p.441). O Realismo separa totalmente a política interna da internacional, sendo que privilegia o poder e a segurança, menosprezando moralismos e considerações humanistas, em prol do interesse nacional. À luz desta teoria, as RI são conflituais pois resumem-se às lutas de poder, autoridade, e sobrevivência por parte dos Estados, que carecem de confiança mútua e harmonia de interesses, sendo que existe um ambiente de constante oposição, um ambiente relacional anárquico, onde a soberania do Estado é vista como a finalidade da ação política (Santos, 2014).

Hans Morgenthau formulou os “seis princípios do realismo político”, que foram sumarizados por Victor Marques dos Santos, os quais passo a citar:

1. *“As relações políticas obedecem a regras objetivas, intrinsecamente inerentes à natureza humana e independentes das preferências dos indivíduos.”*

2. *“A “premissa central” do Realismo é a evidência demonstrada pela história, de que os dirigentes políticos “pensam e atuam em termos de interesse definido como um poder”, o que pressupõe a conflitualidade endémica e a instabilidade próprias de um ambiente relacional anárquico.”*

3. *“As RI caracterizam-se pela luta pelo poder e as políticas externas defendem a sobrevivência e a integridade dos Estados como interesse nacional de prioridade absoluta.”*

4. *“A moral de responsabilidade deve prevalecer sobre a moral de convicção, sendo a moralidade dos Estados na sua defesa do interesse nacional, diferenciada da moralidade das relações interpessoais.”*

5. *“O Realismo político não significa a identificação dos valores morais de um Estado com valores morais universais, logo, reconhece-se que cada Estado pode ter valores e princípios morais próprios.”*

6. *“A preservação de autonomia da esfera política implica que a avaliação das ações deva submeter-se prioritariamente a critérios de efeitos e consequências da decisão política sobre o poder do Estado.”* (Santos, 2014, p.442)

A adoção destes princípios é o resultado de uma priorização do interesse nacional e da desvalorização dos valores éticos e morais. No entanto, este facto não significa a rejeição desses mesmos valores considerando, até, que a sua

identificação inerente ao interesse nacional permite ao Estado justificar e reforçar a sua defesa perante outros Estados (Santos, 2014).

Numa perspetiva atual surge a discussão em torno do dilema assente na seguinte questão: o Realismo mantém-se como teoria relevante no domínio da segurança internacional?. Esta questão está dependente, principalmente, de fatores como a capacidade de persuadir as novas gerações de académicos para a operacionalidade da abordagem Realista, e suas variantes, relativamente aos grandes temas da segurança internacional. Por outro lado, a evolução dos conflitos assimétricos, nos quais estão envolvidos atores não Estatais, e o recurso à aplicação da força através de métodos não convencionais, como por exemplo os ciberataques, suscita a dúvida relativamente à capacidade de resposta do Realismo em face dos desafios suscitados por este fenómeno, sendo que é uma teoria que foi desenvolvida, essencialmente, tendo como *background* os conflitos convencionais entre Estados (Reis, 2016).

A abordagem construtivista *"apresentou novas ferramentas de análise que indubitavelmente possibilitam hoje um entendimento mais sofisticado e completo das tradicionais dinâmicas de segurança*" (Seabra, 2016, p.52).

Segundo Ruggie e Wendt esta teoria tem utilizado as suas ideias para esclarecer questões normativas, focando-se particularmente na identidade dos Estados, e por extensão, nas questões de cooperação entre estes (Brown e Ainley, 2012).

O construtivismo mudou o modo como se tratam questões como dilemas de segurança ou paz democrática, mostrando que o conceito de segurança não está limitado apenas pelas tradicionais capacidades materiais e soberania do Estado, mas também equaciona temáticas e preocupações atuais, como ameaças globais (por exemplo: terrorismo ou ciberataques). Esta abordagem conseguiu evoluir e aprender com diferentes conceitos de segurança e ameaça, apresentando como solução a construção social permanente (Seabra, 2016).

Esta construção social está apoiada no pressuposto de que os Estados partilhariam conhecimento entre si, e como tal, seria construída uma realidade social, que transformaria os dilemas de segurança, como atrás referimos. Através de uma agência e estrutura social, influenciadas por distintas ideias e normas, os Estados poderiam desenvolver novas relações de cooperação numa esfera de segurança (ibidem). Algo que se verifica não estar a ser posto em prática nos dias de hoje tendo em conta acontecimentos recentes, como por exemplo o ataque às torres gémeas, em 11 de setembro de 2001 (um relatório do Congresso norte-americano atribui a culpa do sucesso do ataque a uma falha de comunicação entre as agências *Central Intelligence Agency* (CIA) e *Federal Bureau of Investigation* (FBI), afirmando que o ataque poderia ter sido prevenido se estas tivessem partilhado informação, e dados recolhidos sobre os dois homens que sequestraram a aeronave) (Johnston, 2003).

Tendo em consideração que nenhuma das principais teorias das RI, anteriormente apresentadas, vai ao encontro da perspetiva do autor da presente dissertação de mestrado, na ótica do objeto de estudo é, em seguida, apresentada a teoria que, na sua opinião mais se adequa aos objetivos da investigação.

O institucionalismo neoliberal, desenvolvido por académicos como Robert Axelrod e Robert Keohane, aceita os princípios da *"anarquia internacional"* e do *"egoísmo racional dos Estados"*, mas considera ser possível a cooperação entre *"egoístas racionais"* num sistema anárquico (Brown & Ainley, 2012, p.88).

Esta teoria reconhece a existência de Estados "parasitas" em sistemas de cooperação, os quais iriam aproveitar os benefícios deste, fazendo promessas em circunstâncias em que, antecipadamente se sabia não ser possível a sua execução, e acabando por não contribuir, efetivamente, para o sistema de cooperação formalmente estabelecido limitando-se, ao invés, a retirar apenas benefícios de Estados "superiores". Contudo, sendo possível a criação de regimes ou sistemas internacionais, onde fosse possível trocar informações e formalizar compromissos, existiria uma possibilidade reforçada de cooperação. Mesmo que houvesse partes

a beneficiar de um modo desigual da troca de informações, o mais importante seria que todos ganhariam algo com a sua cooperação (Brown e Ainley, 2012).

Estabelecendo o paralelismo com o ciberespaço numa perspetiva de segurança (objeto da nossa investigação), é nosso entendimento que os Estados e outros atores internacionais, mesmo tendo os seus interesses individuais a salvaguardar precisam de se unir, de cooperar - independentemente de ser possível haver uma grande disparidade no que diz respeito aos benefícios de uma cooperação que se estabeleça entre si - de modo a criar condições para a partilha de informações como elemento fundamental de uma estratégia que tenha em vista assegurar a cibersegurança e, assim, contribuir para a segurança dos povos e salvaguarda da sua soberania no domínio do ciberespaço, que cada vez se revela mais ameaçador para a sociedade moderna.

## 1.7. Motivação e Pertinência

"*O conceito estratégico de defesa nacional define os aspetos fundamentais da estratégia global a adotar pelo Estado para a consecução dos objetivos da política de segurança e defesa nacional.*" (MDN, 2013, p.6).

Neste sentido, e considerando que o mesmo CEDN define a cibercriminalidade como uma das principais ameaças e riscos, tanto numa esfera de segurança nacional como global, é percetível a importância que o ciberespaço, numa dimensão de segurança, tem vindo a desenvolver.

Em 2015, pelo menos 80% das empresas europeias foram afetadas por um incidente de cibersegurança, colocando assim em causa a confiança na economia digital. Como tal, a Comissão Europeia lançou uma parceria público-privada sobre cibersegurança que mobilizará cerca de 1,8 mil milhões de euros de investimento até 2020, sendo esta uma de várias iniciativas desenvolvidas para combater ciberataques e reforçar a cibersegurança (EC, 2016)

A cibersegurança tem assumido um papel importante no modo como se olha para a segurança internacional, de tal modo que as principais potências mundiais têm feito grandes investimentos para apoiar esta prioridade estratégica. O governo dos EUA, por exemplo, prevê gastar cerca de 30 mil milhões de dólares em cinco (5) anos para o desenvolvimento de cibersegurança e ciberdefesa (Bendiek, 2012).

Este investimento no desenvolvimento de cibersegurança é justificável pelas ameaças que advêm do ciberespaço, e pelos ciberataques que têm sido registados nos últimos anos como, por exemplo, o ataque cibernético à Estónia ou Geórgia em 2007 e 2008 respetivamente (Guedes, 2009). Ou, mais recentemente, a polémica que se instalou em torno das eleições presidenciais dos EUA devido ao eventual envolvimento de *hackers* russos na manipulação dos resultados eleitorais (Harding, 2016).

Embora o ciberespaço e a cibersegurança sejam uma prioridade para a segurança internacional, ainda existe uma falta de reconhecimento sobre a possibilidade de um ciberataque ser considerado, ou não, uma declaração de guerra. De facto, constitui um fenómeno que deixa em aberto a resposta à questão sobre se a comum definição de ataque armado, contemplada no artigo 5º do Tratado de Washington, se aplica ou não aos fenómenos cuja ocorrência se verifique naquele espaço. Este é um problema que consideramos relevante e justificável na atual sociedade moderna, sobretudo considerando o potencial disruptivo associado a um ciberataque (Nunes, 2012).

A um nível pessoal esta temática encerra em si um cariz de elevado nível motivacional, não só pela atualidade do seu objeto de estudo (que obriga a uma constante procura de novas estratégias e respostas às atuais ameaças e riscos que apresenta numa esfera de RI), mas também num âmbito institucional e, consequentemente, profissional. Este segundo ponto surge igualmente articulado com a importância que o objeto de estudo representa para a segurança nacional e, como tal, também para uma instituição militar de ensino superior como a Academia da Força Aérea – em termos de missão e objetivos.

Como aluno da AFA no Mestrado em Ciências Aeronáuticas, e como futuro Oficial dos Quadros Permanentes das Forças Armadas, é pertinente a escolha de um objeto de estudo que não seja apenas atual mas, também, significativo no contexto das questões de segurança nacional e global. Sendo assim, este objeto insere-se, igualmente, numa temática que acompanha e espelha os desafios que são atualmente defrontados pelo Estado português, assim como aqueles que um futuro Oficial, na sua qualidade de líder, terá de enfrentar no âmbito da sua carreira.

## 1.8. Panorâmica

Considerando os objetivos de trabalho enunciados anteriormente, a presente dissertação apresenta-se organizada em quatro partes principais: Introdução, Nota Metodológica, três capítulos centrais e Conclusão. Posteriormente, segue-se a Bibliografia e os Anexos, que completam as restantes componentes, anteriormente mencionadas.

Assim, na primeira parte é feita uma breve introdução ao objeto de estudo. Esta secção está dividida em oito pontos, de entre os quais podemos destacar o enquadramento contextual, seguido pelo âmbito e objeto de estudo, a revisão de literatura, a conceptualização operacional, e as perspetivas de análise no âmbito das teorias das Relações Internacionais. Posteriormente, é apresentada a justificação da motivação e pertinência para a elaboração da presente dissertação, e por fim, a sua panorâmica geral.

Na segunda parte estão definidas as linhas metodológicas orientadoras do trabalho a desenvolver, perante os objetivos anteriormente estabelecidos. Nesta parte encontra-se ainda a formulação da pergunta de partida e também das hipóteses de trabalho.

A terceira parte é constituída por três capítulos, sendo que estes constituem o núcleo central desta dissertação e é no âmbito do desenvolvimento dos mesmos que se procurará reunir a informação resultante da investigação a desenvolver de

modo a ser possível equacionar as hipóteses de trabalho formuladas anteriormente, e buscar a sua demonstração de modo a ir ao encontro dos objetivos definidos anteriormente.

No primeiro capítulo é caracterizado o ciberespaço como novo espaço de conflito, analisando as ameaças que a ele estão associadas e que dele advêm.

No segundo capítulo é analisado o *statu quo* da ciberdefesa e cibersegurança no século XXI, sendo efetuada uma análise crítica aos conceitos estratégicos e estratégias em vigor no quadro da Organização das Nações Unidas (ONU), NATO e UE

No terceiro capítulo é desenvolvido um estudo de caso sobre o ataque cibernético à Geórgia, partindo do relato contido no livro “A Guerra dos Cinco Dias” do Professor Marques Guedes e complementado com outras fontes de referência bibliográfica, de modo a buscar articular com a investigação desenvolvida em termos teóricos, dando-lhe consistência e corpo.

Finalmente, na quarta parte, são apresentadas as conclusões e considerações finais, procurando dar resposta à pergunta de partida proposta e também demonstrar as hipóteses de trabalho em estudo.

As conclusões a que for possível chegar no âmbito desta dissertação de mestrado poderão não apresentar um carácter totalmente inovador, mas serão academicamente válidas, e buscarão ser um contributo para o avanço do conhecimento científico.

# Nota Metodológica

A metodologia, como o nome indica, é o estudo dos métodos e tem como objetivo analisar as características destes, avaliando as suas capacidades, potencialidades e limitações. É também considerada uma forma de conduzir uma pesquisa, sendo feita a explicação minuciosa, detalhada, rigorosa e exata de toda a ação desenvolvida no âmbito do trabalho da pesquisa desenvolvido, assim como de todos os procedimentos adotados tendo em vista o resultado final que será apresentado. Assim sendo, requer um planeamento cuidado através de um conjunto de normas e regras específicas que podem variar conforme o modelo teórico ou metodológico adotado pelo autor.

Segundo Quivy e Campenhoudt, são utilizadas técnicas de investigação que variam conforme o tipo de informação e o objetivo ao qual esta se destina. Estas técnicas são instrumentos pertencentes às teorias e vão condensar a informação recolhida. Os resultados científicos obtidos podem variar conforme a lógica de tratamento da informação ou a metodologia escolhida. Contudo, apesar do vasto leque de técnicas utilizadas na investigação científica, parece não haver um procedimento ideal, sendo apenas necessário adotar ou criar um método, ajustado ao tipo de estudo que se pretende executar (Quivy e Campenhoudt, 2008).

Neste contexto, é necessário explicitar os métodos de abordagem e procedimentos assim como as técnicas e meios utilizados, teorias e objetos a investigar.

Segundo Lakatos e Marconi, a maioria dos especialistas diferencia método de métodos, pois estão em níveis distintos quer seja em termos de inspiração filosófica, grau de abstração, finalidade (que pode ser mais ou menos explicativa), ação nas etapas da investigação e, por fim, quanto ao momento nas quais estão situadas. Sendo assim, o método é caracterizado por ter uma abordagem mais ampla, com uma maior abstração, quer dos fenómenos da natureza quer da sociedade (Lakatos e Marconi, 1994).

O tipo de método que o investigador segue vai ser definido pela abordagem que adota no desenvolvimento do seu estudo. Deve-se, contudo, esclarecer não só o tipo de estudo que será desenvolvido (quanto ao modo de abordagem) mas, também, quanto ao seu objetivo geral e quanto aos seus procedimentos técnicos (Vilelas, 2009).

Começando pelo tipo de estudo e quanto ao modo de abordagem, de modo a compreender melhor o problema, o investigador tem que optar por uma abordagem predominantemente quantitativa ou qualitativa como justificação para os métodos utilizados (Quivy e Campenhoudt, 2008).

Segundo a abordagem quantitativa, é utilizada a recolha de dados de modo a testar as hipóteses elaboradas. Esta abordagem baseia-se em medições numéricas e análise de estatísticas para validar teorias (Sampieri, Collado e Lucio, 2013).

Por outro lado, a abordagem qualitativa utiliza a recolha de dados *"sem medição numérica para descobrir ou aprimorar perguntas de pesquisa no processo de interpretação"* (Sampieri et al., 2013, p.33).

Considerando o que foi dito nos dois últimos parágrafos, a investigação a utilizar no âmbito da nossa investigação será mista, contemplando uma componente qualitativa e quantitativa. Embora as abordagens sejam notoriamente diferentes, e considerando que cada uma deve ser utilizada com um propósito de investigação específico, ambas podem ser utilizadas de um modo complementar, beneficiando assim tanto das vantagens da abordagem qualitativa (por exemplo, a aproximação do investigador ao objeto de estudo), como das da abordagem quantitativa (como, por exemplo, possibilitar uma maior confiabilidade relativamente aos dados apresentados) (Vilelas, 2009).

Em relação ao tipo de estudo e quanto ao objetivo geral, Vilelas equaciona três possibilidades: os estudos exploratórios, que procuram proporcionar uma maior familiaridade com o problema, para que se torne mais explícito facilitando a formulação das hipóteses; os estudos descritivos, que visam conhecer as

características de certo fenómeno ou população, ou ainda estabelecer relações entre variáveis, de modo a obter uma visão mais completa do problema. Por fim, os estudos correlacionais, que pretendem determinar as relações entre as variáveis de um estudo, sem tentar estabelecer uma relação causa-efeito, e com o objetivo de quantificar essas relações através de provas estatísticas (Vilelas, 2009).

Considerando a abordagem que se definiu para este estudo, a tipologia utilizada será essencialmente descritiva. Ao recorrer a esta tipologia de estudo, pretende-se especificar os aspetos e características de maior relevo do fenómeno, submetendo-o a uma análise detalhada a partir da recolha de dados que apontem para a manifestação de um evento.

Sendo assim, o investigador tem como objetivo fazer a descrição de um determinado fenómeno, especificando o seu contexto, comunidade ou ambiente, procurando fazer uma análise de um estudo de caso.

Considerando os parágrafos anteriores, e centrando o estudo na problemática do ciberespaço como dimensão de segurança, a investigação conduzida basear-se-á numa tipologia de investigação não só descritiva, como também reflexiva pois é do entendimento do autor que para uma melhor resposta à problemática é necessária a análise reflexiva dos dados, focando-se principalmente na análise dos ciberataques conduzidos contra a Geórgia em 2008.

Relativamente ao tipo de estudo e quanto aos procedimentos técnicos, será desenvolvido no decorrer da investigação o estudo bibliográfico e ainda o estudo de caso (Vilelas, 2009).

O primeiro será elaborado a partir de material já publicado, utilizando maioritariamente monografias, obras de referência e artigos científicos, mas haverá necessidade de recorrer, igualmente, a informação disponível e acessível através da *internet*, pela especificidade da problemática e, também, pela atualidade da mesma. A pesquisa bibliográfica elaborada irá permitir cobrir uma mais vasta gama de fenómenos do que seria possível numa pesquisa direta (ibidem).

O segundo, é enquadrado numa abordagem qualitativa, e é frequentemente utilizado para obter dados nas áreas de estudos operacionais. De modo a discutir um estudo de caso devem ser equacionados três aspetos. O primeiro é a natureza, ou profundidade, da experiência, enquanto fenómeno a ser investigado. O segundo é relativo ao tipo de conhecimento que se pretende adquirir, sendo importante a existência de uma forte relação entre a compreensão e a intencionalidade, ou a extrapolação da experiência. Por último, o terceiro aspeto a considerar é a possibilidade de generalização do estudo (ibidem).

Quanto aos métodos de abordagem definidos por Lakatos e Marconi, que são o indutivo, o dedutivo, o hipotético-dedutivo e o dialético, o método que mais se adequa à presente dissertação de mestrado é o hipotético-dedutivo. Este método começa pela identificação de uma lacuna, e através da formulação de hipóteses e do posterior processo dedutivo, testa a ocorrência dos fenómenos abrangidos pelas hipóteses (Lakatos e Marconi, 1994).

Assim sendo, utilizar-se-á a técnica de pesquisa de observação direta, em que se irá examinar os factos e fenómenos em estudo com o propósito de determinar alguns aspetos da realidade, recorrendo, para tal aos sentidos (ibidem).

## 2.1. Formulação da Pergunta de Partida

A pergunta de partida é o fio condutor de toda a investigação. Como tal, a importância de formular uma boa pergunta de partida é fundamental para o sucesso do trabalho. Esta deve ser não só pertinente como clara e também exequível, de modo a *"desempenhar correctamente a sua função"* (Quivy & Campenhoudt, 2008, p.44).

Considerando o que foi referido anteriormente formulou-se a seguinte **pergunta de partida** e pergunta derivada:

*Pode um ciberataque dar origem a uma ciberguerra, considerando os quadros de referência legal e normativos de organizações como a NATO e UE?*

**Pergunta derivada (PD):**

**PD:** Poderá, face a um ciberataque (ou a uma multiplicidade deles), ser invocado o artigo 5º do Tratado do Atlântico Norte?

Estando formulada a pergunta de partida e de modo a prosseguir com o processo metodológico, é necessário definir as hipóteses de trabalho, que deverão ser confrontadas com os dados do estudo desenvolvido, sendo submetidas ao teste dos factos revelando-se verificáveis ou refutáveis (Quivy e Campenhoudt, 2008).

## 2.2. Hipóteses de Trabalho

Segundo Quivy e Campenhoudt, as hipóteses têm de ser como que uma linha condutora para uma investigação ordenada e rigorosa, sem nunca "*sacrificar o espírito de descoberta e de curiosidade que caracteriza qualquer esforço intelectual digno deste nome*" (Quivy & Campenhoudt, 2008, p.119).

Neste sentido, é importante formular várias hipóteses de trabalho, pois sendo respostas parciais do problema, dificilmente apenas uma hipótese será o necessário para dar resposta à pergunta de partida (Quivy e Campenhoudt, 2008).

As hipóteses são, deste modo, essenciais. No entanto, são apenas tentativas de explicação da problemática em estudo. Estas definem as questões a aferir mas têm de ser comprovadas ou contrariadas por uma investigação metódica e rigorosa, pois não passam de meras proposições. Como tal, as hipóteses são confrontadas com os dados retirados do processo de investigação, testando assim o modelo de análise utilizado (ibidem).

