O Ciberespaço como Dimensão de Segurança

Autor: **Marcelo da Silva Aparício**

Aspirante Aluno no Mestrado Integrado na Especialidade de Pilotagem Aeronáutica

Academia da Força Aérea, Sintra

Orientadora: **Professora Doutora Sandra Maria Rodrigues Balão**

Instituto Superior de Ciências Sociais e Políticas, Universidade de Lisboa

Coorientadora: **Tenente-coronel Luís Manuel Pinto de Almeida Rocha**

Força Aérea Portuguesa, Academia da Força Aérea, Sintra

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.

1. 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.

2. 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.

3. Metodologia

Como metodologia utilizou-se o método hipotético-dedutivo, que 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).

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).

Face à natureza deste estudo, 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).

3.1 Formulação da Pergunta de Partida e Pergunta Derivada

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?

3.2 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).

4. O Ciberespaço como novo espaço de conflito

A sociedade atual está profundamente dependente da tecnologia, verificando-se um crescimento muito acentuado das NTIC, do recurso e acesso à internet. 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).

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).

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.

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, 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.

A rutura de infraestruturas críticas é efetivamente uma preocupação atual dos Estados e das principais Organizações Internacionais. Sendo que 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) (Nunes, 2016).

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.

Nos dias de hoje verificamos também que a informação têm cada vez mais valor, embora este tenha estado sempre associada ao poder, 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).

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 (ibidem).

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).

5. 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).

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).

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).

Uma das mais importantes resoluções é a 56/121, referente ao combate ao uso criminoso das tecnologias de informação, onde é feito o reconhecimento das possibilidades de atividade criminal associadas ao ciberespaço, assumindo a necessidade de desenvolvimento dos Estados na área de TIC e também a sua cooperação para cumprir objetivos de segurança comuns (UN GA, 2002). Outra resolução de destaque é a Resolução para a proteção de infraestruturas críticas de informação, onde mais uma vez se reforçou a necessidade dos Estados Membros cooperarem entre si, nomeadamente aqueles que desenvolveram as melhores estratégias de cibersegurança devem partilhar o seu conhecimento em prol de alcançar a cibersegurança (UN GA, 2004). Em paralelo com as resoluções, todos os anos sai um relatório elaborado por

4 Group of Governmental Experts (GGE), que examinam as potenciais ameaças provenientes do ciberespaço, assim como as possíveis medidas de cooperação para as enfrentar, para a orientação dos Estados Membros (UN GA, 2015).

Devido a incidentes no final dos anos 90 nas operações da nato na Balcãs, a NATO inicia o seu programa de ciberdefesa em 2002, oficializado na cimeira de Praga. Foi então criado nesse contexto o NATO Computer Incident Response Capability para dar resposta a ciberataques (UNIDIR, 2013). Mais tarde, em 2008 é estabelecido na Estónia o Centro de Excelência em CiberDefesa Cooperativa, em Tallinn. Este é composto por peritos civis e militares com formação em várias áreas, de vinte nações diferentes. Este centro realiza exercícios anuais de ciberdefesa e é responsável pela formação, pesquisa, e pela realização de workshops sobre doutrina, legalidade e aspetos técnicos da ciber guerra. O desenvolvimento mais importante deste centro foi o Manual de Tallinn, que investiga de que modo a Lei Internacional pode ser aplicável no ciberespaço (NATO CCD COE, 2013). Ainda em 2008 é estabelecido o Cyber Defence Management Authority, que é o órgão reaponsável pela iniciação e coordenação de ações apropriadas de ciberdefesa, e serve também como um comando central para os esforços de partilha de informação entre os Estados Membros. Em caso de pedido de auxílio 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 foram identificadas as falhas de ciberdefesa da NATO e dos seus Estados Membros e posteriormente refletidas no Conceito Estratégico de 2010. Neste documento assume-se que devido aos potenciais danos que os ciberataques podem causar tanto na indústria como no governo ou até a infraestruturas críticas, estes ataques são uma ameaça à segurança e estabilidade nacional e Euro-Atlântica. Deste modo é necessário o desenvolvimento de capacidades de defesa, alerta e resposta dos Estados Membros (NATO, 2010).

No sentido de apostar numa maior prontidão na resposta a ciberataques foram desenvolvidas em 2011 as Equipas de Resposta Rápida, que estão disponíveis para serem destacadas imediatamente em caso de um pedido de auxílio de um Estado Membro, algo que não foi possível fazer nos ataques à Estónia ou Geórgia onde foram destacadas equipas ad hoc (NATO PA, [s.d.]).

Em 2014 na Cimeira de Gales foi reafirmado o empenho em defender aliados contra ciberameaças, neste sentido foi desenvolvida a Politica de Ciber Defesa Avançada da NATO. A NATO reconhece que a Lei Humanitária Internacional é aplicável no domínio do ciberespaço, e que ciberataques podem ter um impacto tão nefasto para a sociedade como um ataque convencional, como tal considera que a ciberdefesa compõe uma das tarefas base da defesa coletiva, no entanto a decisão da justificação da invocação do artigo 5º do Tratado do Atlântico Norte fica a cargo do Conselho do Atlântico Norte, numa abordagem caso-a-caso (NATO, 2014).

