ESCOLA NAVAL

talant de bien faire

João André Pinto Gonçalves

Enquadramento legal da Cibersegurança em Portugal e no Mundo

O impacto dos crimes cibernéticos no Direito Internacional

Dissertação para obtenção do grau de Mestre em Ciências Militares Navais, na especialidade de Marinha.

Alfeite
[2016]

ESCOLA NAVAL

lalantde bifaire

João André Pinto Gonçalves

Enquadramento legal da Cibersegurança em Portugal e no Mundo. O impacto dos crimes cibernéticos no Direito Internacional.

Dissertação para obtenção do grau de Mestre em Ciências Militares Navais, na especialidade de Marinha

Orientação de: Caetano Fernandes Augusta Silveira

Co-orientação de: Gonçalo Nuno Baptista de Sousa

O Aluno Mestrando	O Orientador
Pinto Gonçalves	Augusta Silveira

Alfeite

[2016]

Agradecimentos

Gostaria de começar por agradecer à minha família, os meus pais, Fernando Gonçalves e Felismina Gonçalves, e ao meu irmão, Pedro Gonçalves, por serem a minha fonte de motivação para ser mais e melhor todos os dias, por terem estado comigo durante toda a minha vida apoiando-me incondicionalmente em todos os momentos.

Em segundo lugar queria agradecer à minha namorada, Patrícia Rosa, por todo o esforço que faz ao me acompanhar todos os dias, e mesmo assim permanecendo ao meu lado, apoiando-me e acompanhando a minha vida no bom e no mau, na presença e na ausência que a minha condição de militar muitas vezes acarreta. Obrigado ainda por me fazeres sempre acreditar que era possível e que nenhuma tarefa é grande demais.

Aos meus camaradas de curso, com os quais durante os últimos cinco anos partilhei boas e más experiências, tanto em terra como a navegar, agradeço toda a disponibilidade, fraternidade, camaradagem e amizade demonstrada, fazendo com que ganhasse mais uma família e uma segunda casa. A todos o meu muito obrigado e que nos voltemos a reunir em breve.

À Fragata *D. FRANCISCO DE ALMEIDA*, navio que me acolheu durante 18 semanas, acompanhado por uma guarnição fantástica que contribuiu enormemente para a minha formação como futuro Oficial da Marinha Portuguesa, salientando o incentivo para que não descurasse na elaboração desta dissertação, ajudando de forma significativa na conclusão da mesma. Um grande obrigado e um grande abraço.

À Escola Naval, por ter feito de mim o homem que sou hoje, por me ter transmitido não só valências técnicas, teóricas e práticas, mas também valores e uma cultura que honrarei até ao final da minha vida.

A todos os meus professores, agradeço a confiança que demonstraram nas minhas potencialidades e na minha pessoa que muito contribuiu para o meu desenvolvimento pessoal e profissional.

Resumo

O cibercrime deixou há muito de ser uma palavra desconhecida para a generalidade da população mundial, sendo cada vez mais comum a execução dos mesmos por parte de indivíduos ou mesmo nações. Como tal, reveste-se de elevada importância a existência de uma resposta jurídica adequada às novas ameaças potenciadas pelo ciberespaço, a nível nacional e internacional.

A evolução tecnológica levou à criação de novos elementos estratégicos, como os conceitos estratégicos de cibersegurança, e legislativos, com o objetivo de fazer face à especificidade da temática, tendo a União Europeia elaborado a Convenção de Budapeste sobre o Cibercrime de 23 de Novembro de 2001, e Portugal promulgado a Lei nº109/2009 de 15 de Setembro de 2009, a chamada Lei do Cibercrime.

Apesar da existência da atual legislação, a ameaça pendente dos ciberataques tornou-se cada vez mais uma preocupação de todos os países, tendo em conta que um ataque no ciberespaço pode pôr em causa a sua segurança e soberania. Tendo estes factos em consideração, importa analisar qual o possível impacto dos ataques cibernéticos a nível nacional e das relações internacionais.

Palavras-chave: Cibercrime, Cibersegurança, Ciberdefesa, Lei do Cibercrime, Convenção sobre o Cibercrime.

Abstract

Cybercrime has long since ceased to be an unknown word for most of the world's population, it is increasingly common the execution of them by individuals or nations. As such, it is of the utmost importance the creation of adequate legislation to face this new threats in cyberspace, enhanced at national and international level.

The technological evolution led to the creation of new strategic elements, such as the strategic concepts of cyber security, and legislative ones, in order to address the specific nature of the subject, as such the European Union created the Budapest Convention on Cybercrime of 23 November 2001 and Portugal drafted the Cybercrime Law, nº 109/2009 of 15 September 2009.

Despite the existence of the current legislation, the pending threat of cyberattacks has increasingly become a concern to all countries, taking into account that an attack in cyberspace may jeopardize its security and sovereignty. Taking these facts into consideration, it is important to analyze what is the potential impact of cyber-attacks on a national level and concerning its international relations.

Key-words: Cybercrime, Cyber Security, Cyber Defence, Cybercrime Law, Convention on Cybercrime.

Índice

Índice de figuras

Lista de Siglas e Acrónimos

CAN – Computer Network Attack

CERT – Computer Emergency Response Team

CIA – Central Intelligence Agency

CIRCs – Computer Incident Response Capability

CND – Computer Network Defense

CNE – Computer Network Exploitation

CRP – Constituição da República Portuguesa

CSIRT – Computer Security Incident Response Team

DDoS – Distributed Denial of Service

DIRCSI – Direção de Comunicações e Sistemas de Informação

DIRCSI – Direção de Comunicações e Sistemas de Informação

DNS – Domain Name System

DNSSEC – Domain Name System Security Extensions

DoS – Denial of Service

EMGFA – Estado-Maior-General das Forças Armadas

EU – European Union

GRISI – Grupo de Resposta a Incidentes de Segurança Informática

ICANN – Corporação da Internet para Atribuição de Nomes e Números

IWWN – International Watch and Warning Network

NATO – North Atlantic Threaty Organization

SI – Sistemas de Informação

SIC –Sistemas de Informação e Comunicações

TIC – Tecnologias de Informação e Comunicações

Introdução

Na sociedade de hoje em dia é cada vez mais comum a utilização de termos específicos originados pelo crescimento da utilização de sistemas informáticos por parte da população mundial, um desses termos é o ciberespaço. Ora é precisamente neste espaço cibernético que se situa o tema que esta dissertação propõe investigar, visto que este novo mundo que surgiu com a evolução tecnológica e que nos catapultou para uma realidade onde não existem fronteiras entre Estados, deu origem a um tipo de crime que até há cerca de trinta anos não existia, os crimes cibernéticos.

Este novo tipo de ameaças, maioritariamente relacionadas com a segurança da informação e operacionalidade dos sistemas informáticos e de comunicação, existentes na maioria das organizações são, cada vez mais, uma preocupação constante de todos os Estados. Estes crimes cibernéticos devem portanto ser analisados com atenção por parte do Estado Português, principalmente com o objetivo de proteger os interesses nacionais mas também os de organizações internacionais das quais faz parte. Tendo isto em mente foi atribuída ao Gabinete Nacional de Segurança em 2012 a missão de criar uma comissão instaladora do Centro Nacional de Cibersegurança, de acordo com a Resolução do Conselho de Ministros nº 42/2012 de 13 de Abril de 2012, e que elaborou uma Estratégia Nacional de Segurança no Ciberespaço a 12 de Junho de 2015 com o objetivo de assegurar os interesses acima referidos.

Com este trabalho indica-se como objetivo primário a análise da legislação existente, tanto nacional como internacional, com o objetivo final de aferir de que maneira o Direito Internacional se está a preparar para lidar com esta nova realidade, uma realidade virtual, se assim se puder definir. Desta forma pretende-se também verificar se existem incongruências entre a legislação internacional e a legislação própria de cada Estado, e se existirem, de que maneira está previsto lidar com essas situações. Esta problemática prende-se principalmente com a inexistência de fronteiras físicas que delimitem o espaço de ocorrência de um delito.

Como tal este trabalho assenta no escrutínio de dois elementos legislativos primários, a Convenção de Budapeste sobre o Cibercrime redigida a 23 de Novembro de 2001 e ratificada por Portugal em 24 de Março de 2010, e a Lei nº109/2009 de 15 de Setembro de 2009, e secundariamente os conceitos estratégicos de cibersegurança de Portugal, Espanha, Reino Unido e Estados Unidos da América. Espanha por ser o nosso vizinho mais próximo, Reino Unido visto serem em vários aspetos um exemplo a seguir em termos de doutrina e Estados Unidos da América, que como se tem vindo a verificar é uma potência pioneira neste campo. A análise destes documentos irá permitir aferir a existência ou não, de uma consonância entre os objetivos dos Estados membros da North Atlantic Treaty Organization (NATO), visto que os problemas no ciberespaço devem ser sempre abordados tendo em vista a sua natureza transfronteiriça.

Tomando como exemplo uma situação hipotética, em que um cidadão português é responsável por um ataque cibernético a Itália utilizando um servidor Russo e situando-se este indivíduo em Berlim, de que maneira deve ser tratado judicialmente este crime? É da responsabilidade do Estado Italiano, do Estado Português, do Estado Russo ou do Estado Alemão? Quem tem o direito de deter o sujeito ou apreender o material utilizado por este?

Todas as questões supramencionadas invocam a utilização de elementos legislativos tanto nacionais como internacionais, e podem inclusivamente debilitar a segurança de um Estado ou pôr em causa a soberania do mesmo. Este último caso sai da esfera de atuação da cibersegurança e passa a ser inserido no conceito de ciberdefesa, conceitos este que serão amplamente abordados nos próximos capítulos, suscitando outras questões: existe uma estrutura de ciberdefesa a nível NATO? E a nível nacional? Estarão essas estruturas preparadas e equipadas para as crescentes ameaças potenciadas pelo ciberespaço? De que forma poderão as debilidades nessas estruturas afetar as relações internacionais?

Estas são algumas das questões que este trabalho de investigação propõe responder com a investigação e análise dos elementos legislativos existentes, bem como elementos não legislativos, como por exemplo tratados e outros documentos

internacionais, e através delas tentar elucidar e alertar os leitores deste trabalho para esta nova ameaça e a forma de combate-la.

1. Enquadramento concetual e metodologia

1.1. Metodologia

1.1.1. Pertinência do tema

Vivemos hoje em dia numa sociedade cada vez mais globalizada graças à utilização da internet como meio de ligação entre lugares sem quaisquer conexões física, cultural ou política. Esta crescente utilização da internet como principal meio de comunicação verifica-se também em todos os ramos das Forças Armadas por todo o globo, e como tal Portugal não é exceção.

Tendo isto em mente, envolve-se de grande prioridade a necessidade de todos os Militares, Militarizados e Civis das Forças Armadas, de qualquer posto e classe, serem detentores de maiores e melhores conhecimentos jurídicos no que a este tema diz respeito. Esta conclusão prende-se com o fato de estas Organizações lidarem com matérias de cariz classificado, tanto a nível nacional como de Organizações Internacionais, matérias essas que podem pôr em causa a segurança nacional de um determinado Estado ou mesmo de, por exemplo, a Organização das Nações Unidas ou a Organização do Tratado do Atlântico Norte.

1.1.2. Objetivos

Com esta dissertação espera-se conseguir clarificar uma questão que para a maior parte da sociedade mundial se encontra pouco clarificado, dado ser um problema que passou a ser preponderante a partir da década de oitenta, e que começa agora a adquirir uma proporção cada vez maior e mais alarmante.

Para além da clarificação dos conceitos de ciberespaço, cibersegurança, ciberdefesa, ciberatauqe e cibercrime e como estas cinco definições são encaradas à luz do Direito, é pretendido analisar quais as ações determinadas pelo Direito Internacional e o Direito interno português, tanto disciplinares como penais, em relação a ciberataques e qual o impacto que estes podem vir a ter nas relações internas e internacionais de um Estado independente.

Como objetivo final espera-se motivar as Forças Armadas, em especial a Marinha, para que seja feito um esforço no sentido de melhor educar os Militares, Militarizados e Civis das Forças Armadas, no que toca à utilização de meios cibernéticos, alertando-os para os perigos decorrentes de utilização descuidade e como prevenir que sejam vítimas deste novo tipo de crime.

1.1.3. Formulação do problema e método de investigação

A identificação e correspondente formulação do problema que deu origem a esta dissertação assenta na metodologia de investigação defendida por Quivy e Campenhoudt[1], representada na Figura 1, tendo sido definida como pergunta de partida: *Qual o impacto dos crimes cibernéticos no Direito Internacional?*. Defenindo como questão derivada: *Estarão as estruturas de Ciberdefesa da NATO e de Portugal preparadas para fazer frente aos ataques no ciberespaço?*

Com o objetivo de responder às questões mencionadas no parágrafo anterior foi levada a cabo uma investigação interpretativa, qualitativa e avaliativa, tendo como base uma análise documental e estudo de caso. Estas análises debruçam-se sobre a Convenção de Budapeste sobre o Cibercrime, a Lei do Cibercrime portuguesa e os casos dos ataques à Estónia e à Georgia.

[1] Quivy, Raymond e Campenhoudt, Luc Van, *MANUAL DE INVESTIGAÇÃO EM CIÊNCIAS SOCIAIS*, http://www.fep.up.pt/docentes/joao/material/manualinvestig.pdf, acedido em Outubro de 2016.

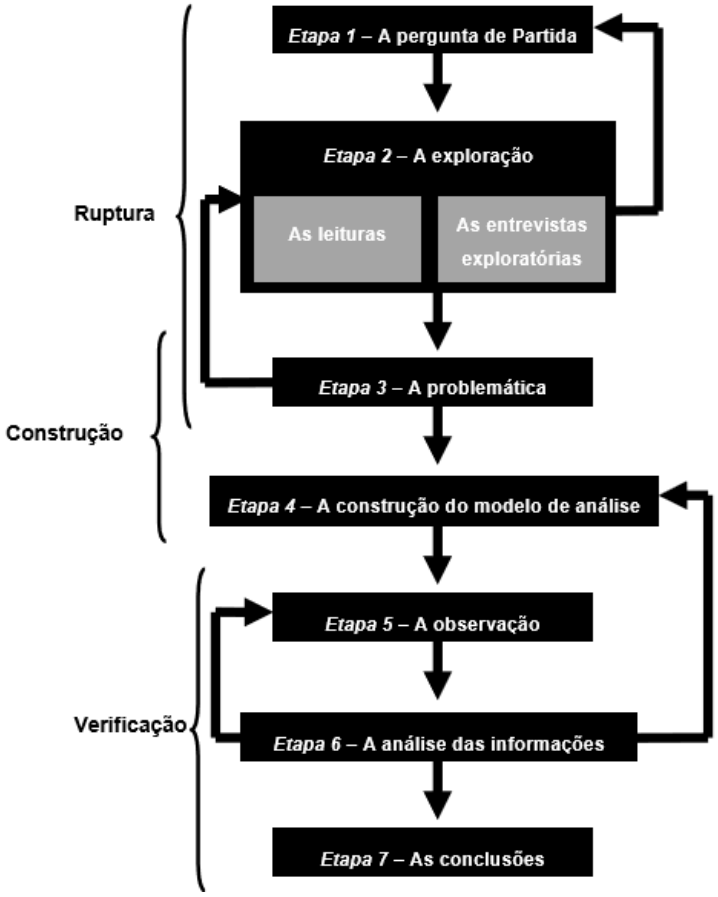

Figura 1. Etapas de formulação do problema.

1.2. Enquadramento concetual

1.2.1. No que consiste o Ciberespaço?

A constante evolução tecnológica que se verifica nos nossos dias, e que não seria espectável com semelhante celeridade a não ser em filmes de ficção científica, levou a uma consequente evolução do modo de vida da população em geral, abrindo novas portas e abolindo as fronteiras que outrora separavam Povos e Estados. No entanto esta evolução deu origem a novas possibilidades e exponenciou uma facilidade de acesso a dados e informação que de outra maneira estariam mais resguardados, pois estes deixaram de ser guardados nas convencionais caixas de arquivo existentes em salas fechadas, para serem arrumadas, na sua maioria, numa nova caixa de arquivo de nome base de dados, numa nova sala não tão fechada denominada ciberespaço.

> "O Ciberespaço toca praticamente tudo e todos. Proporciona uma plataforma para a inovação e prosperidade, e os meios para melhorar o bem-estar geral de todo o mundo."[2]

Podemos então dividir esta palavra em duas, a palavra mãe *espaço* e o seu prefixo *ciber*, derivado do prefixo anglo-saxónico *cyber* que surgiu do termo *cybernetics*, ou em português *cibernética*. Esta última é definida como a "ciência que tem por objeto o estudo comparativo dos sistemas e mecanismos de controlo automático, regulação e comunicação nos seres vivos e nas máquinas"[3]. Logo etimologicamente pode ser aferido que o ciberespaço engloba o espaço onde decorrem ações levadas a cabo tanto por humanos como por sistemas informáticos e as suas consequentes interações.

> "Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphic representation of data abstracted from banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding..."[4].

Apesar da atualidade que esta definição de ciberespaço apresenta ela foi escrita em 1984 por William Gibson, autor de livros de ficção científica, prevendo assim há 32 anos atrás a dimensão que a internet está a tomar nos dias de hoje. No entanto esta visão de ciberespaço apresenta uma natureza bastante artística como é característica de uma novela científica.

Atualmente ciberespaço é definido pela Comissão Europeia como "O espaço virtual no qual os dados eletrónicos dos PCs do mundo circulam"[5], e pela NATO como

---

[2] CASA BRANCA, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, Estados Unidos da América, 2011.
[3] Antônio Houaiss, *Dicionário Houaiss da Língua Portuguesa*, Instituto Antônio Houaiss, Editora Objetiva Ltda., 2009.
[4] William Gibson, *Neuromancer*, Nova Iorque, Ace Books, 1984.
[5] COMISSÃO EUROPEIA, *Glossary and Acronyms,* http://ec.europa.eu/information_society/tl/help/glossary/index_en.htm#c, consultado em 15 de Setembro de 2015.

> "The global domain created by communication, information and other electronic systems, their interaction and the information that is stored, processe dor transmitted in these systems"[6].

No entanto para este trabalho irá ser adotada a definição proposta por Rain Ottis e Peeter Lorents "cyberspace is a time-dependent set of interconnected information systems and the human users that interact with these systems"[7] pois introduz a componente humana na definição deste novo mundo sem fronteiras, sendo esta componente de enorme preponderância para esta temática visto que o principal objetivo da criação de legislação tanto internacional como nacional no que se refere ao tema da cibersegurança é a proteção das pessoas e dos seus direitos.

É portanto neste ciberespaço onde se centra o ponto fulcral desta investigação, os cibercrimes e o seu enquadramento legal nos dias de hoje, importa referir que apesar do conceito de ciberespaço existir há mais de 30 anos muitos indivíduos desconhecem a abrangência do mesmo, desconhecendo também os seus direitos e deveres no que toca à sua existência como utilizadores dos serviços fornecidos através deste novo mundo virtual.

Como tal é da responsabilidade de todos contribuir para uma maior disseminação deste conceito e consciencializar, tanto quanto possível, todos os utilizadores deste espaço para os riscos que decorrem da sua nefasta utilização, riscos esses que podem tomar a forma de uma simples, mas claro não menos condenável, utilização de uma página pessoal de uma rede social para difamar ou abusar psicologicamente de um determinado indivíduo, bem como tomar a forma de um ataque cibernético de proporções globais, pondo em causa a segurança de um Estado soberano, como por exemplo, os ataques cibernéticos decorridos em Julho de 2009 aos *websites* da Casa Branca, do Departamento de Segurança Interna e da Bolsa de Valores de Nova Iorque.

