ACADEMIA MILITAR

DIRECÇÃO DE ENSINO

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

‘A Ciberespionagem no contexto Português’

Susana Maria Lopes da Silva

Dissertação/Trabalho de Projeto para a obtenção do grau de

Mestre em Guerra da Informação

Lisboa
2014

ACADEMIA MILITAR

DIRECÇÃO DE ENSINO

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

‘A Ciberespionagem no contexto Português’

Susana Maria Lopes da Silva

Dissertação de Mestrado em Guerra da Informação

Trabalho realizado sob a supervisão:

Orientador Tenente Coronel Proença Garcia

Coorientador Coronel Fernando Freire

AGRADECIMENTOS

Desde o início do meu percurso que contei com a confiança, o incentivo e o apoio de pessoas muito especiais O trabalho que aqui apresento não seria o mesmo sem todas essas valiosas contribuições. É este o espaço próprio para manifestar a minha completa gratidão a todos eles.

Em primeiro lugar, quero agradecer ao Tenente-Coronel Proença Garcia, orientador desta tese, por ter aceite desde logo orientar este trabalho.

Agradeço igualmente ao meu co-orientador, Coronel Fernando Freire, pelo apoio e tempo que generosamente me dedicou em todas as fases que levaram à concretização deste trabalho, mas também pelas sugestões prestadas.

Ao Luís, um agradecimento especial pelo apoio e carinho diários, pela transmissão de confiança, ajuda e de força, em todos os momentos. Por tudo, a minha enorme gratidão!

À minha amiga Núria, um muito obrigada pela amizade, companheirismo e ajuda, imprescindiveis nesta caminhada e que permitiram que cada dia fosse encarado com mais motivação.

Espero que após esta etapa, que agora termino, possa, de alguma forma, retribuir e compensar todo o carinho, apoio e dedicação que me ofereceram.

ÍNDICE

1. INTRODUÇÃO 1
2. DA ESPIONAGEM À CIBERESPIONAGEM 13
3. O PAPEL DO CIBERESPAÇO E A REALIDADE DOS CIBERATAQUES 27
3.1. O ciberespaço 27
3.2. Os ciberataques 29
3.3. Tipologia dos ataques cibernéticos e dos agentes 36
4. UMA REALIDADE PREOCUPANTE – A CIBERESPIONAGEM 42
4.1. A ciberespionagem: de um mero ciberataque às APT 42
4.2. Formas de ciberespionagem – Dos Estados às empresas 45
4.3. Atores principais 48
4.4. Ciberespionagem como campo de confronto 51
5. O CONTEXTO PORTUGUÊS 56
6. A PERSPECTIVA INTERNACIONAL 69
6.1. União Europeia 69
6.2. EUA 72
6.3. Austrália 76
6.4. OCDE, ONU e Outros Países 79
7. DOS DESAFIOS DAS SOLUÇÕES À COOPERAÇÃO INTERNACIONAL 83
7.1. Como proteger uma empresa ou nação contra a ciberespionagem 83
7.2. Estruturas e meios tecnológicos 90
7.3. Políticas de segurança de informação 91
7.4. A cooperação internacional 93
8. CONCLUSÕES 99
BIBLIOGRAFIA 109

RESUMO

Na era da Sociedade da Informação, as empresas e as matérias-primas deixaram de ser os recursos alvo mais procurados, passando a informação, a ser um alvo privilegiado de ações maliciosas enquanto recurso intangível.

A crescente dependência da tecnologia e da informação por parte de pessoas e Estados, tornam-nos vulneráveis às ameaças do ciberespaço, fazendo com que cada vez mais se criem mecanismos de protecção e segurança para minimizar os riscos que daí advém.

No entanto, a exploração das redes, no ciberespaço, não apresenta apenas uma vulnerabilidade, tendo em conta que produz a capacidade de alguns atores hostis influenciarem a cadeia de funcionamento e de valor das organizações e dos Estados, evidenciando no final um exercício do poder

Assim, esse ciberespaço é utilizado muitas vezes como um local privilegiado para a espionagem de Estados e para uma exploração militar, facto esse que tem naturalmente repercurssões ao nível do ambiente estratégico, nacional e internacional. Aos Estados, enquanto garantes da segurança nacional, exige-se que os mesmos se preocupem com estas questões primordiais e que as mesmas façam parte das suas preocupações, no que respeita às políticas e instrumentos de Segurança e Defesa.

Todas estas preocupações têm fomentado esforços no sentido de se elaborarem Estratégias de Cibersegurança e de mobilizar a cooperação internacional, pois é neste desiderato que se julga também estar boa parte das soluções, nomeadamente no que concerne ao combate à ciberespionagem.

Palavras-chave: *Espionagem; Ciberespionagem; Informações; Cibersegurança; Cooperação Internacional*

ABSTRACT

In the era of the information society, target-resources are no longer just companies and raw materials, but also information, because as an intangible asset it has become a prime target for malicious actions.

The risk connected to cyberspace, highlights threats and vulnerabilities resulting from increasing dependence on technology and information of people and states. Obviously this requires mechanisms of protection and security to be created.

So, if cyberspace is used as a privileged place for spying the states and for military explotation, it is clear that this will be reflected in the national and international strategic environment. The States, as guarantors of national security, are required to have the same worry with these key issues and these questions should be part of their concerns in with regard to policies and instruments of security and defense.

If the possibility of operating the networks on the one hand shows the vulnerability, on the other, produces the ability of some hostile actors influence the chain of operation and value of organizations and states, showing at the end an exercise of power.

All these concerns have fostered efforts to develop strategies for Cyber Security and mobilize international cooperation. This kind of cooperation is believed to also be a good part of the solutions, particularly with regard to combating cyber espionage.

Keywords: *Espionage; Cyber Espionage; Informations; Cyber Security; International Cooperation*

ACRÓNIMOS E SIGLAS

APT – Advanced Persistent Threats

CERT - Computer Emergency Response Teams

CIIP - Critical Information Infrastructure Protection

CSOC - Cyber Security Operations Centre

DDoS - Distributed Denial of Service

DHS - Department of Homeland Security

DoS - Denial of Service

ECOSOC – Economic and Social Council

EEAS - European External Action Service

ENISA - European Network and Information Security Agency

ENSI - Estratégia Nacional de Segurança da Informação

OCDE – Organization for Economic Co-Operation and Development

OCS – Office of Cyber Security

OSCE – Organization for Security and Co-Operation in Europe

NATO - North Atlantic Treaty Organization

NSA – National Security Agency

SIGINT - Signals Intelligence

TIC - Sistemas de Informação e comunicação

UE INTCEN - EU Intelligence Analysis Centre

UK - USA - Security Agreement

CAPÍTULO 1
INTRODUÇÃO

Desde os primórdios da Humanidade, que o ser humano motivado pela ganância, instinto de sobrevivência ou sentimento territorial, se envolveu em conflitos com o seu semelhante ou outras raças animais.

Os primeiros conflitos/disputas começaram por ser realizados contra um indivíduo, mas após a união dos elementos em grupos mais ou menos homogéneos, tais lutas foram dirigidas contra clãs, fações e nações.

Se numa fase inicial em que os conflitos surgiam de forma mais ou menos inopinada, motivado por uma simples disputa de cariz territorial, patrimonial ou sexual, em que o conhecimento sobre o adversário era adquirido no momento, já numa fase posterior em conflitos entre clãs/ nações, existia obrigatoriamente um conhecimento prévio sobre qual o adversário a guerrear e quais as suas armas ou vantagens.

Com o evoluir dos tempos, em que a razão bélica não se imiscuiu ao desenvolvimento da raça humana, foram desenvolvidos conceitos de estratégia e técnicas de guerra, ainda que rudimentares. Tais estratégias ou artes, pressupunham obrigatoriamente a informação das qualidades do inimigo a enfrentar, nomeadamente o número, as armas utilizadas e quais os melhores guerreiros.

Para obter tais dados, a recolha de informação era vital, existindo desde o início elementos treinados e capazes de se aproximarem do inimigo de forma eficaz e assim puderem transmitir as características guerreiras do adversário.

Os elementos acima descritos poderiam ser numa fase inicial batedores, desertores, sendo que posteriormente verificou-se a necessidade imperiosa de contratar ou formar alguém que pudesse conviver com o inimigo ou pelo menos partilhar com ele o mesmo território,

para que de forma concreta e segura conseguisse apurar quais as suas capacidades em determinada fase e principalmente quais os seus planos de ataque ou defesa.

Hoje, tal como antes, os participantes dos conflitos necessitam da *intelligence* do ambiente (terreno, atores, personalidades, ...) do seu "campo de batalha". Porém, por ventura, fruto das potencialidades da sociedade de Informação e das vicissitudes de uma Sociedade Global, o valor da informação mais que nunca tem elevada pertinência na "sobrevivência" do complexo e competitivo mundo empresarial e afeta enormemente o relacionamento entre os Estados, perturbando posições de poder e o seu comportamento em processos decisórios, porque estão em causa interesses nacionais, de que resulta uma aparente "guerra" económica surda-muda mas corrosiva, cujos "rastos" são visíveis, aqui ou ali, pelo menos em atos de (ciber)espionagem industrial e política levados a cabo por empresas ou mesmo, serviços de informações de países hostis e nalguns casos aliados.

Este fenómeno motivou-me a procurar refletir sobre a temática da ciberespionagem, e a procurar perceber a eventual novidade do fenómeno, auscultando a tomada de consciência de cidadãos, empresas e estados e daí inferir do ajustamento e da necessidade de medidas.
Espionagem não é um fenómeno novo. A própria Bíblia faz relato de Deus aconselhando Moisés, o líder do seu povo escolhido, a enviar 12 soldados/delegados para procurar detalhes sobre a Canaã, a dita Terra Prometida.

Sun Tzu, na Arte da Guerra, falava da utilização eficaz de espiões para que a estratégia a adotar fosse a mais eficaz, possibilitando um conflito com o menor número de baixas e despesas, ou então originando como o próprio dizia "*uma guerra sem desembainhar a espada*". *(*Sun Tzu)

Como já foi referido, os primeiros espiões começaram por ser desertores, que aliciados por alvíceras e dividendos prometidos caso a fação aliciadora vencesse, forneceram informações vitais sobre a constituição dos exércitos, as suas debilidades e qual a estratégia a utilizar por determinado general.

A época medieval também não foi exceção à utilização de espiões, existindo diversos casos em que o seu desempenho se mostrou fulcral para o desenrolar de determinadas ações em teatros de guerra específicos. Em Portugal, foram conhecidas as tentativas eficazes do rei

D. João II em colocar elementos fiéis à sua causa no seio da corte de Castela, proporcionando a recolha de dados importantes para a decorrente corrida aos novos mundos.

Diz-se que a primeira organização de informações relativamente bem organizada foi criada no século XVI, no decorrer do reinado da Rainha Elizabeth I, tendo como responsável um cavaleiro de sua inteira confiança chamado Sir Francis Walsingham. Dentro das suas atribuições Sir Francis recrutou dentro e além-fronteiras diversos elementos, entre os quais se enumeram estadistas e diplomatas, que pelas suas capacidades insuspeitas de viajarem forneciam a cobertura ideal para a passagem de informações confidenciais. Interessante é o caso do médico oficial da Rainha Elizabeth I, o português judeu Rodrigo Lopez, que se diz ter sido um espião ao serviço de Sir Francis. (TAVARES, 2007)

Face à clara vantagem de uma nação em determinada situação de conflito iminente ou numa fase preliminar, conseguida através da utilização de informação classificada, depressa se fez notar a necessidade de existirem alguns indivíduos dotados de conhecimentos concretos e eficazes na área da espionagem, para posteriormente então virem a ser criados os primeiros grupos organizados e com apoio institucional neste âmbito.

Devido à falta de elementos históricos fidedignos e completos, somente são conhecidas alguns feitos levados a cabo por espiões nas épocas mais remotas, mas com o decorrer dos tempos, em que a capacidade de narrar historicamente os feitos de determinada cultura se foi aprimorando, foi possível ter acesso aos registos de agentes profissionais que com o risco da própria vida transmitiam as informações necessárias à nação rival.

Foi no século XX, no decorrer de sangrentas e sempre evitáveis guerras que marcaram a existência humana, que a espionagem começou de forma organizada a se solidificar no aparelho marcial das nações, onde de forma metódica se formaram agentes com conhecimentos específicos, em instituições criadas para o efeito.

Durante a II Guerra Mundial, foram criadas as primeiras agências oficiais, com siglas amplamente divulgadas na comunicação social da época. São exemplo, países como os EUA, a Alemanha e a União Soviética. Assim, na década de quarenta os EUA criaram a

OSS (Escritório de Serviços Estratégicos), posteriormente batizada como CIA (Agência Central de Inteligência)[1], a União Soviética tinha NKVD, mais no final da II GM surge o KGB (Comité de Segurança do Estado)[2], uma combinação de operações secretas no estrangeiro unificadas às funções de uma polícia federal. A Inglaterra fundou os seus MI (Military Intelligence), desdobrandos em números de terminologia até ao 19, sendo os mais conhecidos o MI5 (Security Service)[3] e MI6 (Secret Intelligence Service)[4], relativos a assuntos de defesa do estado internos e externos, respetivamente. (CHALOU, 1992)

Foram estas três nações que protagonizaram as maiores guerras de inteligência, degladiando-se em primeiro plano durante a II Guerra Mundial, contra nações como a Alemanha e o Japão e posteriormente entre si, aquando do surgimento da Cortina de Ferro, na denominada época de ouro da espionagem, a Guerra Fria.

A Guerra Fria, foi a designação romancista fornecida à oposição deliberada entre os dois blocos ressurgidos após a II Guerra Mundial. De um lado, encontravam-se os denominados países de Leste, de cariz político e ideológico comunista, como por exemplo a Alemanha de Leste – RDA e a União Soviética – com todos os países aliados, do outro lado países como os EUA, Reino Unido, França e Alemanha Federal.

No que se refere aos países socialistas, firmaram estes na Polónia o denominado Tratado de Varsóvia, que surgiu como resposta à NATO, estabelecendo assim uma aliança de entre ajuda entre os países de Leste caso ocorressem iniciativas militares contra eles por parte das forças ocidentais.

A referida guerra, não era mais do que um tentar "tomar vantagem" relativamente aos planos do bloco rival, em que aceder de forma priveligiada a documentos ou segredos de estado, era considerada a vitória de uma batalha, com valor igual ou superior àquelas anteriormente realizadas num verdadeiro campo de batalha, em que o sangue cobria a terra.

[1] http://pt.wikipedia.org/wiki/Office_of_Strategic_Services (em linha) [Consult. 20 Abril 2014]
[2] http://pt.wikipedia.org/wiki/KGB (em linha) [Consult. 20 Abril 2014]
[3] O MI5, oficialmente designado Security Service (Serviço de Segurança), é o serviço britânico de informações (ou inteligência) de segurança interna e contra-espionagem. MI5 é a abreviatura de *Military Inteligência, section 5*, que é a designação tradicional, ainda vulgarmente usada, do Serviço de Segurança.
[4] http://en.wikipedia.org/wiki/Directorate_of_Military_Inteligência (em linha) [Consult. 20 Abril 2014]

No entanto, as mortes neste tabuleiro de xadrez político também se faziam sentir, fazendo baixas entre alguns peões, quando descobertos, ou sacrificados pelos seus recrutadores a troco de outras vantagens mais favoráveis.

Na época, as informações classificadas eram sobretudo recolhidas em suporte de papel, como por exemplo planos sobre uma arma nova, de uma operação militar ou nomes de agentes infiltrados. Eram esses papéis, que acondicionados em dossiers, tinham que ser entregues ou transmitidos para o "outro lado" de forma segura, para o agente e para documento em si, pois a informação teria que chegar intocável para não comprometer a sua fidedignidade e relevância. Nesta altura, toda a informação, tinha que ser enviada como um tipo de correspondência interna ou externa, quer utilizando as vias consideradas normais, quer através da entrega em mão caso a situação em específico o exigisse. Porém, já se recorria ao meios eletrónicos para a troca de informação ou para facilitar a comunicação. Mas não só, também se utilizava na recolha de informação. (CHALOU, 1992).

Uma aliança secreta de SIGINT[5] teve a sua origem durante a Segunda Guerra Mundial, no sentido de conjugar esforços e tecnologias conjuntas dos Aliados, na interceção e análise das mensagens cifradas, trocadas pelas tropas alemãs, japonesas e soviéticas. A continuação no pós-guerra desta aliança de informações entre o Reino Unido e os Estados Unidos da América foi formalizada por volta de 1947/48 com a assinatura de um acordo de cooperação e partilha de informação, conhecido como o Acordo UKUSA[6], ao qual posteriormente aderiram o Canadá, a Nova Zelândia e a Austrália. Cada um assumiria responsabilidades na superintendência da vigilância em diferentes partes do globo.

É na sequência dste acordo que surge o sistema ECHELON. "*A rede ECHELON foi desenvolvida no final dos anos 60 e constitui uma parte fundamental do sistema global dirigido pela UKUSA, competindo às suas estações espalhadas pelo mundo interceptar e processar as comunicações retransmitidas via satélites de comunicações. Outras partes do mesmo sistema intercetam mensagens da Internet, dos cabos submarinos, das transmissões radiofónicas, dos equipamentos secretos instalados em embaixadas, ou utilizam satélites*

[5] Informação resultante da interceção de sinais com origem em emissão de energia eletromagnética
[6] http://www.nsa.gov/public_info/declass/ukusa.shtml (em linha) [Consult. 21 Abril 2014].

orbitais para monitorização de sinais vindos de qualquer ponto da superfície terrestre". (SACRAMENTO, 2006)

Com o término da Guerra, o sistema Echelon nunca deixou de funcionar, prosseguindo as atividades conjuntas de inteligência, que de uma forma mais objetiva podemos designá-la de espioangem.

É com a utilização de meios electrónicos que terá sido o início da nova era da sociedade da informação, que veio introduzir novas formas de interação e de relacionamento.

Com o surgir da era digital, em que computadores começaram progressivamente a substituir as antigas, mas eficazes máquinas de escrever, toda a informação começou a ser guardada em formato digital dentro quer dos privados quer nos departamentos públicos, possibilitando assim um armazenamento mais eficaz, capacidade de organização de maior eficácia e facilidade na procura dos dados guardados.

Por sua vez, o aparecimento da internet, invenção que veio modificar global e abruptamente a forma de comunicação entre quase todos os habitantes do planeta, veio dotar os Estados de maior capacidade de comunicação, quer a nível interno (entre departamentos governamentais) e a nível externo (troca de informações com outros países).

Tal invenção, veio por seu turno facultar aos agentes infiltrados no terreno a capacidade ou possibilidade de transmitirem mais celeremente toda a informação recém-adquirida. O suporte digital proporcionou que uma caixa de papéis "top secret" fosse acondicionada num dispositivo eletrónico (tipo Pen Drive ou cd), facilitando o seu envio de forma facilmente dissimulada.

No entanto, paralelamente a utilização massiva da internet originou também a abertura de uma porta ao mundo do crime, que até então parecia fechada ou dissimulada – o surgimento da intitulada criminalidade informática ou cibercrime[7]. Este tipo de crime

[7] Lei nº 109/2009, 15 Outubro de 2009 (Lei da Cibercrime).

empeçou por ser perpetrado inicialmente por diversos indivíduos ou associações, sumidades em conhecimentos informáticos e normalmente designados por *hackers*[8].

Estes novos criminosos, motivados por fundamentos criminais, religiosos ou políticos, conseguiam penetrar nos sistemas informáticos governamentais, retirando desta forma informações cruciais das bases de dados.

O surgimento desta nova ameaça informática obrigou os Estados a desenvolver complexos e elaborados métodos de proteção de dados e das redes envolvidas, quer através de sistemas anti-intrusão (antivírus, firewall) ou mesmo através da limitação e credenciação extremamente minuciosa de pessoas com acesso a determinados níveis de informação.

O aparecimento dos denominados *hackers*, ou de especialistas com intenções intrusivas, normalmente malévolas, veio ameaçar as estruturas de *intelligence* mundiais, que se viram despojadas de um sentimento de segurança que sempre julgaram ser permanente. Para piorar a situação, surgia no horizonte a possibilidade bem real e atual de os ciberataques estarem a ser executados por nações rivais, nomeadamente serviços de informação, e não simplesmente por grupos anarquistas pretendendo uma nova ordem mundial ou um mundo mais justo.

A possibilidade de uma nação ver os seus segredos mais valiosos nas mãos de rivais ou nas parangonas dos tablóides, faz gelar qualquer dirigente político, pois um simples acesso a determinada base de dados, especialmente na área da defesa ou dos processos decisórios, pode fazer a diferença no campo de batalha ou da salvaguarda dos interesses nacionais.

Para além da intrusão em sistemas governamentais, a intromissão do meio informático no domínio pessoal de alguns dirigentes políticos, também assumiu relevo em grande monta. Tal situação poderá originar o acesso a dados pessoais e íntimos de determinada figura política proeminente, possibilitando inevitavelmente o seu controlo através de chantagem, uma vez que o receio de um escândalo político ou sexual, de exposição de corrupção quer-

[8] Pessoa com grandes conhecimentos de informática e prohramação, que se dedida a encontrar falhas em sistemas e redes computacionais. = Ciberpirata, Pirata Informático in Dicionário Priberam de Língua Portuguesa [em linha]. http://www.priberam.pt/DLPO/HACKERS [Consult. 22 Abril 2014]

se que seja evitado a tudo custo, para bem de uma suposta aparente estabilidade política nacional e internacional.

Não é só através do acesso ilegítimo a informação crucial pertencente às estruturas fundamentais do Estado que se pode atacar um País. Outra forma de ferir no âmago a estabilidade de uma nação, é através do ataque cibernético ou ações intrusivas, a estruturas económicas, pois a recolha de informação crucial relativa a estratégias comerciais ou delas provenientes poderá fornecer vantagem na elaboração de um qualquer ardil altamente nocivo para o interesse nacional que afete mormente a economia, qual vírus a penetrar nas defesas de um corpo.

Sabemos que qualquer política de desenvolvimento e sobrevivência, em especial a de defesa (em sentido lato) tem que ser apoiada por uma economia que a sustente. Lesando a parte financeira de uma nação é o equivalente a atacar as provisões de um exército, tal como antigamente os militares executavam ações de guerrilha aos fornecimentos de comida e água do inimigo, poderá ser comparado a um ataque a objetivos estratégicos. Nenhum exército ou Estado sobrevive sem o apoio financeiro adequado, nem se consegue dotar dos meios necessários (humanos, logísticos,… e bélicos) para repudiar os ataques ou para o planeamento de missões efetivas contra o mesmo.

Casos como a Operação 'Outubro Vermelho' (2012)[9], a 'Mask' (2013)[10], o ataque ao Google (2010), o Flame (2012)[11], Campanha Safe Net (2012) [2] são exemplo de 'campanhas' de ciberespionagem, algumas delas estiveram ativas por diversos anos, contra instituições governamentais e diplomáticas, mas também empresas de petróleo, gás, instituições de pesquisa, entre outras categorias de alvos. Estas operações procuraram essencialmente 'roubar' informação valiosa através de meios informáticos, que inclui informações sobre conteúdos apresentados no ecrã do computador, informações sobre sistemas específicos, ficheiros guardados, dados sobre contactos e até conversas áudio, entre outros conteúdos.

9 http://www.kaspersky.com/about/news/virus/2013/Kaspersky_Lab_Identifies_Operation_Red_October_an_Advanced_Cyber_Espionage_Campaign_Targeting_Diplomatic_and_Government_Institutions_Worldwide (em linha) [Consult. 21 Abril 2014]

10 Relatório da Kaspersky sobre a APT denominada por 'Careto' ou 'Mask', http://kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/unveilingthemask_v1.0.pdf (em linha) [Consult. 21 Abril 2014]

11 http://www.kaspersky.com/pt/flame (em linha) [Consult. 21 Abril 2014]

Estas preocupações são suficientes para mostrar que a realidade espelha a crescente necessidade dos Estados disporem de serviços especializados que prestem apoio isento, esclarecido e eficaz, ao nível segurança nacional, com especial incidência na cibersegurança, aos diversos órgãos de soberania, mas não só aos setores vitais desse mesmo Estado. É tendencialmente crescente o surgimento de novas formas de radicalismo associadas a outros atores não estatais, em aspetos de ciberespionagem, enquanto variante da espionagem dita tradicional, e nomeadamente em atos de ciberativismo, hacktivismo e cibervandalismo.

Tal necessidade encontra-se no panorama português consubstanciada nos serviços de informação portugueses, imprescindíveis para a segurança e defesa nacionais, e cuja atuação assenta, ao nível defensivo, na identificação de vulnerabilidades e ameaças conduzidas contra os interesses nacionais, e, por outro lado, ao nível ofensivo, na projeção dos interesses, bem como influenciar, determinar e condicionar o quadro geopolítico, geoeconómico e mesmo geocultural de determinadas áreas vitais do Estado de Direito Democrático.

No atual sistema legal português, os serviços de informações refletem-se na atuação do Sistema de Informações da República Portuguesa, que enquanto peça fundamental do primeiro pilar do sistema de segurança interna e externa, desempenha um papel fundamental na prossecução do interesse público, assessorando a tomada de decisão dos competentes órgãos do Estado em matéria de política de segurança interna bem como externa.

É neste âmbito que surge a motivação para o presente trabalho cujo objetivo é debruçar-se sobre a temática da ciberespionagem, percecionando a tomada de consciência deste novo fenómeno e compreender em que medida existem formas estruturadas para a antecipação de ameaças e prevenção de riscos relativos à segurança coletiva dos cidadãos e do Estado de Direito Democrático.

Pretende-se assim apresentar um panorama a nível nacional do que tem sido realizado neste âmbito, saber efetivamente se Portugal está devidamente preparado para enfrentar este tipo de incidentes.

É consabido que no plano nacional tem vindo a ser desenvolvidos esforços no sentido de se vir a criar uma estratégia nacional de cibersegurança, com a definição dos organismos que poderão ter responsabilidade neste quadro de segurança.

No entanto, coloca-se a questão, e em especial no que concerne à temática a que se propõe este trabalho, a da ciberespionagem, se a legislação portuguesa vigente para a espionagem em Portugal é suficiente para aglomerar a ciberespionagem, ou será que é necessário repensar e apresentar propostas de alteração. E será que se encontra preparado para enfrentar uma batalha contra a ciberespionagem.

Tendo como objetivo uma melhor governação da cibersegurança em Portugal, pretende-se de acordo com as competências, capacidades e responsabilidades dos vários intervenientes, determinar se as políticas e estruturas nacionais existentes são suficientes na prevenção e combate à ciberespionagem e apresentar algumas propostas no sentido de promover a convergência de perspetivas e de um conjunto de entidades e iniciativas num fio condutor para a cibersegurança nacional.

Obviamente, um conjunto de questões/dúvidas/incertezas se levantaram e para que pudessem ser respondidas era necessária uma reflexão mais detalhada sobre o assunto, até porque parece ser um tema envolto nalguma ’nebulosidade’, associado desde sempre a atividades secretas, o que faz que esta imagem não se dilua e que ainda haja bastante apreensão em falar sobre ela. O carácter ameaçador de que se reveste a ciberespionagem em especial para os Estados, podendo colocar em causa a integridade democrática e securitária dos mesmos, e também para as entidades não-estatais, que são a imagem do poderio económico e financeiro de qualquer nação, merece a nossa atenção, na procura de resposta e porventura recomendações.

Pretende-se então refletir sobre em que medida a ciberespionagem é um fenómeno alarmista ou plausível, real e de impacto. Tentar igualmente percecionar em que medida a cooperação pode funcionar como instrumento nas relações predatórias dos estados entre si, sendo por isso de efeito contrário ao desejado.

E por fim compreender a coordenação e articulação de medidas das medidas de prevenção e combate à ciberespionagem e proceder a recomendações para melhorias.

O presente trabalho iniciou-se com o levantamento de uma questão central (QC) a responder:

- No Contexto português, a ciberespionagem é uma ameaça com expressão?

Desta derivaram questões subsidiárias (QD) como:

- QD1: Porque é (ciber) espionagem uma ameaça que preocupa os Estados?
- QD2: O que diferencia espionagem de ciberespionagem?
- QD3 : Que mecanismo nacionais na prevenção? E combate à ciberespionagem?
- QD4 : Em que medida a cooperação internacional é possível no combate à ciberespionagem?

Subsequentemente levantaram-se como hipóteses para validar aquilo a que nos propomos refletir que são as seguintes:

H1 – Os ataques de ciberespionagem afetam a vida da sociedade e os processos decisórios do Estado.

H2 – A ciberespionagem é mais do que emigração da espionagem para o ciberespaço.

H3 – As políticas e estruturas nacionais existentes são suficientes para a prevenção e combate à ciberespionagem.

H4 – A cooperação internacional na pr4venção e no combate á ciberespionagem não funciona como um contributo para a espionagem entre cooperantes/parceiros.