De acordo com o objeto de estudo apresentado, e tendo em consideração a pergunta de partida, foram formuladas as seguintes hipóteses de trabalho (HP):

**HP1:** O ciberespaço é atualmente reconhecido como uma dimensão potenciadora de ameaças nacionais e globais.

**HP2:** Os documentos estratégicos de defesa dos Estados Membros da UE e da própria organização já contemplam soluções no âmbito da ciberdefesa e cibersegurança.

**HP3:** Os Estados e as Organizações Internacionais como a UE e a NATO estão preparados para prevenir e dar resposta a ciberataques.

**HP4:** Está prevista a invocação do artigo 5º do Tratado do Atlântico Norte, por parte de qualquer dos Estados Membros da NATO, perante um (ou vários) ciberataque(s).

# Capítulo 1 - O Ciberespaço como novo espaço de conflito

Um conflito no ciberespaço diferencia-se do conflito convencional (por exemplo, uma guerra entre duas Nações), em praticamente todos os aspetos, com exceção do potencial nefasto que representa.

Quer seja na identificação dos agentes envolvidos no conflito (que, num conflito convencional, estão comummente representados por um uniforme), quer seja no ato, propriamente dito (ao ser um conflito declarado e reconhecido pelos envolvidos como tal), tais situações não se verificam num conflito no ciberespaço.

Um ciberataque é imprevisível, sendo a sua origem muito difícil de detetar. É uma ameaça sem rosto e nos dias de hoje relativamente fácil de executar como procuraremos demonstrar ao longo deste capítulo.

## 1.1. Caracterização do ciberespaço

De modo a podermos caracterizar e analisar o ciberespaço como novo espaço de conflito é necessário, em primeira instância, perceber que tipo de espaço é o ciberespaço.

O ciberespaço, tal como é hoje percecionado, representa uma evolução, melhoria e em alguns casos substituição, no que diz respeito ao processo comunicacional em geral e à transmissão de informação, em particular. Desde cartas, livros, ou qualquer outro tipo de documentação que, outrora, era armazenada em caixas de arquivo colocadas, muitas vezes, em depósitos de armazenagem, de difícil acesso e consulta é hoje guardada noutro tipo de “caixas”, de natureza virtual (e já não física), dotadas de enormes capacidades de armazenamento e grande facilidade de acesso.

Segundo a Dra. Rebecca Bryant [1] (Bryant, 2001), para caracterizar o ciberespaço deve-se equacionar quatro pontos com os quais se pode estabelecer o paralelismo para o mundo físico e que irão ajudar a concretizar a ideia de espaço. Os quatro pontos ou conceitos que iremos analisar são os seguintes:

- Sítio ou Local
- Distância
- Tamanho
- Rota ou Direção

O conceito de sítio ou local está relacionado com questões sobre algo que queremos encontrar ou localizar. Queremos saber onde está algo em relação a nós próprios, de modo a ser feito um mapa mental que nos permita ir ao encontro ou evitá-lo. No ciberespaço essa questão também existe. Pode-se questionar em que servidor é que um determinado *website* se encontra alojado, ou para que caixa de *e-mail* é que devo enviar uma mensagem. Esta maneira de pensar e falar reflete a importância de identificar alvos ou locais específicos no ciberespaço.

A distância é um conceito que está relacionado com questões que determinem o quão longe está algo. Esta questão é importante pois quando queremos fazer uma determinada viagem é necessário saber a distância que vamos ter que percorrer, para decidirmos se devemos ir a pé ou de carro, por exemplo. Também relacionado com este conceito está o tempo, ou seja quanto tempo vamos demorar para chegar ao nosso destino. Estabelecendo o paralelismo com o ciberespaço, é fácil compreender que esta questão está presente em várias situações como, por exemplo, o tempo que irá demorar um certo *download* a ser feito, ou ainda quanto tempo é que será necessário para guardar uma apresentação na *cloud*.

O terceiro ponto ou conceito é o tamanho que, por sua vez, está relacionado com questões associadas a dimensões. Uma questão comum neste domínio e que

[1] Pós doutorada em Filosofia na Universidade de Edimburgo e atual responsável pela Editora da Universidade de Oxford.

se coloca no mundo físico seria, por exemplo, saber quantos livros é que consigo levar numa determinada mochila ou quanta roupa consigo transportar numa dada mala de viagem. Fazendo a "ponte" para o ciberespaço, o tamanho assume um carácter relevante quando equacionamos uma determinada capacidade de armazenamento para guardar ficheiros, ou quando queremos fazer um *download* e precisamos de conhecer o seu tamanho para saber se o espaço disponível é suficiente para o armazenar, assim como para calcular quanto tempo tal processo vai demorar até estar concluído. Pode, também, ser equacionada a dimensão de um *website* e o quão extenso é, algo que se torna relevante para saber a quantidade de informação que o mesmo contém (ou pode conter), assim como a quantidade de ligações para outros *websites*.

O conceito de rota ou direção está associado a questões de navegação. No nosso dia-a-dia questionamos várias vezes qual é o melhor caminho para chegar a um determinado sítio ou local. O mesmo se verifica no ciberespaço: quando enviamos um *e-mail* este percorre um determinado percurso; ou mesmo quando estamos a navegar na *internet* e vamos passando de um *website* para outro, sempre a percorrer caminhos no mundo eletrónico em busca da informação de que necessitamos ou, em alternativa, a transmitir informação de que alguém necessita.

Assim, é percetível que mesmo sem nos apercebermos, no nosso quotidiano, já reconhecemos o ciberespaço como um espaço e os nossos comportamentos refletem a consciência dessa mesma existência. Mesmo sem ser algo físico, atribuímos-lhe valores semelhantes ou equivalentes aos que reconhecemos e assumimos em várias atividades do nosso dia-a-dia.

Existe, também, um aspeto físico do ciberespaço – que, é certo, muitas vezes não é reconhecido ou equacionado, pois o acesso a este já está "automatizado" e é algo que fazemos inúmeras vezes por dia de um modo muito simples e através de diferentes plataformas, seja pelo computador portátil ou pelo *smartphone*. Este elemento físico do ciberespaço é o conjunto dos satélites, cabos de fibra ótica, servidores e computadores, que nos permitem aceder à *internet* praticamente em qualquer lugar e a qualquer tempo.

## 1.2. Geografia do ciberespaço

A *internet*, embora não represente todo o domínio do ciberespaço, é a principal rede de acesso ao ciberespaço. Como tal, é na análise do acesso e uso da *internet*, que se pode formar uma ideia de geografia no que diz respeito ao ciberespaço.

O acesso à *internet* está diretamente relacionado não só com os meios financeiros de que cada indivíduo dispõe, como pela sua localização geográfica. Num Estado em desenvolvimento, no qual o acesso à *internet* está impossibilitado; ou num outro local onde, por motivos de controlo político, o acesso está condicionado, é evidente que as suas "pegadas digitais" serão muito diminutas ou inexistentes. Contudo, num Estado onde o ambiente virtual representa uma parte do quotidiano com uma dimensão similar à da "realidade física" e onde não existem quaisquer impedimentos, ou entraves, financeiros e ou políticos ao seu acesso, é natural observar um registo imensamente superior do acesso à *internet* (Martins, 2012).

A análise que permitirá, em primeira instância, obter uma perspetiva da geografia do ciberespaço será a do uso da *internet*. Nomeadamente, o número de utilizadores de *internet* por Continente, por exemplo. E para uma análise mais detalhada com base neste tipo de dados, pode ser feita uma comparação entre países, ou mesmo dentro de um país entre várias regiões ou localidades.

A seguinte tabela equaciona a população total de várias regiões mundiais, e o respetivo número de utilizadores da *internet*.

Tabela 1 - Estatísticas da População e Uso de *Internet* Mundial (25 MAR 2017)

Fonte: (Internet World Stats, 2017)

| Regiões Mundiais | População (2016 Est.) | % População Mundial | Utilizadores de *Internet* a 31 MAR 2017 | % Penetração (% População) | Crescimento 2000 – 2016 | % de Utilizadores |
|---|---|---|---|---|---|---|
| **Ásia** | 4,148,177,672 | 55.2 % | 1,873,856,654 | 45.2 % | 1,539.4% | 50.2 % |
| **Europa** | 822,710,362 | 10.9 % | 636,971,824 | 77.4 % | 506.1% | 17.1 % |
| **América Latina** | 647,604,645 | 8.6 % | 385,919,382 | 59.6 % | 2,035.8% | 10.3 % |
| **África** | 1,246,504,865 | 16.6 % | 345,676,501 | 27.7 % | 7,557.2% | 9.3 % |
| **América do Norte** | 363,224,006 | 4.8 % | 320,068,243 | 88.1 % | 196.1% | 8.6 % |
| **Médio Oriente** | 250,327,574 | 3.3 % | 141,931,765 | 56.7 % | 4,220.9% | 3.8 % |
| **Oceânia** | 40,479,846 | 0.5 % | 27,549,054 | 68.1 % | 261.5% | 0.7 % |
| **Total** | 7,519,028,970 | 100.0 % | 3,731,973,423 | 49.6 % | 933.8% | 100.0 % |

Como pode ser observado a região com uma maior penetração de utilizadores de *internet* é a América do norte com 88.1% e logo a seguir está a Europa com 77.4%, mas é na Ásia que se verifica o maior número de utilizadores com 50.2% dos utilizadores do mundo. A região na qual se verificou um maior crescimento do número de utilizadores de 2000 a 2017 foi África, com um aumento de mais de 7550%.

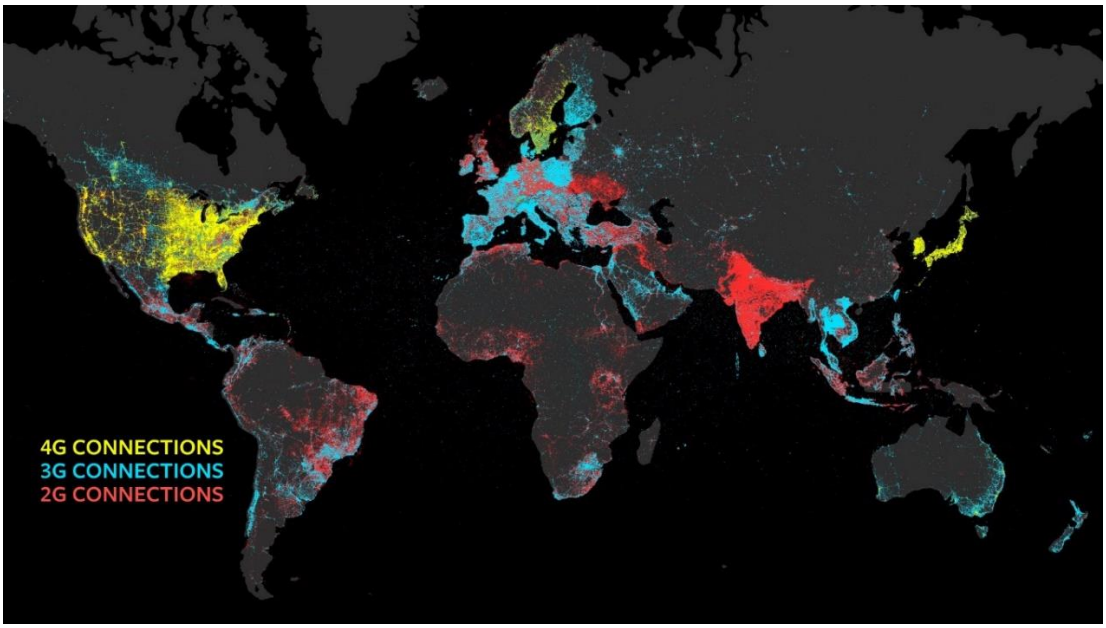


Figura 1 - Mapa-mundo com a distribuição de rede 4G, 3G e 2G (FEV 2016)

Fonte: (mybroadband, 2016)

Nesta figura é possível ver as diferentes ligações de rede e a sua distribuição mundial. Deste modo é possível termos uma perceção da intensidade das conexões à escala planetária, algo que também permite ver o desenvolvimento tecnológico dos diferentes Estados e mesmo Continentes.

Como é possível verificar, a região europeia é dominada por ligações 3G enquanto que a América do Norte já apresenta uma maioria de ligações 4G. A Índia apresenta quase exclusivamente ligações 2G, por outro lado, o Japão é constituído principalmente por ligações 4G.

Tabela 2 - Estatísticas da População e Uso de *Internet* Mundial (30 NOV 2015)

Fonte: (Internet World Stats, 2016)

| Europa | População (2015 Est.) | Utilizadores de *Internet* 30 NOV 2015 | % Penetração (% População) | % Utilizadores na Europa |
|---|---|---|---|---|
| **Islândia** | 334,303 | 323,045 | 98.2 % | 0.1 % |
| **Portugal** | 10,374,822 | 7,015,519 | 67.6 % | 1.2 % |
| **Ucrânia** | 44,008,507 | 19,099,692 | 43.4 % | 3.2 % |
| **Rússia** | 146,267,288 | 103,147,691 | 70.5 % | 17.1 % |
| **Total Europa** | 821,555,904 | 604,147,280 | 73.5 % | 100.0 % |

Na tabela 2 está refletido o País com a menor percentagem de penetração de utilizadores de *internet* - a Ucrânia, com apenas 43.4% da população -, e também o país com a maior penetração que é a Islândia, onde 98.2% da população acede à *internet*. É necessário também destacar a Rússia, pois é o país com a maior quantidade de utilizadores da Europa (mais de 103 milhões de utilizadores).

Temos também representada a informação relativa a Portugal, onde cerca de duas em cada três pessoas acedem à *internet*. A informação da percentagem de utilizadores em função da população total de cada país é importante porque permite ter uma perceção (ainda que relativa, é certo) do nível de prosperidade e riqueza dos países e dos seus cidadãos.

A imagem seguinte relaciona o salário médio anual *per capita* e o custo mensal da subscrição de banda larga.

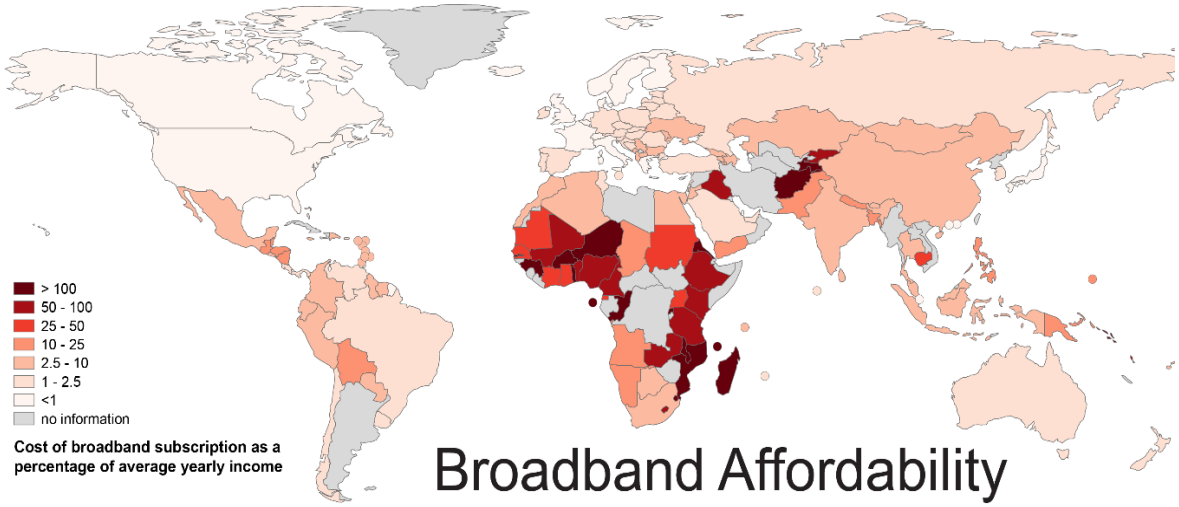


Figura 2 - Custo da subscrição de serviço de banda larga como percentagem do salário médio anual

Fonte: (Oxford II, 2011)

A figura 2 demonstra, de forma bastante clara, o custo do acesso à *internet* à escala mundial. Relacionando estes dados com os valores observados a partir da análise das tabelas referentes à percentagem de utilizadores de *internet*, podemos afirmar que a geografia do ciberespaço está diretamente relacionada com a qualidade de vida dos cidadãos de cada país. Sendo assim, nas regiões onde o acesso à *internet* é mais barato, verificamos que a "impressão geográfica" em matéria de ciberespaço é superior.

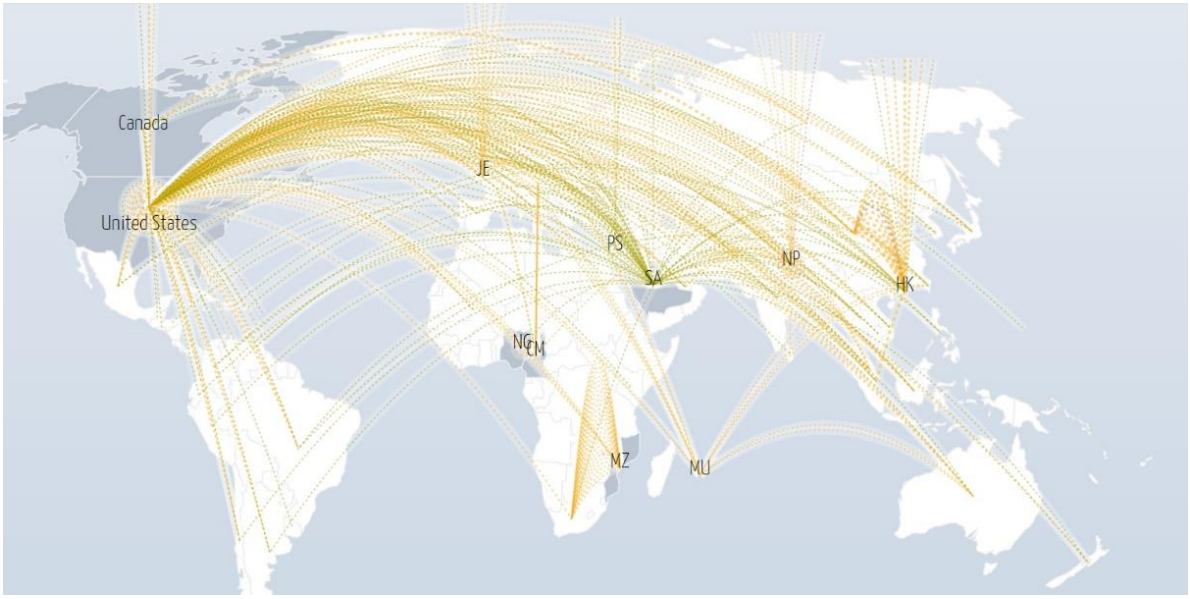


Figura 3 - Ataques DDoS a acontecer no mundo a 17 Março 2017 (pelas 18:00 horas)

Fonte: (Digital Attack Map, 2017)

A figura 3 representa os ataques Distributed Denial-of-Service (DDoS) que estavam a acontecer em direto no dia 17 de Março de 2017. O *website* www.digitalattackmap.com permite, a qualquer pessoa, verificar não só os ataques que estão a acontecer em tempo real como ataques ocorridos 2 anos antes da presente data de acesso. Embora se verifique uma grande quantidade de ataques todos os dias, estima-se que o *website* só mostre cerca de 0.1% dos ataques em acontecimento (Digital Attack Map, 2017).

Este tipo de ataques são extremamente comuns nos dias de hoje e verificam-se a uma escala global como podemos verificar.

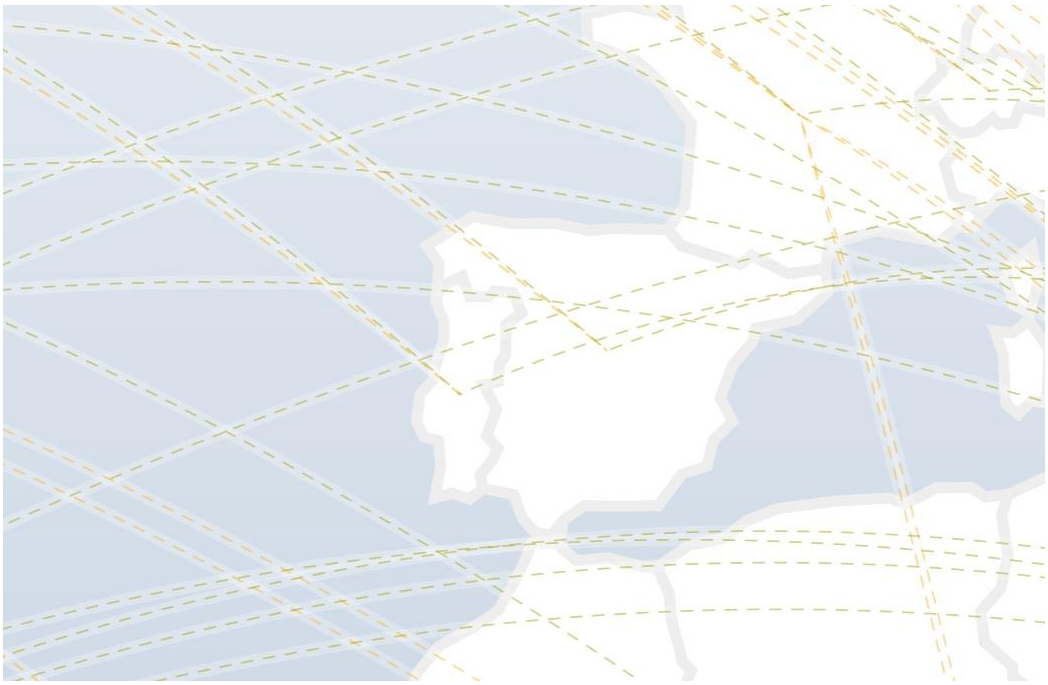

Figura 4 - Ataques DDoS a acontecer em Portugal a 17 de Março de 2017 (pelas 18:20 horas)

Fonte: (DIGITAL ATTACK MAP, 2017)

Em Portugal registavam-se 3 ataques com origem interna. Dois ataques de fragmentação de *Internet Protocol* (IP), um direcionado aos EUA e outro à Arábia Saudita, e um ataque volumétrico direcionado aos EUA. O primeiro tipo de ataque serve para negar ou perturbar o acesso a um computador *host* ou da rede, através da transmissão de grandes quantidades de unidades de dados divididas em pequenos fragmentos, de modo a fazer com que o *host* deixe de funcionar (CP, [s.d.]). Os ataques do segundo tipo são conhecidos como as “inundações”, pois têm o objetivo de causar um congestionamento pelo envio de um grande volume de tráfego, que vai deste modo sobrecarregar a largura de banda local. Estes são normalmente realizados através do uso de *botnets,* que atualmente devido ao desenvolvimento tecnológico e à “*internet* das coisas” tornam-se cada vez mais poderosos e fáceis de realizar (Verisign, 2015).