[6] NORTH ATLANTIC COUNCIL, *NATO Cyber Defence Taxonomy and Definitions*, Norfolk, NORTH ATLANTIC TREATY ORGANISATION, 2014.
[7] Ottis, Rian e Lorents, Peeter, *Cyberspace: Definition and Implications*, Tallinn, Cooperative Cyber Defence Centre of Excellence, [s.d.].

Tendo em conta esta vastidão e versatilidade dos cibercrimes, neste trabalho estes irão ser primeiramente divididos em dois tipos, cibercrimes que afetem um utilizador individual, i.e. um cidadão comum, e os que afetam um Estado diretamente, atacando os seus serviços básicos, ou que sejam direcionados a indivíduos que tenham no seu poder materiais sensíveis à manutenção dos direitos básicos e consagrados internacionalmente desse Estado. Para tal é necessário definir os conceitos de ocorrências[8] no ciberespaço, bem como os níveis em que estas são classificadas, e ainda distinguir os conceitos de cibersegurança e ciberdefesa, que apesar de aparentarem definir uma mesma definição caraterizam dois conceitos algo distintos, tanto no seu propósito como na sua abrangência.

1.2.2. Ocorrências no ciberespaço

No ciberespaço existe uma vastidão de ações que podem ser executadas por qualquer pessoa com o mínimo de conhecimentos informáticos por forma a lesar, intencionalmente ou não, um qualquer outro individuo, no entanto nem todas estas ações podem ser consideradas crimes ou ataques como é vulgar serem tratadas no módico diálogo quotidiano. Todas estas ações[9] são denominadas como ocorrências no ciberespaço, e como forma de as diferenciar foram agrupadas em vários níveis pela NATO:

- Cyber event;
- Cyber incident;
- Cybercrime;
- Cyberattack;
- Cyber crisis.

No enquadramento do tema abordado nesta dissertação é essencial uma focalização nos conceitos de cibercrime e de ciberataque, como tal serão definidas

[8] Nestas ocorrências estão contemplados os cibercrimes, ciberataques, ciberterrorismo entre outros.
[9] Desde um simples mas incómodo malware que é injetado no nosso computador por forma a abrir uma página de publicidade na internet ao ataque a um sistema de segurança de um Estado.

cada uma das ocorrências definindo-as e dando exemplos das mesmas com uma maior incidência nestes dois referidos anteriormente.

Cyber event - "A cybersecurity change that may have an impact on organizational operations (including mission, capabilities, or reputation)."[10]

Cyber incident – "Actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein."[11]

Cyber crisis consiste numa ocorrência no ciberespaço, seja esta um evento ou um incidente, que pela natureza da sua complexidade e capacidade de propagação possa gerar uma situação em que uma ou mais entidades[12] sejam comprometidas, dificultando ou mesmo impossibilitando o funcionamento das mesmas podendo em casos extremos por em causa a segurança nacional de um Estado. Neste âmbito a Critical Infraestructures Protection reconheceu a necessidade de criar uma estratégia a nível internacional de resposta a possíveis crises cibernéticas, estabelecendo respostas pré-definidas para os Estados membros, agendando exercícios regularmente com os diferentes Estados por forma a elevar a proficiência na resposta a estas crises, bem como o controlo de danos e recuperação após um incidente.

Como resultado desta iniciativa levada a cabo em 2009 foi também criada a *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, que tem como principais objetivos alcançar uma resiliência cibernética, a redução de cibercrimes, a criação de políticas de ciberdefesa e de cibersegurança e o desenvolvimento de recursos industriais e tecnológicos que assegurem as mesmas e o estabelecimento de uma política europeia para o ciberespaço[13].

[10] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Estados Unidos da América, 2014.
[11] Richard Kissel, *Glossary of Key Information Security Terms*, National Institute of Standards and Technology, U.S. Department of Commerce, 2013.
[12] Sejam estas empresas privadas, públicas ou mesmo organizações governamentais.
[13] EUROPEAN COMMISSION, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace,* Bruxelas, European Commission, 2013.

Esta categorização não é fixa e imutável, tal seria pouco prático tendo em conta a volatilização dos sistemas de tecnologia e informação que se encontram no ciberespaço, assim sendo uma ocorrência pode proceder a uma escalada nesta categorização apresentada pela NATO, que é aceite pela maior parte da comunidade, podendo assim um evento aparentemente inofensivo tomar proporções à escala continental ou mesmo global. Não obstante a afirmação anterior as crises cibernéticas na sua maioria têm a sua génese num ataque cibernético ou num crime cibernético, visto que nestes dois conceitos ao contrário dos anteriormente referidos é necessário que o sujeito que inicia e perpetua estas ações tenha a intencionalidade de prejudicar um individuo em concreto ou terceiros em geral.

Como tal podem ser definidos como:

- "Cyberattack" – "An act or action initiated in cyberspace to cause harm by compromising communication, information or other electronic systems, or the information that is stored, processed or transmitted in these systems.";[14]
- "Cybercrime" – "the use of cyberspace for criminal purposes as defined by national or international law".[15]

O conceito de cibercrime será amplamente explorado nos capítulos que se seguem ao abrigo do direito internacional e nacional.

Ao analisar estes dois conceitos verifica-se a intencionalidade referida no anterior parágrafo, à primeira vista estes dois conceitos podem aparentar-se sinonímicos podendo levar a alguma confusão e a questões como: um ato ou ação com objetivo de lesar algo ou alguém não é também um crime? E o roubo de informação será um crime ou um ato de ataque à soberania de uma nação? De uma forma geral pode ser distinguido um ciberataque de um cibercrime atentando na dimensão e foco do ataque, um ataque cibernético tem em vista o comprometimento do funcionamento ou a lesão de um Estado, pondo em risco o seu funcionamento

[14] NORTH ATLANTIC COUNCIL, *NATO Cyber Defence Taxonomy and Definitions*, Norfolk, NORTH ATLANTIC TREATY ORGANISATION, 2014.
[15] James B. Godwin III, et all, *Critical Terminology Foundations 2 Russia-U.S. Bilateral on Cybersecurity,* The EastWest Institute & Information Security Institute Moscow State University, 2014.

sustentável e a sua independência e soberania. Seja tomado como exemplo destes ataques os atos de ciberterrorismo, que consistem no uso de tecnologias de informação para causar o pânico geral numa determinada população, exemplo disto foi o caso decorrido em Agosto de 2013 em que o Syrian Electronic Army[16] tomou conta das páginas web do New York Times, Twitter e do Huffington Post tendo publicado mensagens no Twitter com a assinatura digital das outras duas instituições, e os atos de ciberespionagem com o intuito de ter acesso a informação sensível e muitas vezes classificada de uma organização ou Estado, podendo originar conflitos internacionais à escala mundial à semelhança do que se passou com a Guerra Fria[17] por exemplo.

Todos estes eventos podem no pior dos cenários originar uma ciberguerra, um conflito entre dois ou mais intervenientes internacionais que tenham como objetivo levar a cabo ciberataques por forma a debilitar as capacidades de um determinado alvo. Esta possibilidade de uma guerra cibernética esta cada vez mais presente nos Gabinetes de Defesa de vários países, membros da União Europeia e não só, incluindo Portugal que em 12 de Junho de 2015 aprovou uma Estratégia Nacional de Cibersegurança.

1.2.3. Ciberdefesa e Cibersegurança

Face à constante evolução e expansão do espaço cibernético é constatável uma crescente sensibilização e preocupação no que toca aos riscos que este meio possibilita. Isto é verificável tanto na esfera de Estados e organizações de todas as dimensões, que têm cada vez mais presente a capacidade facilitadora que o ciberespaço representa para que sejam efetuados atos de espionagem ou mesmo de roubo de capital destas mesmas, como no quotidiano das pessoas, que cada vez mais se preocupam com a segurança da sua informação pessoal que se encontra armazenada em bases de dados acessíveis através desta rede virtual de informação

[16] Um grupo de hackers hostil a Bashar al-Assad.
[17] Conflito não armado entre Estados Unidos da América e Rússia na qual proliferou o recurso à atividade da espionagem.

que atualmente liga o mundo. Por conseguinte surgiram dois novos termos na sequência dos apresentados anteriormente, a ciberdefesa e a cibersegurança.

De acordo com a publicação *NATO Cyber Defence Taxonomy and Definitions*, ciberdefesa é definida como

> "The means to achieve and execute defensive measures to counter cyberattacks and mitigate their effects, and thus preserve and restore the security of communication, information or other electronic systems, or the information that is stored, processed or transmitted in these systems."[18]

Os meios para alcançar e executar medidas defensivas contemplam a criação de políticas de proteção de dados de utilizador no ciberespaço, o desenvolvimento de conceitos teóricos[19], por forma a incrementar o conhecimento situacional por parte de todos, o treino das próprias instituições e organizações, bem como as medidas técnicas, como a evolução de sistemas de antivírus, ferramentas de deteção e remoção de "malicious software", vulgo malware[20], e spywares[21].

À semelhança do que acontece com os conceitos de cibercrime e de ciberataque, os conceitos de ciberdefesa e de cibersegurança podem parecer algo semelhantes, esta vem definida na publicação NATO *SECURITY WITHIN THE NORTH ATLANTIC TREATY ORGANISATION* como "the application of security measures for the protection of communication, information and other electronic systems, and the information that is stored, processed or transmitted in these systems with respect to confidentiality, integrity, availability, authentication and non-repudiation."[22] Como pode ser verificado o conceito de cibersegurança assenta em alguns termos que o distinguem de ciberdefesa, na medida em que apresenta como principal sujeito da sua intervenção o individuo singular ao invés do coletivo[23]. São estes termos a segurança

[18] NORTH ATLANTIC COUNCIL, *NATO Cyber Defence Taxonomy and Definitions*, Norfolk, NORTH ATLANTIC TREATY ORGANISATION, 2014.
[19] Tais como cibercrime, ciberataque, ciberterrorismo, ciberespionagem, ciberespaço.
[20] Software criados com o propósito de causar ou roubar informações de um utilizador.
[21] Software criado com o intuito de registar informações sobre um utilizador sem a sua permissão.
[22] NORTH ATLANTIC COUNCIL, *SECURITY WITHIN THE NORTH ATLANTIC TREATY ORGANISATION*, North Atlantic Council, 2002.
[23] Por sujeito coletivo entenda-se um Estado ou um conjunto de Estados.

ao invés de defesa, a diferença entre estes dois termos na fonética anglo-saxónica pretende distinguir uma defesa individual do sujeito de uma defesa de um sujeito em relação a vários, a confidencialidade, que nesta definição representa não o problema da confidencialidade como uma quebra de segurança devido à obtenção de matérias classificadas às quais o delator não pode ter acesso, mas sim mais no sentido de obtenção de informação privada de determinada pessoa por parte de outro sem o consentimento do primeiro, e o não-repúdio[24], este último acentua de forma clara o foco desta definição no sujeito individual visto que este princípio visa garantir provas em questões de suspeita de burla e furto digital.

[24] Garantia de não negação de uma assinatura ou criação de informação por parte do utilizador.

2. A Cibersegurança no panorama internacional

2.1. Um olhar sobre Conceitos Estratégicos de Segurança no Ciberespaço

No encadeamento do surgimento destes conceitos de cibersegurança e ciberdefesa e da crescente consciencialização deste assunto, verificou-se uma cada vez maior preocupação por parte de Estados no que diz respeito à sua segurança no ciberespaço, preocupação esta que é verificada na elaboração de Estratégias Nacionais de segurança no ciberespaço e na criação de gabinetes especializados nesta matéria. Como tal foram analisados diferentes conceitos de segurança no ciberespaço, incindindo com especial atenção nos conceitos elaborados por Portugal, como se afigura óbvio visto ser um dos principais objetivos desta dissertação o enquadramento legal deste Estado, Espanha, visto ser o país vizinho mais próximo de Portugal, Reino Unido, devido ao fato de ser a nível doutrinário um dos melhores exemplos a seguir tanto dentro da União Europeia como a nível mundial, e Estados Unidos da América, que se afirma como uma das maiores potências mundiais em termos de evolução tecnológica e pioneira nesta área em concreto.

Como seria expetável todos estas estratégias assentam em pilares semelhantes apresentando diferentes visões e linhas de ação para assegurar os seus principais objetivos, que em linhas gerais são a defesa da informação e das infraestruturas críticas, bem como a garantia de uma utilização segura do ciberespaço por parte dos seus habitantes, e o fomento de uma cooperação internacional capaz de aproveitar as infinitas potencialidades oferecidas pelo ciberespaço de uma forma segura e responsável nunca colocando em perigo os seus interesses nacionais, nem os de outros sujeitos internacionais.

2.1.1. Conceito Espanhol

Com a elaboração de conceitos de Estratégias Nacionais para a cibersegurança um pouco por todos os países desenvolvidos, fruto da crescente preocupação europeia e mundial no âmbito do uso da internet, o Governo Espanhol publicou a *NATIONAL*

CYBER SECURITY STRATEGY, aprovada pelo Primeiro-Ministro Mariano Rajoy no ano de 2013.

A Estratégia Nacional de Cibersegurança espanhola encontra-se dividida em cinco capítulos: o primeiro aborda os conceitos de ciberespaço e a sua segurança, caraterizando-o e apresentando os riscos bem como as oportunidades a ele associados; o segundo capítulo trata do propósito e dos princípios que devem guiar a cibersegurança no país; o terceiro define especificamente os objetivos da cibersegurança em Espanha atribuindo responsabilidades tanto às Autoridades Públicas como a companhias e infraestruturas privadas; no capítulo quarto são apresentadas as linhas de ação para alcançar os objetivos definidos nos anteriores capítulos; e por fim o capítulo quinto que assenta na análise da relação entre a cibersegurança e o sistema de Segurança Nacional.

Este documento apresenta quatro caraterísticas associadas aos ciberataques, o seu baixo custo de execução, sendo que as ferramentas utilizadas pelos atacantes podem ser obtidas por valores muito baixos ou mesmo sem qualquer custo[25], refere ainda a facilidade de uso destas ferramentas e a independência geográfica da qual o atacante carece, denota a sua eficiência e capacidade destrutiva e por fim, e em consonância com a referência à independência geográfica, o reduzido risco que o indivíduo que leva a cabo este tipo de ações tem associado.[26]

Analisando esta estratégia, verifica-se que a sua principal preocupação é garantir o uso seguro do ciberespaço, e para que tal aconteça são definidos quatro princípios gerais:

- Uma liderança nacional e coordenação de esforços;
- Partilha da responsabilidade;
- Proporcionalidade, racionalidade e eficácia;

[25] Um exemplo desta facilitada disponibilização de meios são os imensos spywares e malwares que são providenciados para descarregamento gratuito na darkweb.
[26] Governo Espanhol, *NATIONAL CYBER SECURITY STRATEGY*, Presidência do Governo Espanhol, 2013, p.8.

- Cooperação Internacional.[27]

Tendo em consideração estes quatro princípios gerais Espanha definiu como objetivo geral para este documento "Assegurar que Espanha usa os serviços de Informação e de Telecomunicações de forma segura reforçando a proteção, defesa, deteção e capacidade de resposta a ciberataques"[28]. Para cumprir com esse objetivo global define ainda seis objetivos específicos:

- Assegurar que os sistemas de Informação e Telecomunicações utilizados pelas Autoridades Públicas possuam um nível apropriado de cibersegurança e resiliência;
- Promover a segurança e resiliência dos sistemas de Informação e Telecomunicações usados no setor empresarial em geral e pelos operadores de Infraestruturas Críticas em particular;
- Aumentar as capacidades de prevenção, deteção, reação, análise, recuperação, resposta, pesquisa e de coordenação frente a atividades terroristas e ao crime no ciberespaço;
- Aumentar a consciencialização dos cidadãos, profissionais, companhias e Autoridades Públicas Espanholas acerca dos riscos que advêm do ciberespaço;
- Adquirir e manter conhecimentos, capacidades, experiência e capacidades tecnológicas necessárias para que Espanha possa sustentar todos os objetivos da cibersegurança;
- Contribuir para o melhoramento da cibersegurança à escala internacional.

Com vista a alcançar todos estes objetivos este documento estabelece oito linhas de ação:

1. Capability to prevent, detect, respond to and recover from cyber threats;
2. Security of the Information and Telecommunications Systems that underpin the Public Authorities;

[27] *Ibidem*, p.16.
[28] Governo Espanhol, *op. cit.*, p.21.

3. Security of the Information and Telecommunications Systems that underpin Critical Structures;
4. Capability to investigate and prosecute cyber terrorism and cybercrime;
5. Security and resilience of ICT in the private sector;
6. Knowledge, skills and R&D&I;
7. Cyber security culture;
8. International commitment.[29]

Por forma a garantir que os 6 objetivos acima referidos são cumpridos foi elaborada uma organização específica no seio do Sistema de Segurança Nacional sob a direção do Primeiro-Ministro Espanhol, consistindo na criação do Conselho Nacional de Cibersegurança, do Comité Especializado em Cibersegurança e do Comité Situacional Especializado[30].

2.1.2. Conceito Inglês

Já em 2008 no Reino Unido, as problemáticas associadas aos conceitos de ciberespaço, cibersegurança e ciberataques encontravam-se na lista de preocupações do governo britânico, ainda não apresentando estas designações fonéticas sendo apenas referidos como ataques de origem não convencional, ou englobados em ataques a infraestruturas critícas, a sistemas elétricos e a redes de transportes. Em Março de 2009 foi publicado um estudo que denota a crescente preocupação com estas matérias *Cyberspace and the National Security of the United Kingdom,* estudo este que já contemplava uma proposta de uma estratégia ativa de cibersegurança[31]. Por forma a responder às ameaças do mundo virtual foi publicado em Novembro de 2011 a estratégia de cibersegurança do Reino Unido, *The UK Cyber Security Strategy.*

Este documento encontra-se divido em quatro capítulos abordando no primeiro o ciberespaço na sua generalidade focando o seu célere crescimento e o seu impacto na sociedade britânica, em termos de lazer e uso pessoal bem como de uso

[29] Governo Espanhol, *op cit.*, p.40.
[30] *Ibidem,* p.44.
[31] Paul Cornish, Rex Hughes e David Livingstone, *Cyberspace and the National Security of the United Kingdom*, Chatham House, Londres, 2009, p.24.

por parte de empresas e outros organismos como método de levar a cabo negócios[32]; no segundo debruça-se sobre as novas ameaças que este espaço possibilita e os efeitos nocivos que podem advir dos ciberataques a nível empresarial, social e individual, destacando a complexidade deste problema referindo a globalidade do ciberespaço, a multiplicidade de componentes materiais constituintes deste mesmo espaço e o acesso por parte de inúmeros indivíduos na sua produção, na difícil previsão das utilizações futuras do ciberespaço e as vulnerabilidades e riscos que possam surgir, finalizando com a rapidez dos ciberataques e a sua natureza *covert*[33]. No terceiro capítulo é designada a visão para a cibersegurança no Reino Unido definida como

> "…the UK in 2015 to derive huge economic and social value from a vibrant, resilient and secure cyberspace, where our actions, guided by our core values of liberty, fairness, transparency and the rule of law, enhance prosperity, national security and a strong society."[34]

Para tornar esta visão uma realidade foram definidos quatro objetivos:

- Enfrentar o cibercrime e tornar-se num dos sítios mais seguros no mundo para a condução de negócios no ciberespaço;
- Aumentar a resiliência face aos ciberataques e aumentar a capacidade de proteção dos seus interesses no ciberespaço;
- Ajudar a esculpir um ciberespaço estável, aberto e vibrante, que possa ser utilizado de forma segura e que suporte sociedades abertas;
- Adquirir o conhecimento, habilidades e capacidades transversais para sustentar os seus objetivos de cibersegurança.[35]

Tendo em consideração a sua visão e objetivos, o documento define a manutenção da segurança no ciberespaço como uma responsabilidade de todos, nomeadamente o setor privado, o governo e os cidadãos em particular, acentuando a

[32] *Ibidem*, pp.11 – 13.
[33] Paul Cornish, *op. cit.*, pp.15 – 19.
[34] *Ibidem,* p.21.
[35] *Ibidem*, p.21.

importância da aquisição de competências básicas de proteção individual contra ameaças *online*. No quarto capítulo são estabelecidas as linhas de ação para o cumprimento dos objetivos referidos anteriormente.