Metodologia

A metodologia partiu de um estudo de carácter descritivo, baseando-nos na análise documental, bibliográfica, quer de fontes nacionais, quer de fontes internacionais. Deste modo, procedeu-se ao levantamento do estado da arte, através da revisão de literatura, nos conceitos chave para este trabalho, nomeadamente de Ciberespionagem de forma a ficarmos munidos de ferramentas que nos permitam fundamentar a orientação seguida. Pretende-se com isso contribuir para uma melhor interpretação do conceito de Ciberespionagem, dos seus intervenientes, e do seu impacto nas estruturas governamentais e económicas.

Consideramos que as obras citadas ao longo da dissertação, sendo que só essas são referenciadas na bibliografia, constituem o mínimo indispensável para a realização de uma investigação desta natureza.

Num primeiro capítulo, fizemos a introdução do fenómeno (ciber)espionagem para num segundo capítulo procurar abordar o conceito de espionagem e de forma esta evoluiu para a ciberespionagem. Um terceiro capítulo tem por objetivo descrever o papel do ciberespaço e a realidade dos ciberataques na atualidade. O quarto capítulo irá debruçar-se de forma mais específica sobre a ciberespionagem enquanto uma ameaça aos Estados e entidades privadas, mas também tentará abranger uma análise às formas que assume a ciberespionagem e sobre quem são atores principais.

Tendo por pano de fundo a ciberespionagem procurou-se nos capítulos seguintes, quinto e sexto, analisar, respetivamente, o contexto nacional e o internacional.

Num sétimo capítulo procurou-se identificar os desafios que se colocam aos Estados e empresas, quais políticas adoptar e igualmente percecionar em que medida a cooperação pode funcionar como instrumento nas relações predatórias dos estados entre si.

A finalizar com a parte das conclusões, apresentamos o capítulo oitavo que consiste numa sumula da reflexão de todo o trabalho, apresentando eventuais recomendações e propostas de possível continuidade futura de trabalhos.

CAPÍTULO 2.
DA ESPIONAGEM À CIBERESPIONAGEM

A espionagem já vem sendo referenciada desde o tempo dos fenícios, persas, hebreus e egípcios. Sendo visível em alguns hieróglifos egípcios referências a algumas técnicas de espionagem[12].

No século VI a.c, Sun Tzu falava da espionagem no seu livro "Arte da Guerra" aquando a sua abordagem à importância de se conhecer o inimigo. Defendia a ideia que o general criterioso e o governo esclarecido deviam utilizar as mais dotadas inteligências do exército para a espionagem.

"*Um governante esclarecido e um general sábio são vencedores porque suas ações se baseiam em sua vidência. A vidência não pode ser a alcançada por meio de espíritos, nem deuses, nem por analogia com o passado, nem mesmo por cálculos; depende, exclusivamente, dos homens que conhecem o inimigo[13]" [Sun Tzu].*

Para o general chinês eram considerados cinco tipos de espiões:

1. **nativos**, que seriam camponeses do povo inimigo a serviço do nosso exército;
2. **internos**, oficiais inimigos empregados em nosso exército;
3. **duplos**, espiões inimigos que empregamos em nosso exército; eles seriam recrutados entre os espiões que trabalham para o inimigo;
4. **dispensáveis**, espiões nossos a quem entregamos informações falsas de propósito;
5. **vivos**, os que voltam com informações sobre o inimigo;

[12] Encyclopedia of Espionage, Inteligência, and Security. (Lerner KL, Lerner BW). Thomson (Reuters) /Cengage | Gale; 2004. (em linha) [Consult. 20 Maio 2014] Disponível em: http://militero.files.wordpress.com/2010/10/espionage-inteligência-and-security-encyclopedia-of-volume-3.pdf

[13] Sun Tzu Arte da Guerra Capitulo XIII.

Sendo para ele a categoria dos espiões duplos a mais importante "*É indispensável descobrir os espiões que trabalham para o inimigo; suborna-os, e tente fazê-los passar para o seu lado. Cuide bem deles e oriente-os. Eles se tornarão espiões duplos".*

A palavra espionagem deriva do ato de espiar[14], que por sua vez significa[15]: "observar secretamente" ; "espreitar"; "seguir ocultamente os passos de ", tendo a sua origem sido no âmbito da estratégia militar, é ainda hoje utilizada para definir a recolha de informações dos alvos sem o seu conhecimento com o intuito de se ganhar vantagem sobre o inimigo.
Classificando-se como espião *uma pessoa utilizada por um governo ou outra organização para obter secretamente informações sobre um inimigo ou concorrente*[16].

Passados mais de 2000 anos, a palavra espionagem, continua quase que diariamente presente nos memorandos dos Estados. Tendo sido promovida essencialmente pelos Estados com o objetivo de obter informações políticas ou militares e utilizá-las na formulação de estratégias de defesa ou ataque, hoje em dia tem sido também utilizada pela iniciativa privada tanto na área industrial e comercial com também na própria área doméstica. O meio ambiente global e a tecnologia moderna fez hoje da espionagem uma ameaça crescente que exige respostas cada vez mais sofisticadas de governos e empresas.
Segundo o Departamento de Defesa dos Estados Unidos da América, designa-se por espionagem: o ato de obter, entregar, transmitir, comunicar ou receber informações sobre a defesa nacional com a intenção, mesmo que não declarada, de serem utilizadas para a prejuízo dos EUA ou para se obter vantagem sobre o Estado por parte de uma nação estrangeira. A espionagem é uma violação do "Title 18 United States Code, Sections 792-798 and Article 106, *Uniform Code of Military Justice"* dos EUA[17].

Embora muitas vezes se confunda o termo "espionagem " com "intelligence", não significam de todo a mesma coisa.

---

[14] Dicionário online Priberan (em linha) [Consult. 15 Maio 2014] Disponível na internet: http://www.priberam.pt/DLPO/espiar
15 Dicionário online Priberan (em linha) [Consult. 15 Maio 2014] Disponível na internet: http://www.priberam.pt/DLPO/espionagem
16 Oxford dictionaries (em linha) [Consult. 15 Maio 2014] Disponível na internet::://www.oxforddictionaries.com/definition/english/spy
17 Department of Defense – Dictionary of Military and Associated terms , Joint Publication 1-02 , 2010, Alterado em Junho 2014 (Em linha) [Consult. Junho 2014] Disponível na internet: http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

De acordo com Cepik (2003)[18], não obstante o termo *intelligence* seja um eufemismo anglo-saxão para a espionagem, esta é apenas uma parte do processo de inteligência, que é muito mais amplo. A *intelligence* designa um conflito entre atores que lidam predominantemente com obtenção/negação de informações. Propositadamente vago e eufemístico, o termo i*ntelligence*, segundo este autor, refere-se ao que serviços de *intelligence* "fazem" concretamente em contextos político-organizacionais específicos. Ainda assim, conclui, que *intelligence* descreve melhor o arco operacional contemporâneo dessa função do que outras noções muito restritivas (espionagem) ou excessivamente amplas (informação) (CEPIK, 2003).

Pode-se encontrar no site[19] do MI5 um pequeno resumo sobre os dois termos:
- Entende-se *intelligence* por informações recolhidas por governos ou organizações para orientarem as suas decisões. Nela se incluem informações que podem ser tanto públicas como privadas, obtidas a partir de várias fontes, quer públicas, quer até secretas ou até da junção de ambas;
- Entende-se por "espionagem" um processo que envolve recursos humanos (agentes) e/ou meios técnicos para a obtenção de informações usualmente não disponíveis publicamente. Processo esse que também pode envolver a tentativa de influência de tomadores de decisão e formadores de opinião para beneficiar os interesses de uma potência estrangeira.

Por definição, espionagem concentra-se normalmente em informações não-públicas recolhidas através de meios encobertos. As informações classificadas são mantidas em segredo, devido ao facto que tais informações podem prejudicar a segurança nacional, pondo em risco o bem-estar económico e /ou também podem prejudicar as relações internacionais do país. A "sensibilidade" de algumas informações faz com que se tornem apetecíveis para espiões, fazendo com se tenha de ter um cuidado acrescido na sua proteção.

E a questão é pertinente, até porque constata-se que a espionagem não tem um estatuto privilegiado, pelo contrário, contínua a ser classificada de clandestina e secreta. A comunidade internacional faz questão de mostrar isso mesmo, excluíndo do estatuto de

[18] Cepik , Marco A.C. – Espionagem e Democracia – Editora FGV. ISBN 85-225-0437-7
[19] https://www.mi5.gov.uk/home/the-threats/espionage/what-is-espionage.html (em linha) [Consult. 25 Maio 2014].

combatente os 'espiões', conforme definido pelo *Direito Internacional Humanitário (DIH).*

"A procura de informações sobre o inimigo não é proibida pelo DIH (nem o é aliás em tempo de paz pelo Direito Internacional Público, desde que não haja uma violação de soberania), no entanto os Estados têm a possibilidade de reprimir a espionagem em função da «qualidade» de espião. Na hipótese de os espiões serem civis, é evidente que em caso de captura, não lhes será reconhecido o estatuto de prisioneiro de guerra, podendo estes ser detidos, processados e julgados desde que seja respeitado o artigo 75.º do primeiro Protocolo e, nos casos dos artigos 64.º a 78.º da quarta Convenção, se a atividade de espionagem for cometida num território ocupado. Na hipótese de o espião ser um combatente, agindo de uniforme ou com uma indumentária que o distinga dos não combatentes, deve beneficiar do estatuto de prisioneiro de guerra, sendo que quem age sem se distinguir dos não combatentes pode ser tratado como espião, a menos que seja somente capturado após ter regressado às forças a que pertencia"[20].

A recolha de informações disponíveis ao público é uma atividade de rotina do pessoal diplomático, adidos militares e delegações comerciais. Estes usam fontes abertas, como os meios de comunicação, conferências, eventos diplomáticos e feiras, bem como contactos abertos com representantes de governos para fazerem o acompanhamento da evolução política, económica e militar do seu país de acolhimento e manter informados os seus próprios governos. Os representantes estrangeiros, auxiliam assim, os governos a moldar suas políticas externas, comerciais e militares. Este tipo de trabalho não é prejudicial aos nossos interesses nacionais. Sendo muitas vezes útil para a construção de boas relações com as outras nações.

Assim, a título de resumo pode dizer-se que a espionagem é uma técnica utilizada pela *Intelligence* sendo esta de que área for. O que distingue a espionagem é o fim para a qual ela é utilizada, a recolha da informação pode envolver segredos militares e planos de negócio, segredos comerciais ou de informação tecnológica.

[20] http://www.gddc.pt/direitos-humanos/DIHDeyra.pdf (em linha) [Consult. 25 Maio 2014].

Independentemente dos conceitos possíveis, a espionagem é uma atividade que sempre esteve presente na humanidade, desde os tempos primórdios as atividades secretas de recolha de informação fizeram parte da rotina de comunidades e indivíduos.

À medida que a sociedade foi evoluindo e as necessidades se alterando, também as atividades de espionagem sentiram uma necessidade em se adaptar. Mas o verdadeiro objetivo da espionagem nunca se alterou ao longo das décadas, a vontade de obter informações tidas como confidenciais ou secretas[21] sobre governos ou organizações, de forma ilegítima, para alcançar uma vantagem militar, política, económica, tecnológica ou social face ao adversário, tem sido desde sempre o grande objetivo de quem recorre a estas atividades para alcançar os seus intentos.

Sem grande surpresa, constatamos que os Estados foram desde os primórdios os grandes impulsionadores desta atividade com a criação de serviços, os quais possuíam à partida uma razão de existir muitas vezes camuflada mas a sua verdadeira essência consistia em capacitá-los de meios de recolha e processamento de informações, que os auxiliasse na tomada de decisões estratégicas para os seus interesses. A sua definição mais recentemente parece ter sido alargada também a propósito do mundo empresarial, envolvendo empresas que são concorrentes entre si, a espiar-se, o que é conhecida por espionagem industrial.

Com o surgimento da Sociedade da Informação, conjugada com o desenvolvimento das tecnologias de informação e comunicação, a obtenção de informação deixou de representar um esforço tão grande como o era anteriormente. A informação passou a estar ao dispor de qualquer um e à rapidez de um clique. Os atos que anteriormente apenas poderiam ser desempenhados por humanos devidamente especializados e treinados para o efeito, mais conhecidos por espiões, com alguma ligeireza, passaram a poder ser executados por qualquer um e em qualquer parte do mundo, desde que disponham de competências no âmbito das TIC e sejam frequentadores do espaço virtual que é o ciberespaço.

Uma interrogação que nos parece interessante é perceber se efetivamente a ciberespionagem se diferencia da espionagem convencional, que nos foi dada a conhecer até pelo menos meados dos anos 80. Em que se diferencia? Nas características? Na

[21] Isto é, que não são públicas, de difícil acesso, e que por serem essenciais e pertinentes representam uma vantagem.

natureza? Nas contramedidas à proteção dos seus efeitos? Na compreensão dos seus actores?

Não será a ciberespionagem um prolongamento da atividade de espionagem com recurso a novos meios e instrumentos ou um novo fenómeno?

"A verdade é que para alguns Estados a ciberespionagem é uma ferramenta essencial para atingir a segurança nacional e a prosperidade económica – que incluem intrusões em redes e exploração de acessos privilegiados em redes corporativas e proprietárias – no sentido de adquirir informação que lhe atribua vantagem competitiva".[22]

Para nós, a ciberespionagem pode ser vista como um subtipo mais evoluído e recente da espionagem tradicional. A verdade é que poucos aspetos as distinguem, comungam os mesmos intuitos e objetivos, ambas possuem o finto de desestabilizar e obter vantagem em termos de 'intelligence' no campo militar, político, e comercial. Então o que as diferencia na realidade? A resposta está no ambiente em que opera, um ambiente virtual que abre portas a todo um novo mundo de oportunidades em matéria de espionagem. Então, porque não dizer que a ciberespionagem consiste na arte de espiar com recurso a meios e técnicas evoluídas tecnologicamente no seio do ciberespaço, que possibilitam a obtenção de dados e informação de forma ilícita.

Mas a importância que hoje é dada à ciberespionagem só acontece porque a sociedade e as entidades e cidadãos que a compõem se renderam às potencialidades e vantagens da Sociedade da Informação e dos sistemas e redes de informação, migrando para elas. Acresce que as mesmas estão cada vez mais interconectados e por isso interdependentes.

Com o aparecimento e consequente desenvolvimento das novas tecnologias, determinados atores descobriram um novo espaço alternativo para a prossecução dos seus objetivos criminosos ou maliciosos, que vão desde a simples propaganda, passando pelo recrutamento de voluntários para a sua causa, até à utilização do ciberespaço para executarem os seus ataques digitais sobre as variadas instituições (políticas, de defesa e económicas/financeiras), causando prejuízos de milhões de dólares todos os anos. É neste

[22] http://www.sirp.pt/cms/view/id/90/ (em linha) [Consult. 02 Junho 2014].

contexto que surge uma nova linha de atuação, a ciberespionagem, que à primeira vista pode ser nada mais do que uma convergência entre ciberespaço e espionagem.

Ainda que seja uma temática que tem feito parte da ordem de trabalhos de muitos Estados e organismos não-estatais, nos dias de hoje não existe uma definição universalmente reconhecida para o termo ciberespionagem, no entanto, diversos foram aqueles que quiserem dar uma conceptualização mais precisa e distinta ao termo ciberespionagem.

Mas antes de introduzirmos alguma das citações, arriscamo-nos numa definição sucinta mas clara do termo, dizendo que ciberespionagem consiste na apropriação ilícita de informação sensível e secreta por meio informático e dele derivado.

Fazendo então referência a alguns autores, iniciamos com a definição do autor Hersh para ciberespionagem, que a descreve como a ciência que secretamente captura o tráfego de mensagens eletrónicas, mensagens escritas, e outras comunicações eletrónicas, e de informação organizacional com o propósito de reunir informação referente à segurança nacional e ao setor comercial. (HERSH, 2010)

Para os autores Janczewski & Colarik a ciberespionagem resume-se a toda a atividade de espionagem ou de obter segredos dos inimigos ou rivais com o objetivo de obter uma vantagem militar, política, ou de negócio. Acrescentam ainda que os perigos relacionados com a ciberespionagem aumentaram consideravelmente graças aos avanços alcançados ao nível das Tecnologias de Informação e na proliferação dos dispositivos de armazenamento de dimensões reduzidas. (KOSTADINOV, 2013)

Lin define o termo como "*o uso de ações e operações – prolongadas no tempo – para recolher informação que de outra forma era mantida confidencial e que depois é transferida ou mantida aí de forma definitiva no sistemas ou redes informáticas dos adversários*". (LIN, 2010 e KOSTADINOV, 2013)

O Manual de Tallinn sobre o Direito Internacional elaborado por um grupo independente especialistas que aborda os aspetos legais sobre as ameaças virtuais, define a ciberespionagem como "*qualquer ato praticado clandestinamente - o autor tenta esconder sua identidade- ou sob falsos pretexto - a sua intenção é a de apresentar-se como uma*

pessoa com direitos e autorização para aceder as informações alvo - que utiliza capacidades cibernéticas para obter (ou tentar obter) informações com a intenção de a transmitir à parte oponente do conflito." (*Tallinn Manual, 2013*)

O termo também é definido pelo Lexicon do Financial Times[23] como "*o roubo de segredos armazenados em formatos digitais ou em computadores e redes de Tecnologia de Informação*" mas também por um outro dicionário de referência, o Oxford Dictionaire [24], como "*o uso de redes de computadores para obter acesso ilícito a informações confidenciais, tipicamente na posse por um governo ou uma organização*."

Aparentemente, todas estas definições têm características comuns, semelhanças e palavras ou frases importantes que podem revelar a imagem que está por trás da obscuridade do sentido do presente termo. Identificam-se assim um conjunto delas que no nosso entendimento traduzem a essência desta atividade (KOSTADINOV, 2013):

- entre Estados e Nações, mas podem incluir atores não-estatais;
- que consiste no roubo de informações através de meios informáticos;
- sigilo ou confidencialidade da informação;
- não têm a intenção de causar a morte/ lesão ou destruição/ danos;
- é conduzida secretamente;
- provavelmente executada por períodos de tempo longos.

A ciberespionagem entendida na lógica de um conjunto de forças que utiliza e partilha as vantagens e as motivações da espionagem dita tradicional traduz-se na exploração das falhas e das vulnerabilidades tecnológicas, com o objetivo de pressionar um Estado, empresas ou os seus cidadãos.

A par do que sucede ao nível da espionagem, existem três formas de ciberespionagem (KOSTADINOV, 2013):

- Económica/ Industrial (arranjar exemplos para a ciberespionagem, estes são da espionagem, por exemplo, "Operação Brunnhilde[25]");
- Militar (por exemplo, caso Albert T. Sombolay [26]);

[23] http://lexicon.ft.com/Term?term=cyber-espionage (em linha) [Consult. 26 Abril 2014];
[24] http://www.oxforddictionaries.com/definition/english/cyberespionage (em linha) [Consult. 24 Abril 2014];
[25] http://en.wikipedia.org/wiki/Industrial_espionage (em linha) [Consult. 25 Abril 2014].

- Política (por exemplo, o escândalo de Watergate[27]).

Efetivamente, quer ao nível dos Estados e das organizações verifica-se uma maior dependência destas nos sistemas de comunicação e nas tecnologias de informação, pois é através da exploração das vulnerabilidades neste âmbito, que assenta a atuação dos espiões e a condução das suas ações. É a este nível que as ações de espionagem podem causar um dano e impacto elevados, a prossecução de intrusões em estruturas críticas industriais é cada vez mais uma ameaça real e iminente.

É necessário tomar consciência que os atores/agentes/atacantes não delimitam barreiras à sua atuação, o mundo é o seu campo de atuação, e que os ataques informáticos a aplicações na Internet e a espionagem digital são as principais ameaças à segurança *online*, concluiu o mais recente relatório sobre investigações à violação de dados da Verizon, empresa norte-americana de telecomunicações[28]. Segundo esse mesmo relatório os ataques de espionagem continuam a aumentar e chegaram mesmo a triplicar em relação a 2012, segundo o relatório. Os principais alvos foram empresas, agências governamentais e instituições militares.

Muitos dos setores de ataque são similares no ciber qualquer coisa. Maioritariamente, numa fase inicial, é quase impossível discernir o que verdadeiramente está acontecer e tecnicamente é possível transferir os efeitos ciber de um campo para outro (cibercrime versus ciberterrorismo) mas parece que a motivação associada aos ataques dificilmente mudará. Contudo todos têm em comum a utilização do ciberespaço e da Internet na prossecução dos seus propósitos.

O fenómeno da ciberespionagem assenta em dois pressupostos, sem os quais não se podia estar a falar deste conceito, que são, por um lado, a existência de objetivos suceptíveis de

---

26 http://books.google.pt/books?id=MggfVVuu7q0C&pg=PA39&lpg=PA39&dq=Albert+T.+Sombolay&source=bl&ots=ag2KVDKlrf&sig=CFXOA80rhukG8jBhaRAI305Sj80&hl=pt-PT&sa=X&ei=bnO9U6PQEcHb0QX-oIDAAw&ved=0CE4Q6AEwBQ#v=onepage&q=Albert%20T.%20Sombolay&f=false (em linha) [Consult. 26 Abril 2014].

27 http://www.academia.edu/4433790/_Watergate_-_The_Presidential_Scandal_that_Shook_America_ (em linha) [Consult. 26 Abril 2014].

28 http://www.publico.pt/tecnologia/noticia/ataques-a-aplicacoes-e-ciberespionagem-lideram-ameacas-online-1633178 (em linha) [Consult. 26 Abril 2014]

serem invadidos/atacados que por causa da sua natureza crítica e sensível têm um impacto visível, e, por outro lado, a existência de pessoas com capacidade e com motivação para perpetrar essas atividades maliciosas.

Se já no tempo áureo da espionagem, pese embora o risco elevado que estava associada à realização de qualquer atividade desta natureza, em especial a que era atribuída aos seus atores, estas atividades eram desempenhadas sempre que tal fosse necessário, o que dizer nos tempos modernos. E neste contexto que se identificam algumas particularidades no desempenho destas atividades, que por serem consideradas vantajosas são promotoras da sua própria execução.

A observância destas atividades parece estar em crescendo, e tal parece dever-se a vários fatores, o primeiro consiste no fato de o campo geográfico de atuação ser ilimitado; o segundo assenta na inexistência de risco físico para o elemento que executa tais atos, uma vez que atua sob o anonimato, e que é a sua maior vantagem; e, o terceiro apoia-se na relação custo-benefício, a realização de um ato invasor envolve na maioria das situações custo de baixo valor. (SANTOS, 2011)

Muitas são as vezes que surgem nos *media* notícias aludidas à existência de atividades que pelas suas características parecem assumir a figura da ciberespionagem. O conhecimento público de que um sistema informático que suporta interesses críticos de determinada nação ou empresa foi comprometido, pode ter visões contrárias, consoante seja interpretada, ou pela parte ‘invasora’, ou pela parte do ‘invadido’. Hoje em dia parece ainda haver bastante relutância em assumir que se esteve num dos lados, quer pela vulnerabilidade que tal representa quer pela conotação negativa que assume.

E essa relutância pode ser responsável pelo crescimento de uma nova dimensão da economia que envolve toda esta atividade, embora a sua dimensão seja diminuta e a circunstância oculta, falamos de um nicho do mercado negro. A procura constante de segredos sobre os rivais ou concorrentes, permitiu a eclosão de serviços por conta própria, que atuando de forma furtiva no submundo da internet, oferecem os seus conhecimentos a quem lhes pagar melhor. A venda de produtos e serviços no mercado negro no âmbito do ciberespaço parece ganhar novos contornos, constituindo-se como uma alternativa bastante apetecível para quem quer determinado tipo de informação, é como uma loja onde

qualquer um pode comprar o produto que deseja. O crescimento e diversificação de produtos que são colocados à disposição de quem os quer adquirir sub-repticiamente são notórios.

Os indivíduos, possuidores de capacidades ou de ferramentas a nível informático capazes de superar o comum dos técnicos nessa área, vendem os seus serviços, a todo o tipo de entidades ou pessoas, para que dentro da necessária confidencialidade e descrição possam se introduzir no mais seguro e aparentemente inacessível sistema informático.

Embora a adesão a estes serviços não seja oficial, algumas empresas ou quem sabe Estados têm recorrido aos serviços destas para aceder aos ficheiros das empresas rivais, para assim poderem delinear uma estratégia de segurança ou financeira de acordo com os segredos das outras firmas, ou mesmo de Estados.

Dentro do pretendido, encontra-se a recolha de informação acerca de determinado tipo de assunto sensível e que a intrusão seja realizada sem ser notada, para não levantar suspeitas sobre os possíveis "mandantes" e para que os sistemas de segurança das empresas vitimadas não venham a sofrer um "upgrade[29]" e que desta forma dificultem novo "ataque".

O preço praticado por estes criminosos freelancer's[30] está associado ao valor do serviço pretendido, e podemos estar a falar de milhares de dólares. O sigilo, como se depreende, é obrigatório e também pago a peso de ouro. A corroboração de que estas atividades geram lucros avultados, são as fortunas alcançadas online por atacantes criminosos[31].

No entanto, as firmas e Estados que recorrem a estes serviços acabam por de certa forma ficar reféns desta situação, pois a qualquer momento os contratados podem chantagear os seus clientes, caso algo ocorra fora do estabelecido inicialmente, ou simplesmente para auferir maiores dividendos.

Existem também "indivíduos" ou "grupos" dentro do ramo da 'pirataria' informática que acedem por decisão própria a diversas bases de dados de empresas de renome, furtando-lhe diversos "segredos". Posteriormente contatam as empresas rivais e vendem-lhes as

[29] Substituição de algo por outro melhor pu de categoria superior.
[30] Profissional que efetua um trabalho independentemente de uma entidade.
[31] https://www.ted.com/talks/mikko_hypponen_three_types_of_online_attack?language=es#t-177054 (em linha) [Consult. 8 Julho 2014].

informações roubadas às concorrentes, atuando como um loja onde qualquer um pode comprar o produto desejado. Neste último caso, já não há só o contentamento em realizar os trabalhos encomendados, mas sim jogar num plano de antecipação, oferecendo a informação que outros podem estar a necessitar.

Para os Estados que recorrem a ciberespionagem tendem a evidenciar a necessidade de possuir ou angariar quem possua capacidade e aptidões de elevada técnica e complexidade, seja na fase preparatória seja na fase de execução de tais atos. As perdas que determinado Estado e ou entidade sofre com as atividades de ciberespionagem; pese embora as constantes notícias dos enormes custos associados, na verdade não são conhecidas a real extensão da ciberespionagem e pode muito bem ser incalculável.

No entanto, parece unânime que a atividade da ciberespionagem, contrariamente ao que acontece com outros tipos de ataques, não tem por propósito destruir ou danificar o seu alvo, pelo contrário pretende tão e somente recolher os dados ou a informação de que necessita, e se o conseguir fazer sem ser detetado, pelo menos naquele momento, então o ato foi, sem dúvida, realizado com sucesso (LIN, 2010).

Existe a tendência para estas atividades assumam uma longevidade temporal superior aos dos outros tipos de ataques. Efetivamente, as notícias indicam que uma atividade desta pode estar ativa durante anos, sem que seja notada, o que leva a pensar nas repercussões que podem ser inúmeras.

Disso são exemplo as demais declarações, com destaque para a proferida pela administração do Presidente Obama ao afirmar que a ciberespionagem é atualmente uma ameaça mais perigosa e iminente que as diferentes formas de terrorismo[32]. Semelhantes declarações vieram de uma nação vizinha, um membro sénior da comunidade de intelligence do Canadá referiu que a ameaça da ciberespionagem requer mais recursos do que aqueles que atualmente têm sido aplicados no combate ao terrorismo[33].

Para encerrar este capítulo parece importante introduzir um grande escândalo de espionagem a nível internacional, o sistema de interceções de comunicações ECHELON.

[32] http://www.thetimes.co.uk/tto/news/world/americas/article3712294.ece. (em linha) [Consult. 8 Junho 2014]
[33] http://intelnews.org/2012/11/20/01-1136/ (em linha) [Consult. 8 Junho 2014]

A polémica com a espionagem surge em grande monta com as notícias que davam conta que tal como havia acontecido no tempo da Guerra Fria, os EUA estavam a espiar as nações do mundo, através do sistema Echelon coordenado pela agência americana NSA. O sistema Echelon teve como objetivo controlar as atividades dos membros do Pacto de Varsóvia, mas desde então as capacidades evoluíram em resultado da crescente sofisticação tecnológica de satélites e computadores. Este sistema Echelon distinguiu-se dos outros sistemas de informação pelo fato de apresentar duas características que lhe atribui um nível de qualidade muito específico: 1) capacidade praticamente global de vigilância. Recorrendo a estações recetoras via satélite e a satélites de espionagem, permite que se intercete qualquer comunicação via telefone, telefax, internet, ou e-mail, acedendo ao respetivo conteúdo; 2) o sistema funciona a nível mundial graças a uma cooperação entre vários países. (COELHO, 2004)

O secretismo envolto a este sistema tem sido polémico, porque o seu desenvolvimento e operação foram ocorrendo sem qualquer controlo judicial ou parlamentar. Por isso, em rigor, as suas capacidades e áreas de empenho foram de alguma forma uma incógnita. Que pode incluir áreas tais como, proliferação nuclear, combate ao terrorismo e ao crime organizado e atividade comercial.