## 1.3. A Sociedade *Online*

A sociedade contemporânea encontra-se assente numa dimensão virtual, estimulada pelas Novas Tecnologias de Informação e Comunicação (NTIC), onde as interações sociais foram transportadas para uma socialização em rede desde o aparecimento da *internet*. A sociedade em rede constitui a nova morfologia social da nossa sociedade (Castells, 1999).

O sentimento de liberdade absoluta que facilmente se sente ao navegar pela *internet*, aliado à facilidade que nos dias de hoje se verifica existir para aceder ao "espaço virtual", fez com que a ideia inicial da propagação da livre circulação de conhecimento à escala mundial se tornasse num pretexto para construir alguns dos alicerces da sociedade atual (Martins, 2012).

Neste sentido, tem havido um aumento na procura de serviços de comunicação e informação com uma maior largura de banda, o que, por sua vez, esteve na origem da construção de infraestruturas com uma maior capacidade de afluência de transmissões de dados para suportar esta tendência atual. Estas infraestruturas constituem, nos dias de hoje, um fator de desenvolvimento e progresso para esta sociedade de informação, mas também um alvo determinante em matéria de ações subversivas ou de Guerra (Nunes, 2016).

A massificação do uso da *internet* veio criar alguns problemas, suscitando (novos) riscos em face de (novas) ameaças, reais e ou potenciais. Mas, em primeira instância, veio proporcionar inúmeras oportunidades de crescimento económico que, não só a nível pessoal ou privado foi aproveitado, mas também houve uma adaptação por parte dos Estados para esta nova realidade. Apostando numa virtualização de processos administrativos e na "governação eletrónica", os Estados procuram garantir um desenvolvimento social sustentável e também melhorar a sua competitividade económica global, ajustando-se assim às novas tendências do mundo atual (Nunes, 2016).

Nos dias de hoje estão disponibilizados inúmeros serviços, utilizados tanto pelo cidadão comum como por empresas ou pelo Estado, como por exemplo, os mais comuns serviços de compra e venda, serviços de jogos *online,* ligação em rede de instituições, empresas e bancos, serviços de redes sociais universais como o

Facebook, ou mesmo a enorme oferta de conhecimento desde cursos *online* a livros em formato digital para consulta (Martins, 2012).

O Eurostat publicou um artigo com dados de junho de 2015, onde foram apresentadas as estatísticas relativas à disponibilidade de tecnologias de informação e comunicação, e à sua utilização, nos países da UE. A análise dos dados sobre o desenvolvimento da sociedade de informação é determinante para confirmar as tendências da sociedade perante a massificação do uso da *internet*, quer seja a nível pessoal, como por exemplo no uso de redes sociais, como a nível económico com a utilização do "comércio eletrónico".

Neste estudo, é possível constatar que na UE, em 2014, cerca de 46% da população, com idades compreendidas entre os 16 e 74 anos, utilizava redes sociais, que 65% da população acedia diariamente à *internet*, e 75% a nível semanal. Estes valores estavam inicialmente previstos para 2015, o que revela o célere crescimento desta tendência tecnológica e de disseminação/acesso à informação em rede (Eurostat, 2016).

O crescimento constante e sustentado da *internet*, levou à exploração de serviços, oferecidos por outras plataformas, como as telecomunicações, o armazenamento de informação, transmissão de vídeo, a televisão, entre outros. Como tal, houve a necessidade de desenvolver serviços e equipamentos capazes de estabelecer a ligação à *internet*, entrando assim na "era *smart*", desde o comum *smartphone* e *smarttv,* a frigoríficos e outro tipo de grandes eletrodomésticos, levando à criação do conceito da "*internet* das coisas" (Nunes, 2016).

Este conceito tem sido debatido intensamente pois oferece tanto grandes oportunidades e facilidades - não só na dimensão pessoal (desde a esfera estritamente individual, à domótica, por exemplo), como ao nível da esfera produtiva, nas empresas, onde contribui, por exemplo, para a diminuição dos custos de produção – como, por outro lado, envolve grandes riscos para as pessoas e essas mesmas empresas. Peritos na área de cibersegurança já alertaram para o facto de que a "*internet* das coisas" é uma das áreas mais vulneráveis das empresas e um dos modos mais eficazes de "lançar" um ciberataque (Szoldra, 2016).

De um modo simples, a "*internet* das coisas" ou *Internet of Things* (IoT) consiste na ligação de dispositivos à *internet,* de maneira a conseguirmos "comunicar" com esses mesmos dispositivos e, do mesmo modo, a criar condições para que também eles consigam comunicar quer entre si, quer com aplicações (Kobie, 2015).

Em primeira instância estes dispositivos representam a evolução das nossas casas para "o futuro", isto é: já é possível ter um frigorífico que nos avisa que estamos a ficar sem leite, ou que ajusta a temperatura em função das condições climáticas que o rodeiam para que os alimentos mantenham uma temperatura estabilizada, de modo a salvaguardar, por exemplo, a sua decomposição prematura. No Reino Unido, por exemplo, já se verifica o incentivo à utilização de *smart meters* que mostram, num ecrã de simples acesso, toda a informação dos gastos da casa em termos de energia, e ainda como conseguimos fazer poupança nesse domínio (ibidem). Alguns equipamentos, de modo a poderem funcionar com todo o seu potencial, requerem o auxílio de sensores nas nossas casas, câmaras, ou mesmo um sensor na nossa roupa que permita precisar a nossa localização, estando todos os equipamentos preparados para se ajustarem quando estivermos a chegar a casa ou a sair desta (McOwan e McCallum, 2014).

Mas para esses equipamentos nos "ajudarem" no nosso dia-a-dia, têm de estar ligados à *internet,* contendo a nossa informação pessoal e criando um ponto de acesso através dos quais os *hackers* podem conseguir não apenas controlar esses mesmos dispositivos, como aceder aos outros a que estes estão ligados como, por exemplo, os nossos telemóveis (*smartphone*) ou computadores portáteis.

O mais preocupante é que os vários produtores destes dispositivos falham em passar nos testes de segurança mais básicos: manifestam problemas que vão desde fracas encriptações a ter a *password* codificada diretamente nos dispositivos, o que cria condições propícias a que os equipamentos sejam facilmente "*hackeados*", comprometendo a nossa segurança e da nossa informação pessoal (Szoldra, 2016).

Num estudo realizado ao longo de dois anos pelo departamento de *Intelligence* do *website* americano Business Insider, foi determinado que em 2015 existiam 10 biliões de dispositivos com ligação à *internet*, e projetou-se que até 2020 esse número cresça para 34 biliões. Foi, igualmente, considerado expectável que o investimento na área da "*internet* das coisas" atinja valores próximos dos 6 triliões de dólares americanos, e que os maiores consumidores destes dispositivos sejam as empresas, tendo em vista o cumprimento de objetivos como baixar os custos de operação, aumentar a produtividade e apostar na expansão para novos mercados ou no desenvolvimento de novos produtos (Greenhough, 2016).

Mais preocupante que a potencial "invasão" da esfera pessoal através do *hacking* destes dispositivos é a utilização dos mesmos para coordenar grandes ataques DDoS. Estes ataques são levados a cabo através do aumento exponencial do fluxo de tráfego de um *website* de modo a impedir que um utilizador real queira aceder a este, e conduzindo em última análise ao encerramento, durante um dado período temporal, do mesmo.

Sabendo que alguns destes equipamentos "facilitam" o acesso de *hackers* pelas suas fracas capacidades de segurança, estimando-se que cerca de 2 milhões de dispositivos estão já a ser controlados (incluindo *hotspots wi-fi* e antenas satélite) (Lohr, 2016), e que estes são, também, utilizados para grandes ataques DDoS contra empresas e mesmo contra Estados (como se sabe, hoje, por exemplo, que foi o caso do ataque à Estónia em 2007), é necessário perceber quais são os "pontos fracos" deste sistema considerando as várias escalas em que o mesmo tem que ser equacionado, e as infraestruturas críticas que são ou podem ser alvo desse tipo de ameaças – quer por serem potencialmente mais vulneráveis, quer por serem mais apetecíveis devido ao interesse estratégico a elas associado.

Michael Walker, um perito em segurança de computadores da Divisão de Pesquisa Avançada do Pentágono, afirmou que: "*se queremos introduzir as tecnologias ligadas à rede em mais e mais coisas, temos também de arranjar uma maneira de as tornar seguras"*, dizendo ainda que este assunto é "*um desafio para a civilização*" (ibidem).

## 1.4. Infraestruturas Críticas

A rutura de infraestruturas críticas é uma preocupação atual dos Estados e das principais Organizações Internacionais. No entanto, devido à atual dependência de serviços que impera sobre a rede de telecomunicações, um eventual ciberataque "ganha" o poder de deixar um Estado sem a capacidade de assegurar o cumprimento de alguma(s) das funções sociais vitais associadas à *raison d'être* da sua própria existência, à satisfação das necessidades coletivas que a justificam e legitimam, e a um nível de vulnerabilidade generalizada com grande impacto económico-financeiro mas, sobretudo, securitário (EC, 2012).

Atualmente, em Portugal, podemos identificar algumas infraestruturas críticas como: a Rede de Transportes, onde se inclui o controlo de tráfego aéreo ou o metropolitano; o Sistema Financeiro, por exemplo a banca e ou a bolsa; o Sistema de Defesa, do qual dependem os sistemas de radares e de mísseis; a Proteção Civil, como os Bombeiros; o Sistema de Saúde ou o Sistema de Distribuição de Água, apenas para mencionar alguns exemplos. Estas infraestruturas críticas estão, por sua vez, diretamente dependentes da Rede de Telecomunicações que, por sua vez, está dependente da Rede Elétrica Nacional (REN), como demonstrado na figura seguinte (Nunes, 2016).

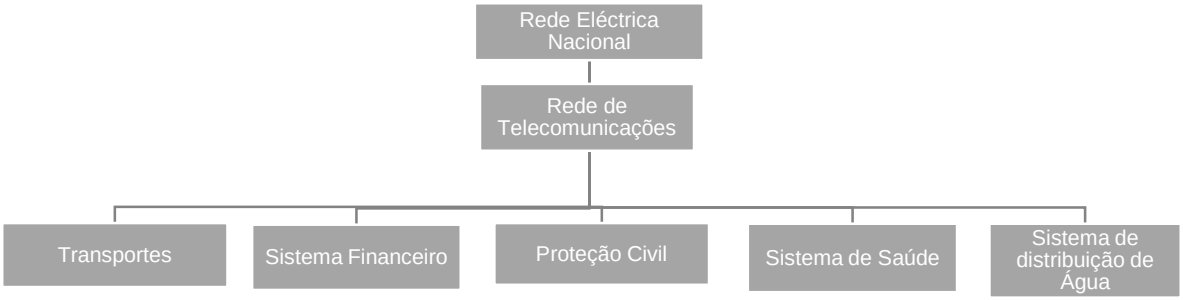


Figura 5 - Diagrama da Interdependência das Infraestruturas Críticas Nacionais

Fonte: (Adaptado de: (Nunes, 2015))

Na sociedade atual, um eventual ciberataque, capaz de condicionar a rede de telecomunicações nacional, iria produzir efeitos diretos em todas as infraestruturas críticas mencionadas anteriormente - algo que é preocupante pois o não funcionamento das mesmas implica o não funcionamento do Estado.

Esta não é uma realidade distante ou improvável, pelo contrário. Temos, já, vários exemplos. Na sequência do ciberataque conduzido contra a Estónia em 2007 (que já anteriormente mencionámos), os bancos e jornais deixaram de funcionar e as comunicações do Governo foram comprometidas. Um ano depois, em 2008, imediatamente antes de a Rússia invadir a Geórgia, este país sofreu um ciberataque que debilitou as tecnologias de informação militares, inclusivamente a sua defesa aérea (Rehman, 2013).

## 1.5. Era da Informação

A informação e o conhecimento sempre estiveram associados ao poder, e a realidade atual é que, devido às novas tecnologias e à facilidade do acesso à *internet*, a informação está disponível numa escala global, algo que é preocupante pois envolvendo o Poder, é expectável que se verifiquem tentativas no sentido de garantir a capacidade de monopolização da mesma (Balão, 2014).

Se considerarmos um caso recente de Edward Snowden, podemos observar que tal monopolização e controlo da informação já se verifica. Esta é preocupante no sentido de os Estados estarem a direcionar-se para uma tendência de Infraestrutura de Informação global (IIG) ou Sistema de Informações Global (SIG), onde cada vez mais um maior número de atores do sistema político internacional passa a fazer parte (ibidem). Este sistema leva, na prática, à substituição de várias redes por uma única rede de informação que transcende os limites físicos dos Estados, e sendo assim é natural que estes diversos atores procurem controlar e manipular o conteúdo dessa mesma informação (Nunes, 2016).

Torna-se necessário perceber em que sentido este controlo da informação condiciona a autoridade política e social dos Estados. Particularmente, no que se refere aos Estados ditos inferiores em poder no domínio das tecnologias de informação ficarem dependentes de Estados com um maior poder nesse aspeto, ou mesmo de Organizações Internacionais, que dispõem de uma grande capacidade de influência e pressão (Balão, 2014).

Na sociedade atual, a utilização em massa da *internet* está a levar a um aproveitamento estratégico de agentes Estatais, Organizações Internacionais e outros agentes do cenário político, estando cada vez mais voltados para o ciberespaço. A noção de liberdade de informação que se verificou com o aparecimento da *World Wide Web* (WWW), está cada vez mais dissimulada, pois existe a vontade de aproveitar este novo espaço para ganhar poder e como tal, é do interesse destes atores internacionais que não só se controle a informação, como ainda se tente anular a capacidade e o potencial benéfico que esta representa por

ser de livre e fácil acesso, pelo uso de “desinformação” e pela propagação de informação de fraca qualidade (ibidem).

Outra consideração importante é perceber que toda esta informação, inclusivé a confidencial, está ligada em rede, e como tal, é possível para indivíduos, ou organizações altamente experientes e qualificadas, como por exemplo os “*Anonymous*”, o acesso a esta e a sua divulgação. Algo que já se verificou nos últimos anos, sendo que alguma dessa informação *hackeada*, e posteriormente divulgada, é do interesse da sociedade em geral no âmbito do conhecimento e da verdade. Mas, por outro lado, existe informação confidencial que, sendo divulgada, põe em causa e em risco a segurança de cidadãos e de operações que se encontram a decorrer (Balão, 2014).

Neste sentido, a informação ganha cada vez mais valor, principalmente para aqueles que a conseguem usar e manipular para alcançarem os seus objetivos, verificando-se assim um investimento na área das tecnologias de comunicação, algo que potencializa não só o domínio e o poder como as ameaças que a este estão inerentes.

# Capítulo 2 – O *statu quo* da Ciberdefesa e Cibersegurança no século XXI

Nos dias de hoje, falar de cibersegurança é vulgar, mas, no início dos anos ’90 do século XXI, o conceito de segurança ainda não era associado ao ciberespaço a não ser por técnicos informáticos quando queriam apontar falhas informáticas e a respetiva necessidade de as corrigir. Contudo, como no pós 11 de Setembro de 2001 as ameaças não-convencionais começaram a ser tratadas como prioridade estratégica devido à generalização das redes de informação no âmbito económico, social, político e militar, a cibersegurança ganhou foco e tornou-se numa preocupação das principais organizações internacionais e potências mundiais (Barrinha e Carrapiço, 2016).

Por outro lado, devido aos recentes casos de acesso a informação confidencial seguidas de posterior partilha com o público à escala mundial através da *internet* (como, por exemplo, tem vindo a suceder através das atividades da organização “*Wikileaks*” que, desde 2006, tem vindo a recolher e divulgar informação crítica, principalmente de documentação confidencial do governo dos EUA) (Hintz, 2013), ou dos ciberataques que num passado recente foram levados a cabo contra Estados como a Estónia e a Geórgia, verificou-se a necessidade de apostar no desenvolvimento de mecanismos de defesa contra este tipo de ameaças (IDN, 2013).

Os EUA, estando na vanguarda do poder militar convencional, já reconheceram a relevância das ameaças cibernéticas, tendo vindo a desenvolver quadros de respostas no sentido de evitar o que muitos autores referem como um eventual “Pearl Harbour digital”. A criação do *U.S. Cyber Command* é fruto dessa preocupação e demonstra, a nosso ver, que o ciberespaço é reconhecido como um domínio onde são conduzidas operações militares, falando-se assim de uma militarização da *internet.* Atualmente, as operações conduzidas no ciberespaço representam objetivos estratégicos, não só no próprio domínio do ciberespaço como

nas outras dimensões de cenários operacionais, seja no mar, ar, terra ou espaço, tornando-se assim indispensável para as Forças Armadas no que diz respeito ao sistema de informação e de armas (Nunes, 2011).

O *United Nations Institute for Disarmament Research* (UNIDIR) publicou em 2013, um estudo intitulado *"The Cyber Index: International Security Trends and Realities"*. Este foi elaborado com informação dos 193 Estados membros da ONU, concluindo-se que 114 desses Estados já têm programas nacionais de cibersegurança. Desses, 47 incluíam as forças armadas nos seus programas, e os restantes 67 desenvolveram programas apenas civis. O mesmo estudo indicava, ainda, que 12 dos 15 Estados que mais investem nas forças armadas, estavam a desenvolver ou já possuíam unidades dedicadas de *cyber-warfare,* e que 10 desses já dispunham de "ciber-capacidades" ofensivas ou estão atualmente em desenvolvimento, como é o exemplo dos EUA, do Reino Unido, China e Russia (UNIDIR, 2013).

No sentido em que é necessária cada vez mais a cooperação internacional, para contrariar as ciberameaças, é importante perceber qual o papel das Organizações Internacionais no campo do ciberespaço.

Enquanto que o trabalho da ciberdefesa mais em concreto é organizado pelos próprios Estados, as Organizações Internacionais podem, e devem, discutir, coordenar e desenvolver propostas e estratégias para a criação de estruturas, instituições e definição de políticas, tanto internacionais como regionais, em prol de um ciberespaço mais seguro. As suas funções variam desde o estabelecer de normas ou princípios que previnam o uso malicioso de ciber-tecnologias, à correção ou alteração dos acordos existentes no âmbito dos quais são definidos, entre outros, o conceito de conflito armado e a respetiva aplicação da lei. Podem ainda promover a prevenção e preparação dos Estados para recuperarem de um ciberataque. Estas organizações têm o poder de conseguir conciliar todos os diferentes atores do ciberespaço (os Governos, o setor privado, a sociedade civil, e os cidadãos), e como tal, o seu papel é bastante importante rumo a um ciberespaço mais seguro (UNIDIR, 2013).

## 2.1. ONU

Nos próximos parágrafos iremos observar que tipo de ações estão já a ser levadas a cabo pela organização internacional que tem uma participação de Estados Membros que é praticamente global, e como tal é a que podemos considerar ter o maior alcance.

A ONU, já aprovou uma série de resoluções e normas relevantes para as TIC e para a cibersegurança, fazendo um apelo aos seus Estados Membros para os futuros desafios do ciberespaço. Esta organização tem promovido a criação de normas por duas vias de negociação, separando os assuntos político-militares dos económicos. Quanto aos primeiros, a preocupação incide sobre o modo como os meios e tecnologias de informação, podem ser utilizados com propósitos que contrariam os objetivos que têm em vista assegurar a manutenção da segurança e estabilidade internacionais, afetando por consequência a segurança dos Estados. Relativamente aos assuntos económicos, a preocupação centra-se na utilização criminosa das tecnologias de informação (Maurer, 2011).

Neste contexto, uma das mais importantes Resoluções adotadas pela Assembleia Geral da ONU foi a 56/121, referente ao combate ao uso criminoso das tecnologias de informação. Nesta são reconhecidas as possibilidades de atividade criminal associadas à utilização do ciberespaço e é assumida a necessidade da propagação das TIC para o desenvolvimento dos Estados, mas também é dado enfoque à necessidade da cooperação entre os mesmos de modo a garantir o cumprimento de tais objetivos (UN GA, 2002).

Em 2003, a Assembleia Geral adota a Resolução "*Creation of a global culture of cybersecurity*", reconhecendo a crescente dependência dos governos, negócios e organizações do uso das TIC, quer esteja em causa a obtenção de bens e serviços essenciais para a condução de negócios ou para as "simples" trocas de informação, pelo que se torna necessário apostar num aumento da capacidade de

cibersegurança à medida que os Estados assumem um papel cada vez mais participativo na "sociedade de informação" (UN GA, 2003).

Um ano mais tarde é adotada a Resolução para a proteção das infraestruturas críticas de informação onde, entre outras coisas, se encorajou todos os "*Member States and relevant regional and international organizations that have developed strategies to deal with cybersecurity and the protection of critical information infrastructures to share their best practices and measures that could assist other Member States in their efforts to facilitate the achievement of Cybersecurity*" (UN GA, 2004, p. 2).