No enquadramento deste trabalho importa analisar o ponto que engloba a questão da cooperação internacional, defendendo que a utilização de força por parte das autoridades competentes deve ser proporcional, tendo em especial consideração os direitos humanos fundamentais como a liberdade de expressão e o direito de associação, fomenta ainda a organização de fóruns e debates entre os Estados membros das Nações Unidas, como qualquer outro que mostre interesse, com o objetivo de criar uma legislação única para os delitos que decorrem no ciberespaço, um exemplo deste esforço são as conferências iniciadas em 2011 em Londres[36].

2.1.3. Conceito Americano

Sendo os Estados Unidos da América considerados uma potencia económica e tecnológica à escala mundial importa também analisar o seu conceito estratégico no que à cibersegurança diz respeito, não só pela influência que este Estado exerce no resto do mundo mas também pela acrescida preocupação em termos de segurança e implementação de medidas para salvaguardar a mesma, quer a nível nacional quer internacional.

Este tema, que adquiriu uma elevada importância após os ataques terroristas de 11 de Setembro de 2001, dando azo à criação de várias alterações de foro legislativo e de estratégia nacional em diversos campos, sendo um deles precisamente o da cibersegurança que viu a criação de um conceito de estratégia nacional americano em Fevereiro de 2003 intitulado *THE NATIONAL STRATEGY TO SECURE CYBERSPACE*, documento este que resultou da criação de um programa de proteção e segurança dos sistemas informação de infraestruturas críticas autorizado pelo Presidente George W. Bush em 2001.

[36] Conferências alusivas ao tema ciberespaço, ocorrendo com uma periodicidade anual com a participação de governos, empresas e representantes da sociedade cvil.

No âmbito deste documento podemos encontrar uma divisão em dois capítulos principais, sendo apresentados no capítulo intitulado National Policy and Guiding Principles[37] os objetivos políticos nacionais e os princípios que devem seguir de guia por forma a tornar um espaço seguro e de uma crescente confiável utilização. Objetivos estes que são:

- Prevenir ciberataques às suas infraestruturas críticas;
- Reduzir as vulnerabilidades nacionais aos ciberataques;
- Minimizar os danos e o tempo de recuperação de ciberataques que ocorram.[38]

Para a conclusão destes objetivos foram definidos seis princípios gerais:

1. Agilização da cooperação a nível nacional entre todo o tipo de organizações, privadas, governamentais e não-governamentais, e os cidadãos comuns, sendo que estes últimos podem afetar a segurança nacional dependendo do acesso que estes possam ou não ter a matérias classificadas ou de interesse nacional[39];
2. Proteção da privacidade e da liberdade da sociedade civil, apontando como uma medida prioritária a criação de melhores politicas de privacidade[40];
3. Criação de mecanismos de regulação do ciberespaço por parte de empresas e corporações privadas por forma a auxiliar o governo[41];
4. Responsabilidade por parte do *Department of Homeland Security* de levar a cabo a maioria das iniciativas referidas nos seguintes capítulos do documento[42];
5. Existência de uma permanente flexibilidade face às ameaças do espaço virtual;
6. Execução de um planeamento plurianual, tanto para o governo como para as restantes organizações[43].

[37] Governo Norte-Americano, *THE NATIONAL STRATEGY TO SECURE CYBERSPACE*, Casa Branca, Washington, 2013, pp.13 – 17.
[38] Governo Norte-Americano, *op. cit.*, p.14.
[39] *Ibidem* p.14.
[40] *Ibidem*, pp.14-15.
[41] *Ibidem,* p.15.
[42] Iniciativas presentes no capítulo de título National Ciberspace Security Priorities, contemplado no documento *THE NATIONAL STRATEGY TO SECURE CYBERSPACE*.
[43] *Ibidem,* p.15.

Entrando no segundo capítulo intitulado *Natinal Cyberspace Security Priorities* que se subdivide em cinco prioridades:

1. Sistema Nacional de resposta à segurança no ciberespaço;
2. Programa nacional de redução de ameaças e vulnerabilidades da segurança no ciberespaço;
3. Programa nacional de treino e de consciencialização da segurança no ciberespaço;
4. Assegurar organizações governamentais no ciberespaço;
5. Cooperação entre a Segurança Nacional e a segurança do ciberespaço a nível internacional.

Integra-se de forma evidente na temática deste trabalho a quinta prioridade onde são propostas soluções para criar sinergias entre os países do continente americano, devido à sua proximidade e conexão forte com os Estados Unidos da América, e os restantes Estados à volta do globo. Destas propostas é importante destacar os conceitos de criar e desenvolver redes seguras a nível de organizações privadas por todo o mundo, por forma a consequentemente melhorar a segurança individual de todos os países, e estabelecer uma cooperação ativa entre estas entidades privadas e os governos dos países onde estas operam. De destacar ainda a sugestão da criação de redes Watch-and-Warning[44] para a prevenção de ciberataques, estabelecendo assim uma base de dados valiosa no que toca à avaliação e estudo dos eventos no ciberespaço bem como uma mais simples e célere capacidade de obtenção de soluções. No seguimento desta proposta foi criada a IWWN (International Watch and Warning Network) em 2004 contando com a participação de organizações de 15 países[45], não contando com a participação de Portugal.

Como nota de fecho é ainda feito um apelo a todas as nações para que façam uso das Convenções de Cibercrime do Conselho Europeu para o julgamento dos crimes no ciberespaço ou que assegurem que a sua legislação nacional proporcione uma

[44] Rede que visa estabelecer mecanismos de partilha de informação entre países.
[45] Austrália, Canadá, Finlândia, França, Alemanha, Hungria, Itália, Japão, Holanda, Nova Zelândia, Noruega, Suécia, Suíça, Reino Unido e Estados Unidos da América.

compreensão semelhante à prevista nos documentos de cariz internacional, por exemplo convenções e tratados internacionais.

2.2. Cibersegurança à luz da legislação Internacional

2.2.1. Uma análise sobre o Tratado da Convenção sobre o Cibercrime de 23 de Novembro de 2001

Por forma a fazer frente às ameaças no ciberespaço o Conselho da Europa[46] reuniu um Comité de indivíduos especializados neste campo, por forma a definir novos crimes, visto que muita da legislação anterior não contemplava crimes no espaço cibernético, estabelecer um procedimento geral de resolução para estes últimos, endereçar o problema da jurisdição e da cooperação internacional, tanto nos casos de prestação de ajuda na resolução de problemas como nos casos de extradição.

Concluído e aprovado em Novembro de 2001, o Tratado da Convenção sobre o Cibercrime foi apresentado para assinatura e ratificação aos 47 Estados membros, bem como a outros Estados presentes com o estatuto de observadores, entre os quais Estados Unidos da América, Japão, África do Sul e Canadá, de todos os presentes apenas 27 membros assinaram o tratado, enquanto do lado dos observadores todos assinaram. Foi ainda acrescentado um protocolo adicional ao tratado em Janeiro de 2003[47] com o intuito de abordar as questões de natureza racista e xenófobas no ciberespaço. Até à data foi assinada por 45 Estados membros e ratificada por 40 dos mesmos, 8 Estados não constituintes do Conselho da Europa também procederam à ratificação, de destacar a não assinatura e ratificação de apenas dois Estados membros, Rússia e São Marinho. Este tratado entrou em vigor a dia 01 de Julho de 2004 após ser ratificado por 5 países, dos quais 3 são Estados membros do Conselho de Europa[48].

[46] Organização intergovernamental fundada em 1949 com o principal objetivo de salvaguardar os direitos fundamentais e promover uma ação conjunta dos Estados que a compõem, sendo estes 47 onde Portugal se inclui.

[47] Council of Europe, *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems*, Estrasburgo, 2003.

[48] Council of Europe, http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185, acedido em Março de 2016.

O presente texto apresenta 48 artigos distribuídos por 4 capítulos que se subdividem em diferentes secções, sendo que o primeiro capítulo apresenta definições essenciais para a compreensão e análise do documento, o segundo contempla um conjunto de medidas que devem ser levadas a cabo a nível nacional pelos Estados que tenham assinado o Tratado, o terceiro foca-se na cooperação internacional e por fim o quarto capítulo que consiste nas considerações finais.

2.2.1.1. Empenhamento a nível nacional, questões de direito penal, direito processual e jurisdição

A Convenção começa no seu artigo 1º por definir conceitos que são essenciais à compreensão da problemática por ele abordada:

- "**computer system** - means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;"
- "**computer data** - means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;"
- "**service provider**:
  - any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and
  - any other entity that processes or stores computer data on behalf of such communication service or users of such service;"
- "**traffic data** - means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service."[49]

A definição destes conceitos base permite assim a compreensão dos termos estabelecidos na definição das condutas passíveis de serem considerados crimes cibernéticos, que de acordo com a presente convenção são 9:

[49]Council of Europe, *CONVENTION ON CYBERCRIME*, Budapeste, 2001, art.1º.

1. Acesso ilegal;
2. Interceção ilegal;
3. Interferência de dados;
4. Interferência de sistemas;
5. Uso indevido de dispositivos;
6. Falsficação informática;
7. Fraude informática;
8. Crimes relacionados com pornografia infantil;
9. Violações de direitos de autor e de direitos anexos.[50]

Para que estes atos sejam declarados cibercrimes é sempre necessário provar que o sujeito que as pratique apresenta uma intencionalidade de causar danos à entidade que sofre o ataque, ou seja é necessário que exista dolo por parte do executante. O dolo que segundo Eduardo Correia é dividido em dois elementos essenciais: o elemento intelectual e o emocional[51], sendo que o primeiro consiste no conhecimento do tipo legal de crime que o sujeito visa praticar[52], e o segundo no fato de o sujeito querer o resultado da sua ação criminosa[53]. Deste princípio surge uma das maiores dificuldades da ação do direito penal, provar que o sujeito acusado de determinada ação típica a praticou conscientemente, tendo em consideração as consequências decorrentes do mesmo, sendo que estas mesmas consequências podem ou não representar o objetivo do sujeito.

Este mesmo problema verifica-se também no cumprimento do artigo 11º desta convenção que define o auxílio de terceiros nas práticas acima referidas ou a cumplicidade dos mesmos como atos passíveis de serem sancionados[54], acrescendo a pertinência da questão do dolo nestes casos, pelo que o executante de ações

[50] Council of Europe, *CONVENTION ON CYBERCRIME*, Budapeste, 2001, art.2º.
[51] Eduardo Correia, *Direito Criminal Volume I,* Edições Almedina, Coimbra, 1996, p.367.
[52] *Ibidem*, p.368.
[53] *Ibidem,* p.376.
[54] Council of Europe, *CONVENTION ON CYBERCRIME*, Budapeste, 2001, art.11º, "Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed.".

criminosas no ciberespaço poderá fazer uso de equipamentos informáticos pertencentes a outrem sem que estes últimos tenham conhecimento da situação, ou no caso contrário, em que estes tenham conhecimento da situação, é passível que estes invoquem a sua ignorância no ocorrido numa tentativa de iludirem as normas legais em vigor.

Ao prever a existência de crimes no ciberespaço os órgãos competentes, sejam estes os órgãos policiais de investigação ou os órgãos judiciais, deparam-se com um problema bem conhecido que é a identificação de suspeitos supramencionados, no entanto, num espaço de dimensão imensurável e com novos *modi operandorum* constantemente mutáveis. Esta dificuldade resulta do fato de a internet ter sido originalmente criada como uma rede desenvolvida pelos Estados Unidos da América com o objetivo de melhorar o fluxo de informação entre os órgãos de defesa do Estado, sendo que a anonimidade dos constituintes dessa rede não era de nenhuma forma vista como um problema mas sim como uma vantagem[55]. Ninguém conseguiria prever porém o exponencial crescimento do uso da Internet e com o passar do tempo essa capacidade de permanecer anonimo na rede passou a ser uma oportunidade para os cibercriminosos levarem a cabo os seus delitos sem que fossem identificados.

Foram já criadas iniciativas com o fim de solucionar estas adversidades criadas pela facilidade de anonimato e de falta de dolo, sendo um destes exemplos a diretiva 2006/24/EC do Conselho Europeu adotada a 15 de Março de 2006. Esta diretiva tem como objetivo a regulamentação do acesso à informação necessária à instauração de processos de crimes graves, definindo a obrigatoriedade de retenção de dados[56] e que esta deve ser apenas fornecida a autoridades nacionais com o objetivo de facilitar a investigação[57], bem como estabelece também o tipo de informação passível de ser retida por parte das entidades, por forma a facilitar a identificação de suspeitos envolvidos em atos criminosos não colocando em xeque os seus direitos humanos,

[55] Eneken Tikk, *Comprehensive legal approach to cyber security*, Tartu University Press, Estónia, 2011.
[56] Council of Europe, *DIRECTIVE 2006/24/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC*, promulgada a 15 de Março de 2006, art.3º.
[57] *Ibidem,* art.4º.

nomeadamente os consagrados nos artigos 3º[58] e 12º[59] da Declaração Universal dos Direitos Humanos.

Mais um caso é o projeto Domain Name System Security Extensions (DNSSEC)[60] anunciado a 28 de Julho de 2010 pela Corporação da Internet para Atribuição de Nomes e Números (ICANN), neste caso foram tomadas medidas para melhorar a segurança no que toca ao Domain Name System[61], tendo como principal objetivo prevenir dois tipos de cibercrimes o cache poisoning e os ataques man-in-the-middle[62], através do redireccionamento correto de um utilizador para uma página de internet específica[63]. O primeiro como o nome indica consiste no "envenenamento" da cache[64] de um dispositivo, levando a uma possível infeção do dito dispositivo através de vírus, *trojan horses* ou *spyware*, podendo assim resultar na obtenção por parte de terceiros de informação sensível ou pessoal e por conseguinte a crimes de fraude, prescritos no art.8º da Convenção de Budapeste. Um simples mas problemático exemplo da situação acima descrita é a obtenção de dados de acesso a serviços bancários *online*. O segundo caso, man-in-the-middle, consiste na interceção de comunicações entre dois sujeitos em que o criminoso se faz passar por um deles continuando a comunicar com o outro, situação em que o exemplo supramencionado também se aplica, sendo que neste panorama o criminoso não necessita de proceder à aquisição de dados visto que pode interceder após a vítima ter fornecido os mesmos.

[58] "Todo indivíduo tem direito à vida, à liberdade e à segurança pessoal". United Nations Information Centre, *Universal Declaration of Human Rights*, Bélgica, 1948, art.3º.
[59] "Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a protecção da lei". *Ibidem*, art.12º.
[60] Anúncio do projeto DNSSEC, *Global Upgrade Makes Internet More Secure,* http://www.prweb.com/releases/DNSSEC/Cyber_Crime/prweb4321774.htm, visitado em Janeiro de 2016.
[61] Sistema de nomeação de sistemas que tem como objetivo interligar todos os dispositivos que estejam conectados à internet ou a qualquer rede privada, basicamente opera atribuindo um "nome" a cada dispositivo de forma a este ser identificável na rede, atribuindo caraterísticas especificas a esse dispositivo dependo das suas funcionalidades, da sua estrutura de dados, i.e. os endereços IP. Miguel Andrade, *NOMES DE DOMÍNIO NA INTERNET: A regulamentação dos nomes de domínio sob .pt.*,Centro Atlântico, Famalicão, 2004.
[62] *Supranota* 59.
[63] *Ibidem.*
[64] A memória cache consiste num componente que armazena dados por forma a acelerar o processo de resposta de um dispositivo aquando da solicitação de dados anteriormente utilizados.

Ainda no capítulo segundo da convenção é abordada no seu 22º artigo a situação da jurisdição, referindo que cada Estado deve adotar medidas legislativas por forma a estabelecer jurisdição face aos crimes acima referidos[65] quando eles sejam praticados:

- No seu território;
- A bordo de qualquer embarcação que ostente a sua bandeira;
- A bordo de qualquer aeronave registada nesse Estado;
- Por qualquer indivíduo da sua nacionalidade, no caso de a ação em questão for punível pelo direito criminal do Estado onde se encontra ou se a ação for cometida fora da jurisdição territorial de qualquer Estado.[66]

A questão da jurisdição nos crimes ocorridos no ciberespaço adquire contornos de dificuldade acrescida em comparação com os crimes do mundo real, se assim podem ser referidos, pois como Johnson e Post defendem, o ciberespaço usufrui de uma ausência de fronteiras no sentido convencional da palavra[67], dificultando assim a tarefa dos Estados em estabelecer a jurisdição supramencionada assentando fortemente, como defende Cox, na cooperação internacional[68], cooperação esta que também se encontra contemplada na convenção em análise e que será seguidamente referida.

2.2.1.2. O desafio da Cooperação Internacional

> "Cooperation may take various forms. Consulting, information exchange, relocation of resources or supporting services under attack all can be considered potential ways to implement this rule. The international legal framework for cooperation needs to be supported by national provisions for

[65] Crimes contemplados nos artigos 2º ao 11º da seguinte convenção, Council of Europe, *CONVENTION ON CYBERCRIME*, Budapeste, 2001.
[66] Council of Europe, *CONVENTION ON CYBERCRIME*, Budapeste, 2001, art.22º.
[67] David Johnson, David Post, *Law and Borders – the Rise of Law in Cyberspace*, Stanford Law Review 1367, 1996. Disponível para consulta em https://cyber.law.harvard.edu/is02/readings/johnson-post.html.
[68] Noel Cox, *The regulation of cyberspace and the loss of national sovereignty*, Auckland University of Technology, Reino Unido, 2002.

> Internet service provider cooperation, data exchange and partnerships as well as international coalition agreements."[69]

Os princípios acima referenciados por Tikk vão de encontro com os definidos no capítulo terceiro da Convenção de Budapeste, que contempla o processo de extradição passando pelos princípios gerais de assistência mútua e o acesso e partilha de dados. A cooperação internacional compele-se de elevada importância no caso da segurança no ciberespaço, fato este já constatado pela NATO.