Muitas foram as acusações que referiam que os EUA estavam a utilizar este sistema para fazer espionagem industrial, até porque no mundo de hoje aliados militares e estratégicos são igualmente competidores na arena do comércio internacional. E para muitas nações, como a americana, a prosperidade económica faz parte da segurança nacional. No entanto, a existência de espionagem económica foi negada pelo antigo diretor da CIA, James Woolsey, quando confrontado pela Delegação da União Europeia, constituída para avaliar / averiguar o alcance da atividade do Echelon em território europeu. (COELHO, 2004)

Não querendo alongar muito neste campo, importa sublinhar que a preocupação manifestada por diversos países a nível mundial foi elevada, em especial, a nível europeu, traduzindo-se na constituição de uma comissão temporária responsável por averiguar o alcance das atividades do Echelon. O trabalho da comissão, embora tenha sofrido alguns

percalços, foi concluído e saíram 44[34] recomendações que incidiram sobre a proteção dos cidadão e empresas, sobre as necessidades de alterar acordos internacionais, sobre a revisão da legislação nacional, sobre medidas especiais de combate à espionagem económica, sobre a aplicação da lei e o controlo da legalidade e ainda sobre o fomento da autoproteção dos cidadãos e empresas e a adoção de medidas ao nível das instituições comunitárias.

Durante o período de existência desta Comissão temporária sobre o sistema Echelon foram realizadas várias audições com técnicos e especialistas. Um dos mais polémicos e famosos foi o Caso Desmond Perkins, o Chefe de Serviço da Cifragem na Comissão Europeia. No decorrer da sua audição o chefe do gabinete responsável pela criptografia das comunicações no seio do executivo europeu, referiu ter relações privilegiadas com os serviços americanos, em especial com a NSA, facilitadas por lá ter familiares. A questão é que a NSA era precisamente o organismo que verificava regularmente os sistemas europeus de criptografia, para ver se se mantinham invioláveis e se estavam a ser utilizados corretamente, a qual de forma alguma deveria ter acesso às informações que circulavam ao nível do que se passava na Europa. Estas declarações, desde logo controversas, foram de imediato divulgadas pela imprensa internacional, com ênfase para a vulnerabilidade do sistema de comunicação das instituições comunitárias. O assunto foi encarado de forma grave até porque as competências da UE abrangem domínios muito sensíveis, em que é fundamental o secretismo, como seja o comércio internacional ou a concorrência. E neste sentido é legítimo colocar a questão de que, embora o chefe de serviço da cifragem ter dito que a NSA não tenha conseguido penetrar nos sistemas de criptografia, ”*será que se tivesse verificado o contrário, os agentes americanos teriam, por simpatia, avisado Perkins da permeabilidade dos sistemas de confidencialidade comunitária*”. (COELHO, 2004)

A ameaça do sistema ECHELON e de outros tais que surjam com o mesmo impato e alcance “*não deve ser visto apenas em função do poderoso sistema de vigilância que representa, mas também pelo fato de operar num espaço praticamente à margem da lei*”. (COELHO, 2004)

[34] Ver relatório sobre a existência do sistema de interceção Echelon, (Coelho, 2004).

CAPÍTULO 3.
O PAPEL DO CIBERESPAÇO E A REALIDADE DOS CIBERATAQUES

As tecnologias computacionais possibilitaram o aparecimento de uma dimensão virtual, o ciberespaço, que veio revolucionar o mundo em que vivemos, criando uma nova dimensão quer de oportunidades e imprevisibilidades mas também um novo espaço de conflitos. O acesso rápido e fácil a qualquer lugar do mundo e a qualquer informação ou computador tornou-se uma possibilidade. E tornou também possível o aparecimento de novas formas de interação, sejam elas estaduais, organizacionais, ou individuais.

3.1. O CIBERESPAÇO

Hoje em dia não é possível falar de informação, de acesso a informação ou dados sem que se tenha de falar em ciberespaço ou em internet. São conceitos que estão intimamente ligados à sociedade dos dias de hoje.

O Departamento Norte Americano de Segurança[35] define ciberespaço como uma rede interdependente de infraestruturas de tecnologia de informação, que engloba não só a internet, mas também os sistemas de computadores e os inerentes processadores e controladores, e ainda os sistemas de computadores. Para o Reino Unido corresponde a todas as formas de rede e atividades digitais e isto inclui os conteúdos e ações conduzidas através de redes digitais (Government of United Kingdom, 2009). O Canadá refere-se ao mundo eletrónico criado pelas tecnologias de informação interconectadas e pela informação sobre aquelas redes (Government of Canada, 2010).

[35] JP 1-02 - Department of Defense Dictionary of Military and Associated Terms. Washington DC: Department of Defense, 2012.Ver http://ra.defense.gov/Portals/56/Documents/rtm/jp1_02.pdf (em linha) [Consult. 08 Abril 2014).

O termo é também descrito por dois dicionários de referência. O dicionário da Porto Editora, na sua edição de 2012, define ciberespaço como um "*espaço virtual constituído por informação que circula nas redes de computadores e telecomunicações*". O outro define o conceito como o "*espaço onde se estabelece comunicação eletrónica*", "*realidade virtual*" (MOREIRA, 2012)

Martin Libicki ao descrever o ciberespaço apresenta-o dando como exemplo um modelo de três camadas, física-sintática-semântica. "*A camada física corresponde à tecnologia hard, o suporte do ciberespaço, e diz respeito às máquinas e às redes e através das quais elas comunicam. É a camada de hardware e dos sinais que fluem entre os dispositivos. A camada sintática consiste em software e protocolos que formatam e estruturam informação eletrónica digital e que assegura o controlo dos sistemas de computadores e redes. A camada semântica contém a informação que é trocada, armazenada e manipulada nas redes de computadores, usualmente por humanos na forma de linguagem entendível (natural). É aquela camada em que surge a interpretação que é extraída da informação e que faz sentido para as pessoas porque as outras camadas correspondem a meios e processos."* (FREIRE & CALDAS, 2013)

Quando falamos em ciberespaço não está apenas em causa o meio virtual repleto de informação e abrangendo todo um mundo de equipamentos e de sistemas materiais que o integram, mas sim todo um conjunto de particularidades, que o tornam único e de uma magnificência inalcançável.

É no ciberespaço que a interpretação de material deixa de fazer sentido, pois o fluxo de informação não é verdadeiramente palpável, tudo circula e se armazena em ambiente 'imaginário'; mas o de território também ganha outra interpretação, uma vez que deixam de existir fronteiras físicas; deixa de haver a necessidade da presença do elemento humano, porquanto os acontecimentos desenrolam-se em quase anonimato; emerge o termo de intemporalidade, face à quantidade imensa de informação e dados disponíveis; e, por fim, também importa indicar a desordem, uma vez que neste espaço nada está controlado nem tão pouco protegido. (MOREIRA, 2012)

Esta combinação torna a quantidade de informação e os sistemas computacionais e aplicações de suporte em alvos extremamente vulneráveis a eventuais ataques cibernéticos.

Mas tal já não é uma novidade para a atual sociedade, empresas e Estados dependem deste ciberespaço, pois o seu funcionamento e desenvolvimento entrelaçam-se com os sistemas de informação e comunicação (TICs) e boa parte sabem e têm consciência que estão desprotegidos e à mercê da prática de atos ilícitos por atores, mais ou menos relevantes, organizados ou não, que abraçam os mais variados objetivos e possuem as mais diversas motivações. Para estes atores o ciberespaço pode ter duas funções, uma como instrumento para a prática de atos maliciosos, e a outra como alvo ou objeto de ação, consoante o objetivo e danos que tenham como pretensão causar, mas no final tudo se traduz, tão só e apenas, na finalidade de prejudicar uma organização ou até mesmo uma nação.

Efetivamente é neste ambiente virtual em conjugação com a internet, que emergiram certos acontecimentos, que ao longo do tempo a sociedade moderna tem percebido o seu real alcance e perigosidade. Com frequência são noticiados incidentes de natureza informática, que de forma ilegítima pretendem causar um impacto negativo que vulgarmente podemos designar como ciberataques.

3.2. OS CIBERATAQUES

João Moreira define ciberataque como ”*(...) um ataque lançado geralmente a partir de um computador recorrendo ao método de intrusão e que tem como finalidade adquirir, explorar, perturbar, romper, negar, degradar ou destruir informação constante em computadores ou em redes de computadores, em sistemas e equipamentos eletrónicos ligados a outros equipamentos ou sistemas ou que partilham a mesma estrutura de energia ou o mesmo espaço de emissão eletromagnética, bem como os próprios computadores, rede de computadores, sistema e equipamentos*.” (MOREIRA, 2012)

Um ciberataque não é um processo expedito. A empresa americana Dell Inc, num relatório de 2012 admite que um ciberataque é composto por diversas etapas básicas. A primeira consiste no reconhecimento, e tem como primeiro objetivo identificar as vulnerabilidades no sistema e nas redes. As seguintes são a intrusão, que consiste na invasão da rede do

adversário; a inserção de malware[36], que baseia-se na implementação sigilosa do código maliciosos; e, por fim, a limpeza, que tem como propósito eliminar as provas e os vestígios da existência do ataque. (KOSTADINOV, 2013)

Os primeiros casos efetivamente considerados como ciberataques de dimensão e que obtiveram algum relevo no meio político internacional, ocorreram na última década.

Em 2003 as redes computacionais do Departamento de Defesa dos Estados Unidos da América, entre outras agências são alvo de uma série de ciberataques coordenados conhecidos como "Titan Rain"[37], direcionados a roubar informações de diversas empresas e organismos governamentais. Embora não tenha sido possível determinar a localização exata dos computadores que realizaram os ataques ou a identidade dos atacantes, eles tiveram origem na China. Acredita-se que esses ataques estavam associados a uma Ameaça Persistente Avançada (Advanced Persistent Threat – APT [38]), num ataque com alvo específico, que neste caso foi o Governo dos E.U.A., tendo para o efeito utilizado uma rede de proxys e computadores 'zombie' infetados com vírus. Por parte dos responsáveis americanos, foi referido que os sistemas não foram comprometidos, no entanto a preocupação manteve-se na medida em que embora a informação de que houve apropriação fosse inócua, a reunião e análise de diversos dados provenientes de várias fontes poderiam produzir informação útil para o adversário.[39] [40]

Em Abril e Maio de 2007, a Estónia foi alvo de um intenso ciberataque, em que vários dos seus servidores, associados a agências governamentais, instituições financeiras e jornais, foram sobrecarregados por inúmeras solicitações de serviços, causando impossibilidade de resposta (ataque do tipo DoS - denial of service -2 [41]), com consequências constrangedoras a nível nacional. O ataque coordenado que colocou fora de serviço parte dos sítios governamentais e comerciais parece ter tido origem na Rússia, motivado por disputas políticas entre os dois países (iniciadas pela mudança do local de um memorial russo na capital de Estónia erguido em homenagem ao soldado russo - era da dominação soviética

[36] Programas informáticos maliciosos.
[37] http://csis.org/files/media/csis/pubs/051214_china_titan_rain.pdf. (em linha) [Consult.25 Março 2014).
[38] http://www.trendmicro.com/cloud-content/us/pdfs/business/datasheets/wp_apt-survey-report.pdf (em linha) [Consult. 25 Março 2014).
[39] http://spectrum.ieee.org/telecom/security/its-time-to-write-the-rules-of-cyberwar (em linha) [Consult. 25 Março 2014).
[40] http://www.washingtonpost.com/wp-dyn/content/article/2005/08/24/AR2005082402318.html
[41] http://www.infowester.com/ddos.php (em linha) [Consult. 25 Março 2014]

sobre aquele país) e um eventual teste à resposta da NATO. A suspeita do governo da Estónia é a de que os ataques tiveram a cumplicidade do governo Russo, dado o envolvimento de sistemas conetados a servidores russos e outros ainda ligados ao governo, mas tal foi sempre negado pelo porta-voz do governo russo [MOREIRA, 2012]. Este não foi um caso de espionagem mas de disrupção do poder político e económico de um Estado.

No ano de 2008 os EUA foram vítimas de mais uma intensa operação de ciberespionagem, que decorreu durante a corrida eleitoral para a disputa pela presidência dos EUA, em que mensagens eletrónicas com 'malware'[42] foram enviados por *hackers* de outros países para os assessores das campanhas dos dois candidatos à presidência, Barack Obama e John McCain, tendo acesso a documentos internos relativos às campanhas de ambos os candidatos. As autoridades norte-americanas indicaram a China como origem provável dos ataques cibernéticos, mas sem atribuir qualquer apoio efetivo do governo daquela nação[43].

Em Agosto de 2008 foi a vez de a Geórgia ser alvo de ciberataques 'DDoS'[44] às suas Infraestruturas Críticas de comunicação e informações, quer governamentais quer civis. Isto sucede no decurso da Guerra da Ossétia do Sul que opunha a Geórgia contra as forças separatistas ossetas apoiadas pela Rússia. Este incidente precedeu e acompanhou a execução de uma operação militar convencional por parte da Rússia naquele território Geórgio que ajudou a colocar numa situação de extrema debilidade para coordenar e organizar a sua defesa nacional face à invasão russa (MOREIRA, 2012). Não sendo, um caso de ciberespionagem foi um momento marcante porque em boa verdade é talvez o primeiro ato de ciberguerra, que ocorreu em simultâneo com actividades de guerra convencional.

No ano de 2009 foi descoberta uma grande campanha de espionagem *online* que ganhou o nome de GhostNet, onde e-mails com malware foram usados para infectar, em 103 países, 1.285 computadores pertencentes a diversas embaixadas, representantes de governo e centros de exílio em todo o mundo, relacionados aos Tibetanos e ao Dalai Lama. Este

[42] http://www.microsoft.com/pt-pt/security/resources/malware-whatis.aspx (em linha) [Consult. 10 Abril 2014).
[43] http://investigations.nbcnews.com/_news/2013/06/06/18807056-chinese-hacked-obama-mccain-campaigns-took-internal-documents-officials-say (em linha) [Consult. 10 Abril 2014).
[44] http://www.verisigninc.com/pt_BR/website-availability/ddos-protection/what-is-a-ddos-attack/index.xhtml (em linha) [Consult. 10 Abril 2014).

ataque permitiu o acesso sem precedentes a informações potencialmente confidenciais. As evidências apontam para a China como responsável deste ataque[45].

Ainda no ano de 2009, são detectados uma série massiva de ataques do tipo DDoS que atingiu vários sites de empresas financeiras e do governo pertencentes à Coreia do Sul e EUA, que se iniciaram no dia 4 de julho (Dia da Independência nos Estados Unidos) e prolongaram-se até ao dia 9 de Julho. A autoria dos ataques tem sido atribuída à Coreia do Norte e com a motivação, não de ciberespionagem mas de tentar perceber a capacidade de reação e as motivações dos EUA nesta área geográfica, e em especial, em prol dos interesses da Coreia do Sul.

No início do ano de 2010, a empresa americana Google anunciou que tinha sido alvo de um ciberataque coordenado e "altamente sofisticado" contra a sua rede social. O ataque, que de acordo com a própria empresa terá tido origem na China, permitiu ao invasor o roubo de propriedade intelectual e terá procurado o acesso às contas do Gmail de ativistas de direitos humanos. O ataque foi direcionado a mais de 30 empresas americanas, e ficou conhecido como a "Operação Aurora"[46]. Em resposta a Google anunciou que iria retirar suas operações na China.

Ainda em 2010, no mês de Outubro, um *worm*[47] denominado de Stuxnet afetou o software de pelo 14 unidades industriais iranianas, e em especial neutralizou as centrifugadoras de duas centrais nucleares iranianas responsáveis pelo enriquecimento de urânio. O vírus que se espalhou através dos computadores de Controlo da Central era de tal forma poderoso que através de três fases distintas permitia não só controlar o alvo mas também destruí-lo, motivo pelo qual exista quem considere que a extensão conseguida apenas está ao alcance e no domínio de um grande Estado. (MOREIRA, 2012) O New York Times faz referência a um esforço conjunto dos governos Americano e Israelita.[48] Não se trata de um caso de espionagem, embora tenha requerido previamente um trabalho de *intelligence* profícuo,

[45] http://spectrum.ieee.org/telecom/security/its-time-to-write-the-rules-of-cyberwar (em linha) [Consult. 19 Abril 2014].
[46] http://www.washingtonpost.com/world/national-security/chinese-hackers-who-breached-google-gained-access-to-sensitive-data-us-officials-say/2013/05/20/51330428-be34-11e2-89c9-3be8095fe767_story.html (em linha) [Consult. 19 Abril 2014]
[47] Programa autoreplicante, semelhante a um vírus informático.
[48] http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet (em linha) [Consult. 17 Abril 2014]

mas um caso de "ciberterrorismo" ou de "guerra" tipo "escaramuça" para disromper infraestruturas estratégicas de um Estado

No ano de 2010 também se verificou um confronto no ciberespaço entre o Paquistão e a Índia. Um mês depois de sites de vários ministérios do governo paquistanês serem desligados e vandalizados por grupos de hackers indianos, os sites das agências de segurança indianas foram atacados por hackers paquistaneses (id. [24]). Não estamos certamente perante casos de ciberespionagem mas um caso de cibervandalismo e hacktivismo.

Em 2011, o governo canadiense é obrigado a desligar da internet as suas duas maiores agências económicas quando se apercebe que um vírus de computador está a proceder ao varrimento das redes governamentais na procura de documentos classificados e posteriormente ao seu envio para o exterior. Os ataques foram rastreados até a servidores na China (id. [24]).

Em Setembro de 2011 um vírus de origem desconhecida foi introduzido nos sistemas de controlo de Unmanned Aircraft Systems na Base Aérea de Creech no Nevada, EUA. As autoridades referiram que o vírus for removido apenas ao fim de diversas tentativas, mas adiantaram que nesse período não perderam o domínio de nenhum aparelho (MOREIRA, 2012). Desconhecemos se o objectivo era perceber o funcionamento dos sistemas mas acreditamos que a intenção era a futura manipulação dos mesmos.

No ano de 2012, foi detetado um malware que ficou conhecido como Flame utilizado em computadores que executam o Microsoft Windows. Por ser um programa de fácil propagação, aquando da sua deteção este já se encontrava infiltrado por todo o Médio-Oriente, com a maioria dos alvos no Irão. O Flame revelou-se um sofisticado programa de ciberespionagem que procedia à recolha de informação, através de áudio, leitura de teclado, tráfego de rede, e ainda outros documentos armazenados localmente, que posteriormente era enviada para vários servidores dispersos pelo mundo. Ao terminar, o programa passa a inativo, até receber alguma ordem, a partir do qual se inicia todo o processo de recolha de informação (id. [24]). Embora não tenhamos conhecimento de terem sido rastreadas as origens, tudo aponta para países de cultura ocidental ou a ela ligados.

Também no ano de 2012, a rede de computadores da Saudi Aramco[49] foi afetado por um vírus, Shamoon, que infetou cerca de 30.000 das suas máquinas com o sistema Windows. Esta empresa nacional de petróleo e gás da Arábia Saudita, de acordo com relatos, levou quase duas semanas a recuperar do dano. Os vírus frequentemente aparecem nas redes de empresas multinacionais, mas é alarmante que um ataque desta escala tenha sido realizado contra uma empresa tão importante para os mercados globais de energia, no entanto, não afetou a produção de petróleo, uma vez que esta é controlada a partir de redes distintas. Quanto à autoria do ataque existe a opinião que houve a intervenção de 'insiders'. Outros consideram que houve apoio de um Estado, o Irão. Um grupo chamado 'Cutting Sword of Justice' reivindicou a responsabilidade pelo ataque, dizendo que seus motivos eram políticos e citando "crimes e atrocidades 'sauditas em países como Síria e Bahrein.

Em Janeiro de 2013, a Kaspersky Lab[50] identificou uma campanha de ciberespionagem avançada e de grandes dimensões, conhecida como o 'Outubro Vermelho'. Dirigida a organizações diplomáticas e centros de investigação científica e governamentais de todo o mundo, foi percebido que estava em operação há pelo menos 5 anos. A operação tinha como objetivo obter documentação sensível das organizações, que incluem dados de inteligência geopolítica, bem como credenciais de aceso a sistemas classificados de computadores, dispositivos móveis e equipamentos de rede. Atingiu particularmente países da Europa de Leste, a ex-repúblicas da antiga URSS e a países da Ásia Central, embora entre as vítimas se contem também organismos da Europa Ocidental e América do Norte. E admite-se que por detrás dela estava a Rússia, pelo menos os autores do malware sejam russos (o principal idioma nos códigos principais), mas China também poderá estar envolvida, pois muitos dos *exploits*[51] foram desenvolvidos naquela República.

Ainda, no ano de 2013, as redes de computadores pertencentes a emissoras de televisão sul-coreanos e, pelo menos, dois grandes bancos do país foram interrompidas, durante significativo tempo, por via de um ciberataque malicioso originário da Coreia do Norte,

[49] http://www.iiss.org/en/publications/survival/sections/2013-94b0/survival--global-politics-and-strategy-april-may-2013-b2cc/55-2-08-bronk-and-tikk-ringas-e272 (em linha) [Consult. 22 Maio 2014].
[50] Fabricante de antivírus http://www.kaspersky.com.pt/index.php?oid=95 (em linha) [Consult. 22 Maio 2014].
[51] É um pedaço de software, ou um pedaço de dados ou ainda uma sequência de comandos que tomam vantagem de um defeito, falha ou vulnerabilidade a fim de causar um comportamento acidental ou imprevisto a ocorrer no software ou hardware de um computador ou dispositivo eletrónico.

denominado como DarkSeoul.[52] Não foram motivações de espionagem mas sobretudo de provocação e coacção sobre o poder político vigente, afectando a economia e por via indirecta a vida de cidadãos.

Aquele que pode ser considerado um dos maiores escândalos/testemunhos de ciberespionagem é talvez o PRISM, que apesar de uma existência já duradoura veio à luz do dia em 2013, com o caso Snowden. O mundo tomou então consciência e conhecimento dos programas de ciberespionagem através das declarações de um ex-técnico (o referido Snowden) contratado da CIA e antigo consultor da Agência de Segurança Nacional (NSA), que permite consultar registos de chamadas e recolher informação 'online' a partir de redes sociais, e assegurou ainda que o controverso programa PRISM[53], usado pela NSA para armazenar elementos como dados pessoais, e-mails e conversas, abrange também indivíduos, instituições, altas entidades de governos ocidentais e nomeadamente aliados para além de todos os cidadãos norte-americanos. De facto, envolve altos representantes de Estados e governos de países dos vários continentes, desde a Europa à América do Sul e não somente informações relativas à China, ou países conectados (Hong Kong por exemplo).

Não estarão certamente todos os eventos registados mas apenas alguns que já poderão dar uma perspectiva da abrangente da problemática da ciberespionagem e das distintas motivações de ciberataques. Face ao descrito nos exemplos de ataques cibernéticos ocorridos entre 2003 e 2013, facilmente concluímos que este tipo de ameaças é uma das crescentes preocupações de qualquer chefe de estado. Situações como a espionagem, em que a recolha de informações confidenciais e secretas envolvendo principalmente questões económicas e financeiras (propriedade industrial e intelectual), políticas e militares, são recorrentes entre grandes empresas e Estados. Foram também identificadas detetados ataques que podemos qualificar de ciberterrorismo e hacktivismo, e até provavelmente de ciberguerra.

Os ataques tiveram origem principalmente na Ásia, mas também na Rússia e na Europa de Leste, sendo que os Estados Unidos são o país onde está localizada a maioria das vítimas.

52 Mais informações em http://nakedsecurity.sophos.com/2013/03/20/south-korea-cyber-attack/ (em linha) [Consult. 22 Maio 2014].

53 http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/ (em linha) [consult. em 22 de Maio de 2014].

Mas os EUA são igualmente visados enquanto atores responsáveis pela prática de ciberespionagem contra diversos países desde os europeus, asiáticos e sul-americanos.
Da análise a estes acontecimentos constata-se que os ataques com origem na Ásia e EUA apresentam-se com maior expressividade, e relativos à recolha de informações de caráter económico e financeiro contra Estados e empresas. Com menor expressão surgem as situações políticas e ideológicas. Os países da Europa de Leste e Rússia encontram-se mais envolvidos neste tipo de situações, em que se verifica uma disputa política e militar, como uma 'mostra' de força.

3.3 TIPOLOGIA DOS ATAQUES CIBERNÉTICOS E DOS AGENTES

Ainda que existam nações que devido à sua posição política moderada ou neutra, no que concerne ao posicionamento ideológico, julguem nunca vir a ser alvo de ameaça do género em grande escala, atualmente tendem a mudar de postura, parecendo-nos ter optado por uma política de segurança mais abrangente no que respeita à proteção do funcionamento informático das estruturas fundamentais do Estado.

Pese embora esta tomada de consciência relativa ao perigo iminente pode no entanto ser difícil para as agências governamentais e empresas antecipar o próximo ataque ou atividade maliciosa, que normalmente se centram em atividades e setores vitais para a qualidade de vida e segurança das pessoas e Estados, como sejam as redes elétricas energéticas, as telecomunicações, transportes, serviços financeiros, entre outros. Se de algum modo está instituída a relevância da protecção de Infraestruturas Críticas, embora nem sempre reflectido em implementações práticas, porém as questões associadas a espionagem ainda não estão devidamente geridas.

Um simples ataque como os acima mencionados, provoca em qualquer instituição danos incalculáveis, quer em termos monetários para a reparação dos sistemas informáticos, quer na recuperação da informação perdida ou nos transtornos/calamidades que pudessem advir do mau funcionamento das bases informáticas. Paralelamente, ataques como aquele que a Rússia terá dirigido contra a Estónia, mostram de forma catastrófica a impotência de um país em funcionar dentro da normalidade expectável, quando atingido. Para além disso e talvez não menos importante, é a forma como uma nação se pode tornar refém de outra

temporariamente face à incapacidade de se defender eficazmente por si só contra agressões desta natureza e à não vontade de expor publicamente (internacional) a sua fragilidade.

Da mesma forma que os exércitos de antigamente, antes de um conflito, contratavam melhores guerreiros ou aliciavam etnias mais vocacionadas para a guerra, os Estados de hoje têm obrigatoriamente que recrutar técnicos informáticos para cerrar as suas fileiras e dotar de tecnologia adequada os seus sistemas críticos.

Atualmente, quase todas as agências governamentais de espionagem e *intelligence* estão cientes da importância da componente informática utilizada no normal funcionamento das instituições.

Mas a defesa cibernética do estado não se deve limitar a tentar defender os seus sistemas mas deve por outro lado tentar identificar que novas formas de produzir danos podem surgir.

Com a globalização, qualquer acontecimento no mundo, tem consequências a nível mundial, sejam elas de caráter político, económico, de segurança e defesa, entre outras. Deste modo, o desenvolvimento da Internet e a rápida evolução e à utilização do Ciberespaço, proporcionou, por um lado, novas oportunidades e, por outro, novas vulnerabilidades e ameaças. As ameaças que hoje em dia mais podem afetar os Estados são as de origem cibernética ou as ciberameaças. A ciberameaça pode ser definida como "*qualquer circunstância ou evento passível de explorar, intencionalmente ou não, uma vulnerabilidade específica num sistema de TIC, resultando numa perda de confidencialidade, integridade e disponibilidade da informação manipulada ou da integridade ou disponibilidade do Sistema*" (IDN nº 12, 2013). Esse acesso pode ser conduzido a partir do interior de uma organização por mero utilizadores fiáveis ou de locais remotos por pessoas desconhecidas que o fazem com recurso à internet. As ameaças aos sistemas de controlo podem advir de várias fontes, incluindo os governos hostis, grupos terroristas, funcionários descontentes, e intrusos maliciosos[54].

[54] https://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions (em linha) [Consult. 11 Junho 2014].

A proteção contra essas ameaças tem que existir, e para isso é conveniente criar uma 'ciberbarreira' segura que abarque todo o sistema. Embora existam outras ameaças, incluindo desastres naturais e ambientais, falhas mecânicas e ações involuntárias de utilizadores autorizados[48], esta discussão pretende debruçar-se nas ameaças que são deliberadas, até porque são estas últimas cujo potencial impacto, sofisticação e precisão está em constante evolução, elevando o nível de risco a que os sistemas estão submetidos (IDN nº 12, 2013). "*A sua identificação e catalogação correta é a chave para se poderem estabelecer estratégias adequadas de proteção do ciberespaço*" (IDN nº 12, 2013).