Em Fevereiro de 2016 foi elaborado um acordo técnico sobre a ciber defesa entre as equipas de respostas a ciberataques da NATO e EU para partilharem informações e as melhores práticas e métodos de ação. No mesmo ano na Cimeira de Varsóvia, o ciberespaço é reconhecido como um domínio de operações, sendo que deste modo a NATO tem de garantir a sua defesa do mesmo modo que o faz para os tradicionais domínios (NATO, 2017).

Relativamente à UE, em 2003 é publicado o conceito estratégico da EU intitulado de “A secure Europe in a Better World” onde estavam definidos objetivos para o desenvolvimento da organização em termos de segurança, no entanto as ciberameaças e ciberataques não estavam refletidos neste documento, ao contrário de ameaças o terrorismo, proliferação de armas de destruição massiva, ou mesmo o crime organizado. Só em 2008 é que surge a necessidade de rever o documento e nesta revisão já se inclui a cibersegurança como uma das ameaças chave ou desafios globais (EC, 2008). Isto devido ao aparecimento de ataques a tecnologias de informação de instituições privadas e do governo de estados membros da UE, que veio dar uma nova dimensão às ameaças provenientes do ciberespaço, constituindo-se aquele espaço como uma nova arma política, militar ou económica. Neste documento refere-se a necessidade da consciencialização dos estados membros para esta ameaça e da sua cooperação e partilha de informação.

Mais tarde em 2013, foi apresentada a Estratégia de cibersegurança da UE, que define 5 prioridades estratégicas: 1) alcançar a ciber resiliência; 2) reduzir drasticamente o cibercrime; 3) desenvolver políticas e capacidades de ciberdefesa relacionadas com a Common Security and Defence Policy (CSDP); 4) desenvolver os recursos industriais e tecnológicos para a cibersegurança; 5) e estabelecer para a União Europeia uma política internacional coerente sobre o ciberespaço e que, simultaneamente, promova os seus valores. Neste documento ainda está referida a importância do desenvolvimento das capacidades de ciberdefesa dos estados membros, e a necessidade de se desenvolver um quadro político de ciberdefesa (EC, 2013).

Um ano mais tarde, em 2014 é apresentado o EU Cyber Defence Policy Framework, de modo a definir aspetos da Estratégia de cibersegurança da UE, identificar as áreas prioritárias para a ciberdefesa da CSDP e clarificar os papeis a desempenhar pelos vários atores europeus (EU Council, 2014).

Embora já se verifiquem importantes avanços de doutrina e na criação de órgãos técnicos no domínio do ciberespaço, tanto por Organizações Internacionais como pelos seus Estados Membros, 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).

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 no CCD COE da NATO na Estónia em 2013, veio apresentar um conjunto de princípios fundamentais do direito internacional associado ao ciberespaço, algo que foi considerado de extrema utilidade para a criação de legislação para cada Estado (Nunes, 2016).

Nas 95 regras ou princípios apresentados no manual, está definido em que circunstâncias se pode invocar legítima defesa em operações neste domínio. Uma ciber-operação pode ser conduzida em resposta à alegação de legítima defesa, no entanto, apenas se se as condições identificarem o ataque como um ciberataque armado, ou seja um ciberataque que tenha resultado do uso da força. 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 (NATO CCD COE, 2013). Perante este tipo de situações em que podemos invocar a legítima defesa, a maior dificuldade é a atribuição da autoria do ataque a um Estado, sendo que no domínio do ciberespaço é bastante difícil de o fazer, e 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) Deste modo, existe uma grande 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.

6. Estudo de Caso: Ataque cibernético à Geórgia

O ataque cibernético à Geórgia ocorreu em agosto de 2008 e foi articulado com a invasão territorial Russa, e é visto como o primeiro caso de articulação de um ataque no domínio do ciberespaço com as operações militares nos restantes domínios. 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 (Hollis, 2011).

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).

Os ataques 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).

No início de Julho um investigador em Massachusetts um ciberataque contra a Geórgia, verificando um grande fluxo de data direcionado a websites governamentais georgianos que continham a mensagem "win+love+in+Rusia" (Nazario, 2009). Outros peritos 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 fundamental para esta campanha, e um argumento muito forte no envolvimento do Estado Russo nos ciberataques foi o nível de precisão e coordenação 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 (Menn, 2008).

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.

7. Conclusões

Com base no estudo efetuado e na investigação desenvolvida neste trabalho académico, encontram-se materializadas as condições necessárias para responder às perguntas desenvolvidas inicialmente, bem com para se proceder à validação ou refutação das hipóteses 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

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.

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.

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

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>.

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>.

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>.

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

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

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>.

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>.

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>.

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>.

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 - **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 - **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 - **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 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 - **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 - 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>.

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>.

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.

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>.

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: 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>.

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