> "Full complementarity between NATO and the EU will be essential if the Allies are to forge a comprehensive and cost-effective approach to security when both are involved in a stabilisation mission. Better cooperation can also be helpful in addressing unconventional threats such as terrorism, cyber-attacks, and energy vulnerabilities."[70]

Tendo estas preocupações em consideração a convenção em análise apela à cooperação entre quaisquer partes no contexto de investigações criminais no ciberespaço[71], permitindo assim uma melhor transferência de informação preponderante para a resolução de ocorrências que decorram no ciberespaço, fomentando assim uma maior uniformização na condução dos processos tanto de investigação como prossecução de cibercrimes, uma preocupação já denotada pelo Departamento de Defesa dos Estados Unidos em 1999 afirmando que enquanto não existir uma forte e uniforme legislação aplicável aos crimes no ciberespaço, todos os Estados se encontram igualmente vulneráveis apesar das suas leis internas.[72]

A extradição[73] no panorama do mundo cibernético apresenta um desafio face á presente lacuna legislativa que se verifica em vários países como supramencionado,

[69] Eneken Tikk, *Comprehensive legal approach to cyber security*, Tartu University Press, Estónia, 2011, p.108.
[70] NATO, *Analysis and Recommendations of the Group of Experts on a New Strategic Concept for NATO*, 17 Maio 2010.
[71] Council of Europe, *CONVENTION ON CYBERCRIME*, Budapeste, 2001, art.23º.
[72] Departamento de Defesa dos Estados Unidos da América, *An Assessment of International Legal Issues In Information Operations*, Washington, Estados Unidos da América, Maio de 1999.
[73] Eduardo Correia, *Direito Criminal Volume I,* Edições Almedina, Coimbra, 1996, p.183, "…o facto pelo qual um Governo remete um indivíduo que se refugiou no seu território ao Governo de um outro Estado

sendo que a presente convenção define no seu artigo 24º que a extradição de um indivíduo só poderá ser levada a cabo caso o mesmo tenha praticado um dos atos criminais descritos dos artigos 2º a 11º, e que estas ofensas sejam puníveis por ambas as partes com a pena de privação de liberdade com uma duração mínima de um ano.[74] Indo ao encontro do que foi referido no parágrafo anterior, a uniformização de legislação interna tem consequências não só na defesa dos interesses dos Estados, por permitir a detenção de cibercriminosos, que através do que foi anteriormente referido neste subcapítulo veem assim acrescentado aos problemas da sua deteção e identificação e à prova da execução da ação com dolo, uma impunibilidade da qual usufruem em determinadas regiões do globo, e da qual se se verificar uma inexistência de tratados de extradição com outras partes[75], lhes concede assim inúmeras possibilidades de ataque a indivíduos singulares ou coletivos em qualquer lugar do mesmo.

2.3. Conclusões

Face à constante ameaça de crimes no ciberespaço e à assinatura da convenção de Budapeste por parte de vários Estados, tem-se vindo a verificar uma crescente criação de legislação a nível nacional bem como revisão das legislações existentes por parte dos mesmos.

Este fato é comprovado pela alteração dos artigos 197º, 248º, 256º, 264º, 270º e 273º do código penal espanhol[76], alterados pelas leis orgânicas 15/2003 de 25 de Novembro, 5/2010 de 22 de Junho e 1/2015 de 30 de Março, aplicando os princípios legais existentes aos crimes levados a cabo com sistemas de informação e comunicação, bem como a criação do corpo de investigação criminal Brigada de Investigación Tecnológica.

para que ele aí seja julgado pelos respetivos tribunais, ou quando aí já tenha sido julgado, para cumprir a pena que lhe foi aplicada.".

[74] Council of Europe, *CONVENTION ON CYBERCRIME*, Budapeste, 2001, art.24º, ponto 1.

[75] *Ibidem*, art.24º.

[76] Ministério da Justiça Espanhol, *Código Penal y legislación complementaria*, Agencia Estatal Boletín Oficial del Estado, Madrid, 21 de Janeiro de 2016.

Mais a norte o Reino Unido tem também vindo a levar a cabo esforços para cumprir com as diretivas europeias referenciadas na Convenção de Budapeste, através das revisões contempladas no Police and Justice Act de2006[77] ao Computer Misuse Act de 1990[78], habilitando assim com mais ferramentas jurídicas o seu corpo de investigação o National Cyber Crime Unit, corpo que se encontra integrado na National Crime Agency, agência criada em Outubro de 2013 com o objetivo de combater o crime organizado e o cibercrime, através da cooperação entre forças policiais e outras agências de toda a parte do globo[79].

Do outro lado do Atlântico no continente Norte-Americano foram da mesma forma reforçados os conceitos jurídicos relativos ao cibercrime com a introdução de novos crimes e uma nova contextualização de delitos já referidos na legislação anterior[80], e também à semelhança dos países acima referidos criou um ramo especializado dentro do corpo do Federal Bureau of Investigation (FBI), denominado FBI's Cyber Division[81] em 2003 com os objetivos de auxiliar as investigações do FBI, melhorar o treino e educação dos seus membros no que concerne à resposta a ameaças no ciberespaço através de alianças com organismos públicos e privados, e capacitar o FBI para que este se encontre na vanguarda das investigações no ciberespaço através da exploração de novas tecnologias[82].

Como referido em todos os conceitos estratégicos acima analisados conclui-se que uma das maiores e mais preponderante caraterística dos crimes no ciberespaço é a inexistência de fronteiras físicas, sendo coerentes na importância da cooperação internacional para a prossecução de cibercrimes. Mas apesar da elaboração do Tratado de Budapeste, tratado este que como defende Akehurst e imposto pelo Estatuto do

[77] Parlamento do Reino Unido, *Police and Justice Act 2006*, Londres, 8 de Novembro de 2006, disponível em http://www.legislation.gov.uk/ukpga/2006/48/pdfs/ukpga_20060048_en.pdf.
[78] Parlamento do Reino Unido, *Computer Misuse Act 1990*, Londres, 29 de Agosto de 1990, disponível em http://www.legislation.gov.uk/ukpga/1990/18/pdfs/ukpga_19900018_en.pdf.
[79] Página oficial da National Crime Agency, http://www.nationalcrimeagency.gov.uk/about-us/working-in-partnership, visitada a 10 de Março de 2016.
[80] Podem ser consultados no documento *CYBERCRIME LAWS OF THE UNITED STATES*, disponível em https://www.oas.org/juridico/spanish/us_cyb_laws.pdf, visitado em 2 de Fevereiro de 2016.
[81] Jana D. Monroe, *Before House Judiciary Committee, Subcommittee on Courts, the Internet and Intellectual Property*, Washington DC, Estados Unidos da América, 17 de Julho de 2003, disponivel em https://www.fbi.gov/news/testimony/the-fbis-cyber-division.
[82] *Ibidem,* p.14.

Tribunal Internacional de Justiça[83], é uma fonte de Direito Internacional à qual os países que a assinam e ratificam se comprometem a cumprir. No panorama Europeu constata-se que a maioria dos seus Estados assinaram o tratado e estão progressivamente a melhorar as suas capacidades de resposta a ameaças no mundo cibernético, com a elaboração de legislação atualizada e com a criação de organismos de investigação e prossecução de cibercrimes, como foi supramencionado. Por outro lado existem também Estados que não tendo assinado a convenção não estão a atualizar o seu quadro legal o que permite que os cibercriminosos se aproveitem desta vantagem para atacar terceiros. Face a isto devem ser efetuados esforços para que seja fomentada cada vez mais uma eficiente cooperação entre Estados, não só a nível político mas também ao nível das organizações de foro privado, como é defendido por Tikk[84].

[83] Michael Akehurst, *Introdução ao Direito Internacional*, Almedina, Coimbra, 1985.
[84] Eneken Tikk, *Comprehensive legal approach to cyber security*, Tartu University Press, Estónia, 2011.

3. A Cibersegurança em Portugal, conceito estratégico e legislação Lusitana

Foi em 1973 como defendem António Martins *et all* através da entrada em vigor da Lei n.º 2/73, de 10 de Fevereiro[85], que é criado o registo nacional de identificação com o objetivo de garantir a salvaguarda da confidencialidade dos dados individuais de cada um e a responsabilização de quem quebra essa confidencialidade. Na mesma década, em 1976, constava do artigo 35º da Constituição da República Portuguesa (CRP) a proibição de uso da informática para tratamento de dados de cariz privado, i.e. convicções políticas, religiosas e ainda, adicionadas em 1982, as convicções filosóficas, a filiação partidária ou sindical e em 1997 a origem étnica.[86] Mas foi em 1991 que foi promulgada a Lei da Criminalidade Informática, documento que legislava os crimes utilizando as tecnologias de informação e comunicação, no entanto com a participação e posterior assinatura do Tratado da Convenção de Budapeste por parte de Portugal a 23 de Novembro de 2001, procedeu-se a uma revisão da referida Lei tendo esta sido revogada pela Lei nº 109/2009 Lei do Cibercrime.

Conclui-se portanto que a legislação em Portugal referente a questões de cibersegurança tem vindo a evoluir por forma a fazer frente aos desafios que se impõem nos dias de hoje. Neste capítulo serão analisados dois documentos: um de cariz político-estratégico, a Estratégia Nacional de Cibersegurança, e outro de cariz legislativo, a Lei nº109/2009 Lei do Cibercrime. Tendo como objetivo a aferição do cumprimento das medidas a implementar estipuladas pela convenção de Budapeste, ratificada por Portugal a 24 de Março de 2010, referindo ainda a criação e o papel do Centro Nacional de Cibersegurança no combate aos cibercrimes, organismo definido pela Estratégia Nacional da Segurança no Ciberespaço como autoridade nacional nas questões relacionadas com o ciberespaço.

[85] António Gomes Lourenço Martins *et all*, *CYBERLAW EM PORTUGAL. O direito das tecnologias da informação e comunicação,* Centro Atlântico, Famalicão, 2004, p.425.
[86] *Ibidem*, p.426.

3.1. Estratégia Nacional de Cibersegurança

Aprovada a 12 de Junho de 2015 através da Resolução do Conselho de Ministros n.º36/2015, a Estratégia Nacional de Segurança do Ciberespaço foi elaborada com o objetivo de adereçar os novos desafios criados pela evolução tecnológica e consequente dependência das tecnologias da informação por parte dos sistemas que asseguram o normal funcionamento do Estado Português[87].Apesar da maior eficácia e rapidez ganha neste processo surge também uma potencial vulnerabilidade na segurança, por exemplo, dos dados de todos os cidadãos portugueses, como tal é revestida de uma preocupação mais premente a questão da segurança no ciberespaço em Portugal. Preocupação essa que foi respondida pela elaboração da Estratégia Nacional de Segurança do Ciberespaço que apresenta como principais objetivos o aprofundamento da segurança das redes e da informação por forma a permitir uma segura utilização do ciberespaço por parte dos cidadãos, das empresas e das entidades públicas e privadas.[88]

Com o cumprimento deste comprometimento em mente, o documento acima referido estabelece quatro objetivos estratégicos:

1. Promover uma utilização consciente, livre, segura e eficiente do ciberespaço;
2. Proteger os direitos fundamentais, a liberdade de expressão, os dados pessoais e a privacidade dos cidadãos;
3. Fortalecer e garantir a segurança do ciberespaço, das infraestruturas críticas e dos serviços vitais nacionais;
4. Afirmar o ciberespaço como um domínio de desenvolvimento económico e de inovação.[89]

Para alcançar os objetivos acima referidos são definidos seis principais eixos de intervenção: a estrutura de segurança no ciberespaço, o combate ao cibercrime, a

[87] Um dos exemplos mais recentes da utilização das novas tecnologias em matérias de gestão do Estado, e que afeta todos os cidadãos, é a subscrição de todas as declarações de IRS através da internet.
[88] Conselho de Ministros, *ESTRATÉGIA NACIONAL DE SEGURANÇA NO CIBERESPAÇO*, aprovada pela Resolução do Conselho de Ministros n.º36/2015 em 12 de Junho de 2015, Lisboa, p.3738.
[89] *Ibidem,* p.3739.

proteção do ciberespaço e das infraestruturas, educação, sensibilização e prevenção, investigação e desenvolvimento e por fim a cooperação. No seu primeiro eixo denominado *estrutura de segurança no ciberespaço* o documento apela à existência de uma coordenação político-estratégica na dependência do Primeiro-Ministro, visto que são vários os intervenientes que concorrem para a segurança no ciberespaço, esta coordenação é supervisionada pelo Governo, sendo que todas as partes, sejam elas instituições públicas ou privadas, deverão fazer os possíveis para alcançar os objetivos definidos na Estratégia Nacional. Ainda no âmbito deste primeiro eixo o presente diploma defende uma maior consolidação do Centro Nacional de Cibersegurança como coordenador operacional e de autoridade nacional em matéria de cibersegurança no que se refere a entidades públicas e infraestruturas críticas, apoiando também entidades privadas sempre que possível e solicitado, um desenvolvimento da capacidade de Ciberdefesa Nacional, desenvolvimento da sua capacidade de resposta a incidentes e o estabelecimento de um gabinete para gestão de crises no ciberespaço[90]. O papel do Centro na cibersegurança nacional bem como as capacidades de Ciberdefesa em Portugal serão explorados em maior pormenor no capítulo seguinte.

Avançando para o segundo eixo definido pela Estratégia Nacional de Segurança no Ciberespaço que se refere ao *combate ao cibercrime*, no sentido de agilizar a repressão a estes incidentes é referido como essencial uma constante revisão e atualização da legislação, não só da Lei do Cibercrime, documento que será analisado pormenorizadamente mais à frente, mas também da legislação que suporta a investigação criminal para que esta seja aplicável ao espaço virtual. O documento apela ainda para uma melhoria das estruturas e capacidades técnicas, humanas e tecnológicas por parte da Polícia Judiciária.[91] Define ainda três outros eixos fundamentais presentes também nas anteriores estratégias nacionais analisadas no capítulo segundo deste trabalho, *a proteção do ciberespaço e das infraestruturas*, a *educação e sensibilização* de todos em relação às possibilidades e os perigos

[90] Conselho de Ministros, *ESTRATÉGIA NACIONAL DE SEGURANÇA NO CIBERESPAÇO*, aprovada pela Resolução do Conselho de Ministros n.º36/2015 em 12 de Junho de 2015, Lisboa, p.3739.
[91] *Ibidem,* p.3740.

associados ao uso do ciberespaço por forma a promover uma melhor utilização do mesmo, fomenta ainda a *investigação e desenvolvimento* nesta área, comprometendo-se a auxiliar todas as instituições, tanto públicas como privadas, entidades de investigação e academia. Como último eixo é referida a cooperação nacional e internacional, reconhecendo que esta problemática não pode ser abordada por qualquer Estado individualmente, reforçando os mecanismos de cooperação com a União Europeia e a NATO através da participação e organização de exercícios de segurança e defesa no espaço virtual, e da partilha de conhecimentos através da organização de convenções e *fora* subordinados a esta problemática.[92]

É ainda realçada a importância da Computer Security Incident Response Team, definida por Robin Ruefle como sendo uma "concrete organizational entity (…) that is assigned the responsibility of providing part of the incident management capability for a particular organization"[93], cujo principal objetivo é o de minimizar e controlar danos resultantes de incidentes no ciberespaço. No entanto apresenta-se também como uma fonte valiosa na análise de padrões de ameaças e ataques, da suscetibilidade dos alvos e das fraquezas e resistências de infraestruturas críticas[94].

Em Portugal existe desde 2002 um organismo que atuou como Computer Emergency Response Team (CERT) a nível nacional, o CERT.PT, no entanto com a criação do Centro Nacional de Cibersegurança em 2014 foi a este último que ficaram incumbidas as funções de coordenação nacional de resposta a incidentes no ciberespaço, tendo o CERT.PT passado a denominar-se CERT RCTS, focando-se apenas à Rede Ciência, Tecnologia e Sociedade, tutelados pelo Mnistério da Educação e Ciência[95]. A 21 de Janeiro de 2008 foi formada a rede nacional de Computer Security Incident Response Team (CSIRT), que conta agora com 23 membros.

[92] Conselho de Ministros, *ESTRATÉGIA NACIONAL DE SEGURANÇA NO CIBERESPAÇO*, aprovada pela Resolução do Conselho de Ministros n.º36/2015 em 12 de Junho de 2015, Lisboa, p.3740 - 3742.
[93] Ruefle, Robin, *Defining Computer Security Incident Response Teams*, Estados Unidos da América, 24 de Janeiro de 2007, disponível em https://buildsecurityin.us-cert.gov/articles/best-practices/incident-management/defining-computer-security-incident-response-teams.
[94] *Ibidem.*
[95] Site Oficial do CERTRCTS, http://fe02.cert.pt/.

3.2. Panorama legislativo do espaço informático a nível nacional

Desde 1974 que a utilização de meios informáticos está contemplada na legislação nacional através do artigo 35º da CRP que rege a utilização da informática, porém com o passar do tempo verificou-se a desatualização do referido preceito e apesar das alterações de 1982, 1989 e 1997, este prova ser insuficiente para a proteção dos utilizadores, levando assim à adoção dos princípios definidos neste artigo para outros documentos legais, como o Código Penal, no qual estão previstos crimes praticados por meio informático nos seus artigo 193º[96], 194º[97] e 221º[98].

Apesar destas adições ao Código Penal Português o direito nacional continuava a carecer de diplomas que abordassem de maneira eficaz e suficiente a criminalidade informática, como tal foi aprovada em 1991 a Lei 109/91, de 17 de Agosto, a Lei da Criminalidade Informática, que contempla de uma forma mais abrangente as questões criminais ocorridas no seio do ciberespaço fazendo cumprir o direitos previstos na CRP, especificando seis tipos de crimes ligados à informática:

- Falsidade informática;
- Dano relativo a dados ou programas informáticos;
- Sabotagem informática;
- Acesso ilegítimo;
- Interceção ilegítima;
- Reprodução ilegítima de programa protegido.[99]

Com a assinatura e posterior ratificação da Convenção de Budapeste, supramencionada, Portugal procedeu a uma revisão da sua Lei da Criminalidade Informática para que todos os pressupostos exigidos pela Convenção fossem contemplados no seu foro legislativo, como tal foi aprovada pela Lei nº109/2009, de 15 de Setembro, a Lei do Cibercrime.

[96] Artigo 193º - Devassa por meio de informática.
[97] Artigo 194º - Violação de correspondência ou de telecomunicações.
[98] Artigo 221º - Burla informática e nas comunicações.
[99] Artigos 4º a 9º, Lei nº 109/1991, de 17 de Agosto de 1991.

3.2.1. Lei do Cibercrime

Promulgada a 15 de Setembro de 2009, a Lei do Cibercrime apresenta-se com o principal objetivo de adaptar o Direito Português às condições impostas pela Convenção sobre Cibercrime, estabelecendo as disposições penais materiais, processuais e disposições relativas à cooperação internacional em matéria penal relativas ao cibercrime bem como a recolha de provas em suporte eletrónico.[100] No seu artigo 2º são introduzidas na ordem jurídica interna os conceitos referidos na Convenção de Budapeste, são estes[101]:

- "**Sistema informático** - qualquer dispositivo ou conjunto de dispositivos interligados ou associados, em que um ou mais de entre eles desenvolve, em execução de um programa, o tratamento automatizado de dados informáticos, bem como a rede que suporta a comunicação entre eles e o conjunto de dados informáticos armazenados, tratados, recuperados ou transmitidos por aquele ou aqueles dispositivos, tendo em vista o seu funcionamento, utilização, protecção e manutenção;"
- "**Dados informáticos** - qualquer representação de factos, informações ou conceitos sob uma forma susceptível de processamento num sistema informático, incluindo os programas aptos a fazerem um sistema informático executar uma função;"
- "**Dados de tráfego** - os dados informáticos relacionados com uma comunicação efectuada por meio de um sistema informático, gerados por este sistema como elemento de uma cadeia de comunicação, indicando a origem da comunicação, o destino, o trajecto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente;"
- "**Fornecedor de serviço** - qualquer entidade, pública ou privada, que faculte aos utilizadores dos seus serviços a possibilidade de comunicar por meio de um sistema informático, bem como qualquer outra entidade que trate ou

[100] Artigo 1º, Lei nº 109/2009, de 15 de Setembro de 2009.
[101] Artigo 2º, Lei nº 109/2009, de 15 de Setembro de 2009.

armazene dados informáticos em nome e por conta daquela entidade fornecedora de serviço ou dos respectivos utilizadores;"

- "**Intercepção** - o acto destinado a captar informações contidas num sistema informático, através de dispositivos electromagnéticos, acústicos, mecânicos ou outros;"
- "**Topografia** - uma série de imagens ligadas entre si, independentemente do modo como são fixadas ou codificadas, que representam a configuração tridimensional das camadas que compõem um produto semicondutor e na qual cada imagem reproduz o desenho, ou parte dele, de uma superfície do produto semicondutor, independentemente da fase do respectivo fabrico;"
- "**Produto semicondutor** - a forma final ou intermédia de qualquer produto, composto por um substrato que inclua uma camada de material semicondutor e constituído por uma ou várias camadas de matérias condutoras, isolantes ou semicondutoras, segundo uma disposição conforme a uma configuração tridimensional e destinada a cumprir, exclusivamente ou não, uma função electrónica."