Há inúmeras maneiras de organizar estas ameaças e podem encontrar-se inúmeras opiniões diferentes sobre o assunto, mas de acordo com a Estratégia de Informação e Segurança do Ciberespaço, consoante o tipo de motivação, elas podem ser agrupadas em quatro categorias principais (IDN nº 12, 2013, p. 22-23):

- ***"Cibercrime**, centradas essencialmente na obtenção de benefícios económicos através de ações ilegais. As ações relacionadas com a fraude bancária, com cartões de crédito ou a realização de transações em diferentes páginas web, constituem exemplos de ações comuns relacionadas com este tipo de ameaças."*
- ***"Ciberespionagem**, com foco na obtenção de informações, seja para benefício próprio ou para deter um benefício monetário posterior com a sua venda. A informação mais suscetível de identificar-se neste campo pode pertencer, nomeadamente, a um governo ou até a organizações privadas, e ser classificada, sendo esta uma mais-valia para os atacantes."*
- ***"Ciberterrorismo**, onde se procura um impacto social e político significativo pela destruição física. Neste contexto, as infraestruturas críticas constituem os alvos de ataque mais prováveis."*
- ***"Ciberguerra**, pode ser definida como uma luta ou conflito entre duas ou mais nações ou entre diferentes fações dentro de uma nação onde o ciberespaço é o campo de batalha."*

Pese embora a ameaça que esteja em causa que tipo de ataques cibernéticos podem ser lançados por forma a debilitar um sistema TIC. A Estratégia de Informação e Segurança do Ciberespaço identifica-os e atribui uma classificação em função do nível de organização e define o nível de impacto (IDN nº 12, 2013, p. 24):

Tipo de Ataque	Descrição
Ataque simples	Ataques sem coordenação ou com um nível de organização muito reduzido, executados por uma pessoa ou várias mas sem nunca formar uma organização propriamente dita. O seu impacto é médio-baixo.
Ataques organizados	Ataques que são executados e coordenados por um número significativo de pessoas que fazem parte de um grupo organizado. O impacto é normalmente médio, mas depende do tipo de objetivos que buscam.
Ameaças Persistentes Avançadas (APT – *Advanced Persistent Threats*).	Estas ameaças são criadas por um grupo de pessoas com um perfil de elevada perícia tecnológica; permanecem ao longo do tempo e o seu desenvolvimento está particularmente focado num alvo específico. Com uma precisão muito elevada, a probabilidade de ocorrência é alta e o seu impacto pode ser bastante forte[55].
Ataques coordenados de grande escala	Esses ataques são executados e dirigidos por uma organização ou uma nação, e envolvem um elevado número de atores, que podem pertencer ou não à organização. O impacto pode ser elevado ou muito elevado.
Ciberataques coordenados com ataques físicos	O nível de coordenação que requer este tipo de ataque é o mais elevado, e a combinação entre ataques em diferentes dimensões (terra, mar e ar) deve ser executado com grande precisão. O impacto é extremamente elevado.

Para se poder ter uma visão holística das ameaças que nações e entidades não estatais enfrentam, não basta identificar os tipos de ameaças e os tipos de ataque, é necessário estabelecer quais as possíveis fontes de ameaças ou atores/agentes que podem se vítimas destes ataques e que motivações os levam a perpetrar determinado ciberataques. Também nesta dimensão aludimos ao que é narrado no documento que introduz a Estratégia de Informação e Segurança do Ciberespaço (IDN nº 12, 2013, p. 23) mas também ao que é

[55] Ameaças relacionadas com o campo da ciberespionagem são as mais dinâmicas e, dentro deste âmbito, as APT estão a aumentar o risco progressivamente, prevendo-se que venham a proporcionar um nível de risco bastante elevado. Os ataques direcionados podem ser precedidos de uma APT [IDN nº 12, 2013].

definido[48] pela Equipa de Resposta Rápida aos Sistemas de Controlo Industriais americana ICS-CERT [56] (The Industrial Control Systems Cyber Emergency Response Team). As fontes de ameaça podem ser classificadas da seguinte forma:

- Cibercriminosos;
- Espiões industriais;
- "*Hacktivistas*";
- Terroristas;
- Nações;
- Hackers.
- Pessoal interno.

Mas quais serão as motivações que levam estes atores a tornarem-se ameaças no mundo informático e a atentarem contra a segurança dos cidadãos em geral? Será que são movidos simplesmente por dinheiro ou por causas ou mesmo interesses nacionais reflectidos no cumprimento de missões?

As ameaças ao ciberespaço tem tido as seguintes motivações e estão caracterizadas pela seguinte tipologia (IDN nº 12, 2013, p. 23-24):

- ***"Benefícios económicos**. São a motivação mais comum no domínio do ciberespaço. A realização de atos fraudulentos para conseguir dinheiro, o roubo de informações para venda pela melhor oferta ou a execução de ataques (ou fornecer os meios para isso) em troca de um benefício monetário são atos comuns que se enquadram nesta motivação. Cibercriminosos, espiões industriais e o pessoal interno são tradicionalmente os perfis do atacante com essa motivação."*
- ***"Vantagens táticas ou competitivas**. Esta é outra motivação que pode suscitar a atuação de diferentes agentes. Por exemplo, o roubo de informação militar de uma nação no meio de um conflito pode dar uma vantagem tática ao inimigo, ou a obtenção de informações relacionadas com uma organização ou empresa pode dar uma vantagem competitiva a outra entidade. As nações e os espiões industriais são os agentes mais suscetíveis a ter essa motivação."*
- ***"Motivações políticas**. Podem levar diferentes organizações a atacar ou realizar ações prejudiciais contra governos ou organizações públicas. Os perfis de ameaça*

[56] https://ics-cert.us-cert.gov/ (em linha) [Consult. 11 Junho 2014].

que mais se encaixam nesta motivação são os terroristas e os "hacktivistas". Os conflitos entre diferentes nações também se encaixam, por vezes, dentro deste âmbito."

- ***"Destruição ou dano**. Os terroristas surgem também associados claramente a essa motivação, pois tendem a procurar a execução de ataques que têm esse efeito. Por outro lado, as nações que entram em conflito também podem vir a inserir-se neste grupo."*
- ***"Fama ou vingança**. A procura de notoriedade e fama está geralmente associada aos hackers, que buscam reconhecimento em diferentes comunidades e fóruns, tendo como objetivo saltar as barreiras de segurança, mas não causar nenhum dano, embora possam aceder a informações sensíveis. Pessoal interno de uma organização também pode ser movido por esta motivação, mas estes tendem a perpetrar ações mais relacionadas com vingança."*

CAPÍTULO 4.
UMA REALIDADE PREOCUPANTE – A CIBERESPIONAGEM

A ciberespionagem, pelo que até ao momento foi descrito apresenta até determinado ponto semelhanças com o conceito de ciberataque. Por vezes confundidos, os conceitos pelas suas características apresentam diferenças significativas. De facto, os conceitos não devem ser tratados da mesma forma muito menos confundidos.

A grande distinção parece-nos que se coloca-se ao nível do impacto, se foram ou não infligidos danos.

Ao relembrarmos o significado genérico de ciberataque, como as operações de disrupção/perturbar, negar, degradar ou destruir informações existentes em computadores e em redes de computadores, parece-nos evidentes que o campo de atuação deste evento vai muito para além do mero observar e recolher informação confidencial ou secreta. Num ciberataque, utilizando uma terminologia de carácter ofensivo e não meramente intrusivo, o invasor afeta sempre o normal funcionamento do sistema, seja por dano, alterando os atuais componentes do sistema, ou através da introdução de um elemento novo. Isto representa um ciberataque, contrariamente ao que se passa num ato de ciberespionagem, o qual não pressupõe a alteração do normal funcionamento dos sistemas e redes de computadores da vítima, mas antes a obtenção de informação, e se possível de forma não identificável que nem se percebe que a mesma foi procurada.

4.1. A CIBERESPIONAGEM: DE UM MERO CIBERATAQUE ÀS APT

A ciberespionagem pretende apenas obter a informação de que necessita, assemelhando-se à situação de um indivíduo que vai ao supermercado para subtrair um pacote de bolachas, sem que ninguém se aperceba, saindo daquele lugar da mesma como entrou, sem ser detetado. É assim que a ciberespionagem funciona, já na espionagem a recolha de

informações ou subtração de documentação confidencial e secreta processava-se sem que o oponente descobrisse, e caso fosse descoberto, poderia ter consequências fatais para o espião. O mesmo não se passa para o agente espião dos tempos modernos, que se movimenta no ciberespaço. Os movimentos até podem ser detetados mas conseguir determinar quem é o responsável, atribuir um ato a uma cara é de uma dificuldade tremenda senão mesmo impossível. E é precisamente destas dificuldades que a ciberespionagem se aproveita e a torna tão apetecível comparativamente à espionagem convencional, quer em termos de eficácia que em termos de impunidade dos seus autores.

Os efeitos de um ciberataques afiguram-se aos inerentes a ataques armados convencionais, e podem traduzir-se na morte / lesão de seres humanos ou destruição / danos de objetos. Na sua extensão mais abrangente e destruidora faz com que o conceito de ciberataque se diferencie de ciberespionagem (KOSTADINOV, 2013).

Para o autor Ophard (2010), uma proeminente diferença consiste precisamente na motivação que leva a infligir um dano em vez de levar a procurar e colher informação classificada e sensível (OPHARDT, 2010).

Para demonstrar as características distintivas destes dois conceitos apresenta-se em seguida apresentado um quadro comparativo, que coloca frente a frente os ciberataque e a ciberespionagem (KOSTADINOV, 2013):

Ciberataque versus Ciberespionagem		
Propósito	Perturbar, negar, degradar ou destruir	Reunir informações secretas
Abordagem	Direta (por ex., vírus, DDoS)	Clandestina (espiar)
Intervalo médio de tempo	Curto	Longo
Tipo de atacante	Atacantes	Divisão de inteligência
Base legal	jus ad bellum e jus in bellum (termo em Latim para direito à guerra).	Inexistente

Mas será que é praticável delimitar esta fronteira de forma tão estanque?
Mesmo que a ciberespionagem seja qualificada como um ciberataque, a verdade é que embora à primeira vista as consequências de um ato de espionagem não sejam nocivas, estas são intrusivas e podem também infligir consequências graves. Devemos então ter em linha de conta que uma atividade de ciberespionagem, muito embora pretenda ser cirúrgica, a sua execução pode ultrapassar os limites pretendidos e ter um impacto que não era o esperado, como se de um ciberataque se tratasse.

Parece-nos importante refletir sobre uma nova tipologia, ou melhor característica da ameaça, que embora de âmbito global está intrinsecamente ligada às práticas de espionagem. Estas denominam-se por Ameaças Persistentes Avançadas (APTs – Advanced Persistent Threats) (DELOITTE, 2011). As APT's merecem destaque não por serem uma outra tipologia de ataque, mas pela forma como permitem que o tipo de ataque se processe.

Desde já importa apresentar uma explicação sobre o são estas ameaças. As APT's são uma versão automatizada da espionagem dita tradicional. Esta última ao depender de um agente humano que opera no mundo físico apresenta à partida um maior risco de deteção, contrariamente ao que se passa com a ciberespionagem que funciona num mundo virtual, as APTs são de difícil deteção, porquanto mecanismo de alerta. Para além de serem difíceis de detetar também o são de combater. Ao se introduzirem num sistema de informação da empresa ou organização, fazem-no de forma quase invisível e criam um modo para subtrair os dados de informação que pretendem e sempre que quiserem, ou seja, sempre que tal for desejável retornam à mesma fonte de informação e recolhem a informação adicional de que necessitam, permanecendo sempre invisíveis (DELOITTE, 2011).

Elas agem de forma tão inteligente que não só identificam mas escolhem o caminho que lhes oferece menor resistência até obter uma posição confortável, permanecendo aí escondidas na infraestrutura da organização.

Atualmente ainda existem muitas organizações que não se encontram equipadas, munidas de meios humanos e técnicos para procurar evitar a sua intrusão ou no caso de esta ocorrer procurar a existência de APTs.

O grande entrave consiste na forma como estão estruturadas e organizadas as operações e práticas de segurança. A sua organização compartimentada faz com que a informação não seja devidamente agregada, correlacionada e analisada.

Tem-se visto que a cultura de segurança adotada pela maioria das empresas é apenas reativa e de modo geral, só reação às mudanças pouco nocivas, e desde que fáceis de detetar. Contrariamente àquilo que deveria ser expectável em qualquer organização, as ações habilmente planeadas e sustentadas conseguem subverter a existência de comunicação no interior da organização alvo e permitir a intrusão dos invasores externos. Existem diversas técnicas que irão disfarçar as atividades das APTs. Na verdade, as APTs raramente utilizam táticas de destruição da infraestrutura de segurança, apenas a torna vulnerável para a sua entrada, até porque o objetivo é permanecer na infraestrutura sem ser apanhado, permitindo aos agentes externos a sua entrada para a recolha de dados. O prejuízo dessa invasão muitas vezes só é percebido tempo mais tarde quando a informação roubada é utilizada em benefício do invasor (DELOITTE, 2011).

Aquilo que se poderia esperar de uma empresa seria implementar um sistema de segurança que conseguisse prevenir ou neutralizar as tentativas de intrusão ou de ataque perpetradas através do exterior, quer através da utilização da internet quer da rede de computadores.

4.2. FORMAS DE CIBERESPIONAGEM – DOS ESTADOS ÀS EMPRESAS

Tal como já vem sido referido ao longo do presente trabalho, não só os Estados são vítimas de ciberespionagem, empresas e ou organizações não-estatais também estão na mira destas atividades.

Numa sociedade cada vez mais interl,igada e complexa, parece ser difícil para as agências governamentais e empresas antecipar o próximo ataque ou atividade maliciosa, disso são exemplo os inúmeros incidentes que através da internet têm comprometido questões de privacidade e confidencialidade, possibilitado a disrupção das Infraestruturas Críticas (IC) do Estado, ou influenciando os processos decisórios de Estados e de organizações não-estatais.

A estrutura militar e geoestratégica de uma nação também não deverá ficar lesada por uma intrusão e comprometimento dos seus planos. A sua defesa deverá ser mantida em constante alerta e permanente modernização.

Também as entidades não estatais e as organizações empresariais estão expostas a um conjunto de ameaças cibernéticas. As empresas que criam produtos de alta tecnologia e as que possuem departamentos de Investigação e Desenvolvimento (I&D) estão particularmente susceptíveis à espionagem industrial (REPORT TO THE CONGRESS, 2011).

É neste atual ambiente competitivo de âmbito mundial, que a sobrevivência das empresas está cada vez mais relacionada com o acesso ao conhecimento e a sua capacidade de mobilizá-lo. As inovações tecnológicas, as informações sobre os novos mercados e sobre os concorrentes, quer nacionais quer internacionais, são elementos imprescindíveis para a manutenção da competitividade das empresas. O comprometimento desse conhecimento e de informação sensível das organizações, incluindo processos de inovação, pesquisa e desenvolvimento, propriedade industrial, planos e estratégias empresariais, bem como outra informação sensível de negócio, pode colocar em risco a sobrevivência das mesmas e dos postos de trabalho, mas também a segurança económica dos Estados modernos e desenvolvidos, isto é, os interesses ditos nacionais.

Para a salvaguarda dos interesses económicos nacionais os Estados têm sido compelidos a a assumir um papel cada vez mais interventivo, cumprindo desta forma as suas obrigações de defesa e segurança do bem-estar das populações. Mas para que o papel do Estado alcance as suas pretensões, é necessário que as organizações quer públicas quer privadas estejam conscientes dos riscos e das ameaças a que estão sujeitas para que adotem um comportamento securitário mais apropriado e proativo. A inexistência de uma cultura de segurança por parte das organizações empresariais constitui uma vulnerabilidade que pode ser explorada pelos agentes da ameaça.

Por isso aquelas devem dotar-se de recursos e conhecimentos que permitam, não só de forma preventiva mas especialmente proactiva, identificar ameaças e defender os seus interesses, que neste caso serão também os interesses nacionais, para que as informações

sensíveis e confidenciais ou de elevado valor económico não 'caiam' nas mãos dos adversários Paralelamente levanta-se uma questão. Depois da informação comprometida, qual o valor do prejuízo? que consequências podem daí advir?

Chegados aqui parece-nos apropriado destrinçar os elementos que distanciam ou aproximam a espionagem económica da espionagem industrial. Embora os conceitos possam ser confundidos, existem autores que apresentam diferenças. Nesta corrente de pensamento falamos no antigo chefe do setor de contraespionagem brasileiro. Ele entende que a espionagem económica é um ato ilegal moralmente desencadeado por um Estado, que através dos seus serviços de informações tenta recolher dados financeiros, comerciais, económicos e tecnológicos, em proveito das suas empresas nacionais, ou então para influenciar as decisões de caráter económico de outro país. Enquanto a espionagem industrial é iniciada por uma empresa ou organização, normalmente concorrente, e que por estar presente no mercado constitui um alvo prioritário para as atividades de espionagem (BESSA, 2012).

Também o Gabinete Nacional de inteligência americano através dos conceitos legais definidos no Ato Espionagem Económica (Espionage Economic Act - 1996) [57] distingue estes dois conceitos. A espionagem económica ocorre quando um ator, sabe ou pretende que as suas ações beneficiem um governo estrangeiro, instrumentalmente ou com um agente, com conhecimento de causa: (1) rouba, ou sem autorização apropria-se, leva consigo, esconde, ou obtém por meio de engano ou fraude um segredo comercial; (2) copia, duplica, reproduz, destrói, 'uploads', 'downloads' ou transmite um segredo comercial sem autorização: (3) recebe um segredo comercial, sabendo que foi roubado, apropriado, obtido ou convertido, sem autorização do seu proprietário. Por outro lado a espionagem industrial, ou o roubo de segredos comerciais, ocorre quando um ator, sabe ou pretende que as suas ações irão prejudicar o proprietário de um segredo comercial de um produto produzido para ou colocado no comércio interestadual ou estrangeiro, age com a intenção de converter esse segredo comercial em benefício econômico de outra pessoa que não o proprietário através de: 1) rouba, ou sem autorização apropria-se, leva embora, dissimula, ou obtém informações por meio de engano ou fraude relacionadas com o

[57] Economic Espionage Act of 1996 em http://www.fbi.gov/about-us/investigate/counterinteligência/economic-espionage (em linha) [Consult. 8 de Maio 2014]

segredo; 2) copia, duplica, reproduz, destrói, realiza 'upload' ou 'download[58]', ou de outra forma transmite essa informação sem autorização; ou, 3) recebe essa informação, sabendo que essa informação foi roubada, apropriada, obtida ou convertida sem autorização (REPORT TO THE CONGRESS, 2011).

Tal como temos vindo a referir os Estados tal como as organizações empresariais, nas quais assenta e estabilidade económica de um país, estão em constante risco e o ser ou estar a ser alvo de um ciberataque é uma realidade.

4.3. ATORES PRINCIPAIS

Apesar da fenómeno da ciberespionagem fazer atualmente parte do suporte bélico de alguns países, existem aqueles em que tais ferramentas encontram-se num estágio de primazia relativamente aos restantes. Entre tais países destacam-se sem qualquer tipo de dúvida os EUA, a China e a Rússia.

São desde há muito tempo conhecidas a incursões dos três países em território do ciberespaço dos restantes, tendo sempre como objetivo o de roubar informação privilegiada sobre armas e planos do foro económico. Como já foi referido, os estados têm-se socorrido de agentes que pela excelência dos seus conhecimentos e desempenho oferecem as melhores garantias de um serviço de ciberespionagem eficiente e realizado de forma indetetável.

Sucede que alguns dos ataques realizados têm sido visíveis por parte dos sistemas de defesa dos países alvo. Como exemplo, podemos avançar as constantes acusações dos EUA à China, tendo sempre os chineses desmentido, achando que as acusações são sem fundamento e sentido.

A verdade é que a China possui grupos compostos por indivíduos que ocupam instalações governamentais e donde realizam as planeadas ações se espionagem. Para além, disso os

[58] Descarregamento de dados de um computador remoto para um computador local.

EUA dizem possuir sólidas provas que a China tem atacado diversos servidores de empresas e instituições Americanas.

Recentemente surgiram notícias sobre o grupo 61398, formado por técnicos chineses, pertencente ao Exército de Libertação do Povo da China (ELPC), que estaria na origem dos últimos ataques cibernéticos por parte dos chineses e que resultaram no prejuízo de milhões de dólares à economia americana. Sobre esta situação vem a empresa Mandiant alertar para a existência de milhares de ciberespiões do ELPC ou mesmo em regime de 'outsourcing' que atacam de forma concertada redes informáticas dos EUA[59].

Segundo as notícias, os EUA acusaram os cinco oficiais chineses de terem roubado, entre 2006 e 2014, informações comerciais confidenciais de empresas norte-americanas especializadas em energia nuclear ou solar e do setor industrial.

Uma vez que não existe uma guerra declarada entre os dois países não deixa de ser curiosa a forma sub-reptícia e cínica como estes países lutam entre si e o alvo que preferem atacar – a economia.

Aliás as ações contra os sectores económicos funcionam com o desígnio último de auferir quantia monetária, alcançado uma vantagem é possível ganhar os adversários. Mas não é somente a este nível que se consegue debilitar um Estado, retirando as suas mais valiosas empresas do núcleo duro do mercado económico e financeiro mundial. Incapacitar um Estado de se financiar para as necessárias obrigações militares de defesa assim como de assegurar as suas responsabilidade sociais por dificuldades financeiras pode torna-se um fator de pressão acrescido para qualquer Governo.

Aparte deste ataque, já a empresa Google havia anunciado a deteção de ataques oriundos da China, o que motivou à saída da Google do território chinês.

O relatório elaborado pelo Gabinete de Contrainteligência do EUA para o seu Congresso tece um quadro assustador no que respeita à utilização da espionagem cibernética por países estrangeiros para tentar obter segredos comerciais e industriais de empresas norte-

[59] Ver http://exameinformatica.sapo.pt/noticias/mercados/2013-02-19-unidade-61398-os-espioes-que-desviaram-centenas-de-terabytes-dos-eua (em linha) [Consult. a 27 Maio 2014]

americanas. Esse mesmo relatório dá conta de que os atores chineses são os intrusos mais ativos e persistentes ao nível da espionagem económica (REPORT TO THE CONGRESS, 2011).

Para além da China, a Rússia surge como outro dos países que aponta "armas" aos EUA, no que respeita a constantes ataques informáticos. A Rússia, apesar de ser parceira com os EUA em inúmeros tratados de cooperação, ainda vê os americanos como adversários, ou ainda não fossem visíveis resquícios da Guerra Fria. Além do mais, o plano ideológico e a gestão das relações internacionais ainda dividem muito os dois países, originando uma desconfiança que só é acalmada com um hipotético controlo sobre as ações do outro.

De acordo com diversos relatórios, a Rússia com o intuito de diversificar a sua economia e torna-la mais competitiva, apostou fortemente no roubo de planos de empresas estrangeiras, tornando-se a maior economia do mundo o alvo mais apetecível. Este é sem dúvida a parecer do relatório para o congresso, que diz que os serviços de inteligência da Rússia lideram um conjunto de atividades para colher informação económica e tecnológica. Esse relatório prevê ainda que a China e a Rússia "permaneçam agressivas e continuem a ter agentes capazes de obter informação económica sensível e tecnologias dos EUA, particularmente no ciberespaço" (REPORT TO THE CONGRESS, 2011).

A verdade é que os EUA é um líder no desenvolvimento de novas tecnologias e um jogador central no panorama mundial das redes financeiras e comerciais, razão pela qual são constantes e vão continuar a um nível elevado as tentativas de recolher informação tecnológica e económica. Para o país isso representa uma ameaça persistente e em crescimento à sua segurança económica. A natureza da ameaça cibernética vai evoluir com os continuados avanços tecnológicos no ambiente de informação global (REPORT TO THE CONGRESS, 2011).

Por este fato e analisando as últimas notícias, observa-se que os EUA são a vítima no meio no contexto dos incidentes cibernéticos. Mas será que isso corresponderá à verdade nua e crua?

Não devemos esquecer que quando Edward Snowden, ex-técnico da NSA, surgiu com as mais polémicas divulgações sobre ciberespionagem, verificou-se que eram os EUA que

sistematicamente e sem escrúpulos espiavam um grande número de países, inclusivamente a China e a Rússia. As revelações de espionagem em massa provocaram um escândalo diplomático de proporções globais, ao mostrar que os serviços de inteligência americanos vigiavam milhões de comunicações, tanto da população, de empresas e de governos e embaixadas.

Foram divulgados dados que a NSA já realizava incursões em sites chineses e até na empresa multinacional de tecnologia Huawei, para confirmar se esta espiava para o governo chinês e outros países. De acordo com artigo da revista Foreign Policy, a NSA, através do sector Office of Tailored Access Operations, que alegadamente realiza as ações de pirataria para os EUA, ter-se-ia infiltrado com relativo êxito em empresas de telecomunicações chinesas e que tais invasões já durariam há cerca de 15 anos[60].

É também sabido que os EUA foram sempre pioneiros a nível tecnológico constituindo um país de referência para todos os outros. Então nenhum país possuiria mais condições de espiar ciberneticamente um outro, que não os EUA. São muitos os exemplos que mostram que os EUA não são nenhumas vítimas neste tipo de disputas, mas pelo contrário, que foram eles os percursores nestas atividades e que foram imitados pelas outras potências.

Os EUA neste momento estão a ser vítimas da sua própria criação, apesar da sua bem oleada máquina de propaganda apresentar uma imagem bem diferente, culpabilizando a China e a Rússia das mais vis ações de espionagem. No fundo, os EUA simplesmente pretendem desviar as atenções de si para os outros, continuando assim as suas atividades de espionagem de uma forma mais dissimulada.

As ‘disputas’ existentes entre estes atores principais vão tendencialmente continuar, até porque enquanto grandes potências a nível mundial, não vão querer perder o poderio que lhes é atribuído, em especial o económico, e nunca relegando para segundo plano o político e o militar. No entanto haverá sempre a preocupação de não prejudicar as relações institucionais e comerciais entre elas.

4.4. CIBERESPIONAGEM COMO CAMPO DE CONFRONTO

60 http://www.foreignpolicy.com/articles/2013/06/10/inside_the_nsa_s_ultra_secret_china_hacking_group. (em linha) [Consult. 05 Junho 2014].

Por uma combinação de razões tecnológicas, comerciais e políticas tem sido especialmente difícil, em primeiro lugar, recolher e depois revelar as provas do uso agressivo e/ou criminal que se faz do ciberespaço.
O desafio tecnológico que aqui se coloca é atribuir (pode ser difícil mas será que é impossível?) os ataques e intrusões que se processam pelo ciberespaço, mas também o de detectar.
Uma outra situação consiste na vítima aceitar que foi vítima de ataque, aceitando tal condição como resultado do ambiente em que opera.

A prevenção, mesmo que seja possível, pode ser alcançada a um custo direto considerável e indiretamente prejudicar as relações comerciais de médio e longo prazo. O setor financeiro similarmente, tem sido relutante em revelar as violações de segurança com receio que tal leve a uma falta de confiança de investidores e clientes. Da parte estatal, existe uma recusa na revelação de informação sensível e de *intelligence* sobre as atividades criminosas e de assuntos relacionados com a segurança nacional, com medo de comprometer fontes, redes e procedimentos. No entanto, a maior cautela em assumir determinada posição face aos acontecimentos de ciberespionagem que envolve a grande potência asiática, a China, prende-se com questões comerciais, com o objetivo de não danificar as relações que são mantidas com aquela potência, e com questões de segurança, o aparecimento de notícias declarando alguma insegurança nas áreas de pesquisa e desenvolvimentos poderá prejudicar a reputação de um país.
Por isso existem muitas razões para que um governo seja cauteloso sobre as provas existentes de um ciberataque, especialmente quando um dos intervenientes é a China, e sobre a divulgação de determinada informação. Mas tal comportamento parece estar a ser desafiado, e os indicadores apontam para uma aproximação entre aquilo que é a opinião formada e a informação que é veiculada.

As empresas especializadas em cibersegurança têm relatado, ano após ano, uma escalada de ataques cibernéticos. A edição de 2011 do relatório da Symantec sobre 'Internet Security Threat' refere que entre 2009 e 2010 um aumento de 93% no volume de ataques com recurso à internet (Symantec Report, 2011). Este tipo de análises revelam alguma preocupação ao nível da segurança cibernética internacional, e como tal um alerta para a comunidade internacional. Mas ainda assim, não só as estatísticas trazem evidências do que está a passar pelo mundo, esta mudança pode ser resultado de uma nova abordagem

adotada pelos governos e pelo setor não-estatal. As organizações comerciais e industriais parecem estar dispostas a expor-se, agora mais que nunca, divulgando violações de privacidade e segurança.