Esta orientação mais específica para as questões do ciberespaço sucedeu a uma outra que, desde 1998 e ao longo dos anos tem dado origem à adopção de uma Resolução sobre os "*Developments in the field of information and telecommunications in the context of international security*". Em paralelo com estas resoluções anuais, existem quatro *Group of Governmental Experts* (GGE), que examinam as existentes e as potenciais ameaças provenientes do Ciberespaço, assim como as possíveis medidas de cooperação para as enfrentar, lançando nesse âmbito um relatório anual, para orientação dos Estados membros (UN GA, 2015).

Portugal foi um dos Estados que deu resposta à Resolução de 2015, afirmando que a segurança das redes de informação é importante e está em crescimento, além de que, a nível nacional, tem sido feito um esforço para levar a cabo exercícios com parcerias público-privadas, para promover a standardização técnica e também para organizar conferências e seminários com a participação de oradores internacionais, para ir ao encontro da resolução anual das Nações Unidas (NU), sobre o desenvolvimento na área das telecomunicações e sistemas de informação (MNE, 2016).

## 2.2. NATO

A NATO iniciou o seu programa de ciberdefesa em 2002, depois de alguns incidentes no final dos anos ’90 do século XX relacionados com as operações conduzidas nas Balcãs. Quando a NATO começou as suas operações militares contra a Sérvia, uma série de grupos de *hackers* “pro” Sérvia atacaram a infraestrutura de *internet* ali existente de modo a afetarem as capacidades de condução das operações que ali tinham lugar. Na sede da NATO, na Bélgica, estes ataques afetaram as relações públicas e o *website* dos assuntos públicos da Guerra do Kosovo, onde eram atualizadas notícias e informações, ficou inoperativo durante alguns dias devido a ataques DDoS (Verton, 1999). Estes acontecimentos levaram à decisão da implementação de um programa de ciberdefesa da NATO, na cimeira de Praga em 2002 (NATO PA, [s.d.]).

Nesse contexto, foi então criado o NATO *Computer Incident Response Capability*, que ficou responsável por dar resposta a ciberataques contra os sistemas computacionais da NATO. As intrusões, medidas preventivas, o estudo forense digital, e o apoio aos Estados membros são responsabilidade do Centro de Coordenação em Bruxelas e do Centro Técnico em Mons, que fazem parte da *NATO Communication and Information Services Agency* (UNIDIR, 2013).

O *Cooperative Cyber Defence Center of Excellence* (CCD COE) é estabelecido em 2008 na Estónia, em Tallinn. Este é composto por peritos de vinte (20) nações diferentes, com formação em diversas áreas e domínios: desde educadores, analistas ou pesquisadores, com um passado militar, governamental ou industrial, possibilitando assim um vasto olhar sobre a ciberdefesa. O Centro organiza anualmente o maior e mais complexo exercício técnico internacional sobre ciberdefesa, o “*Locked Shields*”, e ainda a conferência sobre ciber-conflitos, a “*CyCon*”. O CCD COE é responsável pela formação e pesquisa, assim como pela realização de *workshop,* sobre a doutrina, legalidade e aspetos técnicos de *cyber warfare* (NATO CCD COE, [s.d.]).

Uma das ações mais importantes do Centro foi, como anteriormente tivemos oportunidade de destacar, o desenvolvimento do Manual de Tallinn, que foi levado a cabo por peritos que, a nível internacional, procuraram investigar de que

modo é que a Lei Internacional, as normas e as suas práticas podem ser suscetíveis de aplicação ao ciberespaço. Passados três anos, o Manual foi publicado numa versão "*draft*", que ficou "aberto para discussão" no domínio da análise dos ciberconflitos, na perspetiva de poder ser melhorado (NATO CCD COE, 2013).

A NATO também criou o *Cyber Defence Management Authority* (CDMA) que, como o nome indica, é responsável pela iniciação e coordenação de ações apropriadas de ciberdefesa, efetivas e imediatas, se for necessário. Este também serve como um comando central, para os esforços de partilha de informação dos Estados membros, e ainda tem a competência de gerir as entidades de ciberdefesa da NATO. Em caso de pedido de auxílio por parte de um Estado membro que tenha sido vítima de um ciberataque, o CDMA está preparado para coordenar ou fornecer assistência ao mesmo (NATO PA, [s.d.]).

Na Cimeira de Lisboa, em 2010, as falhas de ciberdefesa da NATO e dos Estados membros foram identificadas e refletidas no novo Conceito Estratégico (CE) da NATO.

No CE de 2010, o ciberespaço está referido numa ótica de "*Security Environment*" e de "*Defence and Deterrence*" (NATO, 2010).

O 12º ponto da temática "Ambiente de Segurança" refere que os ciberataques estão a tornar-se mais frequentes, mais organizados, e que estão também a tornar-se mais dispendiosos pelos danos que conseguem causar, tanto na indústria, como no governo, ou mesmo em infraestruturas críticas. Em face desta realidade, assumiu-se que poderiam chegar, assim, a assumir o papel de ameaça à segurança e estabilidade nacional e Euro-Atlântica. Diz ainda o mesmo documento, que os ciberataques são provenientes de milícias, serviços de *intelligence*, crime organizado e grupos terroristas ou extremistas (NATO, 2010, p.11).

O ponto 19 do tema "Defesa e Impedimento" do mesmo documento afirma, por seu lado, a garantia de que a NATO terá todas as capacidades necessárias para deter e assegurar a defesa contra quaisquer tipos de ameaças sobre a segurança

das populações. Sendo assim, um dos sub-pontos ali incluído é o que se refere ao desenvolvimento da capacidade de prevenção, deteção, defesa e recuperação contra ciberataques, através do recurso ao processo de planeamento da NATO, de modo a melhorar e coordenar as capacidades de ciberdefesa nacionais, juntando todos os corpos da NATO sob uma ciber-proteção centralizada. Para além disso, equacionou-se igualmente melhorar também a integração de uma consciencialização, alerta e capacidade de resposta dos Estados membros (NATO, 2010, p.16-17).

Em junho de 2011, os Ministros da Defesa da NATO aprovaram um documento classificado, já com a revisão da política de ciberdefesa, e com um plano de ação para que esta seja implementada, o que veio clarificar os mecanismos de resposta, a ciberataques, da NATO. Este documento é classificado e define os esforços referentes à ciberdefesa, assim como o respetivo plano de ação tendo em vista a sua implementação (UNIDIR, 2013).

Nesse mesmo ano, e tendo em vista apostar na capacitação para uma resposta mais rápida a ciberataques que os Estados membros tenham sofrido, foram desenvolvidas as *Rapid ReactionTeams* (RRT). Estas estão disponíveis e preparadas para serem destacadas imediatamente, caso sejam requisitadas pelo Estado membro, ao contrário do que se verificou na Estónia e Geórgia (2007 e 2008, respetivamente), cenários no âmbito dos quais a NATO apenas destacou equipas *ad hoc*. No caso de ser um pedido político de um Estado não-membro, é necessária a aprovação do Conselho do Atlântico Norte (NATO PA, [s.d.]).

Em 2012, no âmbito da Cimeira de Chicago, os Chefes de Estado e Governo da NATO constataram o registo de um número crescente de ciberataques, tendo os mesmos evoluído tanto em sofisticação como em complexidade. Deste modo, foi assumido pelos líderes dos Estados membros da organização o seu empenho em continuar a desenvolver as capacidades de ciberdefesa da NATO, a par com o apelo à necessidade de uma maior cooperação entre os Estados membros no domínio da cibersegurança (NATO, 2012). Dois anos mais tarde, na Cimeira de Gales, o antigo Secretário-Geral da NATO Anders Fogh Rasmussen

reafirmou o empenho daquela organização em defender os aliados contra ciberameaças (NATO, 2014) .

Neste sentido, foi desenvolvida a Política de Ciber Defesa Avançada da NATO, que assenta no facto de que a principal responsabilidade da organização naquele domínio é defender as suas redes de ligação, além de que a assistência a aliados deverá ser realizada no espírito da solidariedade, apesar de ser dado enfâse à responsabilidade de cada Estado no sentido de desenvolver capacidades relevantes para proteger as suas próprias redes de ligação nacionais. Merece destacar, ainda, que a NATO reconhece que a Lei Humanitária Internacional é aplicável no domínio do ciberespaço. Por fim, é também assumido o facto de que os ciberataques podem ameaçar a prosperidade, segurança e estabilidade nacional e Euro-Atlântica, pelo que o seu impacto pode ser tão nefasto para a sociedade moderna como um ataque convencional. Como tal, considera-se que a ciberdefesa compõe uma das tarefas base da defesa coletiva, muito embora a decisão relativa ao facto de um ciberataque poder justificar ou não a invocação do artigo 5º do Tratado do Atlântico Norte, fique a cargo do Conselho do Atlântico Norte, na sequência de uma abordagem “caso-a-caso” (ibidem).

Na sequência de toda a evolução registada neste domínio, há que destacar a cooperação habitual entre peritos da UE e da NATO tendo, em fevereiro de 2016, sido elaborado um Acordo Técnico sobre Ciber Defesa entre a NATO *Computer Incident Responce Capability* (NCIRC) e a *Computer Emergency Response Team of the Eutopean Union* (CERT-EU) (NATO, 2016). Este acordo técnico define o enquadramento para a partilha de informações entre estas equipas de resposta, e também sobre as melhores práticas e métodos (NATO ML, 2017). Mais tarde, em julho do mesmo ano, o Parlamento Europeu adotou a “*Directive on Security of Network and Information Systems*”, que representa o primeiro conjunto de regras sobre o ciberespaço extensíveis e aplicáveis a toda a UE. O objetivo desta Diretiva é alcançar um elevado nível de segurança de redes e sistemas de informação comum a toda a UE através de três (3) meios: a melhoria de capacidades nacionais de cibersegurança; um aumento de cooperação ao nível da UE; e a obrigação da

gestão de riscos e reportes de incidentes, por parte dos operadores dos serviços essenciais e dos fornecedores de serviços digitais (EC, 2016).

Também em 2016, na Cimeira de Varsóvia, o ciberespaço foi reconhecido como um domínio de operações pelo que a NATO tem que garantir a sua defesa do mesmo modo que o faz para os "tradicionais" domínios do ar, terra ou mar. Como a maior parte dos conflitos da atualidade têm uma "dimensão ciber", equacionar o ciberespaço como um domínio específico e autónomo irá permitir, à partida, a existência de condições que assegurem uma melhor proteção, assim como a condução de missões e operações por parte da NATO (NATO, 2017).

Analisando o CE de 2010 e as posteriores atividades desenvolvidas pela NATO, é percetível o esforço da organização no sentido de criar condições que permitam assegurar a prevenção e o combate às ameaças que advêm do ciberespaço, e também a tentativa de apoiar os aliados afetados por ciberataques, nomeadamente através da definição de regras que giram os conflitos no ciberespaço. É também notória a tentativa da clarificação das situações em que se torna legítima a invocação do artigo 5º do Tratado do Atlântico Norte e da defesa coletiva, estando no entanto limitado, em última instância, à decisão do Conselho do Atlântico Norte

## 2.3. UE

No contexto da realidade da União Europeia, o respetivo CE, publicado em 2003 e intitulado "*A Secure Europe in a Better World*", foi o primeiro documento a definir objetivos claros para o desenvolvimento institucional da organização em termos de segurança, tendo como alicerces os valores base da UE. No entanto, neste documento, só o terrorismo, a proliferação de armas de destruição massiva, os conflitos regionais, os Estados Falhados, e o crime organizado, são reconhecidos como as ameaças chave que a UE precisa de abordar, não reconhecendo o ciberespaço ou a cibersegurança como uma prioridade estratégica (EU, 2003).

Mais tarde, em 2008, surge a necessidade de rever o documento, e é apresentado o relatório do Conselho Europeu intitulado "*Providing Security in a Changing World*" (EC, 2008). Neste documento é avaliada a forma como o conceito estratégico de 2003 foi posto em prática e são ponderadas as modificações eventualmente necessárias para melhorar e ou potenciar a sua implementação. Passados cinco anos sobre a apresentação do primeiro documento, a cibersegurança já é incluída como uma das ameaças chave ou desafios globais em 2008. É um facto que, embora tivesse sido adotada em 2006, a Estratégia Europeia para uma Sociedade de Informação apenas focava a cibercriminalidade na *internet* (EC, 2006). No entanto, com o aparecimento de ataques a tecnologias de informação de instituições privadas e do governo, de Estados Membros da UE, as ameaças derivadas do ciberespaço ganharam uma nova dimensão, constituindo-se aquele espaço como uma nova arma política, militar ou económica. Este relatório refere, ainda, que é necessário trabalhar em prol de se atingir uma abordagem compreensiva da UE em relação a esta problemática, cultivar a consciencialização dos Estados Membros e incentivar a cooperação internacional (EU Council, 2008).

Em 2013, no âmbito da "Estratégia de Cibersegurança da União Europeia", são definidas cinco prioridades estratégicas: alcançar a ciber resiliência; reduzir drasticamente o cibercrime; desenvolver políticas e capacidades de ciberdefesa relacionadas com a *Common Security and Defence Policy* (CSDP); desenvolver os recursos industriais e tecnológicos para a cibersegurança; e estabelecer para a União Europeia uma política internacional coerente sobre o ciberespaço e que, simultaneamente, promova os seus valores. Este documento refere, igualmente, que os Estados Membros deveriam concentrar os seus esforços em desenvolver ciber-capacidades de defesa, que a UE precisa de desenvolver um quadro político de ciberdefesa, e que o diálogo civil-militar, deveria ser promovido, tal como o diálogo com parceiros internacionais, como a NATO (EC, 2013).

Um ano mais tarde, em 2014 é apresentado o "*EU Cyber Defence Policy Framework"*, com o objetivo de definir aspetos da Estratégia de Cibersegurança da UE, e identificar as áreas prioritárias para a ciberdefesa da CSDP, clarificando

também os papéis a desempenhar por diversos atores europeus. As prioridades definidas para o quadro político de ciberdefesa da UE foram, então, as seguintes:

1. Apoiar o desenvolvimento das capacidades de ciberdefesa dos Estados Membros relacionadas com a CSDP;
2. Melhorar a proteção das redes de comunicação da CSDP, usadas por entidades da UE;
3. Promover a cooperação civil-militar através de ciber-políticas mais abrangentes, relevantes para as agências e instituições da UE, e também do setor privado;
4. Melhorar as oportunidades de treino, educação e exercícios;
5. Fortalecer a cooperação com parceiros internacionais relevantes (EU Council, 2014).

Atualmente, os atores mais importantes no que diz respeito ao apoio institucional da cibersegurança da UE são: a *European Network and Information Security Agency* (ENISA), a *European Police Office* (Europol) onde está incluído o *European Cyber Crime Center* (EC3), e a *European Defence Agency* (EDA) (Pernik, 2014).

A ENISA é o centro de excelência para a cibersegurança na Europa. Foi criada em 2004, e desde então tem sido responsável por desenvolver uma cultura de *Network and Information Security* (NIS). Esta agência trabalha com os Estados Membros da UE e também com o setor privado a vários níveis e em várias atividades, incluindo os exercícios de cibersegurança pan-europeus, o desenvolvimento de estratégias nacionais de cibersegurança, cooperação com várias *Computer Security Incident Response Team* (CSIRT), fornecendo conselhos e ajuda no domínio do ciberespaço e facilita o diálogo entre os diferentes atores europeus envolvidos na questão da cibersegurança. Como afirma a Professora Sandra Balão, a ENISA é considerada "*o "guardião" da Segurança da Informação na Europa e um Centro de Excelência*", no entanto acrescenta que não tem "*qualquer capacidade operacional, interventiva, efectiva*" (Balão, 2014, p. 139). Contudo, tem também, como funções: desenvolver estudos sobre uma adoção

segura do uso da "*cloud*", trabalhar sobre problemas de proteção de dados, melhorar as capacidades de privacidade da tecnologia, identificar ciber ameaças, entre outros. A ENISA é ainda responsável por ajudar a desenvolver políticas e leis de implementação sobre NIS na UE (ENISA, 2017).

O EC3 foi estabelecido pela Europol em 2013 para ajudar a reforçar a aplicação da lei relativamente a cibercrimes na UE, ajudando deste modo a proteger cidadãos, governos e negócios de crimes *online*. Este centro divide o combate à cibercriminalidade em três abordagens: a estratégia, a peritagem forense, e as operações. Relativamente à estratégia, esta está dividida em duas equipas: a primeira está responsável pelo apoio para estabelecer parcerias e coordenar medidas de prevenção e sensibilização, enquanto a segunda desenvolve análises estratégicas, políticas e medidas legislativas. Quanto ao nível de operações, o EC3 foca-se em três tipos de cibercrimes: crimes cometidos por grupos organizados, particularmente os que possam gerar grandes lucros para os criminosos, como é o exemplo da fraude fiscal; crimes que possam ferir seriamente as suas vítimas, como é o caso da exploração sexual infantil; e ainda crimes que tenham impacto em infraestruturas críticas e sistemas de informação na UE como, por exemplo, ciberataques. Nos casos mais importantes de cibercrime internacional que afetem Estados Membros da UE ou os seus cidadãos, a UE conta com a *Joint Cybercrime Action Taskforce* (J-CAT), que iniciou a sua atividade em setembro de 2014 sob a alçada da Europol, e trabalha em conjunto com o EC3. Este centro utiliza as capacidades de aplicação da lei da Europol, mas também oferece apoio operacional e analítico a investigações conduzidas por Estados Membros (Europol, 2017).

A EDA é responsável por desenvolver as ciber-capacidades da UE em conjunto com os *EU Military Staff* (EUMS). Em 2013 apresentou os resultados de um estudo elaborado sobre as capacidades militares de ciberdefesa. A partir deste, desenvolveu um valor de referência sobre a "Prontidão de Ciberdefesa" de 20 Estados Membros e algumas organizações da UE, que participaram no estudo. Os resultados obtidos demonstraram que a ciberdefesa militar a nível europeu ainda se encontra num estado embrionário e recomendou uma série de ações a serem

desenvolvidas quer ao nível da UE, quer a nível nacional. Por parte da UE, as ações recomendadas foram: melhorar a proteção da rede da UE, fortalecer as capacidades das equipas de *intelligence* e resposta rápida, criar uma cultura de cibersegurança, e por fim reforçar as ligações entre a NATO e a UE. Ao nível nacional, os Estados Membros precisam de: desenvolver iniciativas de educação e treino sobre ciberdefesa, assim como apostar na partilha de informação e de instalações com outros Estados Membros (EDA, 2013).

A *European Defence Agency* está a trabalhar, dentro do conceito de *Pooling and Sharing* em: treino e exercícios de melhoria de ciber *awareness* para operações de CSDP, elaboração da *Cyber Defence Research Agenda* (CDRA), desenvolvimento de soluções contra *Advanced Persistent Threat* (APT), *malware* e em proteção de informação, como a criptografia (EP, 2014).

Embora a revisão feita em 2008, do Conceito Estratégico da UE, reconheça as ciberameaças como um fator chave da segurança europeia de um modo um pouco embrionário, tem havido esforços para regularizar as políticas e estratégias de ciberdefesa e cibersegurança da União em geral e dos seus Estados Membros em particular. Além disso, as principais agências trabalham de um modo complementar para permitir um uso, o mais seguro possível, do ciberespaço, punindo a cibercriminalidade. É igualmente relevante o investimento em capacidades de ciberdefesa por parte dos Estados Membros, mas mais importante ainda é a sua cooperação e a promoção de exercícios que instruam uma mentalidade de ciber *awareness* que, no futuro, permita ter funcionários, militares, instituições ou Governos mais preparados para combater ciberameaças.

Nos parágrafos seguintes procurar-se-á analisar o processo de desenvolvimento de ciber-capacidades de alguns dos Estados mais influentes no domínio do ciberespaço, o que nos permitirá ter uma visão mais pormenorizada das capacidades defensivas e ofensivas que estão a ser adotadas ou em desenvolvimento nas maiores potências neste domínio, e que poderão ser aplicadas em possíveis conflitos nos dias de hoje.

1. EUA

Como foi referido anteriormente, os EUA são detentores de uma resposta militarizada contra ciberataques através do seu *Cyber Comand* que, em 2010, integrou componentes cibernéticos da marinha, do exército e da força aérea num só comando unificado, tornando-se numa das maiores organizações de ciberdefesa do mundo (EP, 2014). Em 2011, o *Department of Defense* (DoD) adotou a "*Strategy for operating in Cyberspace*", que assentava em cinco iniciativas estratégicas, das quais se destaca que o ciberespaço seria tratado como os domínios do ar, terra, mar e espaço; que o DoD iria utilizar novos métodos defensivos para combater ciber-ameaças; e que a cooperação a nível nacional e internacional seria encorajada (US DoD, 2015). No entanto, a estratégia definida pelo DoD não esclarecia factos como o de que o Pentágono possui cerca de 90% de capacidades ofensivas e apenas 10% defensivas, no que diz respeito a ciber-capacidades (EP, 2014). A fuga de informação da *National Security Agency* (NSA), protagonizada por Edward Snowden veio, também, facultar informação sobre o programa dos EUA "*MonsterMind*", que foi desenhado para reconhecer, neutralizar, e responder automaticamente a ciberataques contra os Estados Unidos da América (Zetter, 2014). O Pentágono aumentou os gastos em operações no domínio do ciberespaço, estimando-se custos de cerca de 26 biliões de dólares americanos em 5 anos, e ainda um aumento de recursos humanos para trabalhar neste domínio para um número aproximado de 6000 pessoas até ao ano de 2016 (Hickie, 2014) (quase o número de efetivos na Força Aérea Portuguesa - 6799 no final de 2015 (FAP, 2015)). Este valor torna-se pequeno em comparação com a proposta de orçamento de 19 biliões de dólares americanos só para o ano de 2017, por parte do anterior presidente dos EUA Barack Obama, aumentando assim em 5 biliões comparativamente ao ano de 2016, e demonstrando a urgência em melhorar as capacidades de ciberdefesa e em modernizar os sistemas de informação (Almada, 2016). Os EUA procuram uma definição internacional sobre quais os tipos de operações conduzidas no ciberespaço que são passíveis de constituir um ato de

guerra pelo que, em 2013 e cumprindo uma diretiva presidencial, foram instruídos a ajudar aliados que estivessem sob ciberataques (EP, 2014), revelando assim a urgência da atualização do âmbito de abrangência da definição de conflito armado, definida no artigo 5º do Tratado do Atlântico Norte, bem como a necessidade de definir que tipo de ciberataques representam uma ciberguerra, de modo a que possa ser invocada a defesa-coletiva.