Estes conceitos vêm ampliar o espetro de atividades passíveis de serem punidas por lei em Portugal.

No seguimento do enquadramento do Direito Português com os pressupostos definidos pela Convenção de Budapeste a Lei do Cibercrime define as seguintes disposições materiais:

- Artigo 3º - Falsidade informática;
- Artigo 4º - Dano relativo a programas ou outros dados informáticos;
- Artigo 5º - Sabotagem informática;
- Artigo 6º - Acesso ilegítimo;
- Artigo 7º - Interceção ilegítima;
- Artigo 8º - Reprodução ilegítima de programa protegido.

Os crimes relativos a pornografia infantil, referenciados na Convenção sobre o Cibercrime, não são contemplados neste diploma visto que se encontram legislados

pelo Código Penal Português na alínea c) do artigo 176º, *Pornografia de menores*, introduzido após a alteração imposta pela Lei nº59/2007 de 4 de Setembro de 2007, que afirma que quem "produzir, distribuir, importar, exportar, divulgar, exibir ou ceder, a qualquer título ou por qualquer meio"[102], fotografias, filmes ou gravações pornográficas é punido com pena de prisão de 1 a 5 anos. Abrangendo assim, os crimes relacionados a pornografia infantil no ciberespaço.

3.2.1.1. Falsidade informática

O art. 3º define o delito de falsidade informática como a

> "intenção de provocar engano nas relações jurídicas, introduzir, modificar, apagar ou suprimir dados informáticos ou por qualquer outra forma interferir num tratamento informático de dados, produzindo dados ou documentos não genuínos, com a intenção de que estes sejam considerados ou utilizados para finalidades juridicamente relevantes como se o fossem"[103]

sendo este ato punível com uma pena até 5 anos de prisão ou multa de 120 a 600 dias. Esta situação é agravada de acordo com os números 2 e 4 do artigo 3º, que afirmam que quando as ações acima referidas afetarem dados registados ou incorporados em cartão bancário de pagamento ou qualquer dispositivo que permita acesso a sistemas de pagamento ou a importação, distribuição, venda ou detenção para fins comerciais de dispositivos que permitam acesso aos dados referidos, devem ser punidos com uma pena de prisão de 1 a 5 anos. Este artigo declara ainda que caso os fatos referidos nos anteriores números sejam praticados por um sujeito no exercício das suas funções, este será punido com 2 a 5 anos de prisão.

No número 3 deste artigo é definido que ações conduzidas com o intuito de "causar prejuízo a outrem ou de obter um benefício ilegítimo, para si ou para terceiro", apesar de executadas com dolo específico devem ser punidas de acordo com o definido nos números anteriores do mesmo artigo.

[102] *Código Penal*, Portugal, art.176º, alínea c).
[103] Artigo 3º, Lei nº 109/2009, de 15 de Setembro de 2009.

Ao analisar este artigo constata-se que mais uma vez que o conceito de dolo assume relevância na acusação do sujeito que pratica a ação, ao existir a necessidade de provar a intenção do mesmo, sendo neste caso um dolo específico, "a intenção de provocar engano nas relações jurídicas", este dolo permite-nos diferenciar o crime previsto neste artigo do definido no art. 4º do mesmo documento, que prevê o crime de dano relativo a programas ou outros dados informáticos, visto que ambos contemplam a introdução e destruição de dados informáticos[104].

O disposto neste artigo pretende assim garantir a segurança dos dados informáticos e de tráfego dos utilizadores do ciberespaço, bem como prevenir que estes mesmos dados possam ser utilizados com o propósito de defraudar o sistema jurídico, seja para proveito do próprio infrator ou para prejuízo de terceiros[105].

3.2.1.2. Dano relativo a programas ou outros dados informáticos

Como referido no parágrafo anterior o artigo 4º deste diploma especifica o quadro jurídico relativo ao crime de danos relativos a programas ou outros dados informáticos, que é tipificado no seu nº 1 do seguinte modo:

> "Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, apagar, alterar, destruir, no todo ou em parte, danificar, suprimir ou tornar não utilizáveis ou não acessíveis programas ou outros dados informáticos alheios ou por qualquer forma lhes afectar a capacidade de uso".[106]

Este crime é punível com pena de prisão até 3 anos ou multa, de acordo com o seu número 2 a tentativa é também punível. À semelhança do art.3º a ilegítima produção, venda, distribuição, disseminação ou introdução de dispositivos, programas ou dados informáticos com o objetivo de produzir as ações definidas no número 1 do art.4º, é também punível com pena de prisão até 3 anos ou multa. Segundo os números 4 e 5 do referido artigo a pena pode variar dependendo do valor do dano

[104] Simas, Diana, *O CIBERCRIME*, Universidade Lusófuna de Humanidades e Tecnologias, Lisboa, 2014, p.83.
[105] Verdelho, Pedro et all, *Leis do Cibercrime Volume 1*, Centro Atlântico, Famalicão, 2003, p.250.
[106] Artigo 4º, nº1, Lei nº 109/2009, de 15 de Setembro de 2009.

causado, se este for elevado a pena pode ir até os 5 anos de prisão ou multa até 600 dias, no caso de o dano corresponder a um valor consideravelmente elevado a pena passa a ser de 1 a 10 anos de prisão. Todo este procedimento penal depende da apresentação de queixa por parte do lesado.

Com este artigo o objetivo do legislador foi o de defender "a integridade e o bom funcionamento ou o bom uso de dados e programas informáticos"[107]. Ao contrário do definido no art. 3º neste art.4º não é necessária a existência de dolo específico, podendo assim o sujeito que pratica a ação ser acusado e punido a título negligente. Este artigo pretende assim assegurar o bom funcionamento de sistemas informáticos através da penalização não só das ações que efetivamente danificam esses sistemas mas também das tentativas das mesmas.

Para além de fornecer proteção a infraestruturas críticas, este artigo vem também endereçar um problema bastante premente no seio do cibermundo de hoje em dia, pois assume um papel dissuasor no que toca a situações de menor impacto na opinião pública e nas grandes infraestruturas, mas que no entanto afligem diariamente o cidadão comum, os spam e os malwares, que passam a ser passíveis de ser punidos caso seja apresentada queixa.[108]

3.2.1.3. Sabotagem informática

A Lei do Cibercrime legisla também as questões relativas a sabotagem informática punindo quem

> "sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, entravar, impedir, interromper ou perturbar gravemente o funcionamento de um sistema informático, através da introdução, transmissão, deterioração, danificação, alteração, apagamento, impedimento do acesso ou supressão de programas ou

[107] Verdelho, *op. cit.*, p.253.
[108] Simas, Diana, *op. cit.*, 2014, p.87.

outros dados informáticos ou de qualquer outra forma de interferência em sistema informático"[109]

Este art. 5º define que quem incorrer nos pressupostos acima referenciados é passível de ser punido com uma pena de prisão até 5 anos ou multa até 600 dias. À semelhança dos artigos 3º e 4º, o número 2 deste artigo, contempla quem "ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos"[110] que visem produzir os efeitos referidos no número 1 do mesmo artigo, sendo que no caso dos atos definidos no número 2 deste artigo, ao contrário dos acima referidos, a sua tentativa não é punível.

A pena relativa a este crime pode ser aumentada caso os danos causados pelas atividades acima referidas forem de dano elevado, pena de 1 a 5 anos de prisão, e de 1 a 10 anos caso o dano seja de valor consideravelmente elevado ou se os danos atinjam de "forma grave ou duradoura um sistema informático que apoie uma atividade destinada a assegurar funções sociais críticas"[111], como por exemplo sistemas informáticos que apoiem a segurança ou saúde dos cidadãos portugueses.

Apesar de, analogamente ao referido no art.6º presente na Lei da Criminalidade Informática[112], este artigo proteger o normal funcionamento de sistemas informáticos, enfatizando a importância dos sistemas que garantam os direitos básicos dos cidadãos portugueses, a presente Lei do Cibercrime abrange também a questão da produção e distribuição de elementos que facilitem ou permitam a efetivação de crimes de sabotagem informática, findando assim uma lacuna existente no Direito interno português no âmbito da segurança do ciberespaço.

3.2.1.4. Acesso ilegítimo

O 6º artigo deste diploma define o crime de acesso ilegítimo, referindo no seu ponto número 1 que

[109] Artigo 5º, Lei nº 109/2009, de 15 de Setembro de 2009.
[110] Lei nº 109/2009, de 15 de Setembro de 2009, art.5º, número 2.
[111] *Ibidem,* Artigo 5º, número 5, alínea b).
[112] Lei nº109/1991, de 17 de Agosto de 1991.

> "quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, de qualquer modo aceder a um sistema informático, é punido com pena de prisão até 1 ano ou com pena de multa até 120 dias."[113]

No número dois deste artigo são apresentados como crime a produção, venda e distribuição de "dispositivos, programas, um conjunto executável de instruções, um código ou outros dados informáticos", sendo passível de ser punido de acordo com a pena prescrita no número 1, analogamente ao que se verifica nos anteriores artigos. O número 5 do referido artigo define ainda que a tentativa só é punível nas situações contempladas no número 1, excluindo assim a penalização de quem incorra na tentativa de levar a cabo os atos descritos no número 2.

Verifica-se também um agravamento da pena caso a execução do delito contemple violação de regras de segurança por parte do infrator, incorrendo assim numa pena de prisão até 3 anos ou multa. A situação é ainda agravada, suscetível a uma pena de prisão de 1 a 5 anos, quando no decorrer da infração o sujeito tome conhecimento de segredo comercial, industrial, dados confidenciais, protegidos por lei ou se o benefício obtido seja de valor consideravelmente elevado. O número 6 do presente artigo define ainda que nas situações definidas no seu número 1, 3 e 5 o procedimento penal depende de queixa.

O presente artigo visa proteger informação de importância elevada para a segurança do Estado ou de empresas portuguesas, públicas e privadas, bem como garantir que os dados de todos os cidadãos estão salvaguardados dentro do ciberespaço, preservando desta maneira os direitos fundamentais consagrados na Declaração Universal dos Direitos Humanos nos seus 3º e 12º artigos[114]. Comparativamente ao artigo 7º que consta na Lei da Criminalidade Informática é possível constatar uma alteração relevante, a necessidade de existência de dolo específico nos atos definidos no número 1 do art.6º da Lei do Cibercrime[115] é extinta,

[113] Artigo 6º, Lei nº 109/2009, de 15 de Setembro de 2009.
[114] *Supranota*, 57 e 58.
[115] Simas, Diana, *op. cit.*, 2014, p.93.

abrangendo assim todo e qualquer acesso não autorizado a sistemas informáticos sem a necessidade de prova que o sujeito que pratica a ação tenha agido com o intuito de "alcançar, para si ou para outrem, um benefício ou vantagem ilegítimos"[116], visto que o simples facto de aceder a dados existentes num qualquer sistema informático constitui por si só uma violação da privacidade do proprietário do referido sistema[117].

3.2.1.5. Interceção ilegítima

Os atos que podem ser tipificados como interceções ilegítimas de dados informáticos vêm especificados na lei como qualquer ação levada a cabo por

> "quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, e através de meios técnicos, interceptar transmissões de dados informáticos que se processam no interior de um sistema informático, a ele destinadas ou dele provenientes, é punido com pena de prisão até 3 anos ou com pena de multa."[118]

A tentativa deste tipo de crime é punível, bem como a produção, distribuição, venda, disseminação ou introdução num sistema informático de elementos destinados a efetivar as ações supramencionadas no número 1 deste artigo 7º.

Ao escrever este artigo o legislador pretende não só proteger os dados pessoais dos utilizadores, assegurando assim à semelhança do artigo 6º do mesmo diploma a privacidade do proprietário do sistema, mas também a privacidade da informação de qualquer outro individuo, que não o proprietário, contida no referenciado sistema, e ainda garantir a segurança do Estado, reforçando a sua Ciberdefesa, visto que as ações de ciberespionagem concorrem no disposto do presente artigo. O crime de interceção ilegítima acima mencionado não requer dolo específico, sendo que qualquer sujeito que intercete[119] dados informáticos será punido de acordo com a presente legislação, sem necessidade de provar a intenção de alcançar vantagem ou benefício.

[116] Artigo 7º, Lei nº109/1991, de 17 de Agosto de 1991, número 1.
[117] Simas, Diana, *op. cit.*, 2014, p.93.
[118] Artigo 7º, Lei nº109/2009, de 15 de Setembro de 2009, número 1.
[119] De acordo com o definido na alínea e) do art. 2º da Lei nº109/2009, de 15 de Setembro de 2009.

3.2.1.5. Reprodução ilegítima de programa protegido

A questão da reprodução ilegítima de programa protegido é, de todos os crimes referidos anteriormente, aquele que é mais comum e de amplo conhecimento por parte de todos, visto que este delito contempla a violação dos direitos de autor presentes em filmes, música, programas informáticos, obras literárias. Este problema denota elevada complexidade devido à anterior lacuna a nível nacional e internacional de legislação adequada, pois aquando do espontâneo crescimento da internet, toda a informação passou a estar disponível *online*, quer a informação e conteúdos de acesso público quer os conteúdos e dados que se encontravam protegidos por direitos de autor.

Como tal a Lei do Cibercrime vem através do seu art. 8º punir com pena de prisão até 3 anos, ou com pena de multa quem "Ilegitimamente reproduzir, divulgar ou comunicar ao público um programa informático protegido por lei é punido com pena de prisão até 3 anos ou com pena de multa."[120], sendo também punível quem "ilegitimamente reproduzir topografia de um produto semicondutor ou a explorar comercialmente ou importar, para estes fins, uma topografia ou um produto semicondutor fabricado a partir dessa topografia"[121]. A tentativa de executar os atos mencionados no presente parágrafo é igualmente punível.

Este artigo desencadeou já alguma discordância entre alguns autores face à interpretação que se pode fazer do mesmo, objetivamente na questão da reprodução do programa informático, como defende J. Faria Costa "a reprodução, penalmente proibida, deve entender-se como aquela que visa, ou tem por objetivo, uma comunicação ao público"[122], defendendo assim que a reprodução com vista a utilização interna por parte do sujeito não deverá ser criminalmente punida. Já abordando o assunto de outra perspetiva temos Oliveira Ascensão que afirma que a o conceito de reprodução deve apenas ser restrito à criação de cópias do programa

[120] Artigo 8º, Lei nº109/2009, de 15 de Setembro de 2009, número 1.
[121] *Ibidem*, art.8º, número 2.
[122] Costa, J. Faria, *Les crimes informatiques et d'autres crimes dans le domaine de la technologie informatique au Portugal*, [s.l.], [s.d.], p.538.

informático.[123] A minha análise deste artigo vai no entanto de encontro à análise de Diana Simas que refere "que o legislador pretende punir expressamente a reprodução de um programa que está protegido por lei. Independentemente do programa ficar armazenado no computador ou ser carregado para um outro dispositivo, houve efetivamente uma reprodução"[124], visto que mesmo que o sujeito não distribua o programa informático a outrem, ao reproduzir este mesmo para utilização interna está automaticamente a violar os direitos de autor do proprietário.

3.2.1.6. Disposições processuais

Os artigos 11º ao 19º contemplam as disposições processuais definindo em que situações e de que maneira devem ser utilizados os dados informáticos, estas disposições aplicam-se a crimes previstos na Lei do Cibercrime, crimes cometidos por meio de um sistema informático ou crimes em que seja necessário recolher provas em suporte eletrónico, com exceção dos seus artigos 18º e 19º, e contemplam os seguintes pontos:

- Art. 12º - Preservação expedita de dados;
- Art. 13º - Revelação expedita de dados de tráfego;
- Art. 14º - Injunção para apresentação ou concessão de acesso a dados;
- Art. 15º - Pesquisa de dados informáticos;
- Art. 16º - Apreensão dos dados informáticos;
- Art. 17º - Apreensão de correio electrónico e registos de comunicações de natureza semelhante;
- Art. 18º - Intercepção de comunicações;
- Art. 19º - Acções encobertas.

Estes 8 artigos vêm regular o acesso aos dados informáticos em processos judiciais e investigações judiciárias, relacionadas com os crimes previstos na presente lei ou com qualquer outro crime que utilize meios informáticos para ser perpetuado, balizando assim os limites para o acesso por parte de entidades públicas ou privadas a

[123] Ascensão, José de Oliveira, *Novas tecnologias e transformação do direito de autor, Estudos sobre o direito da internet e da sociedade da informação*, Almedina, 2001.
[124] Simas, Diana, *op. cit.*, 2014, p.99.

informações pessoais ou sensíveis e estabelecendo qual o tipo de dados passíveis de serem utilizados na prossecução de um processo jurídico.

3.2.1.7. Cooperação Internacional

Este diploma aborda ainda a questão da cooperação internacional definindo o ponto de contacto permanente para a referida cooperação, de acordo com o exigido pelo art. 35º da Convenção de Budapeste, definindo também as normas para a preservação e revelação expeditas de dados informáticos em cooperação internacional, os motivos de recusa de cedência de informação, o acesso a dados quando em cooperação, o acesso transfronteiriço a dados publicamente disponíveis ou com consentimento e por fim a interceção de comunicações em situações de cooperação.[125] Com este capítulo o legislador tem como finalidade definir procedimentos que facilitem a prossecução de crimes informáticos fora de Portugal, estabelecendo um sistema de permutação de informação entre Estados com o propósito de assim facilitar a aquisição de dados suscetíveis de serem utilizados como prova.

No entanto o artigo 23º estipula as situações em que essa transferência de dados deve ser recusada, defendendo assim a segurança de Portugal, garantindo que a sua soberania e a ordem pública estão salvaguardadas, nos casos em que:

1. Os dados informáticos em causa respeitarem a infracção de natureza política ou infracção conexa segundo as concepções do direito português;
2. Atentar contra a soberania, segurança, ordem pública ou outros interesses da República Portuguesa, constitucionalmente definidos;
3. O Estado terceiro requisitante não oferecer garantias adequadas de protecção dos dados pessoais.[126]

No mesmo sentido, o artigo 25º vem estabelecer as condições em que dados informáticos armazenados em sistemas informáticos sediados em Portugal podem ser acedidos sem necessidade de autorização por parte do Estado, restringindo este

[125] Artigos 21º a 26º, Lei nº109/2009, de 15 de Setembro de 2009.
[126] *Ibidem,* artigo 23º, número 1.

acesso aos referidos dados em Portugal, que se encontrem disponíveis publicamente no caso de o sistema informático também se encontrar em Portugal, no caso de acesso a dados armazenados em Portugal por um sistema informático localizado noutro território, este acesso estará pendente de um consentimento legal e voluntário de pessoa autorizada a divulgá-los.[127]

3.2.2. Jurisprudência

Por forma a aferir a aplicabilidade e adequação da conjuntura legal nacional, foram analisados os seguintes processos:

a)Acórdão do Tribunal da Relação de Lisboa 22/01/2013

Processo: 581/12.6PLSNT-A.L1-5

Sumário:

"I - A Lei do Cibercrime (Lei 109/2009 de 15 de Setembro) nos seus artigos 12.º a 17.º respeitam a meios de obtenção de prova, mormente sua conservação e recolha. São eles: a "preservação expedita de dados", a "revelação expedita de dados de tráfego", a "injunção para apresentação ou concessão de acesso a dados", a "pesquisa de dados informáticos", a "apreensão de dados informáticos" e, finalmente, a "apreensão de correio electrónico e registo de comunicações de natureza semelhante".