Se as vítimas de ciberespionagem estão mais dispostas a divulgar as suas vulnerabilidades, então é possível que haja uma determinação em desmascarar os responsáveis de tais atos. Acusações surgem do setor privado público, nomeando a China como fonte desses ataques. O ponto de afirmação/viragem ocorre no setor privado com o acontecimento que envolveu a Google. Em 2010 a Google decidiu comunicar que tinha sido vítima de intrusão por *hackers* chineses, numa campanha que ficou conhecida como a 'Operação Aurora'. Mas a existências dos ataques, eram apenas uma questão de tempo, desde o ano de 2009 que especialistas da área de tecnologia de informação diziam que as organizações americanas perdiam regularmente informação que lhe permitia ter vantagem competitiva – resultados sobre a despesa de I&D, planos de engenharias, fórmulas químicas e biológicas, software complexo, e até listas de clientes e informações sobre preços - para entidades estrangeiras (muito provavelmente originárias da China) mas que através da ciberespionagem conseguiam aceder a essa informação.

Mas não só do continente americano surgem acusações contra a China. Na primavera e Verão de 2011, emergem do Reino Unido declarações que noticiavam a invasão de estudantes chineses nas universidades daquele país. A sua presença tinha como objetivo roubar segredos tecnológico e científicos, através da implantação de um software que continha um vírus que permita a comunicação de informação para a China. Sobre esses acontecimentos alude-se a um testemunho de um britânico que afirmou ter assistido a exemplos assustadores, em que os vírus eram deixados nos computadores para que a informação continuasse a ser transmitida mesmo após a partida desses estudantes para o seu país de origem. Tais acusações foram refutadas pela embaixada chinesa presente naquele país, e classificaram-nas como '*chocantes, totalmente infundadas e absurdas'*, e constituam uma calúnia que prejudicava todos os estudantes chineses. (CORNISH, 2012)

A empresa americana de cibersegurança McAfee acusou um ator não estatal de uma longa série de ataques cibernéticos contra um conjunto de empresas, das mais diversas áreas de atividade, entre as quais de destacam as Nações Unidas, o Comité Olímpico Internacional, a Associação das Nações do Sudeste Asiático, a Agência Mundial Anti-doping, e empresas

ligadas aos setores de defesa dos EUA e Reino Unido. Contrariamente ao que poderia ser expetável, a McAfee não citou a China como o responsável pelos ataques, no entanto especialistas independentes referiram acreditar que Pequim seria o responsável mais provável.

Ao longo dos anos têm sido possível tirar ilações do *modus operandi* da China no que toca às suas ações de ciberespionagem, com uma abordagem de longo prazo e silenciosamente paciente. Um recente relatório de 2012 refere que a empresa Nortel (faliu em 2009), antigo fabricante de equipamento de telecomunicações terá sofrido um ataque de ciberespionagem que se acredita ter durado pelo menos 10 anos. A suspeita dos ataques recaiu sobre a China, os atacantes introduziram um spyware[61] cuidadosamente camuflado nos computadores dos clientes, a fim de recolher informações sobre as senhas de acesso. O ataque revelou-se de elevada execução o que fez com que durante anos não fosse detectado. Esse mesmo relatório mencionou que a China é frequentemente acusada de ataques de espionagem económica. Os estados-nações como a China são uma ameaça constante às empresas, que buscam fragilidades para alcançar avanços tecnológicos. A negação tem sido a versão adotada pelos representantes chineses, que negam qualquer envolvimento e até afirmam que os ataques são 'transnacionais e anónimos' (CORNISH, 2012).

Pelo que tem sido referido, as políticas estabelecidas têm escolhido por uma ação cada vez menos reticente em aclamar a China como uma fonte de ciberespionagem. No ano de 2009, um artigo do New York Times relata a preocupação de um conjunto de oficiais americanos da atual Administração Obama, sobre o fato de que uma percentagem significativa dos ataques contra estruturas do governo é proveniente da China e Rússia. Na mesma linha de pensamento, surgem as declarações do Secretário de Estado da Defesa do RU, Dr. Liam Fox, que em 2011 advertiu que o Ministério da Defesa enfrentava diariamente ataques originários da China que colocavam em causa a propriedade intelectual nacional das indústrias de defesa e segurança. Nessa mesma altura, o Serviço de Segurança britânico, o MI5, acusou a China de despender demasiado tempo e energia na tentativa sistemática de roubar tecnologia sensível associada a projetos civis e militares e de informação política e

[61] Consiste num programa automático de computador, que recolhe informações sobre o utilizador, sobre os seus hábitos na internet e transmite essa informação a uma entidade externa na internet, sem o conhecimento ou o consentimento daquele.

económica sensível. Ainda nesse mesmo ano, o responsável pela cibersegurança do Ministério da Defesa do RU, o General Jonathan Shaw, alertou para o fato de o RU enfrentar uma grande ameaça cibernética, envolvendo a componente económica. Disse ainda que os chineses constituem a maior ameaça. (CORNISH, 2012).

O Comité de Inteligência dos EUA, representado pelo responsável republicano, avisou que os *hackers* e os espiões chineses constituem uma ameaça para os EUA. Efetivamente algum tempo antes um relatório produzido pelo Gabinete do Diretor Nacional de Inteligência dos EUA, admitia que as redes de computadores de várias agências governamentais dos EUA, empresas privadas, universidades e outras instituições – todas na posse de um volume de informação económica secreta e confidencial - tinham sido alvo de ciberespionagem, e que a maioria desta atividade teria por origem a China.

No final de 2011, uma página falsa do facebook foi usada para conduzir um ataque de 'engenharia social' contra oficiais da NATO. Sobre os autores do ataque, embora nada de forma oficial, foi levantada a hipótese de estarem a mando do governo Chinês. Ainda nesse mesmo ano a Google foi alvo de um ataque tipo spear-phishing[62], programado para descobrir as senhas de acesso ao Gmail de altos funcionários dos EUA e da Coreia do Sul, assim como de ativistas políticos chineses. A empresa ainda referiu que o ataque teria proveniência em Jinan, capital da província de Shandong e, apesar de ser possível afirmar com certeza quem ou o quê que foi responsável, a escala e o tipo de ataque assumiu as características de um ataque apadrinhado por um Estado. O governo chinês têm desde sempre negado qualquer acusação, alegando que os atacantes são *hackers* chineses não-governamentais, ou de outros governos que fingem ser a China, ou ainda que os ataques são ficcionados por elementos anti-China. No entanto, no entender de especialistas norte-americanos e de países aliados tais declarações parecem difíceis de acreditar. [CORNISH, 2012]

Os países atacantes bem como os países-alvo não estão a mudar o seu comportamento em termos de atos de ciberespionagem mas parecem estar a mudar um pouco de estratégia no que concerne à sua divulgação para o exterior, tentando de forma 'controlada' abalar a imagem dos seus adversários nos tablóides internacionais.

[62] http://us.norton.com/spear-phishing-scam-not-sport/article (em linha) [Consult. 6 Julho 2014]

CAPÍTULO 5.
O CONTEXTO PORTUGUÊS

Como tarefas fundamentais do Estado, destacam-se as questões da Segurança e Defesa, traduzidas na garantia da independência nacional, garantia dos direitos, liberdades e garantias fundamentais dos cidadãos, promoção do bem-estar e da qualidade de vida da população, de acordo com o consagrado no art.º 9 da Constituição da República Portuguesa.

A segurança é configurada constitucionalmente como um direito fundamental, que se encontra consagrado na Constituição da República Portuguesa, no n.º 1 do art.º 27º[63], que refere que todos têm direito à "liberdade" bem como à "segurança".

Ao Estado enquanto órgão de soberania na organização do poder político, cabe-lhe o papel primordial e insubstituível de criar uma cultura democrática de segurança, assente na autoridade do Estado de direito democrático e na compreensão de que a segurança é uma questão de cidadania. De igual modo, o Estado deverá possuir um papel interventivo na definição de políticas de segurança, enquanto responsável pela garantia da segurança pública e interna, por forma a responder às necessidades dos cidadãos, assim como identificar os principais ameaças que o mundo globalizado coloca e que pode por em causa o Bem-Estar Social das populações.

Por tal facto, a segurança tem sido uma preocupação e constitui hoje um conceito complexo e polissémico, na medida, em que engloba não só a segurança individual dos cidadãos, a segurança pública, mas também a segurança interna do próprio Estado, atravessando áreas como a defesa até à económica e/ou financeira.

Assim, o espectro de ameaças que colocam em causa a segurança dos Estados, é transversal às sociedades, e a portuguesa não foge à regra, apresenta um elevado grau de

[63] https://dre.pt/util/pdfs/files/crp.pdf (em linha) [Consult. 29 Abril 2014].

complexidade e é global, e requer do Estado Português respostas eficazes e eficientes, que se enquadrem no direito democrático, o que se traduz no absoluto respeito pelos direitos fundamentais.

Tal como tem vindo a ser referido ao longo do presente trabalho as TICs e a internet abriram portas a toda uma nova realidade de ameaças, muitas delas assumindo novas formas de radicalismo, desde o ciberterrorismo à ciberespionagem. Os acontecimentos diários relatados na opinião pública que dão conta dos inúmeros ataques aos sistemas de informação e comunicações de organismos públicos e privados, não deixam margem para o problema ser negligenciado ou ignorado.

A existência destas ciberameaças são uma realidade que naturalmente tende a ser crescente, quer em perigosidade quer em complexidade, e os Estados necessitam de disporem de serviços especializados que prestem apoio isento, esclarecido e eficaz, ao nível segurança nacional, com especial incidência na cibersegurança, aos diversos órgãos de soberania. Mas a segurança nacional e a estabilidade económica e financeira não se mantém só através de criação de serviços, associados a estes devem ser criados instrumentos jurídicos e operacionais e mecanismo de proteção que possibilitem uma ação reativa mas também proactiva.

O espectro e a configuração das ameaças suscetíveis de fazer perigar a segurança nacional levaram o legislador no panorama português a criar os serviços de informação portugueses, imprescindíveis para a segurança e defesa nacionais, e cuja atuação assenta, ao nível defensivo, na identificação de vulnerabilidades e ameaças conduzidas contra os interesses nacionais, e, por outro lado, ao nível ofensivo, na projeção dos interesses, bem como influenciar, determinar e condicionar o quadro geopolítico, geoeconómico e mesmo geocultural de determinadas áreas vitais do Estado de Direito Democrático.

Atualmente os Serviços de Informação portugueses têm procurado se adaptar e dar resposta quer ao avolumar de ameaças transnacionais quer ao crescimento de fenómenos associados ao processo de globalização, com destaque para a circulação de pessoas, ambiente, disputa de espaços de influência, mercados, matérias-primas ou domínio de setores estratégicos. Neste contexto parece nos pertinente enveredar pelo mundo do Sistema de Informações da República Portuguesa (SIRP), que é composto pelo Serviço de

Informações Estratégicas de Defesa (SIED) e o Serviço de Informações de Segurança (SIS), e entender o que representa na estrutura nacional em defesa dos interesses nacionais.

A preservação da segurança nacional, e consequentemente do Estado, está dependente da funcionalidade e coordenação eficaz das várias instituições, que exercem um conjunto de competências e atribuições na área da segurança e prevenção e investigação criminal, do qual são parte integrante o Sistema de Segurança Interna, o Sistema de Informações da República Portuguesa, o Sistema de Investigação Criminal e o Sistema de Proteção Civil.
Em termos de Segurança Interna, a legislação portuguesa dispõe de um diploma legal designado por "*Lei de Segurança Interna"*[64], no seu primeiro artigo define o conceito de segurança interna como sendo a *"atividade desenvolvida pelo estado para garantir a ordem, a segurança e a tranquilidade públicas, proteger pessoas e bens, prevenir e reprimir a criminalidade e contribuir para assegurar o normal funcionamento das instituições democráticas, o regular exercício dos direitos, liberdades e garantias fundamentais dos cidadãos e o respeito pela legalidade democrática*".

No cumprimento do estipulado no art.º 1º da Lei de Segurança Interna, concorrem para garantir a segurança interna, nos termos do art.º 25º do mesmo diploma legal, um conjunto de forças e serviços de segurança, com destaque para os Serviços de Informações de Segurança.

Neste contexto, em 1984, é aprovada a Lei Quadro do Sistema de Informações da República Portuguesa (SIRP)[65], mais tarde revogada pela Lei n.º 30/84, de 05 de Setembro -, que no n.º 2 do Art.º 2º define as principais finalidades do SIRP, assim, confere-se "*aos serviços de informações a incumbência de assegurar, no respeito da Constituição e da lei, a produção de informações necessárias à salvaguarda da independência nacional e à garantia da segurança interna*".

No domínio da salvaguarda da independência nacional, dos interesses nacionais e da segurança externa e interna, entra em vigor a Lei n.º 9/2007 de 19 de Fevereiro[66], que estabelece a orgânica do Secretário-Geral do Sistema de Informações Estratégicas de

[64] Lei 53/2008 de 29 de Agosto - Lei de Segurança Interna.
[65] Lei n.º 30/84, de 05 de Setembro - Lei Quadro do Sistema de Informações da República Portuguesa (SIRP).
[66] http://www.dre.pt/pdf1sdip/2007/02/03500/12381252.PDF (em linha) [Consult. 24 Abril 2014].

Defesa (SIED) e o Serviço de Informações de Segurança (SIS) (revoga os Decretos-Leis n.º225/85, de 4 de Julho - que define os serviços que integrariam o SIRP -, e o 254/95, de 30 de Setembro – que no âmbito da Lei Quadro do SIRP define a criação de um novo organismo o SIEDM, o Serviço de Informações de Estratégia e Defesa Militares).

As competências de segurança do Estado Português, nas quais se englobam as necessidades dos cidadãos no que concerne à sua segurança física, encontra-se demarcada pela Lei Quadro do SIRP e pela atuação dos dois organismos responsáveis pela produção de informações em Portugal: o Sistema de Informações de Segurança (SIS) e o Serviço de Informações Estratégicas de Defesa (SIED). Quanto ao Sistema de Informações de Segurança (SIS) foram-lhe conferidas pelo art.º 21º do mesmo diploma as seguintes atribuições, a "*produção de informações que contribuam para a salvaguarda da segurança interna e a prevenção da sabotagem, do terrorismo, da espionagem e a prática de atos que, pela sua natureza, possam alterar ou destruir o Estado de direito constitucionalmente estabelecido*", enquanto, por outro lado, o Serviço de Informações Estratégicas de Defesa (SIED), foi-lhe atribuída a missão, de produzir "*informações que contribuam para a salvaguarda da independência nacional, dos interesses nacionais e da segurança externa do Estado Português*" (art.º 20º da Lei Quadro SIRP).

A Lei n.º 9/2007 de 19 de Fevereiro, confere ao Sistema de Informações de Segurança (SIS), no seu art.º 33º, competências específicas no âmbito da pesquisa, análise e o processamento de notícias, e a difusão e arquivo das informações produzidas. Compete-lhe então elaborar estudos e preparar documentos que lhe forem determinados; difundir as informações produzidas às entidades indicadas; comunicar às entidades competentes para a investigação criminal e para o exercício da ação penal os factos configurados como ilícitos criminais; e, por fim, comunicar às entidades competentes as notícias e informações de que tenha conhecimento e respeitantes à segurança interna e à prevenção e repressão da criminalidade.

No mesmo diploma, estabelece o art.º 26º, que o Serviço de Informações Estratégicas de Defesa (SIED), ao nível das suas competências específicas, deve promover a pesquisa, análise e o processamento de notícias, e a difusão e arquivo das informações produzidas.

A distinção entre estes dois organismos preconiza-se ao nível do âmbito da abrangência da missão, perfeitamente esclarecida e produzida nos art.º. 20º e 21º da Lei Quadro do SIRP. Então mas competindo-lhe a garantia da segurança da comunidade bem como dos interesses nacionais, como se enquadra a sua atuação na prevenção de uma aparente nova tipologia de ameaças, que embora possam apresentam características diferentes do que até então era tido como tradicional, poderão produzir efeitos semelhantes, que variam consoante a motivação ou objetivo intrínseco à sua realização. A proliferação de ameaças no ciberespaço na forma ciberataques, merecem a maior atenção e devem ser objeto de e controlo, vigilância sejam eles na forma de ciberterrorismo, cibercriminalidade ou ciberespionagem. Concretamente as competências do SIRP centram-se na antecipação de possíveis ameaças que coloquem em causa a segurança nacional, então qual será o papel destes organismos quando falamos de ciberataques cuja origem é identificada como sendo de entidades ou de indivíduos que não sendo elementos das organizações prestam serviços na prossecução dos objetivos daquelas.

Concretamente, no que concerne à ciberespionagem, a atuação dos Serviços de Informações desenvolve-se na vertente da contraespionagem, que é definido como a "*atividade desenvolvida por um Serviço com o objetivo de antecipar, detetar e impedir atividades de recolha de informações que possam colocar em risco a segurança nacional, habitualmente designadas por Espionagem*"[67].

A atividade de contraespionagem preconizada ao nível do SIS visa contribuir substantivamente para a eficácia do sistema de segurança interna e a garantia do bem-estar económico nacional, em colaboração com outras instituições nacionais e estrangeiras, e realiza-se através de três vertentes: a primeira, diz respeito a um novo desafio, o da ciberespionagem que, pelo seu carácter transversal a todas as áreas que utilizam a Internet, exige novas medidas de prevenção e combate, mas também as já tradicionais formas de espionagem (contra-espionagem); a segunda, em que se defronta a ingerência de entidades estrangeiras que visam influenciar o poder nacional (contra-ingerência); e, por fim, a terceira em que enfrenta ataques às medidas de proteção da informação sobre produtos e projetos em sectores estratégicos e áreas do conhecimento (proteção dos interesses económicos) (*id.* [46])

[67] http://www.sis.pt/espionagem.html (em linha) [Consult. 24 Abril 2014].

Neste sentido, foi criado um programa de sensibilização das empresas, o Programa de Segurança Económica (PSE), que teve como objetivo desenvolver um conjunto de medidas preventivas de sensibilização, de alerta e de apoio à tomada de decisão das organizações. Procurou-se assim que as organizações e as pessoas que trabalham nos sectores público e privado estejam conscientes dos riscos e das ameaças a que estão sujeitas e que estejam melhor preparadas para os enfrentar[68]. Numa forma de caracterizar sumariamente este programa, o seu diretor elaborou um documento no qual afirma que o "PSE atua numa lógica preventiva que passa pela sensibilização dos interlocutores relativamente a vulnerabilidades, potenciais alvos, agentes da ameaça e a indícios de atividades contrárias aos interesses económicos nacionais, contribuindo assim para a segurança económica"[69].
O apoio pretende ser permanente e para tal foi criada uma equipa devidamente apetrechada para tal desempenho.

Efetivamente o PSE pretende alertar para o risco de espionagem económica, acautelando a soberania nacional através da proteção das empresas nacionais que constituem um pilar na estrutura económica nacional. E isto acontece por que se tem verificado um aumento significativo do roubo de informações com valor económico nas empresas e nos centros de investigação científica e tecnológica que a a par do que se tem verificado a nível internacional, esta não é uma situação exclusiva do território nacional. A agressividade das ameaças neste contexto são reais e ameaçadoras[70].

A concorrência feroz dos mercados (ou noutra perspectiva, a tentativa de recuperar das vantagens competitivas) faz que o roubo do *know-how* e de informação reservada duma organização – incluindo processos de inovação, de pesquisa e desenvolvimento, de produção, de distribuição e de promoção, planos e estratégias empresariais ou propostas em concursos – seja uma opção cada vez mais válida e fácil neste encadeado, que se pode traduzir em prejuízos significativos para as empresas e para o país.

Quando assim acontece o Estado, empresários e trabalhadores, todos perdem, já que o eventual sucesso destas ações pode colocar em risco a sobrevivência de empresas e de

[68] http://www.pse.com.pt (em linha) [Consult. 24 Maio 2014].
[69] http://www.iict.pt/GTIeD/arquivo/SIS/SIS-sbm001.pdf (em linha) [Consult. 24 Maio 2014].
[70] http://www.pse.com.pt/ameaca.php (em linha) [Consult 24 Maio 2014].

postos de trabalho. Também os centros de investigação e as universidades sofrem roubos de conhecimentos que poderão ser transferidos para entidades estrangeiras, que a todo o custo desejam ganhar um melhor lugar no mercado.

No atual contexto hostil de concorrência económica mundial, a qualidade dos recursos humanos e a capacidade de inovação das organizações são indubitavelmente uma mais-valia e potenciam a criação de valor, atraindo interesses estrangeiros. As nossas empresas, mesmo aquelas de menor dimensão, não fogem ao escrutínio das entidades estrangeiras.

As ações preconizadas por estas entidades que do exterior tentam transferir para si valor, tendem frequentemente a assumir a forma de espionagem. As ações de espionagem, principalmente na área económica, não são exclusivas dos Serviços de Informações, outras entidades existem que, directa ou indirectamente, trabalham para aqueles Serviços ou para entidades privadas que se dedicam, de forma aberta ou clandestina, à recolha de informações.

Parece-nos evidente a vantagem de um Serviço de Informações, seja em relação a fenómenos isolados ou não estruturados. Aqui pode ser elaborado um trabalho sistemático, baseado num quadro organizacional, que aposta na preparação e condução de recolha de Informação (fases de busca, recolha, organização, recorte, conferição, confirmação, infirmação, avaliação, sintetização), na análise, compreensão e avaliação das situações e subsequentes alternativas de atuação, tendo por persecução última, a utilização da Informação no controlo dos resultados da ação.

Pelo exposto, a produção de informações, é, em regime de exclusividade, da competência do SIS e SIED (organismos integrados no SIRP), com especial incidência nas matérias da sabotagem, do terrorismo, da espionagem, que a todo o custo pretende diminuir a existência de qualquer ameaça que coloque em causa a segurança nacional e interna.

Mas a verdade é que no concerne especificamente à questão da espionagem pouco tem sido revelado, bem se sabe que este continua a ser um tema envolto em segredo e poucos são aqueles que querem afirmar a sua existência. No balanço das orientações estratégicas em matéria de segurança interna, este fenómeno é abordado de forma muito sucinta. O Relatório Anual de Segurança Interna (RASI) relativo ao ano de 2013, "*no domínio da*

contraespionagem salienta as atividades desenvolvidas ao nível do programa de Segurança Económica (PSE), o qual foi criado com o objetivo de promover uma cultura de cibersegurança, junto das entidades públicas e privadas portuguesas, sensibilizando-as para o seu papel de dissuasão efetiva, face a potenciais ameaças ao interesse nacional"[71].

Mas não podemos delimitar a estrutura nacional aos Serviços de Informações, a massificação de uso e digitalização da informação trocada entre o cidadão, empresas e o Estado tem elevado de tal forma o nível de risco para os vários agentes, que a segurança da informação revela-se cada vez mais de um interesse elementar, tanto para garantir o funcionamento eficaz do Estado, organizações e cidadãos como para proteger a privacidade e construir a confiança nos canais eletrónicos. Mas o Estado deve ser sem sombra de dúvidas o grande mentor da sociedade chamando a si as diversas entidades e agências que consigo deverão delinear uma estratégia. Mas para isso existem tarefas que devem ser completadas.

Por isso mesmo, a segurança e a proteção contínua das infraestruturas de informação têm de ser encaradas como parte integrante de um processo contínuo e sistémico, e deve constituir uma preocupação para todos.

Para José Santos há especial responsabilidade dos Estados nesta temática ao dizer que "*a cibersegurança ou a proteção do ciberespaço não é um assunto da exclusiva responsabilidade dos Estados, mas antes uma responsabilidade partilhada*" [SANTOS, 2011].

Mas cabendo ao Estado a defesa da soberania nacional e o bem-estar da sua população, também é da opinião deste autor que "*a cibersegurança deve ser assumida como um bem público com intervenção direta do Estado*" [SANTOS, 2011].

Neste sentido a criação de uma estrutura nacional que permita–acautelar os interesses nacionais quer públicos quer privados ao nível da cibersegurança é parte da solução. Isto acontece também porque a nível internacional bem como europeu tem havido alguma pressão no sentido de se desenvolver mecanismos nesta matéria. Por um lado, é necessário

[71] http://www.portugal.gov.pt/media/1391220/RASI%202013.pdf (em linha) [Consult. 23 Junho 2014].

identificar quem é o interlocutor nacional com quem falar, por outro, sendo as redes interdependentes, a fraqueza de uma rede é definida pelo seu elo mais fraco.

O Estado tem ao seu dispor serviços que se encontram atentos a estas novas ameaças, como seja os Serviços de Informações, no entanto parece que não são suficientes e por isso é essencial alargar o âmbito da sua atuação, até porque o crescente número de incidentes e ataques maliciosos tendo como alvo as infraestruturas de informação do governo português bem como de instituições públicas e privadas, empresas e cidadãos, justifica a necessidade do País de possuir capacidades e valências próprias quer de âmbito estratégico mas também operacional capazes de garantir uma resposta eficaz, não só à ocorrência de incidentes no ciberespaço, mas também, num cenário mais gravoso, à gestão de crises.

Estando em causa as áreas que concretizam a soberania nacional como seja a autonomia política e estratégica do país, tem aparecido reflexões/propostas no sentido de ser criada uma Estratégia Nacional de Cibersegurança[72] e mais recentemente de uma Estratégia Nacional de Segurança da Informação (ENSI)[73], que definiu que Portugal deve procurar alcançar três objetivos principais: *garantir a Segurança no Ciberespaço*; *fortalecer a cibersegurança das infraestruturas críticas nacionais*; e ainda, *fortalecer os interesses nacionais e a liberdade de ação no ciberespaço*"[74].

No primeiro objetivo deve haver a preocupação de alertar empresas e cidadãos e para as ameaças que poderão advir da utilização descuidada e desprotegida do ciberespaço. Os serviços públicos terão um papel fundamental neste campo, ao desenvolverem um modelo que os municie de meios e técnicas capazes de melhorar a proteção dos sistemas de informação e da informação que se encontra no seu domínio. Esse modelo será interpretado pelos restantes agentes como adequado e a implementar num futuro próximo. A elaboração de suporte legislativo será uma ferramenta necessária e permitirá desenvolver a melhoria da cibersegurança e ainda promover a cooperação judicial e internacional.

[72] Em especial ocorrida no seio do GNS por força do pedido do governo aquela Autoridade para preparar os estudos.
[73] No contexto de uma investigação conjunta IDN/CESEDEN. Já em 2005, havia sido proposta, em ambiente não exposto publicamente uma ENSI, que era uma estrutura mas que tinha subjacente pelo menos uma política de informação.
[74] http://www.gns.gov.pt/media/1247/PropostaEstratégiaNacionaldeCiberseguraçaPortuguesa.pdf (em linha) [Consult. 29 Maio 2014].

Para assegurar este primeiro objectivo, Segurança do Ciberespaço, foram identificadas linhas de ação estratégica (id. [49]):

- *Analisar o ambiente de informação e antecipar eventuais ataques de forma a tomar as decisões apropriadas, acompanhando os últimos desenvolvimentos tecnológicos, analisando e antecipando ameaças a fim de estar na vanguarda;*
- *Detetar e bloquear ataques, alertar e apoiar as potenciais vítimas:*
- *Estimular e potenciar as capacidades científicas, técnicas, industriais e humanas do país de forma a manter a independência nacional neste domínio;*
- *Adaptar a legislação nacional de forma a incorporar os desenvolvimentos tecnológicos e novas práticas;*
- *Desenvolver iniciativas de cooperação internacional em áreas ligadas á segurança dos sistemas de informação, cibercrime, ciberdefesa e luta contra o terrorismo de forma a proteger melhor os sistemas de informação nacionais;*
- *Comunicar e informar de forma a influenciar e a aumentar a compreensão da população portuguesa relativamente à extensão dos desafios relacionados com a segurança dos sistemas de informação.*

O segundo objectivo, abrange a melhoria da segurança das Infraestruturas Críticas Nacionais, deverá acontecer em estreita ligação com as operadoras de telecomunicações e os detentores dessas infraestruturas. Para isso foram traçadas linhas de ação estratégicas que reforcem a Cibersegurança das ICN:

- *Reforçar a segurança das TIC nas Redes do Governo e da Administração Pública;*
- *Reforçar a Segurança dos sistemas de informação do estado e dos operadores das infraestruturas críticas para assegurar uma maior resiliência (capacidade de sobrevivência) nacional.*

O último objetivo teve como intenção capacitar as autoridades governamentais e os atores relacionados com a gestão de crise de meios de comunicação fáceis e confidenciais. Também aqui foram identificadas linhas de ação estratégica:

- *Reforçar iniciativas nacionais estruturantes da "Sociedade de Informação e do Conhecimento";*
- *Proteger e defender os mecanismos de Governação Eletrónica do Estado;*

- *Levantar a Estrutura Nacional de Cibersegurança e Ciberdefesa;*
- *Estabelecer mecanismos de cooperação nacional e internacional, neste âmbito.*

A Estratégia Nacional de Segurança da Informação (ENSI) nos termos daquela reflexão (do qual não discordamos na sua natureza de fundo), compreende, designadamente, a criação, instalação e operacionalização de um Centro Nacional de Cibersegurança (CNCSeg)[75], que terá a colaboração de todas as entidades relevantes em razão da matéria em causa e será coordenado pelo Gabinete Nacional de Segurança (GNS), que é a unidade nacional responsável por dar resposta ataques por via informática[76].