## 2. China

A China tem investido grandes quantidades monetárias em infraestruturas de informação, bem como em recursos humanos (ibidem). Contam não só com operadores do People's Liberation Army (PLA), particularmente os da unidade 61398 do PLA, que é considerado o "ciber-exército" do Estado (MS Risk, 2016), como com o recrutamento de civis talentosos, formando assim os *Militia Information Technology Battalions* (Kan, 2009).

O Pentágono considera a China a maior ciber-ameaça para os EUA, enquanto esta, em 2007 denunciou os EUA como uma fonte de ciberataques efetuados contra o Estado Chinês. As revelações protagonizadas por Snowden vieram, pelo menos indiciar a existência de atividades de ciberespionagem por parte dos EUA contra a China piorando assim as suas "relações cibernéticas", para além das diplomáticas. No entanto, em 2013, dá-se aquele que é considerado um passo concreto no sentido de "reconstruir" as relações entre estes dois atores no que se refere a esta matéria: é constituído o primeiro grupo de trabalho sobre o ciberespaço reunindo especialistas das duas nações. No entanto, e apenas um ano decorrido, a China suspendeu a sua participação, face às acusações de ciberespionagem e de roubo de segredos de Estado de que foram alvo, por parte dos Estados Unidos da América, cinco (5) *hackers* chineses. Para além dos EUA, vários outros países já foram alvos de ciberespionagem Chinesa (EP, 2014).

Fruto dos ataques de ciberespionagem lançados contra os EUA, a China terá conseguido não só penetrar as redes de comunicação do *U.S. Transportation*

*Command* (TRANSCOM), que é o sistema responsável pelo movimento das tropas e equipamento americano pelo mundo, como roubar o *design* de armamento avançado como o F-35 *Joint Strike Fighter* (JSF), os drones RQ-4 *Global Hawk* e, ainda, o sistema de mísseis *Patriot* (Sood e Enbody, 2014), algo que revela a qualidade da informação obtida por esta via, assim como a vantagem estratégica que, efetivamente, é passível de ser obtida através deste tipo de ataques.

## 3. Rússia

Para a Rússia, o ciberespaço tornou-se uma prioridade militar e é visto como um novo teatro de guerra, num futuro próximo, tendo suscitado a criação de um ramo das forças armadas dedicado apenas à "*Cyber Warfare".* Andrei Grigoryev, o diretor da *Foundation for Advanced Military Research*, afirma que a sua agência tem três (3) prioridades de *Research and Development* (R&D): armamento, soldados futuristas, e o "*cyber warfare*" (Sputnik International, 2013).

O Estado Russo considera que o recurso a políticas e instrumentos de informação é primordial para proteger os seus interesses nacionais e dos seus aliados, além de que se devem articular capacidades não-militares com as militares de modo a adquirirem superioridade na "guerra de informação" (UNIDIR, 2013).

Neste contexto, pensa-se, ainda, que a Rússia recorre a ciberataques complexos e avançados para apoiar a prossecução dos seus interesses nacionais e objetivos militares, sendo considerado exemplo disso mesmo o caso concreto do ataque à Geórgia em 2008, no âmbito do qual *hackers* russos lançaram ciberataques a servidores georgianos, conseguindo manter inativos durante um período temporal considerável vários *websites* do Governo em geral e militares em particular, assim como prejudicar as comunicações entre as unidades militares e os serviços governamentais. Semanas antes dos ciberataques, foram lançadas ciber-operações ofensivas para infiltrar as redes militares e governamentais, de modo a obter informação útil para a campanha que se aproximava. Tudo isto para preparar

a invasão e o ataque físico das forças Russas, levando assim a um ataque mais eficaz (Haddick, 2011).

À semelhança do que anteriormente se havia verificado com a China, os EUA e a Rússia acordaram entre si, em 2013, na criação de uma linha de apoio para ajudar a impedir e resolver, no futuro, crises relacionadas com ciberataques, de um modo semelhante à linha de apoio utilizada para resolver "tensões nucleares" durante a Guerra Fria. No entanto o Estado russo continua a desenvolver medidas de ciberdefesa, tomando assim uma posição apreensiva relativamente a estas parcerias (Geers *et al.*, 2015).

4. Médio Oriente: Israel, Irão, Síria e Turquia

Israel é um alvo constante de ciberataques, reportando o combate a cerca de 1000 ataques por minuto (EP, 2014), algo que esteve na origem, em 2014, da criação da Autoridade Nacional de Ciber-Defesa. Esta tem o objetivo de proteger os civis contra ciberataques (Dvorin, 2014), e estabelecer uma unidade de elite em ciberdefesa para apoiar os Serviços Secretos (Soffer, 2014).

Os Estado Israelita também recorreu a ciberataques para propósitos políticos e militares, estando envolvido no ataque *Stuxnet*, sendo considerado um dos países tecnologicamente mais avançados neste domínio (EP, 2014).

O Irão já foi alvo de algum do mais avançado *malware* conhecido, incluindo o *Stuxnet* e o *Flame*, o que suscitou respostas na "mesma moeda" por parte de grupos não-Estatais, como os "*Izz ad-Din al-Qassam Cyber Fighters*" e o "*Iranian Cyber Army*", acreditando-se que o segundo está ligado ao exército Iraniano (Wheeler, 2013).

Nos últimos anos, o Irão tem desenvolvido esforços significativos relativamente às suas ciber-capacidades. Em 2011, anunciou que planeava estabelecer um "ciber-comando", primariamente defensivo, para as forças armadas, para se proteger de ciberataques e centralizando, deste modo, as suas operações. Um ano mais tarde, emitiu um decreto que estabelecia um Conselho Supremo do

Ciberespaço, onde estavam incluídos os diretores das agências de inteligência, a milícia, segurança, os media e os *Islamic Revolutionary Guard Corps* (esta unidade tem uma componente de *cyberwarfare* que foi considerada como um dos maiores ciber-exércitos do mundo), com o objetivo de coordenar o *cyberwarfare* nacional e a segurança da informação (UNIDIR, 2013).

Por sua vez, a Síria, em 2011, estabeleceu o Centro de Segurança de Informação como parte integrante da *National Agency for Network Services*. Este é constituído por um departamento de segurança de sistemas computacionais, por um departamento de segurança de rede, e por um *Computer Emergency Response Team* (CERT), tendo como objetivo desenvolver políticas e capacidades para combater cibercrimes e para detetar, analisar e controlar ciber-ameaças (UNIDIR, 2013).

O grupo de *hackers* Syrian Electronic Army (SEA), leal ao presidente Bashar al-Assad, é responsável por ciberataques a governos e media considerados críticos do regime, sendo nesse âmbito equacionado o possível envolvimento em ciberataques contra o auto proclamado Estado Islâmico, nomeadamente para recolha de informações que possam beneficiar o governo Iraniano e Sírio (EP, 2014).

O conceito estratégico militar Turco foi revisto em 2010, tendo nele sido incluídas as ciber-ameaças, consideradas uma prioridade. Neste contexto, foi assim equacionada a criação do *Cyber Army Command* para contra atacar ciberataques dirigidos ao Estado. Com este mesmo objetivo em mente, foi igualmente projetado o desenvolvimento de uma unidade especial, dentro do Estado-Maior, para lidar com ciber-ameaças numa relação de cooperação envolvendo o Ministério da Defesa, o Conselho de Pesquisa Científica e Tecnológica e, ainda, a Universidade Técnica do Médio Oriente. Esta unidade tem, também, como objetivos a monotorização de toda a *internet* na Turquia e a proteção de instituições do Estado (UNIDIR, 2013).

5. Península da Coreia

A Coreia do Sul é, atualmente, um dos países com maior índice de conectividade do mundo, e tem alegado ter vindo a ser alvo de ciberataques por parte da Coreia do Norte, com origem num ramo da milícia, o *Reconnaissance General Bureau*, de Pyongyang. Em 2010, de modo a aumentar a segurança das redes de informação do governo e financeiras, o Ministério de Defesa estabeleceu o Centro de Ciber-Guerra. Neste, foi também instituído um comando independente de *Cyber Warfare*, contando com a afetação de 200 pessoas, e que tem como missão conduzir operações defensivas e ofensivas no ciberespaço (EP, 2014). A Coreia do Sul pretende desenvolver armamento sofisticado de *cyber warfare* (ofensivo e defensivo), e aumentar o pessoal do Comando de *Cyber Warfare* para 1000 pessoas (Yonhap, 2012).

Suspeita-se que a Coreia do Norte tenha recorrido a ciberataques para "desmantelar" sistemas de rede, em particular da Coreia do Sul e dos EUA, e também para aceder a informação sensível ou confidencial. Estima-se, igualmente, que esta invista recursos significativos em capacidades ofensivas de *cyber warfare*, dispondo de um departamento com cerca de 3000 pessoas (EP, 2014). No entanto, devido à natureza isolacionista das relações do seu Estado há pouca informação disponível, e pouca precisão da mesma.

Após esta síntese sobre o *statu quo* de alguns dos Estados mais influentes no domínio do ciberespaço, é necessário perceber que a ciberdefesa e a cibersegurança representam áreas de responsabilidade para órgãos diferentes do Estado. Logicamente, ciberataques com um baixo impacto e risco social têm que ser considerados de forma distinta daqueles que, pelo contrário, possam ter implicações para a segurança e defesa do Estado, assim como para a sua soberania.

Assim sendo, o Estado é responsável por garantir tanto a segurança dos seus cidadãos no domínio do ciberespaço, como por salvaguardar a sua soberania.

No entanto, a cibersegurança do Estado enquadra-se numa perspectiva de supranacionalidade, numa cibersegurança global, cuja responsabilidade cai sobre atores internacionais (Balão, 2014). Dentro da esfera de ação do Estado, o cibercrime e o *hacktivismo* são da responsabilidade das Forças de Segurança, a ciberespionagem e o ciberterrorismo da responsabilidade dos Serviços de Informações da República, e a ciberguerra da responsabilidade das Forças Armadas (Nunes, 2012).

Segundo o professor Ami Pedahzur, existem 3 principais eixos ou domínios de intervenção na proteção e segurança do ciberespaço: o domínio da proteção simples; o domínio da prossecução criminal; e o domínio da defesa do Estado (Pedahzur, 2009).

*"O domínio de actuação da protecção simples engloba os meios técnicos, processuais e humanos que realizam diariamente as componentes preventivas, reactiva e de gestão da qualidade da segurança. É, pois, a primeira linha de protecção das infra-estruturas, dos serviços e da informação presentes no ciberespaço."* (Santos, Bravo e Nunes, 2012, p.4).

Neste domínio, a proteção do ciberespaço não é apenas responsabilidade do Estado, pois uma grande parte dos seus componentes é de privados. Desde os fabricantes de *hardware* e *software*, aos técnicos administradores dos sistemas e redes, aos próprios utilizadores (todos nós), são responsáveis pela sua segurança. Neste sentido, toda a indústria das TIC, é responsável pelas vulnerabilidades que os seus produtos apresentam na exploração de ciberataques, mas também tem de ser potenciadora do desenvolvimento de soluções de segurança, sendo que estas estão dependentes do investimento público e privado em recursos tecnológicos e humanos. Para este domínio contribui, de igual modo, o desenvolvimento de normas que possibilitem a utilização de um referencial de medida para a fiscalização e avaliação dos controlos de segurança. Como tal, a Comissão Europeia, através da ENISA, tem reforçado as medidas de regulação do setor das comunicações eletrónicas, e apostado na criação de CERTs nacionais nos Estados-membros (Balão, 2010). Estes CERT, são responsáveis pelas reações de alerta e resposta

em caso de incidentes de segurança informática, mas num contexto territorial. Sendo assim, há a necessidade de uma cooperação nacional e internacional no caso de um incidente de segurança informática que transcenda a esfera nacional. Para que esta seja otimizada, têm sido feitos esforços de homogeneização das políticas de tratamento de informação sensível, e de trocas de informação (Santos, Bravo e Nunes, 2012).

O domínio da prossecução criminal está diretamente relacionado com as leis aplicáveis por cada Estado. No caso de Portugal, a maior parte dos ciberataques é incluída nos atos ilícitos, puníveis à luz da legislação nacional (Lei do Cibercrime). Neste contexto, e devido à importância das infraestruturas críticas nacionais, qualquer ataque contra estas agrava consideravelmente as penas aplicáveis (DECRETO-LEI nº 109/2009).

Existe, no entanto, uma diferença entre os crimes praticados através do recurso às TIC, que são utilizados geralmente contra pessoas (por exemplo a pornografia de menores e crimes contra a honra), ou contra os interesses patrimoniais (como os crimes relacionados com os direitos de autor), e os crimes informáticos (como por exemplo o dano informático, a sabotagem informática, ou o acesso ilegítimo). O segundo tipo de crimes é o que vai ao encontro das potenciais ameaças às infraestruturas e dados críticos nacionais, como os dados da Banca ou do Registo e Notariado. A prevenção e investigação criminal de crimes informáticos é uma competência, atribuída por lei, à Polícia Judiciária (DECRETO-LEI nº 49/2008). Esta dispõe de uma unidade especializada para combater este tipo de crimes, a Unidade Nacional de Combate ao Cibercrime e a Cibercriminalidade Tecnológica (PJ, 2017).

Nos casos em que a informação obtida através do recurso a cibercrime comprometa a segurança interna, constitua um ato terrorista ou de espionagem, ou que, de alguma maneira, comprometa o Estado de Direito, a competência cai sobre o Serviço de Informações e Segurança (SIS) (DECRETO-LEI nº 50/2014).

Embora tenham competências diferentes, no caso de um eventual cibercrime de sabotagem ou espionagem direcionado a uma infraestrutura crítica,

*"qualquer entidade (Forças Armadas, SIS, Polícia Judiciária) tem o poder-dever de o comunicar ao Ministério Público, iniciando-se uma investigação criminal legalmente reforçada, uma vez que existe um dever geral de cooperação entre instituições do Estado e um dever especial de cooperação expresso nos diferentes estatutos das entidades referidas"*. No final do processo penal, os dados e a informação obtida sobre o processo devem "*reverter em nova informação, com destino à prevenção criminal e /ou "intelligence""* (Santos, Bravo e Nunes, 2012, p.8).

O domínio da Defesa do Estado, neste contexto, é enquadrado pela emergente Guerra de Informação e pelo impacto disruptivo que as ciberameaças representam. Como já foi referido anteriormente, os Estados e as Organizações Internacionais assumem o ciberespaço como um domínio operacional e, como tal, tem sido notório o desenvolvimento e criação de estruturas ou órgãos do Estado que têm como objetivos assegurar o correto funcionamento e proteção das comunicações e sistemas de informação, tendo-se tornado fundamentais no que diz respeito ao comando e controlo do campo de batalha moderno (Santos, Bravo e Nunes, 2012).

"*As Forças Armadas, à luz da Constituição da República Portuguesa, constituem o corpo social responsável pela defesa do Estado contra ameaças externas e devem assegurar, em situações de excepção (ex: estado de sítio), o regular funcionamento das instituições democráticas e o exercício das funções de soberania do Estado.*" (Santos, Bravo e Nunes, 2012, p.9). Devido ao carácter imprevisível e transversal das ciberameaças, sendo que é complicado determinar a sua origem e impacto, torna-se também necessário que as Forças Armadas assumam competências e desenvolvam as suas capacidades no domínio da ciberdefesa, particularmente no domínio da proteção das infraestruturas críticas (Santos, Bravo e Nunes, 2012).

As Forças Armadas, de modo a potenciar a ciberdefesa das infraestruturas críticas, têm que cooperar com outros agentes relevantes neste domínio. Se considerarmos o aumento tendencial das ciberameaças, tanto ao nível nacional

como internacional, é também necessário equacionar o desenvolvimento da capacidade e estratégia nacional de Ciberdefesa, em articulação com as capacidades das Forças Armadas, de modo a fazer frente a potenciais ataques que ponham em causa a soberania do Estado (ibidem).

Para completar a nossa perspetiva de cibersegurança e ciberdefesa, é importante perceber de que modo a ciberguerra ou o *cyber warfare*, é reconhecido ou não, como tal, pela lei internacional, e em caso afirmativo, em que situações.

Atualmente, a Lei Internacional tem dificuldades em estabelecer uma posição quanto à ciberguerra, tanto em relação ao *jus ad bellum* (ou seja às regras pelas quais os conflitos armados se regem e a legitimidade do uso da força por parte dos Estados), como ao *jus in bello* (a maneira como a guerra é feita, particularmente sobre questões do Direito Humanitário Internacional) (EP, 2014).

A este propósito, é importante destacar a existência de dois documentos legais de referência que têm vindo a regular os conflitos entre Estados, desde o fim da Segunda Guerra Mundial: a Carta das Nações Unidas, que está relacionada com o *jus ad bellum*, e a Convenção de Genebra, relacionada com o *jus in bello* (Nunes, 2016).

Se considerarmos um ciberataque que origine ferimentos, que cause a morte de pessoas, ou que cause danos ou destrua recursos, pode considerar-se que está em causa o uso da força. No entanto, há casos em que a situação não é tão clara. O Manual de Tallinn, desenvolvido na Estónia no CCD COE da NATO expôs, em 2013, uma sistematização da legislação internacional aplicada aos ciberconflitos, como constituindo a apresentação de um "*conjunto de princípios fundamentais do direito internacional associado ao ciberespaço*", tendo o mesmo vindo a ser considerado de extrema utilidade para a criação da legislação no seio de cada Estado (Nunes, 2016, p. 211).

As noventa e cinco (95) regras ou princípios apresentados pelo Manual de Tallinn definem, por exemplo, a responsabilidade dos Estados em relação às ciber-

operações, e também as circunstâncias em que se pode invocar a legítima defesa. Sobre o segundo ponto, uma ciber-operação pode, de facto, ser conduzida em resposta à alegação de legítima defesa, mas apenas se as condições identificarem o ataque como um ciberataque armado, ou seja, um ciberataque que tenha resultado em uso da força (EP, 2014). Assim, se uma ciber-operação resultar em sérios danos a infraestruturas críticas, ou serviços que sejam essenciais à soberania do Estado, é possível considerá-la como configurando um ciberataque armado, ou seja, um ataque armado no ciberespaço (Nunes, 2016). Este Manual também define oito (8) critérios para que seja possível identificar em que situações se pode considerar estarmos em presença do uso da força, sendo estes os seguintes: gravidade, imediatismo, direcionamento, capacidade invasiva, mensurabilidade dos efeitos produzidos, caráter militar, envolvimento do Estado, e presumível legalidade (NATO CCD COE, 2013).

Perante o tipo de situações em que podemos considerar invocar a legítima defesa de um Estado, e por consequência a retaliação por parte do mesmo, a preocupação que se segue é a atribuição da autoria e iniciativa da ciber-operação em causa a um determinado Estado, sendo que no domínio do ciberespaço tal se afigura cada vez mais difícil e complexo, além de que, sem essa identificação, fica posta em causa a possibilidade de constituição de um *casus belli*, ou seja, a declaração de guerra ao Estado ofensor derivada de um ato prévio suficientemente grave, perpetrado pelo mesmo (Nunes, 2016).

Se analisarmos o ciberataque sofrido em 2007 pela Estónia, por exemplo, e mesmo considerando a inegável capacidade disruptiva que este apresentou, não pode ser invocado o *casus belli* pois a identificação do seu perpetrador, apesar de ter sido atribuída à Rússia, não foi oficialmente assumida, de modo que apenas foram identificados atores não Estatais (ibidem). Este exemplo demonstra, a nosso ver, a dificuldade de um Estado em poder dar resposta legítima a um ciberataque, mesmo em situações suscetíveis de se aplicar o princípio da legítima defesa, para além de suscitar, ainda, uma maior dificuldade em invocar o artigo 5º do Tratado do Atlântico Norte, face à não existência de uma clara identificação do autor do ataque.

# Capítulo 3 – Estudo de Caso: Ataque cibernético à Geórgia

Após ter sido feita a contextualização e análise sobre o estado atual da ciberdefesa e cibersegurança, tanto em alguns Estados como nas principais Organizações Internacionais, neste capítulo procuramos debruçar-nos sobre um caso concreto em que se verificou a ocorrência de um ataque cibernético contra a Geórgia, em agosto de 2008.

Em 2007, como anteriormente nesta investigação já havíamos mencionado, a Estónia foi alvo de um ataque cibernético fruto do qual o Governo e os media nacionais foram "*hackeados"*, ação que afetou significativamente o seu desempenho. Uma parte do ataque consistiu em vandalismo de *websites* mas a outra parte, que foi responsável pela maior parte dos danos, foi um DDoS, que provocou a interrupção do serviço de *internet*, impossibilitando a utilização de *websites* do governo. Os ataques foram atribuídos à Rússia mas, devido à natureza dos ciberataques perpetrados naquela ocasião, não foi possível provar formalmente o envolvimento russo, nem o Estado Russo alguma vez admitiu estar envolvido nestes acontecimentos (Ashmore, 2009).