II - Com excepção desta última, em que se faz expressa menção à intervenção do juiz, todas as outras diligências são levadas a cabo por ordem da autoridade judiciária competente o que necessariamente inculca a ideia de que essa autoridade judiciária pode ser o Ministério Público ou o Juiz consoante a fase processual.

III - Este novo regime especial de obtenção de meios de prova teve em vista superar a lacuna da Lei nº 109/91 de 17 de Agosto (Criminalidade Informática) que por não conter essas normas processuais que adequassem o regime legal às particularidades da investigação "empurrou" a jurisprudência para a interpretação de que só em relação a crimes de catálogo seria possível a obtenção de certo tipo de dados como os

[127] Artigos 25º, Lei nº109/2009, de 15 de Setembro de 2009.

dados de tráfego e mercê da intervenção do juiz de instrução (cfr. por exemplo, o Ac. T.R.E. de 26.06.2007, proc. 843/07-1, em que estava em causa a investigação do crime de acesso ilegítimo do art. 7º, nº 1 da citada Lei nº 109/91)

IV - Significa isto, na leitura integrada de todo o regime legal, que se julga adequada a interpretação de que se os dados a obter são "dados de tráfego", de acordo com a definição do art. 2º, al. c) da Lei do Cibercrime, e tiverem de ser recolhidos junto de uma operadora localizada em território nacional, independentemente de estarmos perante "crimes graves", enunciados no artigo 2º, nº 1, alínea g) da Lei 32/2008 de 17 de Julho, poderá a autoridade judiciária competente, tendo em vista a descoberta da verdade, ordenar que estes sejam disponibilizados sob pena de punição por desobediência. É o que resulta do disposto no art. 14º, nºs 1, 2, 3 e 4 da mesma Lei.

V - Pedir à operadora que forneça os dados em questão não é a mesma coisa que proceder a uma intercepção de uma comunicação, mesmo que com esta se vise proceder ao registo de "dados de tráfego"."

Decisão:

"Pelo exposto, acordam em conceder parcial provimento ao recurso, ordenando a substituição do despacho recorrido por outro que atribua a competência para a obtenção dos dados em causa ao Ministério Público."

b)Acórdão do Tribunal da Relação de Lisboa 10/07/2012

Processo: 7876/10.1JFLSB.L1-5

Sumário:

"I. O crime de falsidade informática previsto no art.3, nºs1,2 e 3, da Lei nº109/09, de 15Set., não veio esvaziar de sentido a al.c, do nº1, do art.267, do Código Penal, continuando este preceito a abranger a conduta que se traduza em adulteração de cartões de crédito;

II. No crime de contrafacção de moeda o bem jurídico protegido é a integridade ou intangibilidade do sistema monetário legal em si mesmo considerado, aqui representado pelos cartões de crédito por via da sua equiparação àquela;

III. A assinatura dos talões de pagamento não é abrangida pela actividade de passagem de moeda falsa, através do uso dos cartões de crédito adulterados, constituindo crime de falsificação autónomo;"

Decisão:

"Nos termos e com os fundamentos indicados, na parcial procedência do recurso interposto pelo Ministério Público decide-se:

A) - Em substituição do crime de falsidade informática em que foi condenado em 1.ª Instância, julgar o arguido A... incurso na prática de um crime de contrafacção de moeda p. e p. pelo art. 262.º, n.º1, e 267.º, n.º1, al. c), do Cód. Penal, e por ele condená-lo na pena de 4 (quatro) anos e 3 (três) meses de prisão.

- Julgá-lo incurso num crime de burla informática p. e p. pelo art. 221.º, n.ºs 1 e 5 al. a), com referência ao art. 202.º, al. b), todos do Cód. Penal (em vez do crime de burla informática, na forma continuada, p. e p. pelos art.ºs 221.º, n.º1, e 30.º, n.º2, do Cód. Penal, em que o havia sido em 1.ª Instância), e por ele condená-lo na pena de 1 (um) ano e 9 (nove) meses de prisão que lhe havia sido aplicada por aquela última infracção.

Na reformulação das penas parciais em que ficou condenado, na pena única de 5 (cinco) anos e 6 (seis) meses de prisão.

B) Em substituição do crime de falsidade informática em que foi condenado em 1.ª Instância, julgar o arguido B... incurso na prática de um crime de passagem de moeda falsa previsto no art. 265.º, n.º 1, al. a), por referência ao mencionado art. 267.º, n.º1, al. c), todos do Cód. Penal, e por ele condená-lo na pena de 2 anos de prisão.

- Julgá-lo incurso num crime de burla informática p. e p. pelo art. 221.º, n.ºs 1 e 5 al. a), com referência ao art. 202.º, al. b), todos do Cód. Penal (em vez do crime de burla informática, na forma continuada, p. e p. pelos art.ºs 221.º, n.º1, e 30.º, n.º2, do Cód.

Penal, em que o havia sido em 1.ª Instância), e por ele condená-lo na pena de 1 (um) ano e 3 (três) meses de prisão que lhe havia sido aplicada por aquela última infracção.

Na reformulação das penas parciais em que ficou condenado, manter-lhe a pena única de 3 (três) anos de prisão.

C) Julgar improcedente o recurso interposto pelo arguido A.

Pelo seu decaimento, e independentemente do benefício do apoio judiciário de que possa beneficiar, ficará este ultimo condenado em 2 (duas) UCs de taxa de justiça (art.ºs 513.º e 514.º do CPP e Tabela III, e respectivo Regulamento das Custas Judiciais).”

c)Acórdão do Tribunal da Relação de Coimbra 15/10/2008

Processo: 368/07.8TAFIG.C1

Sumário:

“1.O bem jurídico protegido crime de acesso ilegítimo p. e p. pelo art 7º da Lei nº 109/91 de 17 de Agosto é a segurança do sistema informático trata-se da protecção ao designado “domicilio informático” algo de semelhante à introdução em casa alheia

2.O acesso ilegítimo tem como elemento subjectivo do tipo a “intenção de alcançar, para si ou para outrem, um benefício ou vantagem ilegítimos.”

Decisão:

“O crime de abuso de poder exige uma intenção específica que é a de obter para si ou para outrem, benefício ilegítimo ou causar prejuízo a outra pessoa – dolo específico.

Não resulta dos autos que a arguida tenha praticado um crime de abuso de poder, ou seja que tenha abusado ou violado os deveres a que estava obrigada no âmbito da sua actividade profissional, não resultando, também, que a arguida tenha actuado de forma e com o propósito de beneficiar a si ou a terceiro, ou causar prejuízo à recorrente.

Não nos merece pois, qualquer censura, o despacho recorrido.

Termos em que se nega provimento ao recurso.

Custas pela recorrente fixando-se em 10 ucs a taxa de justiça."

d)Acórdão do Tribunal da Relação de Coimbra 17/02/2016

Processo: 2119/11.TALRA.C2

Sumário:

"I - É autor material de um crime de acesso ilegítimo, previsto no art. 6.º, n.ºs 1 e 4, al. a), da Lei n.º 109/2009, de 15-09, quem, sendo inspector tributário - não obstante deter, para exercício da sua função, instrumentos de segurança "username" e "PIN" -, por motivos estritamente pessoais, acedendo ao sistema informático da autoridade tributária, consulta declarações de IRS de outrem.

II - O tipo subjectivo daquele ilícito penal não exige qualquer intenção específica, como seja a provação de prejuízo ou a de obtenção de benefício ilegítimo; fica preenchido com o dolo genérico."

Decisão:

"Nos presentes autos o arguido foi absolvido relativamente à prática de um crime de corrupção passiva na forma tentada (art.º 22º, 23º, 373º-1 do C. Penal), sendo condenado pela prática de um crime de acesso ilegítimo (art.º 6º-1-4-a) da Lei n.º 109/2009, de 15-09).

Não pondo em causa a factualidade apurada, pretende que ela não é a suficiente para a integração da previsão legal desse tipo criminal."

e)Acórdão do Tribunal da Relação de Coimbra 30/03/2011

Processo: 1788/04.5JFLSB.C1

Sumário:

"I - A falta de prova de um facto, não se provando o seu contrário ou uma qualquer outra versão do mesmo facto, dá lugar apenas e tão-só a um non liquet, a um estado de incerteza que deverá conduzir à consideração do facto em questão como não provado, não resultando daí que deva considerar-se provado o facto contrário.

II – O art. 8º, nº 1, da Lei nº 109/2009, de 15 de Setembro (Lei do Cibercrime), que tipifica o crime de reprodução ilegítima de programa protegido, tutela a propriedade intelectual mediante a criminalização da utilização não autorizada de programa informático protegido por lei. Para a consumação do crime basta a reprodução, divulgação ou comunicação ao público, não se exigindo que a lesão do direito de autor se traduza num prejuízo económico (efectivamente verificado) para este.

III – O crime de usurpação p. p. pelos arts. 195º, 197º e 199º do CDADC, tutela o exclusivo de exploração económica da obra, que a lei reserva ao respectivo autor. Este tipo de crime verifica-se, independentemente de qualquer resultado material, desde que ocorra uma utilização não autorizada, independentemente de o agente se propor obter qualquer vantagem económica.

IV – No âmbito do CDADC, a licitude da utilização ou reprodução sem expressa autorização do autor apenas se afirma com a demonstração de que essa utilização ou reprodução se destinou a fim exclusivamente privado, sem prejuízo para a exploração normal da obra e sem injustificado prejuízo dos interesses legítimos do autor, sendo esta tripla conjugação que evidencia a verificação da regra dos três passos, decorrente da assimilação dos princípios previstos originariamente na Convenção de Berna para a Protecção das Obras Literárias e Artísticas, ratificada por Portugal e transposta para o direito nacional através da legislação que tutela aquela matéria."

Decisão:

"Nestes termos, julga-se a acusação procedente, por provada e, em consequência, decide-se:

a) Condenar o arguido FJ... na pena de 50 dias de multa à taxa diária de 7,00€, o que perfaz a quantia global de 350,00€ (trezentos e cinquenta euros), pela prática de um crime de reprodução ilegítima de programa protegido, p.p. pelas disposições combinadas dos artigos 14.º, n.os 1 e 2, do Decreto-Lei n.º 252/94, de 20 de Outubro, e 9.º, n.º 1, da Lei da Criminalidade Informática;

b) Condenar o arguido na pena de 4 (quatro) meses de prisão e de 175 dias de multa à taxa diária de 7,00€ pela prática de um crime de usurpação, p.p. pelos artigos 195.º, 197.º e 199.º, todos do Código dos Direitos de Autor e Direitos Conexos.

c) Substituir a pena de 4 (quatro) meses de prisão concretamente aplicada ao arguido por uma pena de 175,00 (cento e setenta e cinco) dias de multa à taxa diária de 7,00 € (sete euros).

d) Condenar o arguido, em soma da pena de multa aplicada a título principal e da pena de multa aplicada em substituição da pena de prisão, numa pena única de 350 dias de multa (trezentos e cinquenta dias), à taxa diária de 7,00€ (sete euros), perfazendo um montante global de 2.450,00€ (dois mil quatrocentos e cinquenta euros).

e) Em cúmulo jurídico, condenar o arguido na pena única de 375 dias de multa à taxa diária de 7,00€, o que perfaz o montante global de 2625,00€ (dois mil seiscentos e vinte e cinco euros).

f) Condenar o arguido no pagamento das custas do processo, cuja taxa de justiça se fixa em 3 Unidade de Conta, procuradoria em 1/2 da taxa de justiça devida com o acréscimo de 1% a reverter em favor da APAV (cfr. artigos 513.º e 514.º do Código de Processo Penal, artigos 85.º n.º 1 al. b) e 95.º do Código das Custas Judiciais e artigo 13.º n.º 3 da Lei 31/2006, de 21.07);

g) Julgar improcedentes, por não provados, os pedidos de indemnização civil deduzidos pela demandante Sociedade Portuguesa de Autores, CRL, pela Lusomundo – Audiovisuais, SA e pela FEVIP – Federação de Editores de Videogramas e, em consequência, absolver o demandado FJ... dos pedidos contra si formulados.

h) Condenar os demandantes civis no pagamento das custas cíveis, nos termos dos artigos 446.º n.º1 e 3 do Código de Processo Civil.

i) Declaram-se perdidos a favor do Estado os CDs e DVDs apreendidos nos autos, os quais deverão, oportunamente, ser destruídos – cfr. artigos 109º do Código Penal e 201º do Código do Direito de Autor e dos Direitos Conexos.

j) Determina-se a publicação da parte decisória da presente sentença no jornal de âmbito regional mais lido da região de Cantanhede."

f)Acórdão do Tribunal da Relação do Porto 08/01/2014

Processo: 1170/09.8JAPRT.P2

Sumário:

"I – A alínea d) do n.º 2 do art.º 120º do CPP abrange a omissão de actos ou diligências processuais na fase de julgamento e de recurso, que se reputem essenciais à descoberta da verdade.

II – O juízo sobre a essencialidade ou indispensabilidade da diligência de prova cabe ao tribunal e deve basear-se em critérios objectivos, independentes das convicções pessoais dos intervenientes processuais.

III – A sentença é nula quando a fundamentação da convicção for insuficiente para efectuar uma reconstituição do iter que conduziu a considerar cada facto provado ou não provado.

IV – O crime de acesso ilegítimo, previsto no art.º 6º da Lei n.º 109/2009, de 15/9, (Lei do Cibercrime), estruturalmente acolhe o crime anterior, previsto no art.º 7º da Lei 109/91, de 17/8, com alterações decorrentes dos compromissos internacionais que Portugal assumiu e, em particular, da Convenção sobre Cibercrime do Conselho da Europa.

V – A factualidade incriminada é exactamente a mesma que era antes, não se exigindo, agora, qualquer intenção específica, por exemplo, a de causar prejuízo ou a de obter qualquer benefício ilegítimo pois que apenas se exige o dolo genérico.

V - O bem jurídico protegido é a segurança do sistema informático.

VI - O crime de acesso ilegítimo é praticado por quem actue de forma não autorizada, concretizando-se por qualquer modo normalmente idóneo de aceder a um sistema ou rede informáticos.

VII – O crime de devassa por meio de informática, previsto no art.º 193º do C. Penal, decorre do art.º 35º, n.º 3, da CRP, e visa proteger a reserva da vida privada contra possíveis actos de discriminação, que a utilização de meios informáticos torna exponencialmente perigosos."

Decisão:

"Pelo exposto, acordam as juízas da 2ª Secção Criminal do Tribunal da Relação do Porto em conceder parcial provimento ao recurso interposto pelo arguido B… e consequentemente:

a) Absolver o arguido da prática de um crime de acesso ilegítimo, previsto e punível pelo artigo 7º, nº 1 e 2 da Lei nº 109/91, de 17/8.

b) Fixar em € 5,00 (cinco euros) o quantitativo diário da pena de multa imposta ao arguido pela prática de um crime de devassa por meio informático, previsto e punível pelo artigo 193º, nº 1 do Código Penal.

c) Manter quanto ao demais a decisão recorrida.

Sem custas. "[128]

Pode portanto ser concluído que apesar da existência de legislação específica, os arguidos dos processos analisados supra são, na maioria dos casos, acusados de crimes previstos noutros documentos legais, como por exemplo o Código Penal, tendo em conta este facto uma solução seria a exclusão dos crimes já previstos na Lei do Cibercrime de outros diplomas legais, visto que esta Lei é a que melhor se enquadra no âmbito de eventos ocorridos no ciberespaço ou por meio de sistemas informáticos e de comunicações, e cumpre com o previsto na Convenção de Budapeste ratificada pelo Estado Português.

[128] Processos consultados na página do Centro de Investigação Jurídica do Ciberespaço, disponível em http://www.cijic.org/.

4. Repercussões legais da manutenção da Cibersegurança e Ciberdefesa portuguesas no contexto internacional.

Face à já referida natureza transfronteiriça do ciberespaço as questões relativas a este domínio não devem ser ponderadas meramente a nível interno por cada Estado[129], sendo que qualquer dos crimes referidos nos documentos legais analisados nos anteriores capítulos deste trabalho podem revestir-se dessa mesma natureza transfronteiriça, levando a possíveis tensões entre países como se verificou no mediático caso de fuga de informação que teve como principal figura Edward Snowden.[130]

Situações como a supramencionada revestem-se de maior magnitude quando se trata de informação que possa por em causa a soberania de um Estado ou que afete diretamente a capacidade de garantir a segurança do mesmo e dos cidadãos que nele residem, tomando como exemplo um dos primeiros ataques cibernéticos de que há registo em 1982, perpetuado pelos Estados Unidos da América contra a então União Soviética, em que um agente da Central Intelligence Agency (CIA) introduziu uma alteração no sistema de uma estação de abastecimento de combustível na Sibéria, fazendo com que esta funcionasse de forma errática provocando a explosão da mesma.[131]

Passados 34 anos desde o acontecimento supracitado, as capacidades e potencialidades existentes nos sistemas e dispositivos informáticos atualmente, fornecem uma panóplia de soluções a quem deseje efetuar um qualquer ataque no ciberespaço. Esta situação vem justificar a origem do conceito de ciberguerra, posto que cada vez mais a ideia de um confronto à escala continental, ou mesmo global,

[129] Preocupação esta, que é desde já refletida no Direito Interno das nações europeias.
[130] Edward Snowden é um ex-funcionário da Central Intelligence Agency, que publicou sem autorização informação classificada armazenada nos servidores da National Security Agency, tendo fugido dos Estados Unidos da América e mais tarde encontrado refúgio na Rússia, situação que fomentou o crescimento de tensões entre os dois países em virtude da oferta de asilo por parte do governo russo.
[131] The Economist, *War in the fifth domain*, http://www.economist.com/node/16478792, acedido em Junho de 2016.

contemplando o emprego de ataques via ciberespaço, está cada vez mais presente nas preocupações da maioria dos governos espalhados pelo globo.

4.1. O impacto dos eventos cibernéticos nas relações internacionais.

4.1.1. A estrutura de Ciberdefesa no panorama da NATO.

Em resposta à crescente ameaça de ataque a sistemas de informação sustentada pelo referido nos anteriores capítulos deste trabalho, a NATO tem vindo a desenvolver estruturas de controlo, formação e apoio no sentido de preservar a segurança no ciberespaço e a defesa dos interesses nacionais dos seus Estados membros e amigos, e por conseguinte garantir uma política de ciberdefesa cada vez mais resiliente e capaz de enfrentar as ameaças potenciadas pelo ciberespaço.

Em 2008 foi aprovada a primeira política de Ciberdefesa a nível da NATO, no seguimento dos ataques sofridos pela Estónia em 2007[132], em 2010 foi adotado um novo conceito estratégico de ciberdefesa como resultado da Cimeira de Lisboa tendo resultado no ano seguinte na aprovação da segunda política de ciberdefesa da NATO. Foi só a partir de 2012 que o conceito de ciberdefesa foi integrado no Defence Planning Proccess da organização reforçando no mesmo ano a existente NATO Incident Computer Incident Response Capability, estabelecida em 2005. No seguimento das referidas iniciativas em 2014 o Concelho do Atlântico Norte formou o Comité de Ciberdefesa (Cyber Defence Comittee), passando os temas de defesa no ciberespaço a dispor de um comité especializado ao invés de continuar integrado no Defence Planning Proccess, com o objetivo de estabelecer políticas e conceitos estratégicos melhor adaptados ao universo do ciberespaço.[133]

A entidade responsável pela coordenação de respostas a incidentes ocorridos com países membros da NATO é a NATO Computer Incident Response Capability[134,] que se encontra sobre a alçada da NATO Communications and Information Agency,

[132] A 27 de Abril de 2007 a Estónia foi vítima de vários ciberataques que tiveram como alvo o seu parlamento, bancos, vários ministérios, jornais e cadeias televisivas. Estes ataques foram reivindicados por um comissário do movimento pro-Kremlin Nashi, Konstantin Goloskokov.