O GNS é dirigido pela Autoridade Nacional de Segurança (ANS)[77] a quem compete superintender tecnicamente os procedimentos da administração pública e garantir o cumprimento das medidas para garantia da segurança das matérias classificadas nacionais ou da responsabilidade nacional, designadamente as das organizações internacionais de que Portugal é parte, bem como exercer a autoridade de credenciação de pessoas e empresas para acesso e manuseamento dessas mesmas matérias[78].

No quadro das competências do GNS[79], que funciona no âmbito da Presidência do Conselho de Ministros, destacam-se a acreditação e a certificação de segurança de produtos e sistemas de comunicações, de informática e de tecnologias de informação que sirvam de suporte ao tratamento, arquivo e transmissão de matérias classificadas; a promoção do estudo, investigação e difusão das normas e procedimentos de segurança aplicáveis à proteção e salvaguarda das matérias classificadas, propondo a doutrina a adotar por Portugal na matéria e a formação de pessoal especializado nesta área da segurança.

O CNCSeg terá por missão contribuir para que Portugal use o ciberespaço de uma forma segura. As competências que lhe foram conferidas não devem colidir com as atribuições e

[75] Resolução do Conselho de Ministros n.º 12/2012.
[76] Decreto-Lei n.º 69/2014 de 9 de Maio.
[77] http://www.gns.gov.pt/ans.aspx (em linha) [Consult. 07 Junho 2014].
[78] Decreto-Lei n.º 3/2012 de 16 de Janeiro.
[79] O GNS funciona no âmbito da Presidência do Conselho de Ministros, junto do Gabinete Coordenador de Segurança. A ANS funciona na dependência direta do Primeiro-Ministro.

competências legalmente cometidas a outras entidades públicas em matéria de segurança do ciberespaço, nomeadamente no que respeita a infraestruturas críticas e integridade das redes e serviços, sendo exercidas em coordenação com estas entidades.

No entanto importa referir que o funcionamento e a operacionalização apenas poderá acontecer se houver consciência que é necessário promover o desenvolvimento de sinergias nacionais, através da articulação entre diversas entidades com responsabilidades de ordem diversa na matéria. E só estando a operar na sua plenitude, poderá ser possível evitar o desperdício de recursos, ser eficiente e potenciar a cooperação internacional com congéneres estrangeiros.

Efetivamente, o plano de ação do CNCSeg, similar a muitos outros que já estão a funcionar na maioria dos países europeus, visa uma consciência situacional permanente das infraestruturas críticas nacionais (setores da energia, comunicações, transportes, banca, forças armadas, governo e tribunais, por exemplo) para deteção e resposta a ataques por via informática. Efetivamente, o Centro Nacional de Cibersegurança surge com atraso em relação às metas definidas pela Comissão Europeia, que estabeleceu que, até ao final de Dezembro de 2012, todos os Estados-membros deviam ter estas estruturas operacionais.

Portugal até ao momento ainda não foi vítima de um ataque de ciberespionagem em grande escala, na verdadeira aceção da palavra, mas face ao que é relatado diariamente pelo mundo e ao que já tem acontecido em Portugal, o otimismo em relação à continuidade dessa tendência pode ser questionado. A questão é que, quem queira, tem à sua disposição as capacidades necessárias para realizar um ataque cibernético a sério. E por isso o Estado Português deve colocar as defesas em ordem e desenvolver redes e infraestruturas robustas e resistentes, além de modernizar a legislação para adequá-la às necessidades de segurança. As defesas atuais podem dizer-se que estão atualmente inadequadas para repelir ataques de oponentes sofisticados.

Como reporta aquela reflexão, sobre a "Estratégia da Informação e a Segurança do Ciberespaço" a existência de uma ENSI funcionaria como um vetor estratégico estruturante da revisão da sua Estratégia Nacional de Segurança e Defesa porque seria reconhecer a importância de proteger e defender o processo de geração de valor associado ao desenvolvimento potencial estratégico nacional neste domínio.

É importante que Portugal dê passos largos neste domínio da cibersegurança e chamar a este problema as demais entidades que com as suas valências e capacidades podem fazer toda a diferença, contribuindo de forma determinante para o sucesso da estratégia nacional de cibersegurança e para a eficácia do «centro nacional de cibersegurança».

Só depois do início do seu funcionamento ficará claro em que termos Portugal possui as capacidades necessárias para responder eficazmente às ciberameaças. E será que poderá responder de igual forma à ciberespionagem, pese embora toda a especificidade que envolve esta ameaça?

Para determinar se Portugal estará no caminho certo é relevante, num contexto de quase *'benchmarking*[80]*'*, avaliar o que tem sido feito lá fora, a nível das grandes potências, por demais faladas e envolvidas nestas matérias. E nomeadamente identificar se a ciberespionagem tem feito parte das grandes preocupações daquelas, ou apenas se tem limitado a agir por aquilo que é mais concreto, deixando para trás e sem resolução as práticas de espionagem.

[80] É um dos mais úteis instrumentos de gestão para melhorar o desempenho das empresas e conquistar a superioridade em relação à concorrência. Baseia-se na aprendizagem das melhores experiências de empresas similares e ajuda a explicar todo o processo que envolve um excelente desempenho empresarial.

CAPÍTULO 6.
A PERSPECTIVA INTERNACIONAL

Numa análise, relativamente reduzida, fez-se uma incursão por diversas ENCibersegurança e destaca-se nas linhas abaixo aquilo que são as principais preocupações nas questões de ciberespionagem.
Daremos uma especial relevância à ENISA, à NATO e à ONU passando pelos EUA como uma grande potência, por uma Austrália que procura integrar todos os aspectos de cibersegurança e pelo Reino Unido, pelo seu pragmatismo e sobriedade na implementação de medidas de segurança, só então devemos uma perspectiva global sobre outros países.

6.1. UNIÃO EUROPEIA

A União Europeia (UE), tem ao longo dos tempos se apercebido da necessidade de caminhar no sentido da segurança dos sistemas de informação e redes de suporte. Neste sentido criou a Agência Europeia para a Segurança das Redes e da Informação (European Union Agency for Network and Information Security – ENISA)[81], cujo objetivo é funcionar como o centro de competências para aconselhamento dos governos dos Estados membros e das instituições europeias em matérias relacionadas com a cibersegurança.

A ENISA foi então criada para reforçar a capacidade da União Europeia, os Estados-Membros da UE e da comunidade empresarial para prevenir, tratar e responder a problemas de rede e segurança da informação [82].

A Agência definiu linhas de atuação que se elencam em seguida:

- Aconselhar e assistir a Comissão e os Estados-Membros sobre a segurança da informação e no seu diálogo com a indústria para tratar de problemas relacionados com a segurança dos produtos de hardware e software;

[81] http://www.enisa.europa.eu/ (em linha) [Consult. 17 Junho 2014].
[82] http://www.enisa.europa.eu/about-enisa/activities. (em linha) [Consult. 17 Junho 2014].

- A recolha e análise de dados sobre incidentes de segurança na Europa e riscos emergentes;

- Promover a avaliação de riscos e métodos de gestão de risco para melhorar a capacidade de lidar com as ameaças à segurança da informação;

- Sensibilização e cooperação entre os diferentes intervenientes no domínio da segurança da informação, nomeadamente através do desenvolvimento de parcerias público / privadas com a indústria neste domínio.

Em termos operacionais foram criadas as CERT's[83], as Equipas de Resposta a Emergências Informáticas que constituem a ferramenta fundamental para a Proteção de Informações Infraestruturas Críticas (PICI). Cada país que está conectado à internet deve ter na sua posse capacidades para responder de forma eficaz e eficiente a incidentes de segurança da informação. Mas as CERT pretendem conseguir mais além, atuar como prestadores de serviços de segurança primário para os Governos e cidadãos e, ao mesmo tempo, agir como criadores de sensibilização e educadores.

Sublinha-se no âmbito da ENISA a existência da Unidade de Proteção de Informações Infraestruturas Críticas (CIIP). Esta Unidade é responsável por assessorar órgãos competentes nacionais da UE, sector privado e da Comissão Europeia para desenvolver respostas e estratégias de recuperação, políticas e medidas que atendam plenamente as ameaças emergentes que Infraestruturas Críticas de informação enfrentam nos dias de hoje. A Unidade tem por missão auxiliar os Membros da UE e a Comissão e emitir recomendações importantes para influenciar o processo político em diversas áreas; desenvolver boas práticas em áreas como as estratégias de segurança cibernética, exercícios nacionais cibernéticos; Organizar exercícios virtuais; oferecer treinos e seminários para Membros da UE, como exercícios nacionais, planos de contingência, comunicação de incidentes; ajudar as autoridades reguladoras nacionais de telecomunicações na implementação de um conceito harmonizado para a elaboração de um relatório de incidentes; facilitar o diálogo entre os atores públicos e privados sobre questões emergentes; contribuir para as políticas da Comissão e iniciativas estratégicas (por exemplo, a estratégia de segurança da Internet) e verificar que as recomendações são devidamente reguladas por todas as partes interessadas.

[83] http://www.enisa.europa.eu/activities/cert (em linha) [Consult. 13 Junho 2014].

Desta forma a União Europeia pretende responder às ameaças emergentes que derivam do ciberespaço através da rede internet. Assim, recentemente foi publicada uma Estratégia de Cibersegurança[84] que pretende constituir uma base comum para todos os Estados membros. No que respeita à ciberespionagem a estratégia da EU reconhece que a espionagem económica e as atividades patrocinadas por um Estado no ciberespaço representa uma nova categoria de ameaças para os governos e as empresas da EU e por isso quis prever um conjunto de ações: "*Se o incidente parece estar relacionado com a espionagem cibernética ou um ataque patrocinado pelo Estado, ou tem implicações ao nível da segurança nacional, as autoridades de defesa e segurança nacional irão alertar os seus homólogos relevantes, para que saibam que estão sob ataque e devem se defender. Serão ativados mecanismos de alerta precoce e, se necessário, também a gestão de crises ou outros procedimentos. Um incidente cibernético particularmente grave ou ataque pode constituir razão suficiente para um Estado-Membro poder invocar a cláusula de solidariedade da União Europeia (artigo 222 º do Tratado sobre o Funcionamento da União Europeia*". (CSEU, 2013)

No âmbito da Comissão Europeia foi publicado em 2012 pela ENISA um conjunto de normas para garantir a segurança das redes de comunicações da UE como dos próprios Estados membros. No âmbito militar, na sequência da aprovação em 2009 de um Conceito de Operações em Redes de Computadores, o Estado Maior da União Europeia (European Military Staff – EUMS) foi desenvolvido o Conceito de Ciberdefesa que foi entretanto aprovado pelo Conselho da UE.

Também neste domínio a EU quer ir mais além, e tem alargado as suas medidas. Por isso tem dado atenção à questão da estandardização/normalização de normas que possam reger a segurança da informação e a ciberdefesa. A UE, com o apoio da ENISA, começou a incluir normas nas suas políticas e estratégias. Mas parece que muito mais ainda permanece por fazer. O desenvolvimento de normas é necessário, e requer o envolvimento de atores dos setores privados e públicos A Estratégia de Cibersegurança da EU publicada "*reafirma a importância dos stakeholders no atual modelo de governânca da internet e reitera o seu suporte para uma abordagem de governação de multi-stakeholders*". Isto é

[84] http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security. (em linha) [Consult. 21 Junho 2014].

crítico porque uma abordagem de multi-stakeholders é fundamental para o desenvolvimento de normas bem-sucedidas, particularmente na área de cibersegurança, onde os fornecedores dos serviços do setor privado são amplamente envolvidos na realização da implementação dos requisitos do setor público (PURSER, 2014).

Apesar da diferença de prioridades de normalização, tanto práticas de segurança da informação públicas como privadas podem ser melhoradas através da identificação e da resposta à evolução de riscos e desenvolvimentos tecnológicos. Em particular, o lapso de tempo entre o aparecimento de uma nova tecnologia ou um modelo de negócio tecnicamente para a disponibilização de normas aplicáveis ainda é muito longo.

Ainda no que respeita à UE sublinha-se a criação recente do Centro de Análise de Informações da União Europeia (UE INTCEN) é um órgão de inteligência da União Europeia (UE). Neste sentido têm havido tentativas por parte deste organismo internacional na harmonização dos Serviços de Informações, este seria sem dúvida um passo importante para a cooperação ao nível das ameaças cibernéticas.

6.2. EUA

Já quanto à grande referência a nível mundial em matéria de segurança, os EUA desde cedo se aperceberam da ameaça que provinha da utilização indiscriminada, sem controlo e desprotegida do ciberespaço.

Logo no ano de 2003 os EUA tiveram consciência de que a economia e a segurança nacional americana estavam totalmente dependentes da tecnologia de informação e da infraestrutura de informação. No núcleo da infraestrutura de informação está a internet, um sistema originalmente concebido para partilhar informação. É essa mesma internet que hoje liga milhões de redes de computadores e que faz com que os serviços e infraestruturas essenciais dos Estado funcionem.

Um espectro de atores maliciosos pode e consegue conduzir ataques contra as infraestruturas críticas de informação. É aqui que se centra a principal preocupação, que as

existências de ataques cibernéticos organizados sejam capazes de causar uma disrupção das infraestruturas críticas nacionais, da economia ou a da segurança nacional.

As próprias autoridades americanas alertam para o fato de que não se dever ser muito otimista quando à possibilidade da existência de ameaças. Eles referem mesmo que tem havido casos em que atacantes devidamente organizados exploraram vulnerabilidades o que pode ser indicativo de poder existir capacidades mais intrusivas e destrutivas.

A incerteza impera quanto à intenção e às reais capacidades técnicas dos vários ataques observados. É necessária uma abordagem mais holística para determinar quais as tendências de longo prazo para as ameaças e quais as vulnerabilidades a sanar. O que se sabe é que as ferramentas de ataque e as metodologias utilizadas se estão a tornar amplamente disponíveis, e a capacidade técnica e sofisticação dos utilizadores empenhados em causar estragos ou disrupção está a progredir.

É convicção da América que mesmo em tempo de paz os adversários podem realizar espionagem, às instituições governamentais, centros de pesquisa universitários ou empresas privadas. A parte adversária também procura preparar-se para um futuro em que haja um confronto com ataques cibernéticos, e de que forma, através do mapeamento dos sistemas de informações dos EUA, identificando alvos-chave, e munindo as infraestruturas com portas traseiras e outros meios de acesso. Em tempo de guerra ou de crise, os adversários podem procurar intimidar os líderes políticos de uma Nação atacando as infraestruturas críticas e as funções económicas chave ou ainda minar a confiança pública nos sistemas de informação daquele país (NATIONAL STRATEGY USA, 2003).

Os ataques cibernéticos nas redes de informação dos Estados Unidos podem ter consequências graves, como a disrupção de operações críticas, causando elevados custos e perda de propriedade intelectual, ou, numa situação muito extrema, a perda de vidas. Contrariar tais ataques requer o desenvolvimento de capacidades robustas, faz parte das pretensões das autoridades americanas, pois para elas é fundamental reduzir as vulnerabilidades e dissuadir as pessoas que possuem intenção e as capacidades de prejudicar as infraestruturas críticas nacionais.

É neste encadeamento que o governo dos EUA estabeleceu em 2003 uma Estratégia Nacional para Segurança do Ciberespaço ("National Strategy to Secure Cyberespace")[85], articulada com a "National Strategy for Homeland Security", para evitar que o país fosse vítima de ataques que degenerassem em situações de confusão e de alarme generalizado ou que destruíssem informações e sistemas de informação importantes, traduzindo-se em prejuízos de milhões de dólares, definindo os seguinte objetivos:

- Prevenir ciberataques contra infraestruturas americanas críticas;
- Reduzir a vulnerabilidade nacional aos ciberataques;
- Minimizar danos e ganhar tempo antes da ocorrência de ciberataques.

A estratégia americana indica também um conjunto de recomendações e medidas priorizadas (NATIONAL STRATEGY USA, 2003):

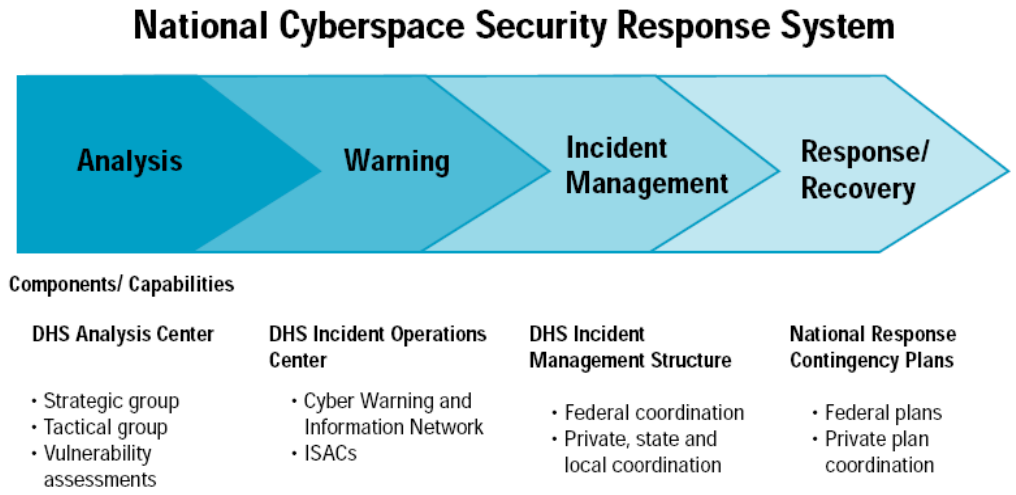
- 1ª: melhorar a resposta a ciber incidentes, reduzindo o dano potencial de tais eventos.
- 2ª, 3ª e 4ª: reduzir as ameaças de, e nossas vulnerabilidades a, ataques cibernéticos.
- 5ª: evitar ataques cibernéticos que possam afetar os ativos de segurança nacional e melhorar a gestão internacional de resposta a tais ataques.

Já em 2002, o presidente Bush criou o Departamento de Segurança Interna (Department of Homeland Security - DHS)[86], com responsabilidades importantes ao nível da segurança do ciberespaço. Enquanto centro de excelência pretendia tornar-se um ponto focal de divulgação para o Governo e entidades não-governamentais, incluindo o setor privado, universidade, e público. Ao DHS foi igualmente atribuída a responsabilidade do desenvolvimento nacional do sistema de resposta de segurança do ciberespaço - prestação de apoio na gestão de crises em resposta a ameaças. Neste domínio foram desde desenvolvidas parcerias vitais com empresas de antivírus para tomar medidas pró-ativas que impeçam possíveis ameaças de atingir parceiros públicos e privados, através do desenvolvimento e partilha padronizada de indicadores de ameaça, prevenção, mitigação, e produtos de informação de resposta.

[85] https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf. (em linha) [Consult. 26 Junho 2014].
[86] http://www.dhs.gov/ (em linha) [Consult. 26 Junho 2014].

Indica-se também a criação da equipa de resposta de emergência informática (U.S. Computer Emergency Readiness Team - US-CERT). Em 2011, o US-CERT respondeu a mais de 106.000 relatórios de incidentes, e lançou mais de 5.000 alertas de segurança cibernética e produtos de informação para parceiros do setor público e privado.[87].

O sistema de resposta à segurança nacional do ciberespaço para fazer face às ameaças que se afiguram pelo ciberespaço e internet pode ser esquematizado da seguinte forma:



Fonte: NATIONAL STRATEGY USA, 2003

O sistema é composto por quatro etapas, uma de análise de vulnerabilidades, uma segunda, que consiste em mecanismos de alerta, uma terceira de gestão de crise – e englobando os setores privados com a criação de parcerias público-privadas - e, por fim, a última consiste no plano de resposta.

Assim, resumidamente o Estado ao nível de segurança do ciberespaço tem diversos objetivos, entre os quais, a utilização da ciência forense na atribuição do ataque, a proteção de redes e de sistemas críticos para a segurança nacional, indicações e advertências, e a proteção contra ataques organizados capazes de infligir danos debilitantes para a economia. As atividades estatais devem também apoiar a investigação e o desenvolvimento tecnológico que permita também ao setor privado proteger melhor as suas próprias infraestrutura (NATIONAL STRATEGY USA, 2003).

[87] http://www.dhs.gov/cybersecurity-results (em linha) [Consult. 30 Junho 2014].

A verdade é que a par do que acontece com a estratégia da EU, também a estratégia americana é parca nas suas menções à espionagem e de que forma esta deve ser contida. No entanto, ainda assim, diz:"os *EUA devem ter a capacidade de proteger e defender os sistemas e infraestruturas que são considerados ativos da segurança nacional, e desenvolver a capacidade de identificar rapidamente a origem da atividade maliciosa è imprescindível melhorar a atitude de segurança nacional no ciberespaço para limitar a capacidade dos adversários realizar espionagem ou pressionar o país*". (NATIONAL STRATEGY USA, 2003).

Considera-se que a sua preocupação relativamente à ciberespionagem pode incluir uma componente psicológica, uma vez que se considera uma primazia a nível mundial não quer, de forma alguma, deixar que outros países o ultrapassem.

6.3. AUSTRÁLIA

Na Austrália, a cibersegurança tem sido considerada pelo Governo como uma prioridade da segurança nacional. David Irvine, em 2012 o Diretor-Geral da Organização de Inteligência de Segurança australiano (ASIO), falou sobre o mundo cibernético como tendo "um impacto significativo sobre qustões de segurança nacional da Austrália", e comentou que "a *ciberespionagem* surgiu como uma séria preocupação generalizada e que vai continuar a ganhar destaque devido à digitalização em curso de dados e o aumento de dependência da tecnologia no negócio comercial, governamental e militar"[88].

Para o Governo Australiano a cibersegurança é definida como um conjunto de medidas relativas à confidencialidade, disponibilidade e integridade da informação que é processada, armazenada e comunicada por meios eletrónicos ou similares. E o seu grande objetivo consiste na promoção de um ambiente em que o ciberespaço é seguro, resistente e confiável suportando a segurança nacional da Austrália e maximizando os benefícios da economia digital[89].

[88] http://www.cmaxcommunications.com.au/public-policy-briefs/cyber-security-in-australia-and-the-usa-the-state-of-play. (em linha) [Consult. 1 Julho 2014].
[89] http://www.ag.gov.au/RightsAndProtections/CyberSecurity/Pages/default.aspx (em linha) [Consult. 1 Julho 2014].

A Cibersegurança foi um ponto principal da Estratégia de Segurança Nacional[90] do ex-primeiro-ministro Julia Gillard, lançado em Janeiro de 2013. A cibersegurança constitui uma parte relevante da estratégia, com o ex-governo trabalhista a supervisionar a criação do Gabinete de Coordenação de Políticas e o Centro de Cibersegurança Australiano (ACSC) (id. [79]).

Na Austrália, a responsabilidade é repartida pelo governo não sendo exclusiva de qualquer agência ou ministério, tendo em conta que os serviços de segurança nacionais são atualmente distribuídos por várias agências, incluindo o Australian Security Intelligence Organisation (ASIO), o Australian Customs and Border Protection Service a Polícia Federal Australiana (AFP), Serviço Secreto de Inteligência australiano, a Direção de Sinais (ASD), o Departamento de Defesa (DSD), o Departamento de Assuntos Estrangeiros e do Comércio e do Escritório de Avaliações nacionais.

Atualmente, os Governos dos EUA e da Austrália por enfrentarem a necessidade crítica de desenvolver uma maior capacidade de proteger a infraestrutura crítica nacional e melhorar as capacidades de resposta a incidentes cibernéticos, decidirem estabelecer diversas parcerias. Na Austrália, o DSD (Defence Signals Directorate) relatou um acréscimo de 39 por cento no número médio de graves ataques *online* contra o governo em 2013 em comparação a 2012. Isso traduz-se em 2,4 graves ataques *online* por dia. Sendo uma preocupação constante o possível ataque a infraestruturas críticas.

Reconhecendo o Governo que tem fragilidades nesta área, está a tentar cada vez mais envolver o sector privado em novas medidas de apoio à cibersegurança. A ASIO, entidade que é responsável por antecipar e avaliar as ameaças à segurança nacional e à DSD, que se ocupa da espionagem eletrónica estrangeira, acordaram no ano passado convidar empresas privadas para combater os ataques cibernéticos mais sofisticados dentro da nova multi-agência ACSC.

A principal missão da ACSC será na proteção em termos de cibersegurança das infraestruturas críticas, como grandes instituições bancárias, redes de telecomunicações, aeroportos públicos, estradas e serviços públicos, muito do que é agora propriedade e

[90] http://www.gns.gov.pt/media/3481/Australia.pdf (em linha) [Consult. 3 Julho 2014].

controlado por interesses privados. A intenção é que se crie uma partilha de conhecimentos entre o público e o privado e que os técnicos especialistas do privado possam aprender com especialistas em cibersegurança do governo, nomeadamente com os órgãos de polícia criminal, serviços de informações e especialistas em defesa, tais como ASIO, DSD, e a AFP.

O Instituto Australiano de Política Estratégica (ASPI) referiu recentemente que existe uma maior necessidade de assimilar que o risco tem de ser verdadeiramente entendido por todos os setores e as respostas adequadas têm de ser postas em prática, apontando para a necessidade de uma maior conscientização, partilha de informação e a elaboração de políticas que sejam capazes de melhorar as relações com o setor privado e a conscientização da comunidade (*id.* [79]).

No âmbito da economia australiana o risco de intrusão no computador e a disseminação de código malicioso pelo crime organizado tem sido avaliada como elevado. Um aumento na da sofisticação e perpetração de cibercriminalidade fez com que este fenómeno seja cada vez mais difícil de identificar e derrotar (*id.* [80]).

O governo australiano está a trabalhar com o setor da indústria para desenvolver aptidões e sistemas que consigam lidar com a falta de preparação das empresas australianas para resistir a ataques cibernéticos cada vez mais sofisticados. A principal agência de segurança cibernética do governo australiano são as CERT Austrália - a equipa nacional Computer Emergency Response. A CERT foi incorporada no Departamento Federal do Procurador-Geral, e tem a responsabilidade de monitorar e avaliar as ameaças cibernéticas e medidas de segurança para grandes empresas australianas. CERT tem parcerias com cerca de 500 empresas na Austrália, proporcionando-lhes o conselho de segurança cibernética e proteção.

O crescente aumento de atores, estatais e não estatais, com pretensões de roubar, alterar ou destruir informações, podendo causar interrupções críticas aos sistemas australianos, leva a que a distinção entre atores de ameaças tradicionais - *hackers*, terroristas, redes criminosas organizadas, espiões industriais e os serviços de inteligência estrangeiros – seja cada vez mais cinzenta.

Face a este cenário o governo australiano para garantir a cibersegurança estabeleceu sete prioridades estratégicas:

- Promover a deteção, análise, mitigação e resposta a ameaças virtuais sofisticadas, com foco no governo, nas infraestruturas críticas e em outros sistemas de interesse nacional;
- educar e capacitar todos os australianos com informação, a confiança e as ferramentas práticas para se protegerem online;
- estabelecer parceiras com empresas para promover a segurança e a resiliência em infraestruturas, redes, produtos e serviços;
- adotar as melhores práticas na proteção de informações do governo e sistemas de tecnologias de comunicação, incluindo os sistemas de transações governamentais on-line;
- promover um ambiente eletrónico global seguro, flexível, confiável e operacional;
- manter uma capacidade de enquadramento e aplicação efetiva para atacar e perseguir a cibercriminalidade;
- promover o desenvolvimento de capital humano qualificado na área da cibersegurança com acesso a pesquisas e desenvolvimento (id [79] [80]).

6.4. OCDE, ONU E OUTROS PAÍSES

A nova geração de estratégias nacionais de segurança cibernética visa impulsionar a prosperidade económica e social e proteger as sociedades contra ameaças cibernéticas do ciberespaço. Um dos principais desafios da política de segurança cibernética consiste em procurar esses dois objetivos ao mesmo tempo, preservando a abertura da Internet como uma plataforma para a inovação e novas fontes de crescimento. Esta tem sido uma área tradicional de interesse para a **OCDE**, as Diretrizes de 1992[91] para a segurança dos sistemas de informação são exemplo disso.

Efetivamente o interesse da OCDE na segurança no ciberespaço está relacionado com o fato de considerar este é um verdadeiro motor para a prosperidade económica e desenvolvimento social. E a definição destas linhas de orientação têm por objetivo consciencializar todos os Governos e entidades de negócio para a necessidade de uma

[91] As Diretrizes de 1992 para a Segurança de Sistemas de Informação foram revistas em 2002.

cultura de segurança de sistemas de informação e redes, devendo esta ser como uma maneira de pensar, avaliar e agir.[92]

Para a Organização das Nações Unidas (ONU) a matéria da cibersegurança[93] também constitui uma preocupação. No ano de 2013 um grupo de peritos governamentais de segurança cibernética da ONU realizou um relatório que procurou a manutenção da paz internacional e da estabilidade na área das ameaças cibernéticas. Este documento permitiu reconhecer a aplicabilidade do direito internacional ao nível do ciberespaço, estabelecendo as medidas de transparência e de reforço de confiança tradicionais, recomendando a cooperação internacional e o reforço da capacidade de tornar a infraestrutura das TIC mais segura em todo o mundo. Para a ONU, já era tempo de agir para enfrentar este novo desafio da segurança internacional. Cada vez mais, as ferramentas cibernéticas juntamente com uma incerteza generalizada sobre as regras que governam o comportamento dos Estados no ciberespaço, aumentaram o risco de ciberconflito entre aqueles. É portanto de crucial importância que se encontre um terreno comum para enfrentar esses desafios, afirmando-se e clarificando a aplicação do direito internacional ao comportamento dos Estados no ciberespaço e recomendando medidas de confiança.