Embora seja inegável a capacidade disruptiva do ataque de "negação de serviço" à Estónia, este não pôde ser considerado como configurando uma situação de uso da força, devido às consequências não letais, ao facto de não ter incapacitado de forma grave infraestruturas críticas, ou mesmo pela "simples" razão de não se poder responsabilizar um Estado como o originador do ataque. Sendo assim, não é possível justificar a invocação do artigo 5º do Tratado do Atlântico Norte neste caso. No entanto, no caso de um acontecimento deste tipo reunir as condições previstas na lei (como anteriormente referido) para poder ser considerado como configurando um conflito armado no ciberespaço, a legislação internacional que rege os conflitos armados é suscetível de ser aplicada. Assim, procuraremos analisar, nesse contexto, aquele que é considerado o melhor exemplo de um conflito

armado no ciberespaço. De facto, a invasão da Geórgia em 2008 por parte das tropas Russas foi precedida e posteriormente articulada com operações no ciberespaço. No âmbito deste acontecimento, provocou-se a indisponibilidade de *websites* do governo, dos média e da área financeira, tendo estas ações sido associadas às operações militares, algo que não aconteceu na Estónia em 2007 (Nunes, 2016).

No decorrer deste capítulo iremos analisar os antecedentes que terão estado na origem do ataque contra a Geórgia em 2008, a descrição da situação e o desenrolar dos acontecimentos da intitulada "Guerra dos Cinco Dias".

## Antecedentes

A análise dos acontecimentos relacionados com a dimensão "ciber" do ataque à Geórgia parece assumir, sem dúvida, o aspeto mais importante deste acontecimento, tendo em consideração o objeto de estudo da presente dissertação de mestrado. Contudo, torna-se necessária uma breve contextualização que assegure o conhecimento da origem do conflito entre a Rússia e a Geórgia para que, posteriormente, se possa compreender o desenrolar dos acontecimentos.


Figura 6 - Mapa da Geórgia, com localização da Abkhazia e Ossétia do Sul

Fonte: (Wikipédia, 2008)

A região do Mar Negro tem sido decisiva para algumas das mudanças que a ordem internacional tem sofrido desde o passado século e meio, podendo invocar-se, a título de exemplo: o Cerco de Sebastopol em 1854-1855, onde britânicos, franceses e turcos se opuseram às tropas russas imperiais; os conflitos entre os impérios Alemão, Russo e Otomano na Primeira Guerra Mundial; a Segunda Guerra Mundial, com os conflitos entre os Aliados e o Eixo ou a partilha de zonas de influência no pós-guerra na Conferência de Yalta (Guedes, 2009).

Durante a Guerra Fria, esta região representava uma confluência de tensões entre o Pacto de Varsóvia (incluindo toda a costa Norte e Este Soviética, e ainda o litoral Oeste, representado pela Bulgária e Roménia) e a NATO (apenas representada pela Turquia). No entanto, com o fim deste período, deu-se uma inversão do domínio da região, ficando repartida por seis Estados. Três destes membros pertencentes à NATO (a Bulgária, a Roménia e a Turquia), outros dois candidatos para se juntarem a esta (a Geórgia e a Ucrânia) e, por fim, a Rússia, com uma linha de costa reduzida relativamente ao que outrora representava. Em 2008, o conflito na Geórgia assumiu uma relevância particular, precisamente quando equacionado em articulação com os interesses geopolíticos e geoestratégicos associados ao domínio da costa leste da região do Mar Negro, pondo na ribalta líderes como Mikheil Saakashvili, Vladimir Putin, George W. Bush e Nicolas Sarkozy (ibidem).

Assim, e se se quiser ficar com uma ideia sobre a cronologia de acontecimentos que precedeu o conflito de Agosto de 2008, considere-se a que a seguir se apresenta (CNN, 2016):

- Entre 1918 e 1921 a Geórgia é um Estado independente após libertar-se do império Russo;
- Em 1921, depois da invasão do Exército Vermelho, a Geórgia é declarada como uma República Socialista Soviética;
- A 9 de abril de 1991 a Geórgia declara a sua independência da União Soviética;

- Durante esse mesmo ano, a Ossétia do Sul declara a sua independência face à Geórgia, o que leva a conflitos na região, forçando milhares de pessoas a abandonar as suas casas;
- Entre 1991 e 1992 dá-se uma Guerra Civil na Geórgia, que termina com a destituição de Zviad Gamsakhurdia como presidente;
- Em 1992 a Abkhazia declara-se independente da Geórgia, originando conflito armado;
- Em outubro de 1992 Eduard Shevardnadze é eleito presidente georgiano (sendo depois reeleito em 1995 e 2000);
- Em setembro de 1993 as forças separatistas de Abkhazia derrotam as forças militares georgianas;
- Em outubro de 1993 a Geórgia junta-se à Comunidade dos Estados Independentes;
- Em maio de 1994 dá-se um acordo de cessar-fogo entre o governo georgiano e os separatistas de Abkhazia. Forças russas de p*eacekeeping* são enviadas para a região;
- Em outubro de 2001 volta a reacender-se o conflito entre a Geórgia e a Abkhazia, e a Rússia afirma que a Geórgia está a dar abrigo aos Rebeldes da Chechénia, algo que foi negado pelo Estado georgiano;
- Em setembro de 2002 o presidente russo Vladimir Putin envia uma carta ao presidente das NU, aos membros do Conselho de Segurança, e aos membros da OSCE (*Organization for Security and Cooperation in Europe*), afirmando que a Geórgia deve responder às acusações relativas aos rebeldes chechenos e que, caso não o fizesse, iria enfrentar ações militares russas;
- Em outubro de 2002 as tensões entre a Rússia e a Geórgia acalmam, depois da promessa do presidente georgiano no sentido de trabalhar em conjunto com a Rússia para combater os rebeldes chechenos;
- Em novembro de 2003 Eduard Shevardnadze é forçado a abandonar o seu cargo devido à “Revolução das Rosas” ou “Revolução Rosa” devido ao

estado instável e pobre, no qual deixou o povo georgiano, e às muitas acusações de corrupção que enfrentava (ADST, [s.d.]);

- Em julho de 2005, sob termos definidos em maio pelos Ministro dos Negócios Estrangeiros, Russo e Georgiano respetivamente, Sergei Lavrov e Salome Zourabichvili, a Rússia começa a evacuar as suas tropas de duas antigas bases militares da era soviética situadas na Geórgia (IRIS, 2005);
- Entre maio e junho de 2006 as tensões entre os Estados georgiano e russo crescem, após a Geórgia exigir visas aos *peacekeepers* russos da Ossétia do Sul;
- A 12 de novembro de 2006 tem lugar um referendo onde os cidadãos da Ossétia do Sul exigem a sua independência mas sem que, no entanto, o governo georgiano reconheça a validade do mesmo;
- Em novembro do ano seguinte a Rússia anuncia que retirou todas as suas tropas que estavam na Geórgia desde 1991, mantendo apenas presença de *peacekeeping* na Abkhazia e Ossétia do Sul;
- A 3 de abril de 2008, na cimeira de Bucareste, os membros da NATO adiam a decisão sobre a aceitação da Geórgia e Ucrânia como membros para dezembro do mesmo ano;
- A 21 de abril de 2008 a Geórgia acusa a Rússia de abater um UAV (*Unmanned Aerial Vehicle*) que sobrevoava a Abkhazia no dia anterior, alegações que o Estado Russo negou;
- A 29 de abril de 2008 a Rússia envia forças militares para a Abkhazia para contrariar aquilo que afirmavam ser os planos georgianos para um ataque a essa região;
- A 26 de maio de 2008 uma investigação das NU veio confirmar que o UAV foi, de facto, abatido por um míssil de um caça russo;

Entre 30 e 31 de maio de 2008, o Estado russo envia várias centenas de forças desarmadas para a Abkhazia, afirmando que estas eram necessárias para ajudar na reparação de caminhos-de-ferro. A Geórgia em resposta, acusa a Rússia de planear uma intervenção militar.

## Descrição e Análise da Situação

Na sequência dos acontecimentos anteriormente elencados por ordem cronológica a Guerra na Geórgia começou oficialmente do dia 7 de agosto de 2008, após semanas de sucessiva escalada nas tensões resultantes dos argumentos "esgrimidos" sobre o futuro da Ossétia do Sul, quando as forças militares georgianas iniciaram o ataque contra esta com o bombardeamento da cidade de Tskhinvali, em resposta a alegadas provocações russas. Na manhã de 8 de agosto a Rússia, em resposta, destacou forças adicionais para a Ossétia do Sul, e retaliou com bombardeamentos sobre território georgiano. Esta ainda destacou forças navais (bloqueando formalmente a Geórgia) que desembarcaram infantaria na costa da Abkhazia. As forças militares russas e sul ossetianas, mais mecanizadas e com armamento mais poderoso que as forças georgianas, foram decisivas no único campo de batalha (de grande escala) de operações de combate no solo: a batalha pela cidade de Tskhinvali. A 10 de agosto, a Rússia já tinha consolidado a sua posição da Ossétia do Sul, levando à retirada das forças georgianas (Friedman, 2008).

A derrota tática georgiana na batalha de Tskhinvali, a derrota operacional devido à invasão territorial russa incontestada na parte oeste da Geórgia, o bloqueio naval também incontestado, e por fim a dificuldade de contactar o resto do mundo através dos *media* (devido às ciber-operações que iremos analisar no decorrer deste capítulo), levou à derrota estratégica georgiana na guerra. Este conflito forçou aproximadamente vinte e cinco (25) mil residentes georgianos a abandonar as operações de combate terrestre como refugiados em deslocamento interno. As duas Nações (Rússia e Geórgia) assinaram um acordo de cessar-fogo uma semana mais tarde. No entanto, a Rússia falhou na implementação de alguns dos termos acordados, resultando numa maior perda de território georgiano para ocupação russa (Hollis, 2011).

Esta guerra não envolveu grandes quantidades de armamento, nem durou muito tempo quando comparada com outras, podendo parecer em primeira

instância só mais um conflito derivado da Guerra-Fria. No entanto, distingue-se como sendo o primeiro caso de articulação de um ataque no domínio do ciberespaço com as operações militares nos restantes domínios (terra, mar, ar e espaço). Sendo assim, a análise das operações conduzidas no ciberespaço torna-se bastante importante para o objeto de estudo em questão permitindo, nomeadamente, equacionar e discutir o aparecimento de um novo tipo guerra (ibidem).

Três semanas antes da guerra "física" entre a Geórgia e a Rússia, assistiu-se ao despoletar de uma série de ciberataques contra *websites* georgianos. Desde então que vários peritos e pesquisadores tentaram descobrir quem orquestrou esses ataques. Mesmo sem se poder afirmar de um modo definitivo quem agendou estes ataques, devido à falta de uma confissão ou provas irrefutáveis do envolvimento do governo russo, esses ataques foram atribuídos à Rússia, afirmando-se que é pouco plausível que as operações cibernéticas agendadas em paralelo com as cinéticas tenham sido apenas coincidência, sendo que o nível de informação que os *hackers* dispunham tinha de vir necessariamente do governo russo ou de uma alta patente militar (Shachtman, 2009).

O alegado ataque Russo contra as redes de comunicação governamentais e militares georgianas, foi extremamente bem-sucedido: conseguiu concretizar o ataque a 54 *websites* georgianos relacionados com comunicações, finanças e governo de tal modo que, enquanto se davam as invasões territoriais e os bombardeamentos, os cidadãos georgianos não conseguiam aceder a informação nem a possíveis instruções, ficando assim bastante debilitados, perante a rápida investida russa (Oltsik, 2009).

Esta guerra fica, também, marcada pela clara utilização de operações no ciberespaço como uma ferramenta para adquirir *intelligence*, ganhando uma clara vantagem estratégica, operacional e tática para as operações militares. Os alegados ataques russos no ciberespaço começaram ainda antes da grande investida cibernética que antecedeu a guerra, como se procurou demonstrar. A um nível estratégico, o ciberataque de reconhecimento russo começou a ser discutido

em *websites* e *chat rooms* várias semanas antes dos conflitos. Em julho foi efetivado um ataque DDoS, por *hackers* russos, ao *website* presidencial georgiano, algo que mais tarde foi discutido nas redes de *internet* russas no sentido de procurar compreender se este ataque DDoS ou outros ataques a *websites* deveriam estar a ser efetuados, pois poderiam ser utilizados mais tarde pela imprensa ocidental (Hollis, 2011).

Um investigador na área de segurança de Massachusetts, José Nazario, estava a observar um ciberataque contra a Geórgia, no início de julho, no âmbito do qual constatou um grande fluxo de *data* direcionado a *websites* governamentais georgianos que continham a mensagem "win+love+in+Rusia" (Nazario, 2009). Outros peritos dos EUA afirmaram que os ciberataques às infraestruturas críticas começaram a 20 de julho, pela utilização de ataques DDoS, que tinham como objetivo sobrecarregar e fazer mesmo o *shut down* dos servidores georgianos. Segundo peritos técnicos informáticos, estes ataques de julho terão sido um ensaio geral para a ciberguerra que iria acompanhar a invasão russa. Estes defendem, também, que foi a primeira vez que um ciberataque coincidiu com o conflito cinético, e que este tipo de preparação extensa implica um processo de planeamento que começou muito antes de julho de 2008 (Markoff, 2008).

Outro aspeto importante a considerar, e que torna mais evidente o envolvimento russo nos ciberataques contra a Geórgia, é a coordenação e precisão das operações no ciberespaço com os objetivos estratégicos do governo russo. A nível tático e operacional, localizações geográficas específicas foram definidas como alvo no domínio do ciberespaço, ainda antes das operações no domínio físico, e assim que as operações no solo tiveram início os ciberataques (previamente preparados) também foram lançados. A escolha dos alvos dos ciberataques é bastante esclarecedora, sobretudo considerando que *websites* oficiais de Gori e de notícias locais sofreram ataques DDoS, ficando incapacitados, mesmo antes dos aviões russos chegarem à cidade. Surge então a questão do investigador da SecureWorks (empresa dos EUA que atua como um sistema de alerta contra possíveis ciberameaças), Don Jackson: "como é que os *hackers* sabiam que as

forças militares Russas iam lançar bombas em Gori e não na capital?". Assim, Jackson afirma, ainda, que teve de haver um nível de coordenação ou direcionamento pelo governo russo, principalmente devido ao *timing* e à localização dos ataques (Menn, 2008).

Em face de tudo o que atrás já foi exposto, parecem não subsistir dúvidas quanto ao facto de a Rússia ter definido como foco dos seus ataques o governo georgiano. No domínio do ciberespaço, as operações conduzidas pela "ciber-milícia" russa conseguiram negar e degradar a habilidade governamental georgiana de comunicar, tanto internamente como com o mundo exterior. Devido a estas operações, aliadas às operações combinadas e conduzidas nos outros domínios físicos, a Rússia demonstrou que o governo da Geórgia não era capaz de defender o seu território soberano quer no domínio físico como no ciberespaço (Hollis, 2011). Parece ficar, assim, demonstrado que as operações conduzidas no ciberespaço são consideradas, de um modo legítimo, tão importantes como aquelas conduzidas nos restantes domínios, e que se encaixam perfeitamente como um meio e parte da estratégia para atingir objetivos geopolíticos.

## Lições sobre a Ciber-Campanha

Em face da análise até aqui efetuada, a primeira lição a retirar é a de que existe a necessidade de coordenar as operações do ciberespaço com as dos outros domínios, e para isso acontecer de um modo eficaz, o governo tem de conseguir transmitir os seus objetivos estratégicos e definir o centro de gravidade, ou o foco principal do ataque (ibidem). Também é importante frisar que será mais provável a utilização de um ataque combinado entre as forças convencionais militares em conjunto com *hackers* civis, pois deste modo é mais difícil estabelecer ligações, ou atribuir responsabilidades, a um Estado soberano. Deste modo, complica-se e dificulta-se a questão associada à legitimidade da invocação do artigo 5º do Tratado do Atlântico Norte, pois um dos critérios definidos no Manual de Tallinn para que possa ser reconhecido o uso da força é a efetiva identificação do envolvimento de um Estado.

A segunda lição a retirar é que existe a necessidade de identificar e desenvolver acessos, ou invasões, ilícitos aos alvos das operações do ciberespaço, antes de serem executadas as restantes operações militares. O planeamento dos ataques e toda a operação tem de ser assegurado de modo a poder testar e aumentar a sua eficácia. Esta situação pode ser favorável para o Estado que é tido como alvo, pois em ciber-conflitos futuros, os Estados precisam de desenvolver operações de treino, atividades de reconhecimento, e mesmo alguns ataques de menor dimensão, antes de começarem as operações reais, de modo a testar a sua eficácia potencial antecipando a real. Deste modo, existe a possibilidade de detetar este tipo de atividades, mesmo que estejam disfarçadas, e sendo assim é possível prever um futuro ataque ou uma futura guerra, permitindo uma preparação prévia e tomada de medidas defensivas (Shakarian, 2011).

A terceira lição é que esta ciber-campanha contra a Geórgia deverá ser vista como o verdadeiro teste à eficácia do uso de ciberataques coordenados com operações militares “tradicionais”. Como tal, existe uma urgência em desenvolver exercícios de resposta, no domínio do ciberespaço, por parte de cada Estado, envolvendo uma participação de todos os departamentos relevantes do governo, das forças militares e do setor privado, que seriam responsáveis por dar uma resposta numa situação real. Além disso, também é assumidamente importante a participação e coordenação com as Organizações Internacionais cujo auxílio, num possível cenário de ciberguerra, seja expectável (US CCU, 2009).

# Conclusão

A sociedade atual está profundamente dependente da tecnologia, verificando-se um crescimento muito acentuado das NTIC, do recurso e acesso à *internet* e mesmo da "*internet* das coisas". Tudo isto facilitou o nosso dia-a-dia mas veio dar origem a (potenciais) novas ameaças. O potencial nocivo destas é enorme, e como tal são reconhecidas nos conceitos estratégicos dos mais influentes Estados e Organizações Internacionais.

As infraestruturas críticas são os alvos com os quais há maior preocupação por parte dos Estados, pois ao sofrerem ciberataques vão ser afetados sistemas como o de distribuição de água, o de saúde, ou o de transportes, o que debilita fortemente o funcionamento da sociedade. Esta realidade acaba por transferir (quer direta, quer indiretamente) para as mãos dos peritos, técnicos ou *hackers*, mal-intencionados ou sob a agenda de algum Estado ou organização, um grande poder (real e ou potencial).

Sendo assim, têm sido desenvolvidas políticas e criados órgãos que buscam possibilitar um desenvolvimento e melhoria de cibersegurança e ciberdefesa. Podemos verificar, ainda, que as principais potências mundiais, a nível tecnológico, começam já a "militarizar" o ciberespaço, verificando-se também operações militares já conduzidas nesta dimensão.

Tanto a NATO como a UE estão a incentivar o desenvolvimento dos sistemas de ciberdefesa dos seus Estados Membros, e já se pode observar um esforço internacional, tanto no reconhecimento do ciberespaço como um domínio operacional equivalente em relevância e preocupação ao ar, terra, mar e espaço, como em buscar assegurar a defesa coletiva perante um ciberataque contra um Estado aliado.

No estudo de caso da invasão da Geórgia pela Rússia, foi possível verificar o potencial ofensivo decorrente do uso de ciber-operações articuladas e coordenadas com as restantes operações convencionais. Com a devida

preparação, e devido aos “treinos”, aos testes que, ao que tudo indica, terão tido lugar semanas antes do início da invasão, a eficácia dos ciberataques russos provou-se determinante para incapacitar o Estado georgiano de dar uma resposta adequada face à magnitude dos acontecimentos de agosto de 2008.

Deste modo, após o estudo efetuado ao longo dos três últimos capítulos, e perante a sua análise, considera-se estarem reunidas as condições necessárias para dar resposta à pergunta de partida e respetiva pergunta derivada, bem como para validar ou refutar as hipóteses inicialmente formuladas.

A pergunta de partida que conduziu toda a investigação cujos resultados aqui apresentamos é a seguinte:

***Pode um ciberataque dar origem a uma ciberguerra, considerando os quadros de referência legal e normativos de organizações como a NATO e UE?***

Conforme analisado no capítulo 2, um ciberataque pode ser considerado um ato de guerra, dando origem a uma ciberguerra. No entanto, tal verifica-se apenas se aquele for considerado um ciberataque armado, ou seja, se o ataque danificar as infraestruturas críticas de um Estado de tal modo que os sistemas essenciais para o funcionamento da sociedade deixem de estar operacionais, e por consequência, a soberania do Estado seja posta em causa, ou se o ciberataque for coordenado com operações militares conduzidas nos domínios operacionais convencionais, como foi o caso do ataque à Geórgia em 2008.

Outra questão que faz depender a origem de uma ciberguerra a partir de um ciberataque é a identificação do agente que o conduziu. Caso não se consiga identificar um ator estatal como o responsável pelo ciberataque, não é possível que se considere estar-se na presença de uma ciberguerra, nem mesmo pode ser invocada a legítima defesa. Esta identificação, devido à própria natureza dos ciberataques, é bastante complicada, pois mesmo que se consiga descobrir a origem geográfica do ataque, não é sinónimo de atribuição do mesmo a um Estado, e ainda que se identifiquem os indivíduos responsáveis pelo ataque também não prova o envolvimento de uma Organização ou entidade Estatal.

A Pergunta Derivada seguinte é respondida parcialmente pela resposta à pergunta de partida:

**Poderá, face a um ciberataque (ou a uma multiplicidade deles), ser invocado o artigo 5º do Tratado do Atlântico Norte?**

O artigo 5º do Tratado do Atlântico Norte pode ser invocado perante um ciberataque, ou uma multiplicidade deles, caso estejam reunidas as condições anteriormente descritas relativamente ao tipo de danos causados, ao acompanhamento de operações tradicionais em conjunto com o ciberataque, e à identificação do ator que é responsável pelo ataque. Contudo, a decisão sobre se é legítimo ou não ser invocado o artigo é da responsabilidade do Conselho do Atlântico Norte, numa avaliação caso-a-caso e cujo veredito é final.