[133] *Cyber defence*, http://www.nato.int/cps/en/natohq/topics_78170.htm, visitado em Março de 2016.

[134] Anil, Suleyman, *NCIRC (NATO Computer Incident Response Capability)*, Madrid, disponível em https://www.terena.org/activities/tf-csirt/meeting11/NCIRC-Anil.pdf, visitado em Abril de 2016.

sediada em Bruxelas, contando ainda com 25 polos espalhados pela Europa, dois dos quais se encontram localizados em Portugal, um em Oeiras e outro na Costa da Caparica. Mais recentemente, em 2015, foi criado o Memorandum of Understanding on Cyber Defence tendo em vista promover a troca de informação e prestação de apoio entre os 28 aliados da NATO, com o objetivo de melhorar as capacidades de prevenção, resiliência e capacidade de resposta a incidentes no ciberespaço.

4.1.2. A constituição da rede de Ciberdefesa nas Forças Armadas.

Foi em Novembro de 2002 na Declaração de Praga que os membros da NATO tomaram a decisão de reforçar as capacidades de defesa contra cibercrimese ciberataques[135], no encadeamento desta decisão foram elaborados dois documentos: o PEMGFA/CSI/004, de 14 de Fevereiro de 2005, contemplando a Organização e Normas de Segurança nos Sistemas de Informação e Comunicações Conjuntos, e o PEMGFA/CSI/301, de 23 de Setembro de 2008, que veio estabelecer a estrutura orgânica, as normas e procedimentos a adotar por forma a assegurar uma capacidade de resposta adequada por parte das Forças Armadas face a incidentes ocorridos em sistemas informáticos[136]. Seguindo estas diretivas os diferentes ramos das Forças Armadas têm vindo a desenvolver valências técnicas, através da disseminação e consequente consciencialização dos seus militares para as questões relacionadas com a temática dos incidentes no ciberespaço, criando e treinando equipas de resposta a eventos ocorridos no espaço cibernético, estabelecendo Capacidades de Resposta a Incidentes de Segurança Informática (CRISIs).

Como órgão de coordenação das CRISIs dos diferentes ramos das Forças Armadas temos a Direção de Comunicações e Sistemas de Informação (DIRCSI)[137], sob a alçada do Estado-Maior-General das Forças Armadas (EMGFA) criado pelo Decreto-Lei nº184/2014 de 29 de Dezembro de 2014, com a missão de "planear, estudar,

[135] NATO, *Prague Summit Declaration*, Praga, 21 de Novembro de 2002, no ponto f do art.4º define "Strengthen our capabilities to defend against cyber attacks.".
[136] Instituto da Defesa Nacional, *ESTRATÉGIA DA INFORMAÇÃO E SEGURANÇA NO CIBERESPAÇO,* Lisboa, Dezembro de 2013, p.57.
[137] Decreto-Lei nº184/2014 de 29 de Dezembro de 2014, art.30º, ponto 6 alínea d), "Assegurar a coordenação e o trabalho colaborativo e integrado com os Núcleos Computer Incident Response Capability (CIRC) dos ramos das Forças Armadas e do EMGFA;"

dirigir, coordenar e executar as atividades inerentes aos sistemas de informação (SI) e tecnologias de informação e comunicação (TIC) necessários ao exercício do comando e controlo nas Forças Armadas"[138]. O mesmo documento define ainda que no que concerne à ciberdefesa a DIRCSI contempla a missão de "coordenar a proteção dos valores da integridade, confidencialidade e disponibilidade da informação e dos sistemas de informação das Forças Armadas."[139]

Esta organização permite efetuar uma defesa em camadas, sendo dividida em três níveis distintos como defende Monteiro da Silva no seu trabalho *SEGURANÇA E DEFESA NACIONAL: O DESENVOLVIMENTO DE CAPACIDADES DE CIBERDEFESA*, "A estrutura da CRISI (…) procura obter uma resposta coordenada dos recursos existentes através de três níveis de atuação e coordenação: o primeiro através do Centro de Coordenação da CRISI, seguido do Grupo de Resposta a Incidentes de Segurança Informática (GRISI) e um terceiro e último nível composto pelas Autoridades de Segurança dos (Sistemas de Informação e Comunicação) SIC"[140].

Importa portanto distinguir a esfera de atuação da DIRCSI e da rede de ciberdefesa do CNCS e da rede CSIRT nacional, que apresentam linhas de ação semelhantes mas com objetivos distintos, tendo sido atribuída ao CNCS a missão de manutenção da cibersegurança a nível nacional, estando incumbido da proteção de entidades do Estado e infraestruturas críticas, em questões relacionadas com eventos no ciberespaço. Por outro lado a DIRCSI e as várias CRISIs dos diferentes ramos das Forças Armadas asseguram a proteção do Estado num cenário de ciberguerra, prevenindo e estando pronto a responder a qualquer ciberataque que lhes seja dirigido.

[138]Decreto-Lei nº184/201 de 29 de Dezembro de 2014, art.30º, ponto 1.
[139] *Ibidem*, art.2º
[140] Silva, Nuno Monteiro, *SEGURANÇA E DEFESA NACIONAL: O DESENVOLVIMENTO DE CAPACIDADES DE CIBERDEFESA*, Lisboa, 2012, p.10.

4.1.3. Escalada de impacto dos eventos no ciberespaço, a génese dos conflitos cibernéticos.

John Arquilla e David Ronfeldt definiram o conceito de ciberguerra defendendo que este

> "refere-se a conduzir e preparar para conduzir operações militares de acordo com os princípios da informação. Significa interromper, se não mesmo destruir, os sistemas de informação e de comunicação, definidos de forma ampla, de modo a incluir até a cultura militar, nos quais um adversário se apoia para se "conhecer" a si próprio: quem é, onde está, o que pode fazer quando, porque está a lutar, que ameaças contrariar primeiro, etc. Significa tentar saber tudo sobre um adversário, enquanto que se evita que este saiba muito sobre nós próprios. Significa modificar a "balança de informação e conhecimento" a nosso favor, especialmente se a balança de forças não é favorável. Significa usar conhecimento, pelo que menos capital e trabalho terão de ser gastos. Esta forma de guerra pode envolver diversas tecnologias – nomeadamente para C3I; recolha de informação, posicionamento e identificação de amigos ou inimigos (IFF); e sistemas de armas "inteligentes" – para dar apenas alguns exemplos. Pode também envolver interferência eletrónica, falseamento, sobrecarga e intrusão nos circuitos de informação e comunicação de um adversário"[141]

No seguimento da análise desta definição surgem algumas questões, quando é que um cibercrime passa a ser um ciberataque? Serão todos os ciberataques e crimes ocorridos no ciberespaço capazes de criar tensões internacionais gerando conflitos? De que forma poderá ser categorizada a escalonamento de um evento ocorrido no ciberespaço?

Eneken Tikk estabeleceu, na sua obra *Comprehensive legal approach to cyber security*, um espectro que visa responder às questões em cima mencionadas.

[141] Arquilla, John, e Ronfeldt, David, *Cyberwar is coming!,* Comparative Strategy. Vol. 12, N.º 2, [s.l.], 1993, p. 28.

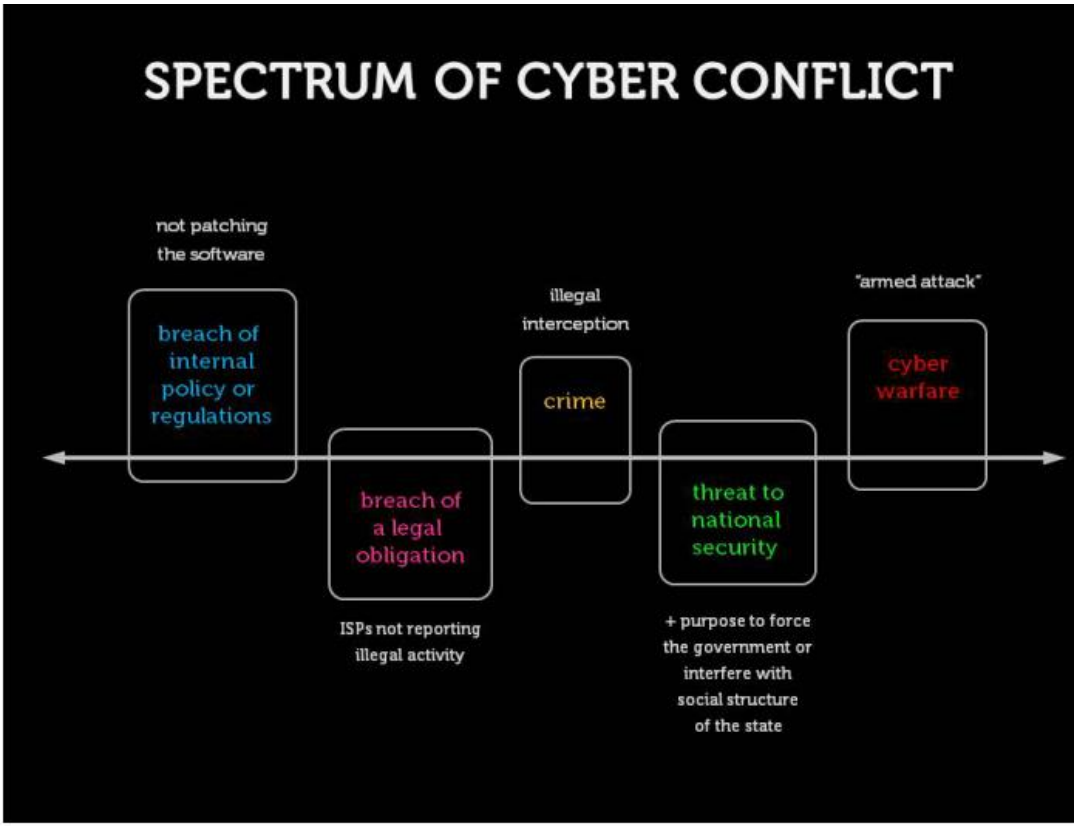

Figura 2. Espectro do conflito cibernético.

Como se verifica na figura 2, Tikk defende que existem várias etapas até que seja desencadeada uma ciberguerra com origem num conflito cibernético, estas etapas passam por um primeiro ciberevento que infringe as regulações internas de um Estado, e no caso de este evento recorrer nas definições impostas pela legislação própria desse Estado passa a ser considerado um cibercrime. Caso o crime perpetuado represente uma ameaça para a segurança nacional, deixa de se estar na presença de um cibercrime para se passar fazer face a um ciberataque, que neste caso segundo Tikk poderá levar a um crescimento de tensões e origem de um conflito internacional, resultando em última análise num confronto bélico no ciberespaço, sendo que em cada um destes patamares tem associado várias vertentes do direito, com início na legislação criminal, legislação de direitos fundamentais e por fim a legislação de conflito armado.[142]

[142] Eneken Tikk, *op.cit.*, Estónia, 2011, p.75.

Este espectro permite também perceber como as questões relacionadas com a cibersegurança e a ciberdefesa se encontram separadas uma linha ténue, visto que um qualquer incidente no ciberespaço pode aparentar tratar-se de um ato de cariz interno, revestindo-se de contornos de um crime, que estando apropriadamente legislado não apresenta uma ameaça à segurança de um Estado, e ao ser investigado em maior profundidade, constituir na verdade um ataque às infraestruturas de segurança por parte de terceiros, passando assim a colocar em xeque a segurança ou soberania do país atacado. A dificuldade de identificação dos verdadeiros objetivos de um ciberincidente levanta ainda outro problema, a definição dos órgãos que devem atuar quando na presença do dito incidente.

Este problema exige portanto uma capacidade de cooperação e agilização entre organizações nacionais, como o CNCS, a rede CSIRT, DIRCSI, as diferentes CRISIs dos respetivos ramos das Forças Armadas e as organizações internacionais. Facto este que no âmbito desta problemática não é fácil face à eficácia e velocidade dos ataques informáticos.

4.2. O desafio da incorporação dos cibercrimes e ciberataques no jus in bello.

A 14 de Junho de 2016 numa reunião de Ministros da Defesa de países pertencente à NATO, foi reconhecido como domínio de desenvolvimento de operações militares[143], juntando-se assim à terra, mar, ar e espaço. Na sequência desta decisão torna-se mais premente a necessidade de estruturação e desenvolvimento das capacidades de defesa contra possíveis ataques perpetuados através do ciberespaço, alargando o já existente conceito de Segurança da Informação[144], por forma a incluir as capacidades de Computer Network Defense (CND), Computer Network Exploitation (CNE), e Computer Network Attack (CNA), definidas como:

[143] Facto noticiado na página oficial da NATO, disponível em http://www.nato.int/cps/en/natohq/news_132356.htm, acedido em Junho de 2016.

[144] Medidas de proteção "essencialmente de natureza reativa e estática, focada na defesa dos sistemas de informação e telecomunicações, através da implementação de medidas preventivas, de deteção e de recuperação de diferente natureza.", Instituto da Defesa Nacional, *ESTRATÉGIA DA INFORMAÇÃO E SEGURANÇA NO CIBERESPAÇO,* Lisboa, Dezembro de 2013, p.11.

- Computer Network Defense (CND), que inclui as medidas adotadas através da utilização de redes de computadores para proteger, controlar, analisar, detetar e responder a atividades não autorizadas nos sistemas de informação e comunica- ções. As ações CND não procuram apenas proteger os sistemas amigos de um adversário externo, mas também contemplam a possibilidade de a sua exploração ocorrer a partir do interior da própria organização;

- Computer Network Exploitation (CNE) que integra as capacidades de recolha de informações (intelligence) levadas a cabo através do uso de redes de computadores para recolher dados das redes de comunicações e dos sistemas de informa- ção de um potencial adversário;

- Computer Network Attack (CNA), que inclui as ações desenvolvidas através da utilização de redes de computadores para interromper, negar, degradar ou destruir a informação tratada pelas redes de comunicações e pelos sistemas de informação (do possível adversário), ou dos próprios sistemas de informação e comunicações amigos.[145]

No âmbito do desenvolvimento destas capacidades e da sua coordenação entre os países membros e aliados da NATO, tem vindo a decorrer, com uma periodicidade anual desde 2008, o exercício CYBER COALITION, que contou com a participação das Forças Armadas portuguesas na edição de 2015[146].

Com esta nova definição do ciberespaço como um teatro de operações e o aprovado conceito de ciberguerra surge um problema de ordem legal, a inclusão dos eventos ocorridos no ciberespaço no direito da guerra, invocando inevitavelmente uma análise do existente enquadramento legal ao nível humanitário e dos conflitos armados, concluindo que tanto a Convenção de Genebra como as Convenções de Haia, e todas as fontes de direito internacional humanitário e dos conflitos armados, não

[145] Instituto da Defesa Nacional, ESTRATÉGIA DA INFORMAÇÃO E SEGURANÇA NO CIBERESPAÇO, Lisboa, Dezembro de 2013, p.12

[146] Informação disponível na página oficial do EMGFA, http://www.emgfa.pt/pt/noticias/909, acedido em 25 de Julho de 2016.

reconhecem a existência do ciberespaço, nem a sua nova definição como domínio de desenvolvimento de operações militares.

Fonte	Título	Data
Convenção de Genebra	Melhoria das Condições dos Feridos no Campo de Batalha	1864
II Conferência de Haia	Leis e Costumes da Guerra em Terra	1899
IV Conferência de Haia	Leis e Costumes da Guerra em Terra	1907
Protocolo de Genebra	Para a Proibição do Uso na Guerra de Gás Asfixiante e dos Métodos de Guerra Bacteriológica	1928
I Convenção de Genebra	Para Melhoria das Condições dos Feridos e Doentes das Forças Armadas no Terreno	1864
II Convenção de Genebra	Para Melhoria das Condições dos Feridos, Doentes e Náufragos das Forças Armadas no Mar	1949
III Convenção de Genbra	Relativa ao Tratamento dos Prisioneiros de Guerra	1929
IV Convenção de Genebra	Relativa à Proteção de Civis em Tempo de Guerra	1949
Convenção de Genebra	Proibindo o Desenvolvimento, Produção e Armazenamento de Armas Bacteriológicas e Tóxicas e sobre a sua Destruição	1975
Protocolo I	Relativa à Proteção das Vítimas de Conflitos Armados Internacionais	1977
Protocolo II	Relativa à Proteção das Vítimas de Conflitos Armados Não Internacionais	1977
Protocolo III	Relativa à Adoção de Um Emblema Adicional Distintivo	2005

Figura 3. Fontes de direito internacional humanitário e dos conflitos armados

Tendo esta situação em consideração torna-se necessária a elaboração de fontes de direito de conflitos armados que incluam os conceitos de ciberataque, ciberterrorismo, ciberespionagem e ciberguerra, limitando e punindo a execução dos

mesmos, pois apesar de até à data não terem sido verificados conflitos à escala de uma guerra informática, essa possibilidade é considerada e ponderada por todos os Estados desenvolvidos. Face a este paradigma poderá ser enquadrada legalmente a ciberguerra no direito internacional se apresentar contornos semelhantes a uma ameaça convencional, abrangida pela legislação em vigor? Ou será que a questão deve ser analisada não aferindo a natureza da ameaça mas sim o resultado final que desta advirá?

Neste sentido, conclui-se que não basta apenas legislar os crimes ocorridos no ciberespaço como apenas crimes, mas ponderar também a sua definição, nos casos aplicáveis, como atos de guerra cometidos através de sistemas informáticos e de comunicação, por forma a promover a estabilidade das relações internacionais e exponenciar o uso e cooperação do ciberespaço por todas as nações.

4.3. Estudos de caso.

No âmbito desta temática existem dois casos que demonstraram os danos que os ciberataques podem causar, a nível da segurança individual mas também das suas relações internacionais, por serem os únicos casos globalmente reconhecidos como atos de guerra: os ataques à Estónia em 2007, e os ataques à Geórgia em 2008.

Nos últimos anos foram amplamente estudados a nível técnico, com o objetivo de identificar o espectro de danos passiveis de serem verificados por ciberataques, bem como a identificação de limitações e debilidades nas estruturas de cibersegurança e ciberdefesa, e também do ponto de vista jurídico, resultando dos referidos casos várias análises e propostas de reformulação das ferramentas de direito internacional e nacional.

Como tal irão ser analisados de forma breve os dois casos suprarreferidos, com base nos estudos de caso previamente efetuados por Eneken Tikk, Kadri Kaska e Liis Vihul, estudos estes que se encontram em anexo nesta dissertação.

4.3.1. Ciberataques à Estónia em 2007.

Na primavera de 2007, mais precisamente entre 27 de Abril e 18 de Maio do mesmo ano, no seguimento de protestos do governo e *media* russos, desencadeados pela recolocação de um memorial da 2ª Guerra Mundial de um local de destaque para um cemitério militar, dos quais resultou um cerco à embaixada estónia em Moscovo, a Estónia foi alvo de vários ataques cibernéticos, tendo sido utilizados maioritariamente quatro métodos:

- DoS (Denial of Service) e DDoS (Distributed Denial of Service)[147];
- Desfiguração de *websites*;
- Ataques a servidores DNS (Domain Name System);
- *Spam* a comentários e e-mails.

Os alvos destes ataques foram infraestruturas críticas responsáveis por garantir o adequado funcionamento da internet na Estónia, o gabinete do parlamento estónio bem como outras instituições governamentais, incluindo os servidores de partidos políticos e do próprio presidente, e ainda serviços associados ao setor privado e ainda sistemas informáticos de cidadãos aleatórios.