Já falamos no que algumas organizações internacionais têm realizado em matéria de cibersegurança, mas ainda nos parece importante falar sobre o que outros países têm realizado neste domínio, e em especial no que concerne à ciberespionagem.

O **Reino Unido** reconhece que está cada vez mais dependente do espaço cibernético e com isso surgiram novas ameaças e consequentemente vulnerabilidades que necessitam de ser reconhecidas e debeladas. Para enfrentar os desafios de segurança cibernética o Governo do Reino Unido delineou em 2009 a sua Estratégia de Cibersegurança[94], mais tarde revista no ano de 2011[95]. Com ela pretendeu aumentar o financiamento de objetivos estratégicos de segurança cibernética, tais como, sistemas seguros e resilientes, 'exploitation', políticas, doutrina e questões legais, Capacidades Técnicas e Pesquisa & Desenvolvimento; trabalhar em estreita colaboração com o sector público em geral, a indústria, o público e com os

[92] http://www.oecd.org/sti/ieconomy/15582260.pdf (em linha) [Consult. 8 Junho 2013]
[93] http://www.un.org/disarmament/topics/informationsecurity/ (em linha) [Consult. 8 Junho 2013]
[94] http://www.gns.gov.pt/media/3499/Reino%20Unido.pdf (em linha) [Consult. 8 Junho 2013]
[95] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf (em linha) [Consult. 8 Junho 2013]

parceiros internacionais; criar um Gabinete de Cibersegurança (OCS) para fornecer liderança e coerência estratégica para e entre o Governo; e, por fim, criar um Centro de Operações de Cibersegurança (CSOC). A questão da espionagem é abordada de forma muito passageira e generalista, ainda que incluída num conjunto de ameaças que podem afetar organizações, indivíduos, infraestruturas críticas, e o Governo, não é apresentada qualquer medida específica para combater e minimizar a ocorrência destas atividades.

A fim de garantir a segurança dos cidadãos, empresas e país no ciberespaço a **França** definiu uma estratégia de Defesa e Segurança dos Sistemas de Informação[96] que assenta em quatro objetivos estratégicos: ser uma potência mundial de ciberdefesa no contexto situacional da ciberdefesa; salvaguardar a capacidade da França para tomar decisões por meio da proteção de informações relacionadas com a sua soberania; fortalecer a segurança cibernética de infraestruturas nacionais críticas, e garantir a segurança no ciberespaço. Para alcançar esses objetivos identificou sete áreas de ação: antecipar e analisar; deteção, alerta e resposta; melhorar e perpetuar as capacidades científicas, técnicos, industriais e humanas; proteger os sistemas de informação do Estado e os operadores críticos das infraestruturas; adaptar a legislação francesa; desenvolver nossas colaborações internacionais; e, comunicar para informar e convencer. Dos objetivos definidos pela França constata-se que não há realce para a ciberespionagem, sendo que o grande objetivo deste país é ser uma potência em ciberdefesa.

A **Rússia** estabelece em 2000 a Doutrina de Segurança da Informação[97] onde se encontram definidos os princípios e as diretrizes básicas para garantir a segurança da informação naquele território. A espionagem, tal como tem constatado da análise às estratégicas delineadas por outros países, também aqui é apenas mencionado de forma muito breve. A referência acontece porque para a Rússia a possibilidade de espionagem industrial constitui uma ameaça externa à segurança da informação no campo da ciência e da tecnologia.

Para a **Estónia** a utilização do ciberespaço por organizações terroristas, criminosas e atores patrocinados pelo Estado representam uma séria ameaça à segurança do país e do mundo. Na estratégia de Cibersegurança[98] da Estónia as ameaças no ciberespaço foram

[96] http://www.gns.gov.pt/media/3490/França.pdf (em linha) [Consult. 3 Julho 2014].
[97] http://www.gns.gov.pt/media/3505/Russia.htm (em linha) [Consult. 3 Julho 2014].
[98] http://www.gns.gov.pt/media/3517/Estonia.pdf (em linha) [Consult. 3 Julho 2014].

identificadas com base em fatores motivacionais: o cibercrime, o ciberterrorismo e ciberguerra. Para a Estónia, embora diga que as ameaças são difíceis de definir, pois é não é fácil identificar a origem dos ataques e os motivos que os originaram, ou até mesmo prever o curso de um ataque, a verdade é que a espionagem cibernética não foi contemplada de forma clara.

Esta análise revela que as políticas de segurança cibernética tornaram-se para os países uma prioridade da política nacional apoiada por uma liderança mais forte e consciente. A única definição de cibersegurança não pode ser derivada a partir dessas estratégias. No entanto, todas as novas estratégias estão se tornando integradas e abrangentes. Elas aproximam-se da segurança cibernética de uma forma holística, abrangendo aspetos de âmbito económico, social, educacional, jurídico, policial, técnico, diplomático, militar e relacionadas à inteligência. As “questões de soberania" tornaram-se cada vez mais importantes. (OCDE, 2012).

Das várias estratégias percebemos que os países preocuparam-se em criar medidas e procedimentos que permitam não só assegurar o valor da informação mas também a segurança do ciberespaço, em função das ameaças que provêm deste mesmo espaço virtual. Mas parece que, e ao que tudo leva a crer parece ser comum a quase todas as estratégias, senão mesmo a todas, a espionagem cibernética não é uma verdadeira preocupação. Ou seja, no conteúdo das estratégias não existe uma abordagem clara e específica. No entanto, não queremos dizer que ela não é falada, isso efetivamente não acontece, o que verdadeiramente se constata é que ela é identificada como uma ameaça a empresas e Estados. E que qualquer ação ou medida de proteção que se adopte ou implemente que tenha por objetivo identificar ameaças e dirimir vulnerabilidades influencia ou cria barreiras, mesmo que indiretamente, à pratica da espionagem, mas não a resolve.

Contudo Portugal deve analisar o que está feito e tem muito a aprender com as experiências dos outros países não só naquilo que tem resultado de forma eficaz, mas também com aquilo que sido melhorado, sem nunca esquecer que esta é uma realidade em constante mutação e evolução.

CAPÍTULO 7.
DOS DESAFIOS DAS SOLUÇÕES À COOPERAÇÃO INTERNACIONAL

Face às emergentes ciberameaças, onde se inclui a nefasta ciberespionagem, os Estados devem criar estratégias que visem a sua proteção, a fim de evitarem o delapidar das suas instituições através do roubo de informações vitais. Essas estratégias deverão ser vistas como novos desafios que se avizinham num horizonte bem mais próximo do que poderiamos imaginar e impossível de prever há alguns anos atrás.

A constante poossibilidade de atos de ciberespionagem aos Estados mas também empresas significa sem qualquer tipo de dúvida que as estruturas atacadas encontram-se francamente fragilizadas e sem linhas de defesa eficientes, pois se assim não fosse, não nos debateríamos neste hiato com este tipo de questão.

Os desafios de soluções são variados. Desde medidas básicas para se proteger contra ciberspionagem, passando pela dotação de estruturas adequadas, criação de políticas de segurança de informação, cooperação internacional, harmonização de medidas e resolução cooperativa até de que maneira é possível influenciar a diplomacia internacional sobre as questões de cibersegurança. É isso que se irá desenvolver nas linhas seguintes.

7.1. COMO PROTEGER UMA EMPRESA OU NAÇÃO CONTRA A CIBERESPIONAGEM

Depois de apresentar as ameaças e as vulnerabilidades que os Estados e empresas enfrentam, e o que tem sido feito ou que se pretende fazer a nível nacional e internacional parece-nos bastante pertinente abordar o pode ser possível fazer em sua defesa.

A espionagem está à espreita e espera a sua oportunidade para ‘atacar’. No mundo empresarial esta é uma questão de preocupação e interesse na resolução, no entanto provavelmente não tem sido o suficiente. Dado o seu crescente impacto negativo tem havido uma procura de respostas que permitam melhorar a atuação das empresas face a este fenómeno. Até agora esta parece ser uma batalha desigual que opõe sistemas rígidos e demasiado vulneráveis à flexibilidade e conhecimentos dos que dominam a arte de espionar por meios informáticos.

Pese embora aquelas organizações que já têm um conhecimento profundo das ameaças que habitam à sua volta, muitas são aquelas que desconhecem que os criminosos os podem invadir ou já os invadiram. Isto acontece porque muitas destas organizações ainda possuem uma abordagem reativa altamente explorável e pouco eficiente a identificar incidentes relacionados com a segurança dos sistemas de informação e comunicações. A questão coloca-se precisamente aqui, é que uma cultura de segurança que paute apenas pela reação cria enormes oportunidades aos agentes criminosos que facilmente conseguem tira proveito das vulnerabilidades conhecidas e daquelas que ainda estão por realizar. Configurações erradas na infraestrutura tecnológica instalada, por falhas no software ou ainda o erro humano, são alguns dos exemplos das vulnerabilidades dos sistemas.

Os agentes intrusos estão cada vez mais qualificados e sofisticados o que faz com que sejam mais bem-sucedidos ao derrotar a tecnologia que supostamente devia proteger uma organização.

Neste sentido é necessário que a mentalidade organizacional mude e isso começa pela necessidade de sensibilizar a gestão de topo e fazê-la perceber o que está em causa e o que é necessário fazer para mudar.

Uma empresa que se quer manter no mercado e melhorar a sua posição dia após dia não pode deixar à mercê de outros os ativos valiosos da empresa. A chave para proteger essa informação pode passar por realizar avaliações de risco (auditorias) que levem em conta as potenciais situações negativas que são capazes de ocorrer.

As estratégias de segurança e defesa requerem hoje em dia rever todo o sistema e todas as interdependências.

A atualização de um software antivírus, sendo um importante ponto de partida, não é a solução para o problema. Este software apenas está equipado para lidar com os processos tecnológicos não com o elemento humano que está por detrás de um ataque de espionagem.

É necessário caminhar para um futuro em que a organização tenha ferramentas e mecanismos para atenuar o risco a um nível aceitável ao ser capaz de demonstrar o valor definido para o negócio. A capacidade de inteligência cibernética pode posicionar um negócio para tomar decisões mais eficazes na prossecução de iniciativas estratégicas, bem como reforçar o nível de segurança para os produtos e serviços atuarem (DELOITTE, 2011).

O cientista George Westerman, na MIT Sloan School of Management's Center for Digital Business, pertencente ao Instituto Tecnológico de Massachusetts - uma das mais famosas faculdades do mundo especializada em negócios – é igualmente da opinião que proteger a informação de uma empresa é um problema que aflige muitas empresas, desde as mais pequenas às grandes multinacionais, e que cada vez mais urge ser resolvido. No entanto, alerta para o fato de as empresas de pequenas dimensões tenderem a ignorar o problema por considerarem que estão de fora do alcance de quem procura corromper os sistemas para a recolha de informação privilegiada. Isto vê-se muito em, em especial, no que respeita à segurança na internet, em que não é dada a devida importância e atenção, por acharem que são demasiado pequenas para ser alvo de ameaça cibernética.

Um estudo recente da U.S. House Small Business Subcommittee on Health and Technology vem pronunciar-se sobre isso mesmo, dizendo que cerca de 20% dos ataques cibernéticos atingem pequenas empresas com menos de 250 funcionários. E que destas, 60% fecham as portas seis meses após o acontecimento.

Para este cientista a verdade é que '*quando se está num negócio, é-se naturalmente um alvo. E quando se está ligado à internet então está-se sob ataque'*. Diz ainda que os dias de hoje viram o problema agudizar-se, com as empresas agora a enfrentar aquilo que é conhecido como uma ameaça persistente avançada (APT), uma categoria de ciberataques que envolve uma espionagem através da Internet dirigido a alvos políticos e empresariais.

Por isso mesmo ele considera que a segurança na internet deve ser um ponto basilar da política de segurança de qualquer empresa ou nação, até porque não se trata só de um problema de caracter tecnológico, mas também de um problema de pessoas. Para dar ênfase a este problema o autor alude para o que é dito pela CyberFactors[99], que 40% das intrusões/violações relatadas são preconizadas por funcionários internos. Sem os passos apropriados de proteção qualquer funcionário pode recolher informações sensíveis sem sair do seu posto de trabalho.

Mas então o que pode fazer um governo ou uma gestão de topo para proteger melhor a sua estrutura. Este autor apresenta três diretrizes a seguir. A *primeira* consiste em treinar os seus funcionários para o risco associado à utilização das Tecnologias de Informação (TI). Não há necessidade de ter conhecimento sobre cada ameaça ou cada detalhe técnico, mas é preciso saber o básico. Deve-lhes ser explicado como é que os computadores estão desprotegidos e como é que são feitos os ataques maciços sobre esses pontos fracos. É importante explicar-lhes como proteger os dados dos seus computadores, tablets, smartphones e outros dispositivos, mesmo quando estão a viajar e têm de aceder a informações confidenciais da empresa a partir de uma rede estrangeira. Educá-los sobre os perigos de colocar informações pessoais na Internet, que pode ser usado para adquirir as senhas ou executar golpes. Em *segundo* lugar o autor refere que é importante a empresa criar políticas claras e simples no que toca à tecnologia. Os funcionários devem entender quando e como estão autorizados a utilizar dispositivos pessoais nas redes da empresa. Que o acesso ou alteração à rede fica automaticamente registrado. É importante o uso de senhas classificadas como fortes e mudadas com regularidade. Criar um protocolo de como lidar com um dispositivo perdido ou roubado. Ocasionalmente auditar computadores e rede de logins por atividade suspeita. Verificar as secretárias das pessoas à procura de papéis onde estejam inscritas senhas e outras informações confidenciais. Estabelecer consequências e responsabilizar as pessoas por não seguirem as políticas definidas. Por fim, em *terceiro* lugar, deve haver um responsável pela segurança. Para exemplificar a importância deste item, está a atuação de grandes empresas, estas possuem' exércitos' de especialistas em segurança que trabalham em tempo integral sobre estas questões e protegem as informações da sua empresa. Obviamente, isso é mais difícil de alcançar quando se trata de

[99] CyberFactors é uma plataforma inteligente de negócios em tempo real projetada exclusivamente para medir o risco de dependência de TI pela captura de informações sobre eventos adversos relacionados a tecnologia e suas consequências, http://cyberfactors.com/cyberfactors/ (em linha) [Consult.12 Junho 2014].

uma pequena empresa, sem grandes recursos. Mas até mesmo as pequenas empresas devem ter alguém a quem seja atribuída a responsabilidade pela segurança[100].

Para a Kaspersky o combate a estas ameaças cibernéticas tem uma vertente mais técnica, o que terá alguma lógica até porque estamos a falar de empresas ligadas à criação de soluções capazes de assegurar a fiabilidade dos sistemas informáticos e de informação. Fez previamente o levantamento dos métodos de propagação de malware (software malicioso) usados para espiar.

Identificaram três métodos, o primeiro consiste na exploração de vulnerabilidades nos sistemas operacionais ou aplicações, que inclui produtos de software mais vulgarmente utilizados, tais como: Java, Adobe, Reader, Microsoft Office, Internet Explorer, Adobe Flash, entre outros. Um outro método consiste em aplicar as técnicas de engenharia social, incluindo campanhas de 'spear-phishing'[101]. O terceiro método indicado consiste no 'Drive-by downloads'[102], em que o computador do utilizador fica infetado quando visita um website que está comprometido em termos de segurança (KASPERSKY, 2013).

O caminho de tecnicidade é eficaz no combate a atos de ciberespionagem. Aliás, como é compreensível os alertas das empresas privadas de cibersegurança vão nesse sentido A Kaspersky indica alguns passos que as empresas deveriam seguir na defesa das suas empresas. E porque não as agências governamentais em defesa dos seus sistemas seguirem igualmentye estes passos? Assim, numa primeira fase é importante uma empresa avaliar os riscos que se colocam ao seu negócio e em seguida erigir a sua própria política de segurança que se coadune com as emergentes ameaças. A sua política deveria então:

- Definir os procedimentos de segurança para o dia-a-dia;
- Estabelecer um plano de "resposta a ataque;
- Incluir um mecanismo para atualização de procedimentos - para que eles acompanhem a natureza evolutiva das ameaças;
- Estabelecer uma rotina para a realização regular de auditorias de segurança às TI.

[100] http://www.forbes.com/sites/forbesleadershipforum/2013/05/13/your-business-is-never-too-small-for-a-cyber-attack-heres-how-to-protect-yourself/ (em linha) [Consult. a 20 Junho 2014].
[101] http://pt.norton.com/spear-phishing-scam-not-sport/article (em linha) [Consult. 15 Junho 2014].
[102] http://www.microsoft.com/security/sir/glossary/drive-by-download-sites.aspx (em linha) [Consult. 15 Junho 2014].

Em seguida apontou também como requisito fundamental educar os funcionários sobre os riscos. Muitos ataques de ciberespionagem dependem de erro humano ou da sua ingenuidade para criar as condições que permitem aos cibercriminosos aceder sistemas e dados das empresas. Quando se trata de defender contra ataques então é essencial aumentar a consciência sobre determinados aspetos:

- Os riscos de segurança e como os cibercriminosos podem tentar roubar informações e senhas;
- Os custos potenciais para o negócio caso haja um ataque;
- Os simples cuidados que os funcionários podem adotar para melhorar a segurança;
- A política de segurança da sua empresa e como os funcionários podem ajudar.

Uma outra questão a considerar será a estratégia do seu sistema operacional. É preciso ter em mente que os sistemas operacionais recentes - como o Windows 7, Windows 8 ou Mac OS X - tendem a ser mais seguros do que os seus homólogos mais antigos. Da mesma forma, as versões da maioria dos sistemas operacionais de computadores de 64 bits tendem a ser mais resistentes contra ataques cibernéticos.

Deve-se igualmente estabelecer uma solução global de segurança das TI. A existência de uma proteção anti-malware é extremamente importante, mas por si só não é considerada suficiente. A escolha deve passar por uma solução de segurança que incluía outras tecnologias, tais como, avaliação de vulnerabilidades; gestão de falhas, controlo de dispositivos e da internet, encriptação de dados; encriptação de dados; entre outras.

Ao nível da segurança cibernética também é importante prestar especial atenção à segurança móvel. Hoje em dia é necessário perceber que aparelhos como os ‘smartphones’ são muito mais do que apenas telefones, eles são computadores poderosos que podem armazenar uma grande quantidade de informação corporativas – por exemplo senhas de acesso – de grande valor para os espiões cibernéticos. Por isso, é importante proteger os dispositivos móveis - incluindo tablets e smartphones - rigorosamente como se protege os sistemas de TI. Com o aumento do risco de roubo ou perda, é possível argumentar que os níveis de proteção dos dispositivos móveis devem ser realmente elevados, em especial os que são trazidos pelos funcionários.

A proteção dos ambientes virtuais deve também ser uma medida a tomar em consideração em termos de matéria securitária. O uso de máquinas virtuais a operar em servidores físicos, faz com que estes estejam vulneráveis a ataques maliciosos.

Por fim, é aconselhado uma combinação entre a segurança e a gestão de sistemas, que permite alcançar uma maior visibilidade e uma menor complexidade. Se for possível ver tudo o que passa na rede, então será mais fácil aplicar as medidas de segurança mais apropriadas (KASPERSKY, 2013).

Tudo isto faz sentido porque, enquanto os cibercriminosos usam métodos cada vez mais sofisticados, os negócios acolhem uma solução de segurança capaz de debelar as ameaças que são constantes.

Também o centro de excelência europeu para os Estados-Membros europeus e as instituições europeias em segurança de redes e de informação, a ENISA se tem preocupado com esta temática. No ano de 2009 elaborou um manual de boas práticas que aborda questões cruciais e importantes de consciencialização das tecnologias da informação e comunicação (TIC) para as organizações.

A ENISA tem por pretensão influenciar positivamente no comportamento dos funcionários em relação à segurança da informação, mudar a mentalidade do elemento humano, a fim de alcançar uma maior auto-consciência na segurança da informação.

É importante que as organizações públicas e privadas compreendam que as políticas e a tecnologia devem ser postas em prática de forma a proteger informações sensíveis. Proteger começa com a certeza de que os seus funcionários entendem os seus papéis e responsabilidades na salvaguarda de dados sensíveis, protegem os recursos da empresa e ajudam a organização a manter computadores e rede seguras.
Foram identificadas 10 boas práticas que se elencam a seguir (ENISA, 2009):

1) Usar password;
2) Proteger o seu computador;
3) Use o e-mail e a Internet com cuidado;
4) O uso cuidado de dispositivos portáteis corporativos: laptops, drives USB, telefones celulares e BlackBerrys;

5) Manipular informações com cuidado;
6) Todos os visitantes devem ser registrados e a entrada e saída devem ser assinaladas;
7) Reportar a perda e/ou danos nos dispositivos portáteis da empresa e incidentes;
8) Proteger as informações fora da organização;
9) Cumprir com as políticas e procedimentos de segurança da empresa;
10) Fornecer feedback para possíveis novas soluções afinar e políticas de segurança. [

Uma estratégia de proteção deve envolver diversas vertentes, e a implementação de apenas uma delas não vai resolver o problema, pelo contrário irá apenas adiar uma questão que à partida pode ser um problema.

7.2. ESTRUTURAS E MEIOS TECNOLÓGICOS

Em primeira mão, o Estado deveria ter uma consciência situacional e dotar as suas estruturas e por arrasto capacitar todas as empresas públicas, de meios tecnológicos assim como de procedimentos e medidas técnicas que permitam uma defesa segura e capaz e, que minimizasse a maior parte dos ataques de ciberespionagem até ao momento conhecidos.

A nível estrutural importa referir a necessidade de os Estados terem um Centro Nacional de Cibereguranca. E na dependência deste criar uma entidade que tenha capacidade para reagir a ataques cibernéticos, o CERT, e ainda um Orgão de Gestão de Crises. A nível estratégico e com características políticas deverá existir um Conselho Nacional de Cibersegurança.

De referir que, este tipo de melhoramento a nível tecnológico na defesa de ciberataques originará um maior desgaste económico a nível da despesa do Estado, exigindo a atribuição de um orçamento maior para o ministério superintendente nestas matérias. Tal pode ser visto como um investimento porque os resultados futuros são melhores e os custos de ineficiência menores.

Este tipo de dispêndio financeiro não poderá mais tarde vir a pôr em causa a manutenção destes mecanismos de defesa, pois, por hipótese, a determinada altura um Estado poderá ou

terá de optar entre uma maior segurança cibernética ou a atribuição de verbas para outras áreas fundamentais da sociedade, por exemplo, como a Saúde ou a Justiça?

Porém um Estado só se sentirá seguro e capaz de debelar quaisquer tentativas de intrusão, protegendo aquilo que considera como seu e de interesse nacional.

Deveriam então haver a preocupação de instalar em todos os servidores estatais programas antipirataria de eficácia comprovada para proteger as informações consideradas fulcrais para o bom funcionamento dos serviços, quer em termos de operacionalidade funcional, quer de segurança. Mas para isso é fundamental a implementação de procedimentos e medidas técnicas comprovadas que impeçam o acesso não autorizado ou a subtração de informações.

Neste campo, existe o Ipv6 , o novo protocolo da internet. Este protocolo aparece com regras mais seguras. O IPv6 ou Protocolo de Internet Versão 6 é a próxima geração de protocolo para a Internet. [103]

Seria também importante rever e de seguida alterar, alguns procedimentos de segurança utilizados por todos os organismos, limitando o número de utilizadores com acesso a informação privilegiada, bem como, a criação de passwords ou códigos específicos de acesso para quem possa por inerência do serviço necessitar de aceder a dados de natureza mais reservada.

7.3. POLÍTICAS DE SEGURANÇA DE INFORMAÇÃO

A nível empresarial deveria haver uma maior preocupação na definição de métodos, políticas e procedimentos organizacionais que assegurem os ativos críticos das organizações, em especial da informação, garantindo a precisão e a fiabilidade dos seus registos informáticos.

[103] http://ipv6.com/articles/general/ipv6-the-next-generation-internet.htm (em linha) [Consult. 7 Julho 2014]

Nesta área as empresas devem repensar as suas abordagens de segurança, ter políticas de segurança de informação. Em primeiro lugar, começar por perceber o ciclo de vida de uma ameaça emergente e como o sistema de fluxo de trabalho pode ser projetado e automatizado para ajuda a mitigar o nível de risco de uma organização. Em segundo, identificar os dispositivos e sistemas de suporte críticos dos processos de negócio. Qualquer dispositivo que tenha um computador ligado ao protocolo internet deve ser identificado e inspecionado, pois qualquer um destes dispositivos pode potencialmente oferecer aos criminosos múltiplos caminhos para aceder e extrair informação (DELOITTE, 2011).

Por muitas que sejam as medidas empregues pelas empresas, existe uma, muitas vezes esquecida ou não contemplada, que persiste, é o elemento humano. Os empregados de uma empresa podem ser a fronteira de defesa ou a maior ameaça, muitas vezes sem perceberem. Os empregados têm hoje em dia mais acesso a informação do que alguma vez antes tiveram. Copiar grandes quantidades de informações potencialmente confidenciais para dispositivos de mão, de armazenamento fácil é difícil de controlar. Sem os passos apropriados de proteção a cultura de negócio que suporte esses passos, qualquer funcionário, em potencial pode ‘furtar peças’ altamente sensíveis de informação, sem sair do seu posto de trabalho.

A cultura de segurança das empresas deve mudar e passar de ser apenas reativa para uma forma preventiva, até porque a ameaça cibernética continua a evoluir e disfarçar-se com técnicas engenhosas para burlar a maioria dos programas tradicionais de segurança da informação. As nações ao redor do mundo continuam a anunciar e a desenvolver capacidades de cariz cibernético. Mas esses devem ser mais do que meros controlos tradicionais de segurança que permitem que milhares de futuros agentes cibernéticos com habilidades únicas se instalem onde for necessário. Para mitigar os riscos dessas ameaças que avançam de uma forma eficaz, as organizações devem evoluir as suas capacidades atuais, e incluir, a proatividade, a monitorização contínua, reforçando simultaneamente a práticas de segurança existentes para alavancar a inteligência cibernética (DELOITTE, 2011).

Aparte destas medidas de cariz mais operacional, ao nível dos Estados podendo também adoptar algumas das medias acima indicadas, seria importante os Estados dotarem a sua estrutura orgânica de maior apoio, exigindo ou permitindo a colaboração de entidades

privadas. A intervenção destas entidades deveria ser realizada no âmbito das redes de comunicações no espaço cibernético, pois são as entidades privadas que na sua maioria disponibilizam/comercializam o acesso à rede para o comum dos cidadãos.

Para além disso, poderia ser fornecida parceria a determinadas empresas de segurança informática, para que com base nos seus conhecimentos, elaborassem um plano de defesa mais ativo, quer a nível da configuração de redes ou de servidores, mas também na criação de firewall's[104] com melhor desempenho.

Ainda assim, deveria igualmente existir uma cooperação operacional entre os diversos organismos de defesa dos Estado, entre os quais serviços de segurança interna e externa e a criação de organismos específicos no combate à ciberespionagem.

No caso Português, estaríamos a falar de serviços como a Polícia Judiciária, o SIS, no que se referem a estruturas de investigação e recolha de informação, ou o recém-criado Centro Nacional de Cibersegurança, sistema que vem de certa forma canalizar e encabeçar a luta contra a ciberespionagem numa dimensão de maior especificidade e relevo.

A nível nacional poderemos concluir que as estruturas oficiais de defesa e entidades privadas deverão atuar num tipo de sinergia, bem orientada sob uma mesma direção, para que todos os esforços possam ser canalizados para resolução do problema nas suas variadas vertentes.

7.4. A COOPERAÇÃO INTERNACIONAL

Apesar das medidas de âmbito nacional e à semelhança do que sucede em várias áreas da criminalidade mundial, seria sempre adequado, para não se dizer de extrema necessidade, a colaboração de outras nações que sejam ou venham a ser consideradas alvos preferenciais dos ciberespiões.

[104] É um dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede

Efetivamente é conveniente a adoção de medidas cooperativas no âmbito das relações internacionais.

Como primeira solução tendo em vista a proteção das estruturas dos Estado, apontaria a realização de reuniões entre os vários organismos de diferentes Estados, que superintendam a área da defesa no meio informático e ciberespaço, para que entre todos se pudesse relatar em primeira mão quais os tipos de incidentes que têm sido alvos, para que desta forma se pudesse ter acesso aos variados tipos de métodos que estão a ser adotados e utilizados.