Após ter sido dada a resposta à pergunta de partida e respetiva pergunta derivada, é necessário validar ou contestar as hipóteses de trabalho formuladas na decorrência das anteriores perguntas.

No que diz respeito à primeira hipótese, “O ciberespaço é atualmente reconhecido como uma dimensão potenciadora de ameaças nacionais e globais.”, as Organizações Internacionais e os Estados já reconhecem de uma forma clara, como ameaças, aquelas que se verificam no e decorrem do ambiente do ciberespaço, estando estas já contempladas nos documentos estratégicos e nos documentos das políticas de defesa, dos principais Estados e Organizações Internacionais, verificando-se deste modo a sua validação.

Para além disso, como podemos verificar no decorrer da investigação, a UE e os próprios Estados Membros, desenvolveram e continuam a investir em soluções de ciberdefesa e cibersegurança, desde a criação de órgãos ou divisões que foram criadas especificamente para lidar com este tipo de atividades, à organização de exercícios internacionais de preparação contra ciberataques. Assim, consideramos verificada, também, a veracidade da segunda hipótese de trabalho “Os documentos

estratégicos de defesa dos Estados Membros da UE e da própria Organização já contemplam soluções no âmbito da ciberdefesa e cibersegurança.".

O desenvolvimento de políticas relativas ao uso do ciberespaço (como é o caso, por exemplo, do Manual de Tallinn), juntamente com o desenvolvimento de equipas de resposta rápida a ciberataques da NATO (NCIRC) e da UE (CERT-EU) (que formularam um acordo para que partilhem entre si informações e as melhores práticas operacionais, de modo a melhorarem as suas capacidades), e ainda com o reconhecimento oficial do ciberespaço como um domínio de operações (na Cimeira de Varsóvia em 2016, referindo ainda a obrigação da defesa do ciberespaço como qualquer outro domínio de operações), vieram permitir uma maior proteção do ciberespaço e uma maior capacidade de prevenção e resposta a ciberataques. Deste modo, considera-se validada, também, a terceira hipótese de trabalho "Os Estados e as Organizações Internacionais como a UE e a NATO estão preparados para prevenir e dar resposta a ciberataques.".

A quarta hipótese de trabalho "Está prevista a invocação do artigo 5º do Tratado do Atlântico Norte, por parte de um dos Estados Membros da NATO, perante um (ou vários) ciberataque(s)." foi validada no decorrer da investigação para dar resposta às perguntas de partida e derivada. Como verificámos anteriormente, a invocação deste artigo está prevista, mas a sua legitimidade prende-se com a decisão do Conselho do Atlântico Norte, que é tomada numa análise "caso-a-caso". No entanto, como referimos anteriormente, esta tomada de decisão é influenciada por fatores como o tipo de danos resultantes dos ciberataques, se o ciberataque foi acompanhado de operações militares convencionais, ou ainda se foi possível identificar o Estado ou Organização que orquestrou o ataque e pelo qual é responsável.

Deste modo, verifica-se que o ciberespaço é um dos maiores desafios políticos, estratégicos, económicos, judiciais, sociais e militares da atualidade, e devido à expansão tecnológica e à propagação de dispositivos capacitados de aceder à *internet*, vai continuar a sê-lo em anos futuros.

Constatamos assim que as principais Organizações Internacionais das quais Portugal faz parte, e também o Estado português, estão atualmente não só a desenvolver as suas capacidades de ciberdefesa e cibersegurança, como também políticas e estratégias que permitam uma maior capacidade de resposta a esta ameaça atual que tem um potencial tão nefasto.

A criação de equipas de resposta rápida contra incidentes no âmbito do ciberespaço é bastante importante, mas mais ainda é a sua cooperação entre equipas de diferentes organizações, potenciando deste modo o desenvolvimento de técnicas e medidas de prevenção e resposta a ciberataques.

Neste sentido, destacamos também a importância da cooperação entre Estados e entre Organizações Internacionais, facultando informações relevantes sobre incidentes e ciberataques, mesmo expondo possivelmente falhas inerentes aos seus sistemas de informação, mas que no futuro possibilitem o desenvolvimento de sistemas que não apresentem estas mesmas falhas.

Em suma, a reposta contra as ciberameaças reside na prevenção, cooperação e partilha de informação, no desenvolvimento e investimento em capacidades de ciberdefesa, e ainda na educação e divulgação de medidas de cibersegurança, para que seja possível combater um dos maiores desafios do século XXI.

## Sugestões

Para além do exposto anteriormente, é ainda importante referir que a presente investigação não é um documento imutável nem dá resposta a todas as questões e desafios inerentes ao domínio do ciberespaço. Devido à acelerada expansão das NTIC na atual vivência da sociedade, e também do reconhecimento e posterior aproveitamento do ciberespaço como domínio operacional, consideramos essencial a manutenção de um olhar crítico e analítico sobre esta temática.

Deste modo, consideramos que é necessária uma análise contínua sobre o ciberespaço como dimensão de segurança, que faculte novas reflexões e perspetivas, expondo também possíveis soluções estratégicas e políticas, sobre esta temática e os desafios que apresenta.

Sendo assim, apresentamos em seguida um vetor de análise que consideramos pertinente e desafiante, sugerindo então a sua consideração como uma possível futura investigação:

- As *Rules of Engagement* (RoE) aplicáveis no domínio do ciberespaço, caso estejam estabelecidas, e a extensão da sua aplicabilidade.

Através da investigação científica deste vetor, acreditamos que será adicionado um contributo para o aumento do conhecimento sobre a visão do ciberespaço numa perspetiva de segurança e defesa. Algo que se pode revelar importante em conflitos futuros, possibilitando uma maior preparação sobre toda uma multiplicidade de questões políticas e legais que possam surgir derivadas do domínio de operações do ciberespaço, traduzindo-se desta forma num benefício para a comunidade internacional e para a humanidade em geral.

# Referências Bibliográficas


ADST - **Georgia's Rose Revolution** [Em linha] [Consult. 16 mar. 2017]. Disponível em WWW:<URL:http://www.huffingtonpost.com/adst/georgias-rose-revolution_b_8638118.html>.

ALMADA, Tulio - **Governo norte-americano prevê gastos de US$ 19 bi com segurança digital** [Em linha], 2016. [Consult. 15 mar. 2017]. Disponível em WWW:<URL:http://br.blastingnews.com/mundo/2016/02/governo-norte-americano-preve-gastos-de-us-19-bi-com-seguranca-digital-00779785.html>.

ANSSI - **Information systems defence and security France's strategy** [Em linha], Paris : ANSSI, 2011. [Consult. 20 fev. 2017]. Disponível em WWW:<URL:http://www.ssi.gouv.fr/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf>.

APDSI - **Glossário da sociedade da informação** [Em linha], Caparica : APDSI, 2007. [Consult. 22 fev. 2017]. Disponível em WWW:<URL:http://www.apdsi.pt/uploads/news/id138/glossário da si - versão 2007_9040-02.pdf>.

ASHMORE, William C. - **Impact of Alleged Russian Cyber Attacks** [Em linha], Kansas : SAMS USACGSC, 2009. [Consult. 15 fev. 2017]. Disponível em WWW:<URL:http://www.bdcol.ee/files/files/documents/Research/BSDR2009/1_ Ashmore - Impact of Alleged Russian Cyber Attacks .pdf>.

BALÃO, Sandra - Geopolítica e Geoestratégia do Ciberespaço: Para Uma Estratégia Da Informação Nacional. **Proelium**. Lisboa. Julho (2010) 1–20.

BALÃO, Sandra - Enisa e a Estratégia Europeia de Cibersegurança: Fundamentos supranacionais de uma Estratégia Nacional de (Ciber)Segurança de Informações. Em LARA, António S., coord. **Crise, Estado e Segurança**. Lisboa : MGI (Portugal), 2014. ISBN 978-989-97668-6-0. p. 127–167.

BALÃO, Sandra - Globalização. Em MENDES, Nuno C.; COUTINHO,

Francisco P., coord. **Enciclopédia das Relações Internacionais**. 1ª ed. Alfragide : Dom Quixote, 2014. ISBN 978-972-20-5505-5. p. 227–229.

BARRINHA, André; CARRAPIÇO, Helena - Cibersegurança. Em DUQUE, Raquel; NOIVO, Diogo; SILVA, Teresa A., coord. **Segurança Contemporânea**. 1ª ed. Lisboa : PACTOR, 2016. ISBN 978-989-693-054-7. p. 245–262.

BENDIEK, Annegret - **European Cyber Security Policy** [Em linha], Berlim : SWP, 2012. [Consult. 10 fev. 2017]. Disponível em WWW:<URL:https://www.swp-berlin.org/fileadmin/contents/products/research_papers/2012_RP13_bdk.pdf>.

BROWN, Chris; AINLEY, Kirsten - **Compreender as Relações Internacionais**. 1ª ed. Lisboa : Gravida Publicações, 2012. ISBN 978-989-616-465-2.

BRYANT, Rebecca - **What kind of space is cyberspace?** [Em linha], [s.l.] : Minerva, 2001. [Consult. 2 fev. 2017]. Disponível em WWW:<URL:http://www.minerva.mic.ul.ie/vol5/cyberspace.html>.

BRYANT, William D. - **International Conflict and Cyberspace Superiority: Theory and practice**. Nova Iorque : Routledge, 2016. ISBN 978-1138918917.

BURCHILL, Scott - Liberalism. Em **Theories of International Relations**. 4ª ed. Londres : Palgrave Macmillan, 2009. ISBN 978-0-230-21923-6. p. 57–85.

BURCHILL, Scott; LINKLATER, Andrew - Introduction. Em **Theories of International Relations**. 4ª ed. Londres : Palgrave Macmillan, 2009. ISBN 978-0-230-21923-6. p. 1–30.

CASTELLS, Manuel - **A Sociedade em Rede**. São Paulo : Editora Paz e Terra, 1999. ISBN 85-219-0329-4.

CNN - **2008 Georgia Russia Conflict Fast Facts** [Em linha], 2016. [Consult. 5 mar. 2017]. Disponível em WWW:<URL:http://edition.cnn.com/2014/03/13/world/europe/2008-georgia-russia-conflict/>.

COUTINHO, Luís Pereira - Teoria das Relações Internacionais. Em MENDES, Nuno C.; COUTINHO, Francisco P. coord. **Enciclopédia das Relações Internacionais**. 1ª ed. Alfragide : Dom Quixote, 2014. ISBN 978-972-20-5505-5. p. 506–508.

COUTO, Abel - **Elementos de Estratégia, Apontamentos para um Curso**. 1ª ed. Lisboa : IAEM, 1988

CP - **O que é um ataque de fragmentação** [Em linha] [Consult. 17 mar. 2017]. Disponível em WWW:<URL:http://ptcomputador.com/Networking/internet-networking/67808.html>.

DECRETO-LEI nº 49/2008. "D.R. I Série". 165 (2008-08-27) 6038-6042.

DECRETO-LEI nº 109/2009. "D.R. I Série". 179 (2009-09-15) 6319-6325.

DECRETO-LEI nº 50/2014. "D.R. I Série". 155 (2014-08-13) 4206-4221.

DELTICA; OCSIA - **The cost of Cyber Crime** [Em linha], Guildford : Deltica, 2011. [Consult. 2 mar. 2017]. Disponível em WWW:<URL:https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60942/THE-COST-OF-CYBER-CRIME-SUMMARY-FINAL.pdf>.

DIAS, Mónica; SAMÕES, Orlando - Liberalismo e Institucionalismo Liberal. Em DUQUE, Raquel; NOIVO, Diogo; SILVA, Teresa A., coord. **Segurança Contemporânea**. 1ª ed. Lisboa : PACTOR, 2016. ISBN 978-989-693-054-7. p. 23–39.

DIGITAL ATTACK MAP - **Digital Attack Map** [Em linha], 2017. [Consult. 17 mar. 2017]. Disponível em WWW:<URL:http://www.digitalattackmap.com/#anim=1&color=0&country=ALL&list=2&time=17241&view=map>.

DONNELLY, Jack - Realism. Em **Theories of International Relations**. 4ª ed. Londres : Palgrave Macmillan, 2009. ISBN 978-0-230-21923-6. p. 31–56.

DOUGHERTY, James E.; PFALTZGRAFT JR., Robert L. - **Relações**

**Internacionais: As Teorias em Confronto**. Lisboa : Gravida, 2003. ISBN 978-972-662-934-4.

DVORIN, Tova - **Israel Launches National Cyber-Defense Authority** [Em linha], 2014. [Consult. 23 fev. 2017]. Disponível em WWW:<URL:http://www.israelnationalnews.com/News/News.aspx/185349#.VEUT_W3DVgg>.

EC - **A strategy for a Secure Information Society – «dialogue, partnership and empowerment»** [Em linha], Bruxelas : EC, 2006. [Consult. 23 jan. 2017]. Disponível em WWW:<URL:ec.europa.eu/information_society/doc/com2006251.pdf>.

EC - **Report on the Implementation of the European Security Strategy–Providing Security in a Changing World** [Em linha], Bruxelas : EC, 2008. [Consult. 14 dez. 2016]. Disponível em WWW:<URL:http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Report+on+the+Implementation+of+the+European+Security+Strategy+-+Providing+Security+in+a+Changing+World#0%5Cnhttp://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Report+on+the+Implemen>.

EC - **Critical Infrastructure** [Em linha], 2012. [Consult. 12 jan. 2017]. Disponível em WWW:<URL:https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure_en>.

EC - **Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace** [Em linha], Bruxelas : EC, 2013. [Consult. 5 jan. 2017]. Disponível em WWW:<URL:http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf>.

EC - **Comissão assina um acordo com a indústria sobre cibersegurança e intensifica os esforços para combater as ciberameaças** [Em linha], 2016. [Consult. 7 jan. 2017]. Disponível em WWW:<URL:http://ec.europa.eu/regional_policy/pt/newsroom/news/2016/07/07-05-2016-commission-signs-agreement-with-industry-on-cybersecurity-and-steps-

up-efforts-to-tackle-cyber-threats>.

EC - **Directive on Security of Network and Information Systems** [Em linha], 2016. [Consult. 26 fev. 2017]. Disponível em WWW:<URL:http://europa.eu/rapid/press-release_MEMO-16-2422_en.htm>.

EDA - **EDA Study Identifies Cooperation Prospects in Cyber Defence** [Em linha], 2013. [Consult. 27 fev. 2017]. Disponível em WWW:<URL:https://www.eda.europa.eu/info-hub/press-centre/latest-news/2013/05/24/eda-study-identifies-cooperation-prospects-in-cyber-defence>.

ENISA - **About ENISA** [Em linha], 2017. [Consult. 27 fev. 2017]. Disponível em WWW:<URL:https://www.enisa.europa.eu/about-enisa>.

EP - **Cyber defence in the EU Preparing for cyber warfare?** [Em linha], [s.l.] : EP, 2014. [Consult. 17 fev. 2016]. Disponível em WWW:<URL:http://www.europarl.europa.eu/EPRS/EPRS-Briefing-542143-Cyber-defence-in-the-EU-FINAL.pdf>.

ESCRAVANA, Nelson; LIMA, João; RIBEIRO, Carlos - **Ciber(in)segurança da Infraestrutura de Transportes Públicos** [Em linha], Lisboa : IDN, 2012. [Consult. 15 dez. 2016]. Disponível em WWW:<URL:http://www.idn.gov.pt/publicacoes/nacaodefesa/textointegral/NeD133.pdf>.nunes

EU - **European Security Strategy: A secure Europe in a better world (2003)** [Em linha], Bruxelas : EU, 2003. Disponível em WWW:<URL:http://www.consilium.europa.eu/uedocs/cmsUpload/78367.pdf>.

EU COUNCIL - **A Secure Europe in a Better World** [Em linha], Bruxelas : EU Council, 2008. [Consult. 17 fev. 2017]. Disponível em WWW:<URL:http://www.consilium.europa.eu/en/documents-publications/publications/2009/pdf/european-security-strategy-secure-europe-better-world/>.

EU COUNCIL - **EU CYBER DEFENCE POLICY FRAMEWORK** [Em linha],

Bruxelas : EU Council, 2014. [Consult. 4 jan. 2017]. Disponível em WWW:<URL:http://www.europarl.europa.eu/meetdocs/2014_2019/documents/sede/dv/sede160315eucyberdefencepolicyframework_/sede160315eucyberdefencepolicyframework_en.pdf>.

EUROPOL - **EUROPEAN CYBERCRIME CENTER - EC3** [Em linha], 2017. [Consult. 27 fev. 2017]. Disponível em WWW:<URL:https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3>.

EUROSTAT - **Estatísticas sobre a sociedade da informação - agregados familiares e indivíduos** [Em linha], 2016. [Consult. 5 jan. 2017]. Disponível em WWW:<URL:http://ec.europa.eu/eurostat/statistics-explained/index.php/Information_society_statistics_-_households_and_individuals/pt#Acesso_.C3.A0_Internet>.

FAP - **Relatorio de Gestao FAP** [Em linha], [s.l.] : FAP, 2015. [Consult. 3 fev. 2017]. Disponível em WWW:<URL:https://www.emfa.pt/www/conteudos/galeria/info-fap/relatorio-gestao-2015_1684.pdf>.

FCRA - **Austrian Cyber Security Strategy** [Em linha], Viena : BMI, 2013. [Consult. 11 mar. 2017]. Disponível em WWW:<URL:http://www.bmi.gv.at/cms/BMI_Service/cycer_security/130415_strategie_cybersicherheit_en_web.pdf>.

FERNANDES, José - **Utopia, Liberdade e Soberania no Ciberespaço** [Em linha], 2012. [Consult. 16 dez. 2016]. Disponível em WWW:<URL:http://www.idn.gov.pt/publicacoes/nacaodefesa/textointegral/NeD133.pdf>.

FERREIRA, Marcos Farias - Construtivismo. Em MENDES, Nuno C.; COUTINHO, Francisco P., coord. **Enciclopédia das Relações Internacionais**. 1ª ed. Alfragide : Dom Quixote, 2014. ISBN 978-972-20-5505-5. p. 111–113.

FERREIRA, Maria João - Idealismo Liberal. Em MENDES, Nuno C.;

COUTINHO, Francisco P. coord. **Enciclopédia das Relações Internacionais**. 1ª ed. Alfragide : Dom Quixote, 2014. ISBN 978-972-20-5505-5. p. 253–255.

FRIEDMAN, George - **The Russo-Georgian War and the Balance of Power** [Em linha], 2008. [Consult. 6 mar. 2017]. Disponível em WWW:<URL:https://www.stratfor.com/weekly/russo-georgian-war-and-balance-power>.

GEERS, Kenneth *et al.* - **World War C: Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks** [Em linha], California : FireEye, 2015. [Consult. 4 mar. 2017]. Disponível em WWW:<URL:https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/fireeye-wwc-report.pdf>.

GH - **National Cyber Security Strategy** [Em linha], [s.l.] : [s.n.], 2013. [Consult. 1 mar. 2017]. Disponível em WWW:<URL:https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/HU_NCSS.pdf>.

GIBSON, William - **Neuromancer**. 1ª ed. Nova Iorque : Ace, 1984. ISBN 978-0441569595.

GODWIN III, James B. *et al.* - **Critical Terminology Critical Terminology Foundations 2** [Em linha], Nova Iorque : EWI, 2014. [Consult. 25 fev. 2017]. Disponível em WWW:<URL:https://www.files.ethz.ch/isn/178418/terminology2.pdf>.

GREENHOUGH, John - **How the «Internet of Things» will impact consumers, businesses, and governments in 2016 and beyond** [Em linha], 2016. [Consult. 13 fev. 2017]. Disponível em WWW:<URL:http://www.businessinsider.com/how-the-internet-of-things-market-will-grow-2014-10>.

GUEDES, Armando Marques - **A Guerra dos Cinco Dias**. Lisboa : IESM, 2009. ISBN 978-989-652-043-4.

HADDICK, Robert - **This Week at War: Lessons from Cyberwar I: How Russia pioneered the use of cyberattacks as military tactic** [Em linha], 2011. [Consult. 23 fev. 2017]. Disponível em WWW:<URL:http://foreignpolicy.com/2011/01/28/this-week-at-war-lessons-from-cyberwar-i/>.

HARDING, Luke - **What we know about Russia's interference in the US election** [Em linha], 2016. [Consult. 9 jan. 2017]. Disponível em WWW:<URL:https://www.theguardian.com/us-news/2016/dec/16/qa-russian-hackers-vladimir-putin-donald-trump-us-presidential-election>.

HEALEY, Jason - **A Fierce Domain: Conflict in Cyberspace, 1986 to 2012**. Ashburn : Cyber Conflict Studies Association, 2013. ISBN 098932740X.

HICKIE, Scott - **Trends in remote-control warfare** [Em linha], Londres : Open Briefing, 2014. [Consult. 12 fev. 2017]. Disponível em WWW:<URL:https://www.openbriefing.org/docs/Trends-in-remote-control-warfare-March-September-2014.pdf>.

HINTZ, Arne - **Beyond Wikileaks: Implications for the Future of Communications, Journalism and Society**. Londres : Palgrave Macmillan, 2013. ISBN 978-1137275738.

HOLLIS, David - **Cyberwar Case Study: Georgia 2008** [Em linha], [s.l.] : Small Wars Journal, 2011. [Consult. 1 mar. 2017]. Disponível em WWW:<URL:http://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf>.

IDN - **Estratégia da informação e segurança no ciberespaço** [Em linha], Lisboa : IDN, 2013. [Consult. 23 fev. 2017]. Disponível em WWW:<URL:http://www.idn.gov.pt/publicacoes/cadernos/idncaderno_12.pdf>.