Esta série de ataques provocou o funcionamento incorreto, ou mesmo a cessação de funcionamento, dos seus alvos comprometendo assim o normal funcionamento da economia doméstica da Estónia, impossibilitando o regular desenrolar de transações bancárias e de documentação, afetando maioritariamente as instituições governamentais e as pequenas e médias empresas. Existiram também repercussões a nível social, visto não existirem vias de comunicação com os serviços básicos da administração pública e a comunicação com o mundo exterior se encontrava altamente condicionada.

[147] Estes dois tipos de ataques têm como objetivo a indisponibilização dos recursos de um sistema informático aos seus utilizadores,quer através da denominada inundação, que consiste na aumento de trafégo de dados sobrecarregado assim o sistema atacado abrandando ou mesmo parando o funcionamento do mesmo, quer através da exploração de protocolos, que consiste em encontrar vulnerabilidades nas fundações de funcionamento de determinado sistema informático. Um ataque DDoS é simplesmente um ataque DoS com a utilização de um sistema informático denominado *Master* que controla o funcionamento das denominadas máquinas *zombies*, sendo que o seu objetivo final é o mesmo de um ataque DoS.

Quando confrontada com estes ataques a CERT da Estónia entrou em ação, com o objetivo de recuperar o controlo dos seus sistemas informáticos e identificar os responsáveis. Contou com o apoio de vários especialistas estónios e estrangeiros e das CERTs de vários parceiros dentro da EU e da NATO. Com esta cooperação foi identificada a utilização de sistemas informáticos responsáveis por levar a cabo os ataques, dentro da Estónia e em mais 178 países. Foi ainda desvendado que a primeira série de ataques foi levada a cabo por indivíduos com fortes motivações políticas que seguiam instruções em *forums* e *websites*, descritas em russo.

Apesar das tensões existentes entre os dois países, quando inquirido sobre o seu envolvimento nestes ataques, o governo russo declarou que não havia tido qualquer envolvimento nos eventos descritos.

Tikk, Kaska e Vihul definiram as seguintes lições a serem identificadas a nível jurídico:

- "The traditional view of substantive criminal law considers cyber crime foremost as an economically motivated activity, which may not be sufficient to satisfactorily respond to politically motivated cyber attacks where the damaged legal interest is not the integrity, availability, confidentiality or the proper functioning and use of computer data, programs, or networks, but the political, constitutional, economic or social structure of the state;"
- "There are often differing legal requirements for what is permissible in criminal proceedings in the countries involved; and the attackers may resort their activities to jurisdictions that the attacked country – or the country receiving a request for assistance – does not recognise, which will foreclose the success of criminal proceedings. International law lacks effective enforcement mechanisms to ensure cooperation from the country in which the attacks originate, if the latter in refuses to cooperate. But international cooperation in criminal matters, in its mainly bilateral nature, may be ineffective even if both parties are willing and able to cooperate, as the Internet

> facilitates easy splitting up of a given illegal act to several small trails that can be left in a number of countries – such as the formation of a botnet to attack servers in a particular country."[148]

Indo de acordo com o defendido no ponto 4.2. deste dissertação, onde foi referida a necessidade de um enquadramento dos atos perpetuados no ciberespaço no direito da guerra, quando estes apresentassem contornos de atos de guerra.

4.3.2. Ciberataques à Geórgia em 2008.

Um ano depois da ocorrência dos ataques à Estónia, foi a vez de a Geórgia ser alvo de uma sequência de ciberataques entre 8 de Agosto e 28 de Agosto do mesmo ano, fruto do conflito armado entre a Geórgia, a Rússia e os separatistas da Ossétia do Sul pelo controlo da mesma[149]. À semelhança do caso anterior os métodos identificados para efetuar os ataques foram os seguintes:

- DoS e DDoS;
- Desfiguração de *websites*;
- Distribuição de *software* malicioso;
- *Spam* a comentários e e-mails.

Neste caso os alvos foram mais específicos, tendo sido atingidos *sites* do governo, presidente, parlamento, ministérios, de notícias e *media*, bem como *forums online* e instituições financeiras. Face a esta situação a CERT da Estónia atuou por forma a mitigar o impacto dos ataques ocorridos, com a ajuda de CERTs de outros países, impondo ainda um bloco ao acesso de *sites* russos por forma a controlar e libertar o fluxo de informação, alocou ainda serviços a servidores que se encontravam fora do país.

Foi concluído que os ataques teriam sido levados a cabo por um grupo organizado de *hackers* russos, não tendo sido obtida nenhuma prova que os ligasse ao

[148] Anexo C, Tikk, Eneken, Kaska, Kadri e Vihul, Liis, *INTERNATIONAL CYBER INCIDENTS – LEGAL CONSIDERATIONS*, [s.l.], [s.d.], p.33 – 34.

[149] Conflito armado pelo reconhecimento da Ossétia do Sul e da Abecásia como repúblicas independentes, com a Rússia a apoiar as forças destes últimos. O conflito terminou com a expulsão dos cidadãos georgianos do território em questão e do reconhecimento da Ossétia do Sul e Abecásia como repúblicas independetes.

governo russo, que mais uma vez negou qualquer envolvimento nos ataques ocorridos. Tendo resultado deste caso as seguintes conclusões:

- "The right of the injured state to use force as a response against another state depends on the level of involvement of the source state. While state direction and/or support of attacks can be seen as active involvement and therefore justify a stronger reaction, mere toleration (making no effort to suppress or stop the perpetrators) or inaction (being unable to effectively deal with the perpetrators) on behalf of the source state as passive forms of involvement do not make the source state a target of lawful military operations. Also, the remedy has to be proportionate to the threat – the smaller the overall harm arising from the attacks, the less there is reason to speak of holding the state responsible for cyber attacks. While the direct effect of the Georgian cyber attacks is difficult to estimate, the low overall dependence of the Georgian population on online services indicates that the effect of cyber attacks was not serious enough to amount to severe economic damage or significant human suffering. Considering this threshold, it is highly problematic to apply Law of Armed Conflict to the Georgian cyber attacks – the objective evidence of the case is too vague to meet the necessary criteria of both state involvement and gravity of effect."
- "Effective response to cyber attacks of scale and type like the Georgia incident are quite limited under law. In the long-term perspective, most value is to be derived from developing a legal and organisational structure that supports the development of a resilient infrastructure and service capacity, and provides a lawful basis to collect the data necessary for investigation of any future cyber attacks. Also important is the promotion of effective international

> cooperation, as there is no way for a country to coordinate defences against attacks originating from other jurisdictions."[150]

Estes dois estudos de caso permitem concluir que para uma melhor e mais adequada resposta face aos ciberataques, deve existir um esforço à escala internacional por forma a criar diretivas que possibilitem reger estes casos, incorporando-os no direito da guerra, visto que como é defendido na citação acima referida, o enquadramento dos ataques cibernéticos à luz do presente contexto do direito da guerra trata-se de uma questão bastante intricada.

Porem não se pode esperar que esta integração seja a solução definitiva e substancial no combate às ocorrências no ciberespaço, há também que reforçar as estruturas jurídicas de todos os Estados, tanto a nível documental como ao nível da criação e desenvolvimento de infraestruturas que habilitem os mesmos com uma maior capacidade de resposta e resiliência, este facto é substanciado com a informação obtida no estudo de caso dos ataques à Estónia, onde foram detetados sistemas informáticos que efetuaram os ataques em cerca de 180 países, comprovando uma vez mais que a problemática da segurança e da defesa no ciberespaço assume um carácter global.

[150] Anexo C, Tikk, Eneken, Kaska, Kadri e Vihul, Liis, *INTERNATIONAL CYBER INCIDENTS – LEGAL CONSIDERATIONS*, [s.l.], [s.d.], p.89 – 90.

Conclusão

Os sistemas informáticos e de comunicações, com a sua crescente evolução, fazem já parte do regular quotidiano de grande parte da comunidade mundial, este facto é verificável através da utilização dos mesmos pelos diversos setores da sociedade, seja para uso pessoal ou para prestação de serviços a outrem.

Esta constante evolução proporcionou um melhor e mais confortável estilo de vida às pessoas, possibilitando uma capacidade de comunicação rápida e transfronteiriça, através da transferência, armazenamento e tratamento de dados que deixaram, na sua maioria de ter uma dimensão física passando a ostentar um formato digital. Esta capacidade é apenas passível de existir devido ao surgimento do ciberespaço, uma nova dimensão que transcende as limitações físicas e temporais previamente associadas aos sistemas de informação e comunicações.

No entanto, como em todas as situações, este mar de possibilidades acarreta também uma conjuntura que facilita a sua utilização para levar a cabo atos com intenções menos nobres, surgindo assim os conceitos de cibercrime e ciberataque. Face a esta realidade tornou-se necessário tomar medidas de prevenção, resposta e retaliação a estas situações. Com o objetivo de fazer frente a esta nova problemática, têm vindo a ser criadas entidades especializadas, com o intuito de agilizar e aprimorar as capacidades de deteção e neutralização de ataques cibernéticos. Do ponto de vista jurídico foram já tomadas várias medidas, como a criação da Convenção de Budapeste e vários documentos complementares à mesma, a nível internacional, e ao nível doméstico o número de Estados com legislação nacional específica ao setor da cibersegurança tem vindo a aumentar.

Apesar de todas estas iniciativas e da sua constante atualização, as entidades responsáveis pelas questões do ciberespaço deparam-se com um desafio revestido de uma característica imensurável, a globalização e o cariz transfronteiriço associados ao conceito de ciberespaço, realçando assim a importância da cooperação internacional nestes casos. Esta cooperação torna-se complicada face ao facto de muitos países não terem ratificado ou assinado a Convenção de Budapeste, nem têm tão pouco,

instrumentos legislativos que rejam os crimes cibernéticos, fragilizando assim a sua estrutura de cibersegurança mas também a de outros Estados

O ciberespaço e as capacidades que do mesmo advêm, fizeram com que fosse definido, pela NATO, como domínio de desenvolvimento de operações militares, esta decisão indica que as preocupações da inclusão dos ciberataques no direito da guerra estão a ser consideradas, visto que atualmente as fontes de direito da guerra não contemplam os conceitos de ciberespaço, cibercrime ou ciberataque. Esta atualização torna-se necessária face à especificidade dos atos executados no ciberespaço, visto que é difícil considerar um ciberataque um ato de guerra de acordo com as presentes fontes de direito que orientam os conflitos armados, e face à crescente utilização de ataques a sistemas de informação e comunicações em cenários de conflito, esta atualização reveste-se ainda de maior importância.

Conclui-se portanto que o cibercrime é um problema de hoje e será um problema de amanhã, dada a constante e exponencial evolução tecnológica que é presenciada nos dias de hoje, não obstante, estão a ser tomadas medidas a nível nacional e internacional por forma a combater esta nova ameaça, apostando na melhoria das capacidades tecnológicas de deteção, resposta e retaliação, bem como na formação de recursos humanos habilitados a fazer frente a esta ameaça e na criação de mais e melhor adaptados instrumentos legislativos.

Contudo, todas estas iniciativas de pouco servirão se não existir uma cooperação internacional das entidades responsáveis pela investigação de cibercrimes e ciberataques.

Bibliografia

Livros e artigos:

AKEHURST, Michael, *Introdução ao Direito Internacional*, Almedina, Coimbra, 1985.

ANDRADE, Miguel, *NOMES DE DOMÍNIO NA INTERNET: A regulamentação dos nomes de domínio sob .pt*.,Centro Atlântico, Famalicão, 2004.

ANIL, Suleyman, *NCIRC (NATO Computer Incident Response* Capability), Madrid, https://www.terena.org/activities/tf-csirt/meeting11/NCIRC-Anil.pdf, acedido em Abril de 2016.

ARQUILLA, John, e Ronfeldt, David, Cyberwar is coming!, Comparative Strategy. Vol. 12, N.º 2, [s.l.], 1993.

ASCENSÃO, José de Oliveira, *Novas tecnologias e transformação do direito de autor, Estudos sobre o direito da internet e da sociedade da informação*, Almedina, 2001.

CASA BRANCA, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, Estados Unidos da América, 2011.

CENTRO DE INVESTIGAÇÃO JURÍDICA DO CIBERESPAÇO, http://www.cijic.org/, acedido em Junho de 2016.

COMISSÃO EUROPEIA, *Glossary and Acronyms*, http://ec.europa.eu/information_society/tl/help/glossary/index_en.htm#c, acedido em 15 de Setembro de 2015.

CONSELHO DE MINISTROS, *ESTRATÉGIA NACIONAL DE SEGURANÇA NO CIBERESPAÇO*, aprovada pela Resolução do Conselho de Ministros n.º36/2015 em 12 de Junho de 2015, Lisboa.

CORNISH, Paul, HUGHES, Rex e LIVINGSTONE, David, *Cyberspace and the National Security of the United Kingdom*, Chatham House, Londres, 2009.

CORREIA, Eduardo, *Direito Criminal Volume I*, Edições Almedina, Coimbra, 1996.

COSTA, J. Faria, *Les crimes informatiques et d'autres crimes dans le domaine de la technologie informatique au Portugal*, [s.l.], [s.d.].

COX, Noel, *The regulation of cyberspace and the loss of national sovereignty*, Auckland University of Technology, Reino Unido, 2002.

DEPARTAMENTO DE DEFESA DOS ESTADOS UNIDOS DA AMÉRICA, *An Assessment of International Legal Issues In Information Operations*, Washington, Estados Unidos da América, Maio de 1999.

DEPARTAMENTO DE JUSTIÇA DOS ESTADOS UNIDOS, *CYBERCRIME LAWS OF THE UNITED STATES*, https://www.oas.org/juridico/spanish/us_cyb_laws.pdf, acedido em 2 de Fevereiro de 2016.

EUROPEAN COMMISSION, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Bruxelas, European Commission, 2013.

GIBSON, William, *Neuromancer*, Nova Iorque, Ace Books, 1984.

GODWIN III, James B., et all, *Critical Terminology Foundations 2 Russia-U.S. Bilateral on Cybersecurity*, The EastWest Institute & Information Security Institute Moscow State University, 2014.

GOVERNO ESPANHOL, *NATIONAL CYBER SECURITY STRATEGY*, Presidência do Governo Espanhol, 2013.

GOVERNO NORTE-AMERICANO, *THE NATIONAL STRATEGY TO SECURE CYBERSPACE*, Casa Branca, Washington, 2013.

HOUAISS, Antônio, *Dicionário Houaiss da Língua Portuguesa, Instituto Antônio Houaiss*, Editora Objetiva Ltda., 2009.

INSTITUTO DA DEFESA NACIONAL, ESTRATÉGIA DA INFORMAÇÃO E SEGURANÇA NO CIBERESPAÇO, Lisboa, Dezembro de 2013-

JOHNSON, David e POST, David*, Law and Borders – the Rise of Law in Cyberspace*, Stanford Law Review 1367, 1996.

KISSEL, Richard, *Glossary of Key Information Security Terms*, National Institute of Standards and Technology, U.S. Department of Commerce, 2013.

MARTINS, António Gomes Lourenço et all, *CYBERLAW EM PORTUGAL. O direito das tecnologias da informação e comunicação*, Centro Atlântico, Famalicão, 2004.

MINISTÉRIO DA JUSTIÇA ESPANHOL, *Código Penal y legislación complementaria, Agencia Estatal Boletín Oficial del Estado*, Madrid, 21 de Janeiro de 2016.

MONROE, Jana D., *Before House Judiciary Committee, Subcommittee on Courts, the Internet and Intellectual Property*, Washington DC, Estados Unidos da América, 17 de Julho de 2003.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, *Framework for Improving Critical Infrastructure Cybersecurity*, Estados Unidos da América, 2014.

NATO, Prague Summit Declaration, Praga, 21 de Novembro de 2002.

NORTH ATLANTIC COUNCIL, *NATO Cyber Defence Taxonomy and Definitions*, Norfolk, NORTH ATLANTIC TREATY ORGANISATION, 2014.

NORTH ATLANTIC COUNCIL, *SECURITY WITHIN THE NORTH ATLANTIC TREATY ORGANISATION*, North Atlantic Council, 2002.

NORTH ATLANTIC TREATY ORGANIZATION, *Analysis and Recommendations of the Group of Experts on a New Strategic Concept for NATO*, 17 Maio 2010.

OTTIS, Rian e LORENTS, Peeter, *Cyberspace: Definition and Implications*, Tallinn, Cooperative Cyber Defence Centre of Excellence, [s.d.].

Parlamento do Reino Unido, *Computer Misuse Act 1990,* Londres, 29 de Agosto de 1990.

Parlamento do Reino Unido*, Police and Justice Act 2006*, Londres, 8 de Novembro de 2006.

QUIVY, Raymond e CAMPENHOUDT, Luc Van, MANUAL DE INVESTIGAÇÃO EM CIÊNCIAS SOCIAIS,

http://www.fep.up.pt/docentes/joao/material/manualinvestig.pdf, acedido em Outubro de 2016.

ROBIN, Ruefle, *Defining Computer Security Incident Response Teams*, Estados Unidos da América, 24 de Janeiro de 2007.

SILVA, Nuno Monteiro, SEGURANÇA E DEFESA NACIONAL: O DESENVOLVIMENTO DE CAPACIDADES DE CIBERDEFESA, Lisboa, 2012

SIMAS, Diana, *O CIBERCRIME*, Universidade Lusófuna de Humanidades e Tecnologias, Lisboa, 2014.

TIKK, Eneken, *Comprehensive legal approach to cyber security*, Tartu University Press, Estónia, 2011.

VERDELHO, Pedro et all, *Leis do Cibercrime Volume 1*, Centro Atlântico, Famalicão, 2003.

Legislação nacional e internacional:

COUNCIL OF EUROPE, *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems*, Estrasburgo, adotada a 28 de Janeiro de 2003.

———, *CONVENTION ON CYBERCRIME*, adotada em Budapeste a 23 de Novembro de 2001.

———, *DIRECTIVE 2006/24/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL*, adotada a 15 de Março de 2006.

REPÚBLICA PORTUGUESA, Assembeleia da República, Lei nº 83/2015, *Código Penal*, Diário da República, I série nº151, 5 de Agosto de 2015.

———, Assembeleia da República, Lei nº 109/1991, *Lei da criminalidade informática*, Diário da República, I série nº188, de 17 de Agosto de 1991.

———, Assembeleia da República, Lei nº 109/2009, *Lei do Cibercrime*, Diário da República, I série nº179, de 15 de Setembro de 2009.

_____, Ministério da Defesa Nacional, Decreto-Lei nº184/2014, *Lei Orgânica do EMGFA*, Diário da República, I série nº250, de 29 de Dezembro de 2014,

Portais da internet:

NATIONAL CRIME AGENCY, *Working in partnership,* http://www.nationalcrimeagency.gov.uk/about-us/working-in-partnership, acedido em 10 de Março de 2016.

NORTH ATLANTIC TREATY ORGANIZATION, *Cyber defence*, http://www.nato.int/cps/en/natohq/topics_78170.htm, acedido em Março de 2016.

PRWEB, *Global Upgrade Makes Internet More Secure*, http://www.prweb.com/releases/DNSSEC/Cyber_Crime/prweb4321774.htm, acedido em Janeiro de 2016.

THE ECONOMIST, *War in the fifth domain*, http://www.economist.com/node/16478792, acedido em Junho de 2016.

Anexo A – Convenção de Budapeste sobre o Cibercrime[151]

[151] Ver supra, nota 49.

Anexo B – Lei nº 109/2009 Lei do Cibercrime[152]

[152] Ver supra, nota 100.

Anexo C – Estudo de caso dos ciberataques à Estónia e à Geórgia[153]

[153] Ver supra, nota 148.