INTERNET WORLD STATS - **Internet in Europe Stats** [Em linha], 2016. [Consult. 12 fev. 2017]. Disponível em WWW:<URL:http://www.internetworldstats.com/stats.htm>.

INTERNET WORLD STATS - **Internet Usage Statistics: The Internet Big**

**Picture** [Em linha], 2017. [Consult. 27 mar. 2017]. Disponível em WWW:<URL:http://www.internetworldstats.com/stats.htm>.

IRIS - **Georgia's Russian Hurdles: Negotiating Russian Troops Withdrawal from Georgia** [Em linha], Sófia : IRIS, 2005. [Consult. 2 mar. 2017]. Disponível em WWW:<URL:http://www.iris-bg.org/fls/Georgia.pdf>.

JOHNSTON, David - **9/11 Congressional Report Faults FBI-CIA Lapses** [Em linha], 2003. [Consult. 18 fev. 2017]. Disponível em WWW:<URL:http://www.nytimes.com/2003/07/24/us/9-11-congressional-report-faults-fbi-cia-lapses.html>.

KAN, Shirley A. - **U. S. -China Military Contacts: Issues for Congress** [Em linha], [s.l.] : CRS, 2009. [Consult. 24 fev. 2017]. Disponível em WWW:<URL:http://books.google.com/books?hl=en&lr=&id=4MGrQ76EsKsC&pgis=1>.

KITCHIN, R. - **Cyberspace: The World in the Wires**. 1ª ed. Nova Jersey : John Wiley & Sons, 1998. ISBN 978-0471978626.

KOBIE, Nicole - **What is the internet of things?** [Em linha], 2015. Disponível em WWW:<URL:https://www.theguardian.com/technology/2015/may/06/what-is-the-internet-of-things-google>.

KOWALSKI, Mateus - Ameaça. Em MENDES, Nuno C.; COUTINHO, Francisco P., coord. **Enciclopédia das Relações Internacionais**. 1ª ed. Alfragide : Dom Quixote, 2014. ISBN 978-972-20-5505-5. p. 23–25.

LAKATOS, Eva M.; MARCONI, Marina A. - **Metodologia do Trabalho Científico**. 4ª ed. São Paulo : Atlas, 1994. ISBN 978-8522448784.

LIN, Herbert S.; GOODMAN, Seymour E. - **Toward a safer and more secure cyberspace**. Washington, D.C. : National Academies Press, 2007. ISBN 9780309103954.

LOHR, Steve - **Stepping Up Security for an Internet-of-Things World** [Em

linha], 2016. [Consult. 10 fev. 2016]. Disponível em WWW:<URL:https://www.nytimes.com/2016/10/17/technology/security-internet.html?_r=0>.

MARKOFF, John - **Before the Gunfire, Cyberattacks** [Em linha], 2008. [Consult. 6 mar. 2017]. Disponível em WWW:<URL:http://www.nytimes.com/2008/08/13/technology/13cyber.html>.

MARTINS, Marco - **Ciberespaço: uma Nova Realidade para a Segurança Internacional** [Em linha], Lisboa : IDN, 2012. [Consult. 21 dez. 2016]. Disponível em WWW:<URL:http://www.idn.gov.pt/publicacoes/nacaodefesa/textointegral/NeD133.pdf>.

MAURER, Tim - **Cyber norm emergence at the United Nations** [Em linha], Massachusetts : HKS, 2011. [Consult. 18 jan. 2017]. Disponível em WWW:<URL:http://belfercenter.hks.harvard.edu/files/maurer-cyber-norm-dp-2011-11-final.pdf>.

MAURER, Tim; MORGUS, Robert - **Compilation of Existing Cybersecurity and Information Security Related Definitions** [Em linha], [s.l.] : New America, 2014. [Consult. 21 fev. 2017]. Disponível em WWW:<URL:https://giplatform.org/sites/default/files/Compilation of Existing Cybersecurity and Information Security Related Definition.pdf>.

MCGREW, Anthony - Globalization and Global Politics. Em BAYLIS, John; SMITH, Steve; OWENS, Patricia, coord. **The Globalization of World Politics**. 5ª ed. Nova Iorque : Oxford University Press, 2011. ISBN 978-0199569090. p. 14–31.

MCOWAN, Peter; MCCALLUM, Louis - **When fridges attack: the new ethics of the Internet of Things** [Em linha], 2014. [Consult. 10 fev. 2016]. Disponível em WWW:<URL:https://www.theguardian.com/science/alexs-adventures-in-numberland/2014/sep/08/when-fridges-attack-the-new-ethics-of-the-internet-of-things>.

MDN - **Conceito Estratégico de Defesa Nacional** [Em linha], [s.l.] : MDN,

2013. [Consult. 15 nov. 2016]. Disponível em WWW:<URL:http://www.idn.gov.pt/conteudos/documentos/CEDN_2013.pdf>.

MENN, Joseph - **Expert: Cyber-attacks on Georgia websites tied to mob, Russian government** [Em linha], 2008. [Consult. 7 mar. 2017]. Disponível em WWW:<URL:http://latimesblogs.latimes.com/technology/2008/08/experts-debate.html>.

MILITÃO, Otávio - **Guerra da Informação: a cibersegurança, a ciberdefesa e os novos desafios colocados ao sistema internacional**, Lisboa : FCSH, 2014. [Consult. 7 jan. 2017]. Disponível em WWW:<URL: https://run.unl.pt/bitstream/10362/14300/1/Dissertacao_OMilitao_35664.pdf>.

MNE - **UNGA Resolution 70/237 on «Developments in the field of information and telecommunications in the context of international security»** [Em linha], Portugal : MNE, 2016. [Consult. 5 jan. 2017]. Disponível em WWW:<URL:https://unoda-web.s3-accelerate.amazonaws.com/wp-content/uploads/2016/10/Portugal.pdf>.

MOREIRA, Adriano - **Teoria das Relações Internacionais**. 8ª ed. Coimbra : Almedina, 2014. ISBN 978-972-40-5551-0.

MPSC - **Canada' s Cyber Security Strategy** [Em linha], Canadá : MPSC, 2010. [Consult. 8 mar. 2017]. Disponível em WWW:<URL:https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf>.

MS RISK - **China's Offensive Cyber Warfare** [Em linha], 2016. [Consult. 22 fev. 2017]. Disponível em WWW:<URL:http://www.msrisk.com/china/chinas-offensive-cyber-warfare/>.

MYBROADBAND - **What the world looks like in 2G, 3G, and 4G** [Em linha], 2016. [Consult. 20 fev. 2017]. Disponível em WWW:<URL:https://mybroadband.co.za/news/internet/172964-what-the-world-looks-like-in-2g-3g-and-4g.html>.

NATO - **The North Atlantic Treaty ( 1949 )** [Em linha], Washington D.C. : NATO, 1949. [Consult. 6 jan. 2017]. Disponível em WWW:<URL:http://www.nato.int/nato_static/assets/pdf/stock_publications/20120822_nato_treaty_en_light_2009.pdf>.

NATO - **Active Engagement , Modern Defence: Strategic Concept for the Defence and Security of the Members of the North Atlantic Treay Orgnisation** [Em linha], Bruxelas : NATO, 2010. [Consult. 24 jan. 2017]. Disponível em WWW:<URL:http://www.nato.int/strategic-concept/pdf/Strat_Concept_web_en.pdf>.

NATO - **Chicago Summit Declaration** [Em linha], 2012. [Consult. 15 mar. 2017]. Disponível em WWW:<URL:http://www.nato.int/cps/en/natohq/official_texts_87593.htm?selectedLocale=en>.

NATO - **Wales Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales , 05-Sep.-2014** [Em linha], 2014. [Consult. 25 fev. 2017]. Disponível em WWW:<URL:http://www.nato.int/cps/en/natohq/official_texts_112964.htm>.

NATO - **NATO and the European Union enhance cyber defence cooperation** [Em linha], 2016. [Consult. 15 mar. 2017]. Disponível em WWW:<URL:http://www.nato.int/cps/en/natohq/news_127836.htm>.

NATO - **Cyber defence** [Em linha], 2017. [Consult. 26 fev. 2017]. Disponível em WWW:<URL:http://www.nato.int/cps/en/natohq/topics_78170.htm?>.

NATO CCD COE - **About Cyber Defence Center** [Em linha] [Consult. 24 fev. 2017]. Disponível em WWW:<URL:https://ccdcoe.org/about-us.html>.

NATO CCD COE - **Tallinn manual on the international law applicable to cyber warfare: prepared by the international group of experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence** [Em linha], Cambridge : Cambridge University Press, 2013. [Consult. 4 fev. 2017]. Disponível em WWW:<URL:http://csef.ru/media/articles/3990/3990.pdf>.

NATO ML - **NATO LibGuides: Cyber Defence: Home** [Em linha], 2017. [Consult. 26 fev. 2017]. Disponível em WWW:<URL:http://www.natolibguides.info/cybersecurity>.

NATO PA - **73 DSCFC 09 E BIS - NATO AND CYBER DEFENCE** [Em linha] [Consult. 17 fev. 2017]. Disponível em WWW:<URL:http://www.nato-pa.int/default.asp?SHORTCUT=1782>.

NAZARIO, Jose - **Politically motivated denial of service attacks** [Em linha], EUA : Arbor Networks, 2009. [Consult. 26 fev. 2017]. Disponível em WWW:<URL:https://ccdcoe.org/sites/default/files/multimedia/pdf/12_NAZARIO Politically Motivated DDoS.pdf>.

NUNES, Paulo Viegas - Impacto das Ciberameaças na Segurança e Defesa: da Ciberdefesa ao Levantamento da Estratégia da Informação Nacional. **Estratégia**. Lisboa. XX: (2011) 360–388.

NUNES, Paulo Viegas - **A Definição de uma Estratégia Nacional de Cibersegurança** [Em linha], Lisboa : IDN, 2012. [Consult. 15 dez. 2016]. Disponível em WWW:<URL:http://www.idn.gov.pt/publicacoes/nacaodefesa/textointegral/NeD133.pdf>.

NUNES, Paulo Viegas - **Sociedade em Rede, Ciberespaço e Guerra de Informação: Contributos para o Enquadramento e Construção de uma Estratégia Nacional da Informação**. Lisboa : IDN, 2015. ISBN 978-972-9393-34-1.

NUNES, Paulo Viegas - Ciberameaças e Quadro Legal dos Conflitos no Ciberespaço. Em BORGES, João V.; RODRIGUES, Teresa F., coord. **Ameaças e Riscos Transnacionais no novo Mundo Global**. 1ª ed. Porto : Fronteira do Caos, 2016. ISBN 978-989-8647-60-3.

OLTSIK, Jon - **Russia Cyber Attack on Georgia: Lessons Learned?** [Em linha], 2009. [Consult. 6 mar. 2017]. Disponível em WWW:<URL:http://www.networkworld.com/article/2236816/cisco-subnet/russian-

cyber-attack-on-georgia---lessons-learned-.html>.

OSCE - **Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace** [Em linha], Viena : OSCE, 2013. [Consult. 19 fev. 2017]. Disponível em WWW:<URL:http://www.osce.org/atu/103500?download=true>.

OXFORD II - **Information Geographies: at the Oxford Internet Institute** [Em linha], 2011. [Consult. 12 fev. 2017]. Disponível em WWW:<URL:http://geography.oii.ox.ac.uk/?page=home>.

OXFORD LD - **hacktivism** [Em linha] [Consult. 20 mar. 2017]. Disponível em WWW:<URL:https://en.oxforddictionaries.com/definition/hacktivism>.

OXFORD LD - **Cyberwar** [Em linha] [Consult. 18 mar. 2017]. Disponível em WWW:<URL:https://en.oxforddictionaries.com/definition/cyberwar>.

PEDAHZUR, Ami - **The Israeli Secret Services & the struggle against Terrorism**. Nova Iorque : Columbia University Press, 2009. ISBN 978-0231140430.

PERNIK, Piret - **Improving Cyber Security : NATO and the EU** [Em linha], Tallinn : ICDS, 2014. [Consult. 3 mar. 2017]. Disponível em WWW:<URL:https://www.icds.ee/fileadmin/media/icds.ee/failid/Piret_Pernik_-_Improving_Cyber_Security.pdf>.

PJ - **Unidade de Combate ao Cibercrime e a Criminalidade Tecnológica** [Em linha], 2017. [Consult. 24 fev. 2017]. Disponível em WWW:<URL:https://www.policiajudiciaria.pt/PortalWeb/page/%7BEC96A2D3-BA0F-4F51-9A3A-5BA3D222FE8B%7D>.

QUIVY, Raymond; CAMPENHOUDT, Luc - **Manual de Investigação em Ciências Sociais**. 5ª ed. Lisboa : Gravida Publicações, S.A., 2008.

REHMAN, Scheherazade - **Estonia's Lessons in Cyberwarfare** [Em linha], 2013. [Consult. 30 jan. 2017]. Disponível em WWW:<URL:http://www.usnews.com/opinion/blogs/world-

report/2013/01/14/estonia-shows-how-to-build-a-defense-against-cyberwarfare>.

REIS, Bruno C. - Realismo, ainda a teoria dominante? Em DUQUE, Raquel; NOIVO, Diogo; SILVA, Teresa A., coord. **Segurança Contemporânea**. 1ª ed. Lisboa : PACTOR, 2016. ISBN 978-989-693-054-7. p. 3–22.

ROUSE, Margaret - **Botnet (zombie army)** [Em linha], 2012. [Consult. 20 mar. 2017]. Disponível em WWW:<URL:http://searchsecurity.techtarget.com/definition/botnet>.

SAMPIERI, Roberto H.; COLLADO, Carlos F.; LUCIO, Pilar B. - **Metodologia de Pesquisa**. 5ª ed. São Paulo : Penso, 2013. ISBN 978-85-65848-28-2.

SANTOS, Lino; BRAVO, Rogério; NUNES, Paulo V. - **Protecção Do Ciberespaço: Visão Analítica** [Em linha], [s.l.] : [s.n], 2012. [Consult. 2 fev. 2017]. Disponível em WWW:<URL:http://comum.rcaap.pt/bitstream/10400.26/3578/1/Artigo_ENRSF_Revisto.pdf>.

SANTOS, Victor Marques Dos - **Introdução à Teoria das Relações Internacionais**. Lisboa : Instituto Superior de Ciências Sociais e Políticas, 2007. ISBN 978-972-8726-86-7.

SANTOS, Victor Marques Dos - Realismo. Em MENDES, Nuno C.; COUTINHO, Francisco P., coord. **Enciclopédia das Relações Internacionais**. 1ª ed. Alfragide : Dom Quixote, 2014. ISBN 978-972-20-5505-5. p. 441–443.

SEABRA, Pedro - Construtivismo e Segurança. Em DUQUE, Raquel; NOIVO, Diogo; SILVA, Teresa A., coord. **Segurança Contemporânea**. 1ª ed. Lisboa : PACTOR, 2016. ISBN 978-989-693-054-7. p. 41–54.

SHACHTMAN, Noah - **Top Georgian Official: Moscow Cyber Attacked Us – We Just Can't Prove It** [Em linha], 2009. [Consult. 6 mar. 2017]. Disponível em WWW:<URL:https://www.wired.com/2009/03/georgia-blames/>.

SHAKARIAN, Paulo - **Análise da Campanha Cibernética da Rússia**

**Contra a Geórgia, em 2008** [Em linha], Kansas : Military Review, 2011. [Consult. 14 fev. 2017]. Disponível em WWW:<URL:http://usacac.army.mil/CAC2/MilitaryReview/Archives/Portuguese/MilitaryReview_20111231_art011POR.pdf>.

SHYLES, Leonard C. - **Deciphering Cyberspace: Making the Most of Digital Communication Technology**. 1ª ed. California : SAGE, 2002. ISBN 978-0761922209.

SINGER, Peter W.; FRIEDMAN, Allan - **Cybersecurity and Cyberwar What Everyone Needs to Know**. 1ª ed. Nova Iorque : Oxford University Press, 2014. ISBN 978–0–19–991809–6.

SOFFER, Ari - **Security Services «Foiled Massive Cyber-Attack on Israel»** [Em linha], 2014. [Consult. 23 fev. 2017]. Disponível em WWW:<URL:http://www.israelnationalnews.com/News/News.aspx/184518#.VEUVX23DVgg>.

SOOD, Aditya; ENBODY, Richard - **U.S. Military Defense Systems: The Anatomy of Cyber Espionage By Chinese Hackers** [Em linha], 2014. [Consult. 22 fev. 2017]. Disponível em WWW:<URL:http://journal.georgetown.edu/u-s-military-defense-systems-the-anatomy-of-cyber-espionage-by-chinese-hackers/>.

SPUTNIK INTERNATIONAL - **Russian Military Creating Cyber Warfare Branch** [Em linha], 2013. [Consult. 23 fev. 2017]. Disponível em WWW:<URL:https://sputniknews.com/military/20130820182856856-Russian-Military-Creating-Cyber-Warfare-Branch/>.

SZOLDRA, Paul - **Here's how the «Internet of Things» is being used for major cyberattacks on corporations** [Em linha], 2016. [Consult. 8 fev. 2016]. Disponível em WWW:<URL:http://www.businessinsider.com/internet-of-things-corporate-cyberattacks-2016-10>.

US DHS - **Cyber Safety** [Em linha], 2016. [Consult. 17 mar. 2017]. Disponível em WWW:<URL:https://www.dhs.gov/cyber-safety>.

UN - **A more secure world : Our shared responsibility** [Em linha], [s.l.] : UN DPI, 2004. [Consult. 12 fev. 2017]. Disponível em WWW:<URL:http://www.un.org/en/peacebuilding/pdf/historical/hlp_more_secure_world.pdf>.

UN GA - **General Assembly: 56/121. Combating the criminal misuse of information technologies** [Em linha], [s.l.] : UN, 2002. [Consult. 22 fev. 2017]. Disponível em WWW:<URL:https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_56_121.pdf>.

UN GA - **General Assembly: 57/239. Creation of a global culture of cybersecurity** [Em linha], [s.l.] : UN, 2003. [Consult. 22 fev. 2017]. Disponível em WWW:<URL:https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf>.

UN GA - **General Assembly: 58/199. Creation of a global culture of cybersecurity and the protection of critical information infrastructures** [Em linha], [s.l.] : UN, 2004. [Consult. 22 fev. 2017]. Disponível em WWW:<URL:https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf>.

UN GA - **General Assembly: Developments in the field of information and telecommunications in the context of international security** [Em linha], [s.l.] : UN, 2015. [Consult. 14 fev. 2017]. Disponível em WWW:<URL:http://www.un.org/ga/search/view_doc.asp?symbol=a/res/70/237>.

UNIDIR - **The Cyber Index: International Security Trends and Realities** [Em linha], Genebra : UNIDIR, 2013. [Consult. 21 fev. 2017]. Disponível em WWW:<URL:http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf>.

US CCU - **CYBER CAMPAIGN AGAINST GEORGIA IN AUGUST OF 2008** [Em linha], EUA : US CCU, 2009. [Consult. 23 fev. 2017]. Disponível em WWW:<URL:http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf>.

US DoD - **The DoD Cyber Strategy** [Em linha], EUA : DoD, 2015. [Consult. 18 fev. 2017]. Disponível em WWW:<URL:https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf>.

VERISIGN - **Tipos de ataques DDoS** [Em linha], 2015. [Consult. 17 mar. 2017]. Disponível em WWW:<URL:https://www.verisign.com/pt_BR/security-services/ddos-protection/types-of-ddos-attacks/index.xhtml>.

VERTON, Dan - **Serbs launch cyberattack on NATO** [Em linha], 1999. [Consult. 15 mar. 2017]. Disponível em WWW:<URL:https://fcw.com/articles/1999/04/04/serbs-launch-cyberattack-on-nato.aspx>.

VIEIRA, José Pedro - Sociedade das Nações. Em MENDES, Nuno C.; COUTINHO, Francisco P., coord. **Enciclopédia das Relações Internacionais**. 1ª ed. Alfragide : Dom Quixote, 2014. ISBN 978-972-20-5505-5. p. 495–496.

VILELAS, José - **Investigação: O processo de Construção do Conhecimento**. 1ª ed. Lisboa : Sílabo, 2009. ISBN 978-972-618-557-4.

WEIMANN, Gabriel - **Cyberterrorism: The Sum of All Fears?** [Em linha], Oxford : Routledge, 2005. Disponível em WWW:<URL:https://pdfs.semanticscholar.org/71e5/49cc7081348581b48cefbad32769ad0defd4.pdf>.

WHEELER, Ashley - **The Iranian Cyber Army is Still a Maturing Threat** [Em linha], 2013. [Consult. 23 fev. 2017]. Disponível em WWW:<URL:https://phoenixts.com/blog/iranian-cyber-army-still-maturing-threat/>.

WIKIPÉDIA - **Ficheiro: Georgia, Ossetia, Russia and Abkhazia (en).svg** [Em linha], 2008. [Consult. 15 fev. 2017]. Disponível em WWW:<URL:https://pt.wikipedia.org/wiki/Ficheiro:Georgia,_Ossetia,_Russia_and_Abkhazia.svg>.

WILSON, Woodrow - **President Wilson's Fourteen Points** [Em linha],

[Consult. 21 fev. 2017]. Disponível em WWW:<URL:https://wwi.lib.byu.edu/index.php/President_Wilson's_Fourteen_Points>.

YONHAP - **South to upgrade defense against North cyberattacks** [Em linha], 2012. [Consult. 23 fev. 2017]. Disponível em WWW:<URL:http://koreajoongangdaily.joins.com/news/article/article.aspx?aid=2958649>.

ZETTER, Kim - **Meet MonsterMind, the NSA Bot That Could Wage Cyberwar Autonomously** [Em linha], 2014. [Consult. 22 fev. 2017]. Disponível em WWW:<URL:https://www.wired.com/2014/08/nsa-monstermind-cyberwarfare/>.