Só através da partilha de experiências se poderá definir quais os métodos empregados pelos espiões para posteriormente serem delineadas estratégias de eficiência consolidada. A discussão entre os Estados, para além de mostrar quais os recentes ataques com que as várias instituições têm sido atingidas, poderia também ajudar a estabelecer um perfil de alvos escolhidos pelos espiões e definir quais os métodos mais utilizados pelos mesmos, ou seja, perceber se algumas instituições, empresas ou organismos possuem fragilidades "tipo" e se perante tais fraquezas existe um vírus ou malware utilizado pelos ciberatacantes de forma sistemática para o efeito.

Para além da partilha de experiências semelhantes entre os vários Estados, existindo entre eles o óbvio e comum interesse na defesa desse tipo de ataques, deveria ser criada uma task force com três objetivos:

- a criação de um projeto técnico com vista à produção de um manual de protocolo e procedimentos relativos à prevenção dos ciberacidentes e posteriormente da sua defesa posteriormente à sua deteção;
- a criação de ferramentas informáticas que visassem a proteção dos Estados numa fase ainda a montante, diminuindo assim a ocorrência de incidentes.
- a criação de legislação no âmbito da cooperação entre Estados, de aplicação nacional e internacional, que visasse legalizar operações das forças de segurança com vista ao auxílio entre países, por forma a agilizar a realização das diligências úteis e necessárias no que concerne à identificação dos autores e respetiva punição.

Tudo isto pretende que os Estados ou indivíduos intentados a realizar atividades de cariz espião se sintam demovidos de as praticar, seja por receio de serem apanhados quer por

uma questão de reputação ou imagem, neste último caso, em especial quando os envolvidos são Estados e/ou organizações de renome internacional. A grande questão aqui coloca-se que quem pratica a ciberespionagem tem bem a noção que esta é uma atividade ’protegida’, em virtude das características lhe estão subjacentes, como seja, o anonimato, o baixo investimento e a taxa de sucesso elevada. E que a deteção e identificação dos seus autores ainda é atualmente uma tarefa difícil. Os Estados e os organismos não-estatais sabem disso e aproveitam-se dessa fragilidade. Cada vez é mais percetível que porém exista ainda algum pudor ou ética a atratividade de determinada informação supera qualquer um destes valores.

Como é sabido para aceder à Internet, basta ter um computador e ou a um outro dispositivo eletrónico, ou ter acesso a estes meios e conhecer as senhas de acesso. A partir daqui, qualquer pessoa pode ter acesso a toda a informação hospedada noutros dispositivos, também eles ligados à internet. Ainda que a maioria que aí navega o faça sem má intenção, existe uma outra parte que utiliza o ciberespaço para uma prática mal-intencionada, destruição de informação, de dados e de sistemas de informação, fraude, entre outros efeitos prejudiciais.

A inexistência de legislação que de forma clara regule as atividades de ciberespionagem é sem dúvida um outro fator que prejudica as vítimas destas atividades mas beneficia e muito quem as pratica. Todavia os esforços desenvolvidos pelas instâncias internacionais e pelo Estados na procura de legislar algumas das atividades informáticas que se desenrolam através do ciberespaço e pela internet, tal não tem tido a abrangência que se seria necessária para a defesa dos Estados, empresas e cidadãos. A elevada dependência das atividades destes agentes relativamente aos sistemas de computadores e às telecomunicações não tem contribuído neste combate.

A nível internacional tem sido criada legislação para a cibercriminalidade, no entanto para a ciberespionagem não se verifica grandes progressos.

Apesar de existir a tendência para separar os conceitos de cibercriminalidade e ciberespionagem, e será que estes na sua génese não se tocam?. Não é nossa intenção desenvolver o conceito de cibercriminalidade, a verdade é que, a ‘intromissão indevida’, que é o que define a ciberespionagem, só por si consiste numa violação que de alguma

forma consubstancia os pressupostos de um cibercrime. Só o fato de alguém entrar num sistema ou computador sem qualquer autorização está por si só a cometer um crime, que por ser veiculado através de meios informáticos, denomina-se por cibercriminalidade[105].

No entanto, rapidamente estes dois conceitos se distanciam divergindo na motivação que levou à realização de tal ato. Esta é sem dúvida uma questão que deveria ser colocada e que devidamente debatida poderia encontrar junto das legislações nacionais e internacionais destinadas à cibercriminalidade, um caminho para a ciberespionagem.

Mas este passo, parece-nos um pouco distante, e precisaria de um esforço conjunto entre Estados e entidades, em que a cooperação internacional seria um instrumento de extrema importância, podendo fazer toda a diferença.

Uma maior e intensa participação em organizações internacionais é vital para reconhecimento dos problemas de cibersegurança em geral, e em especial no que concerne à espionagem, mas também para chamar a atenção do decisores de outros países. Muitos países ainda acreditam que a cibersegurança é apenas um problema de tecnologia que não requer nenhuma intervenção política. No entanto, a intervenção política é importante para que sejam iniciados esforços na definição de normas e regras necessárias para assegurar a cibersegurança e para facilitar a cooperação entre países.

É neste contexto que a Estónia tem feito 'doutrina', efetivamente na sua Estratégia de Estónia é perceptível que as reuniões internacionais são encaradas de forma muito completa e eficiente, ao definir e planear o que os seus representantes vão fazer[106].

Ao nível dos Estados, porque não através do Ministério do Negócios Estrangeiros (MNE), seria importante que os representantes nacionais, estivessem articulados entre si e fossem habilitados para tomar uma posição, aliar-se, e tomar decisões estratégicas, sempre chamados a estar presentes em reuniões em organismos internacionais de influência, como

[105] Em 2001, a Convenção sobre Cibercrime do Conselho da Europa definiu o cibercrime como sendo um vasto leque de atividades que se enquadram em quatro categorias genéricas de crimes relacionados com computadores: (1) violações de segurança; (2) fraude e falsificação; (3) pornografia infantil; e (4) violação de direitos de autor -Natário, Rui. 2013. O Combate ao Cibercrime: Anarquia e Ordem no Ciberespaço, Revista Militar nº 1254, http://www.revistamilitar.pt/art_texto_pdf.php?art_id=854 (em linha) [Consult. 2 Julho 2014].

[106] http://www.gns.gov.pt/media/3517/Estonia.pdf (em linha) [Consult. 3 Julho 2014].

seja, Nações Unidas, União Europeia, Organização do Tratado do Atlântico Norte - OTAN, Conselho da Europa, Organização para a Segurança e Cooperação na Europa- OSCE, OECD, entre outros

A cooperação internacional faz todo o sentido, não só por aquilo que já foi referido, mas porque uma parte dos ataques de ciberespionagem são realizados por países e entidades estrangeiras, o que nos leva ao velho problema de saber em quem confiar ou se devemos "abrir o jogo" aos parceiros de uma coligação deste cariz. A OTAN realiza neste domínio diversas reuniões, com os Estados membros, onde são abordados, entre outros, os assuntos ligados à segurança da internet e do ciberespaço, bem como as ações que por haver a desconfiança de poder ser de origem duvidosa fazem parte da ordem de trabalhos.

O simples facto de denunciarmos a outros países determinadas debilidades dos nossos organismos ou empresas, permite especular se não torna mais apetecível a intrusão de atacantes subsidiados por outros Estados para se apoderarem de informação confidencial. Em ultima análise, poderíamos temer que numa dessas reuniões se poderia mais perder do que lucrar.

Apesar do atrás exposto e atendendo a tais perigos, reiteramos que a cooperação internacional revela-se de alguma importância no combate contra ciberataques e possibilita maiores relações de confiança para inibir a ciberespionagem. Hoje ainda há alguma penumbra e talvez por isso, se possa equacionar os prós e os contras de tal cooperação. Se fossem os primeiros passos, poderia dizer-se porque não calcular o risco no caso de partilha de problemas com outros países, pelo que seria interessante criar uma plataforma de congéneres com os quais exista uma relação de confiança inquestionável (ou que pelo menos assim seja aceite). Talvez ajude se juntar países que foram alvo de ataques idênticos e ao mesmo tipo de estruturas e que ideologicamente sejam próximos uns dos outros. A OTAN ainda que nalguns detalhes seja demasiado pró-americano constitue-se num património de 60 anos de "confiança" mútua, que importa perseverar, pelo menos entre os seus estados-membros.

De acordo com as diversas variantes possíveis, o mais correto será pensar que com este tipo de iniciativas se teria mais a beneficiar em termos de proteção e entreajuda do que a perder no que concerne ao revelar as fragilidades de um Estado. Em alguns momentos,

talvez isso não corresponda à total verdade, porque os interesses nacionais poderão sobrepor-se à vontade de cooperação.

Provavelmente que países como os EUA, a Rússia, a China e o Irão, por mais benefícios que pudessem auferir de um tipo de união como a referida (aliás os EUA defende-a, certamente que não com estes países, por via da sua Estratégia para Cooperação Internacional para a Cibersegurança), dificilmente iriam partilhar a totalidade de informações ou aquela que é mais sensível ou pelo menos com a total honestidade e transparência, pois sabemos que esses países são vítimas de ataques de ciberespionagem pelos restantes.

Se porventura, fosse realizada uma aliança por estes países específicos, com vista à entreajuda nestas matérias, o mais certo seria o aproveitamento das reuniões como oportunidade de ações de contra informação, a fim de induzir os restantes membros num ardil. Mais uma vez estaríamos a assistir a estratégias de contra informação já utilizadas durante o decorrer da Guerra Fria, só que agora num outro campo de batalha.

Certamente que nenhum destes países, líderes na ciberespionagem, aceitaria sentar-se à mesa com um dos seus atacantes, mesmo existindo laços de cooperação diplomática entre alguns desses Estados, com a total disposição de pôr todas as cartas na mesa, até porque os interesses que estão inerentes são sobejamente superiores.

CAPÍTULO 8.
CONCLUSÕES

Pese embora todas as medidas e procedimentos que tem vindo a ser adoptados em especial com a estratégia nacional de cibersegurança, parece que continuamos com uma lacuna ao nível da prevenção e do combate à ciberespionagem.

Assim do que foi referido ao longo do trabalho importa em modo de conclusão apresentar algumas questões abordadas.

No contexto Português conclui-se que o Sistema de Informações da República Portuguesa (SIRP), é o organismo com responsabilidades na salvaguarda da segurança interna e dos interesses nacionais e a prevenção da espionagem, entre outras ameaças. Tem como principais preocupações as ciberameaças, com particular relevo para os atos de espionagem praticados com recurso a meios eletrónicos. Também com a elaboração do PSE o Governo procurou alertar as pessoas e dar conta da ameaças que as entidades públicas e privadas enfrentam ao nível desta ameaça. Assim, a 'intelligence' é importante e tem por objetivo aprofundar funções de deteção/dissuasão de ataques, que, no nosso entender, deve acontecer em articulação com o Centro Nacional de Cibersegurança, o qual deve agir em tempo útil e em colaboração com outras entidades, de forma a evitar ataques em larga escala e disruptivos[107]. Mas a atuação deste serviço poderá estar limitada. Mais nada é dito sobre esta ameaça.

Por isso parece-nos que o seu combate tem que se debruçar mais especificamente sobre a ameaça da espionagem, e para isso consideramos necessário repensar a política de segurança interna mas também a nacional. À imagem do que tem sido feito por organismos e empresas internacionais, o Centro Nacional de Cibersegurança pode ter um papel preponderante em termos de intervenção neste contexto. Então o que pode ser feito para evitar e combater eficazmente a ciberespionagem. Ao nível da espionagem consideramos

[107] http://www.sirp.pt/cms/view/id/90/ (em linha) [Consult. em 28 Maio 2014]

que a única coisa que mudou foi o espaço onde essas práticas operam e por isso tem-se seguido a filosofia convencional de abordagem ao problema, o que sendo bom nos parece ser globalmente insuficiente.

É percetível que as autoridades nacionais têm ganho consciência e que cada vez mais entendem que estas ameaças, das quais se inclui a ciberespionagem, devem ser percebidas por todos e adequar respostas susceptíveis de pôr em prática. Das respostas dadas pela EU e países como os EUA, a Austrália e o Reino Unido conclui-se que, de longe, que a partilha de conhecimento entre entidades públicas e privadas é umas das mais referidas. Em que umas entidades contribuem com os meios técnicos, outras com o conhecimento técnico e ainda outras com a capacidade de intervenção. A promoção da segurança e a resiliência das infraestruturas podem ser facilitadas com a realização de parcerias/consórcios. É neste sentido que Portugal tem de caminhar.

Mas os instrumentos e medidas a aplicar ou já aplicadas não devem ser estanques, pois os criminosos cibernéticos continuam a desenvolver e a melhorar as técnicas de atividade maliciosa. Portugal tem que ter essa consciência, e para acompanhar esta evolução, deve começar por identificar as ameaças e estudar novas oportunidades de formação e educação assim como as oportunidades de negócios em parceria com o governo (parcerias público-privadas) para desenvolver redes aperfeiçoadas e fornecer capacidade e serviços para a indústria pública e privada. Também no domínio económico conclui-se que uma maior colaboração, através da partilha de inteligência, informação e recursos pode ser possível desenvolver uma abordagem global para o desafio.

Concluiu-se que uma estratégia não se define só de políticas e instrumentos. Sabemos que até pode ser fácil definir um conjunto de linhas de orientação, o difícil é concretizá-lo e garantir no terreno a sua operabilidade. Conclui-se que para Portugal é importante um centro de resposta rápida, o CERT, a par do que tem sido desenvolvido pelas grandes nações ao nível da sua estrutura de cibersegurança, mas não se deve ficar só por aí. Deve igualmente ser criado um Conselho Nacional de cibersegurança, que permita dar orientações políticas e estratégicas, e ainda um Gabinete de Gestão de Crises.

Em termos operacionais sugere-se uma medida muito interessante, numa vertente muito mais proactiva do que reativa, já adoptada pelo RU, as denominadas ‘Red Teams’ ou

Equipas vermelhas. Por exemplo, empresas comerciais, tais como IBM e alguma agências governamentais, há muito que usam as equipas vermelhas para reduzir os riscos e melhorar a sua resolução de problemas. A equipa vermelha consiste numa equipa que é formada com o objetivo de detectar vulnerabilidades (expondo-as a testes) ao submeter planos, programas, ideias e pressupostos da organização para uma análise rigorosa e desafiante. Desde o ano de 2011, o agrupamento vermelho tornou-se amplamente utilizado no Reino Unido. Hoje, é reconhecido como um grande auxílio da tomada de decisões ao nível das funções de planeamento e de políticas de defesa[108].

A criação destas equipas ou ainda o recrutamento de hackers 'éticos'[109] [110] [111] que têm por função penetrar nos sistemas e nos servidores e descobrir as falhas existentes, de forma a antecipar intrusões maliciosas, podem constituir um avanço significativo no combate às ameaças e deteção de vulnerabilidades. Para se ter uma melhor noção do papel dessas equipas podemos compará-las ao papel dos polícias infiltrados, é semelhante, porque procuram vulnerabilidades na rede para garantir que se está ciente da existência de fraquezas, falhas ou portas abertas. Ou seja, com elas é possível ter uma imagem completa do 'status' de segurança dos sistemas do ponto de vista um hacker externo na internet que navega na internet. Com uma imagem real do que é realmente necessário fazer, a organização pode numa perspetiva proactiva aplicar um plano de atuação com vista à introdução de melhores medidas e mecanismos que salvaguarde toda a estrutura informática organizacional. A formação destas equipas parece ser uma medida perfeitamente executável e eficiente, pois envolve uma abordagem proactiva, não se resignando à mera figura de espetador, pelo contrário atua como um agente participativo, que também dá cartas no jogo, combatendo na dianteira os agentes intrusos [112].

O próprio Sun Tzu alude um pouco a esta forma de estar, ao dizer no seu livro "A Arte da Guerra" que "*para conhecer o seu inimigo, é preciso se tornar no seu inimigo*". [TZU, Sun].

[108] https://www.gov.uk/government/publications/a-guide-to-red-teaming (em linha) [Consult. 3 Julho 2014).
[109] São pessoas habilitadas para proteger os seus clientes, através da descoberta de falhas na segurança dos sistemas e ajudando a reparar as falhas. (em linha) [Consult. 3 Julho 2014).
[110] http://cert.eccouncil.org/certified-ethical-hacker.html (em linha) [Consult. 3 Julho 2014).
[111] http://www.eccouncil.org/Certification/certified-ethical-hacker (em linha) [Consult. 3 Julho 2014).
[112] http://www.red-team.co.uk/ (em linha) [Consult. 3 Julho 2014).

Conclui-se também que a implementação de normas estandardizadas ao nível da Segurança da Informação e da ciberdefesa, como as que tem sido realizadas a nível da UE, podem consituir uma boa medida para Portugal. Achamos que Portugal poderia estimular a adopção de um manual de boas práticas com a definição de normas que entidades públicas ou privadas se pudessem seguir, englobando desde os processos de normalização e aplicação de regulamentos, a definição de práticas eficazes para a verificação da segurança em sistemas relevantes de segurança nacional, e a identificação de padrões para áreas específicas de I&D. Neste campo os decisores políticos devem incentivar os fornecedores a fazer mais uso de normas e a submeter-se a auditorias de segurança (obrigatórias quando em negócios com o Estado), e encorajar as organizações privadas e do setor público a incluir referências a esses padrões em processos de aquisição; por sua vez, os governos deviam incorporar a normalização como parte das suas estratégias de segurança cibernética nacional Aquilo que nós aqui queremos alertar é que é importante uma melhoria da coordenação entre os níveis político e operacional assim como um reforço do papel das parcerias público-privadas nos processos de normalização; e as próprias autoridades reguladoras nacionais devem fazer um maior uso de padrões como um ponto de referência na aplicação de regulamentos. Por fim, e porque a componente da cooperação pode ter um papel preponderante, porque não também atuar ao nível dos países cooperantes na definição de um amplo regime de certificação que permite aos usuários finais verificar que produtos ou serviços cumprem as normas de segurança [PURSER, 2014].
Esta medida fiscalizadora poderia ser transposta para o contexto nacional, com a adesão das entidades públicas e privadas

Portugal no dominio da cibersegurança deve preocupar-se igualmente em educar e capacitar todos os cidadãos com informação, a confiança e as ferramentas práticas para se protegerem online. Já o ditado o diz, não se deve dar o peixe, mas sim antes deve-se ensinar a pescar, só assim o indivíduo não é dependente de outrem e fica habilitado a arranjar comida para si sem recorrer a terceiros.

A cooperação internacional deverá ser um mecanismo a adoptar grandemente por Portugal. Como já foi referido, grande parte dos incidentes de segurança informática têm âmbito transnacional, pelo que ao envolverem uma diversidade de intervenientes isso requer a participação de várias entidades na coordenação da sua resposta. Esta mesma cooperação

deve ir além da mera resposta a incidentes. *Sozinho, um Estado é incapaz de enfrentar ataques em grande dimensão*" [IDN Nº 12, 2013].

Importa ainda salientar que uma outra conclusão do trabalho é que as Estratégias e o modo de cooperação internacional adotado por diversos Estados, neste âmbito, poderão não estar a concorrer no sentido de um verdadeiro combate à ciberespionagem. Neste enquadramento é necessário implementar uma Estratégia que mobilize a liderança do Estado e arquitete as intervenções das agências estatais para a resolução das preocupações da ciberespionagem enquadrada naquilo a que se pretende que seja uma estratégia global de cibersegurança.

Importa não esquecer que para um país se posicionar com vantagem no domínio cibernético é preciso ser 'atrevido', nomeadamente gerir a afirmação dos seus interesses a nível internacional, refletir o valor da informação em seu proveito e valorizar os seus interesses nacionais económicos quer na área da prosperidade económica quer na exposição de competências na área de cibersegurança. (FREIRE & CALDAS, 2013)

Após apresentar algumas conclusões do trabalho que considero ser de relevo e motivo de reflexão sobre o que Portugal poderia fazer para melhorar a sua abordagem ao nível da ciberespionagem parece-me pertinente agora, e porque este trabalho se iniciou com uma questão central e várias questões derivadas, saber se estas foram ou não alcançadas, ou seja se a hipóteses levantadas são verdadeiras, ou se alguma das questões ainda se mantém.

Face ao coligido no presente trabalho concluímos facilmente e sem qualquer tipo de dúvida ou hesitação que o fenómeno da ciberespionagem assume-se como uma clara ameaça para o normal funcionamento da sociedade e das instituições reguladoras da mesma.

A intrusão nos sistemas informáticos de qualquer Estado, instituição ou empresa podem provocar danos no plano da segurança nacional, arrastando qualquer nação para um tal estado de vulnerabilidade e dependência, de onde dificilmente poderá escapar. Até porque o próprio Estado tem uma função de proteção das instituições, assumindo-se como um dos garantes da confiabilidade perante os diversos parceiros institucionais.

Ora, quando a capacidade de autodefesa de qualquer instituição estatal ou de qualquer empresa de determinado país é posta em causa, o próprio estado transmite uma imagem de fraqueza e incapacidade que consequentemente o fará cair em descrédito, prejudicando-o a vários níveis, sobretudo no político e económico.A nível social, também as consequências se fazem sentir.

No plano governamental, uma fuga de informação proveniente de organismos governamentais de segurança como a que ocorreu no caso Snowden, poderá originar uma desconfiança desmedida sobre determinados países ou então vir a minar as relações diplomáticas existentes entre diversos estados.

Para além do atrás exposto, podemos com isto afirmar peremptoriamente que os processos decisórios do Estado são francamente afetados com os efeitos da ciberespionagem, pois muitas das decisões que qualquer governo possa vir a tomar sobre determinado assunto, encontram-se reféns da dimensão do ataque que foi alvo e das intenções que o detentor da informação furtada possa vir a demonstrar.

Numa segunda fase foi demonstrado que a espionagem desde sempre foi utilizada como uma ferramenta na gestão política e militar de várias nações. Não se diferencia do que agora conhecemos com ciberespionagem.

E entendo que não diferencia porque por detrás dos vários métodos utilizados o objetivo continua a ser o mesmo - conseguir informação classificada, de forma sub-reptícia, para ser utilizada de forma proveitosa por adversários políticos e comerciais.

Apesar da espionagem remontar a eras bíblicas, o seu intuito sempre foi o mesmo, ganhar vantagem sobre determinado grupo ou nação. No entanto, aquilo que tem mudado são os métodos utilizados, variaram desde sempre conforme a evolução social e tecnologia das épocas a que se inseriam tais fenómenos. O aparecimento de um novo espaço virtual, o ciberespaço, possibilitou apenas outra forma de espiar.

Desta forma, a ciberespionagem não é mais do que um método de espionagem adaptada aos dias de hoje, devido à forma com o hoje comunicamos e à maneira como se armazena a informação. Possivelmente, daqui a uns anos os métodos utilizados na ciberespionagem

deixarão de fazer sentido e talvez sejam utilizados outros mais eficazes e moldados à época em curso.

Mas para a realidade atual da ciberespionagem somente se poderá afirmar que as estruturas e políticas nacionais serão as suficientes para o combate à ciberespionagem se forem alicerçadas numa estrutura sólida, profissional e um com grau de especialização elevado. E mais, só após o seu funcionamento ficará claro se Portugal possui as capacidades para responder eficazmente a esta ciberameaça.

Sem os três itens acima referidos nunca poderemos possuir organismos com a capacidade de defender o País de ataques de ciberespionagem, independentemente do seu número ou das especificações que possuam.

No caso Português, existem organismos como os Serviços de Informações e Segurança, que há muito tempo assumem um papel de controlo e recolha de informação na área da espionagem. Também aqui houve a nível político uma preocupação de através do PSE sensibilizar os agentes institucionais e empresariais para estas ameaças.

Com a crescente preocupação de Portugal e consciencialização para as ameaças decorrentes do ciberespaço e da utilização da internet foi criado o Centro Nacional de Cibersegurança, organismo criado especialmente para o combate exclusivo a estes fenómenos. Também aqui considera-se importante a inclusão de uma estrutura operacional do CNC ou do SIS.

São organismos do tipo deste último, que se julga serem os adequados para este combate, pois a estrutura e especialmente a especialização encontram-se contempladas no âmago da sua criação.

Relativamente ao tipo de ações que deverão ser aplicadas por uma estrutur de âmbito nacional, achamos que para além da vigilância ao ciberespaço e formação fornecida a entidades estatais e empresas, deverão ser realizadas ações pró ativas, que procurem em tempo útil recolher informação credível sobre grupos ou indivíduos que estejam a agir criminalmente no campo da ciberespionagem.

Com isto, não pretendemos aplicar a célebre expressão "o ataque é a melhor defesa" mas sim, que se deverá apostar na preparação preventiva mas também proactiva, pois só desta forma poderão ser minimizados os riscos resultantes de um ataque deste género.

Por fim, convém referir que somente com um investimento governamental, a nível de equipamentos, pessoal e financeiro se poderão lograr resultados, de outra forma, as estruturas de combate à ciberespionagem criadas virão o seu trabalho pecar por defeito, definhando à nascença e mostrando-se fracas e ineficazes contra as ameaças que diariamente germinam.

Tal como já tem sido bastante referido, sendo esta, inclusivé, uma das questões chave do presente trabalho: qual o papel da cooperação internacional, e que contributo poderá dar na redução do nível da ciberespionagem? A verdade é que sempre que se fala na cooperação internacional, esta nunca aborda o tema da ciberespionagem, poderá ser falada em termos genéricos, com a tomada de decisões no que concerne à adoção de medidas que permitam uma maior segurança da informação que circula no ciberespaço, ou numa vertente mais técnica, a exploração de situações que permitam capacitar as empresas de meios para se defenderem de incidentes que prejudiquem quer empresas nacionais quer os organismos públicos. Mas nada se fala quanto à cooperação para a ciberespionagem. Parece que a cooperação internacional ao nível da prevenção e combate à ciberespionagem não tem funcionado como um contributo neste domínio, até porque, daquilo que já foi apresentado ao longo do trabalho, além de suscitar alguma estranheza governos que se espiam permitirem e adotarem mecanismos de âmbito internacional que possibilitem descortinar as suas atividades de espionagem, com o único propósito de não se quererem ver numa situação debilitante ou precária perante a comunidade internacional. Tal situação poderia ter implicações económicas graves, e qualquer Estado quer evitar isso a todo custo. Para poder sancionar um Estado ou empresa era necessário alargar uma resposta ao campo criminal e penal, e nenhuma nação está interessada que isso aconteça até porque nenhuma quer estar daqui a uns anos no bancos dos réus, ser acusada e condenada formalmente por espionagem.

Tudo isto mudaria se todos os Estados e empresas adotassem o lema de que 'a união faz a força', mas neste caso a união não significa somente um esforço conjunto no combate ao infratores, mas sim, a parceria na troca de informações sobre casos já sofridos. Aprender

com casos concretos, possibilita acima de tudo conhecer os erros e sucessos de outros países nesta área e acima de tudo estabelecer uma plataforma de entendimento e de trabalho entre os estados membros dessa união. Até porque um problema técnico normalmente tem sempre solução.

Efetivamente já houve tentativas de conversação entre os EUA e a China no que respeita à ciberespionagem, mas estas não deram grandes frutos.

Só através da partilha de experiências seria possível criar um conjunto de regras protocoladas, de eficácia comprovada, para a proteção de futuros ataques ou então no combate aos mesmos após a deteção das intrusões.

A criação da implementação de legislação uniforme entre vários países poderá de certa forma impedir que determinados indivíduos ou grupos possam aventurar-se no lançamento de um ato de espionagem, pois para além da possível deteção e rastreio do mesmo, podem vir ser identificados, independentemente do país onde estejam a operar.

É crucial que não existam países definidos como "off-shore" no plano cibernético, onde tudo possa ser realizado contra as demais nações sem qualquer medida penalizadora para os autores. A cooperação internacional nesta matéria seria benéfica e extremamente vantajosa em termos de desencorajamento efetivo a futuros acontecimentos deste género, obrigando aos agentes invasores a repensar a sua estratégia ou demove-los simplesmente dos seus intentos.

Transportando esta afirmação para o plano aqui discutido, podemos concluir que o isolamento dos Estados nestas áreas sensíveis acarretará atrasos que dificilmente poderão ser compensados e ultrapassados mesmo com a existência de um esforço hercúleo isolado por parte de qualquer nação.

Não querendo repetir o que tem vindo a ser explanado no presente trabalho a verdade os países tem que ter consciência situacional. As vulnerabilidades estratégicas, as ameaças e os riscos que podem advir do cibereespaço tem que ser considerado na definição de uma Estratégia de Cibersegurança Nacional, e Portugal não foge à regra, terá também ele que realizar uma avaliação de riscos decorrentes da utilização de 'armas' de informação por

parte de atores hostis se quiser manter à distância um potencial ato de ciberespionagem ou de qualquer outra ameaça, porque as consequências são hoje em dia uma incerteza.

Chegar a esta conclusão parece fácil, o que se pode dizer que até foi, até porque aquilo que tem sido tornado público pelos Estados nesta matéria e as notícias dos *media* faz pensar isso mesmo. Mas embora se pense que a espionagem ou a ciberespionagem é um assunto sem tabus, não corresponde à verdade. A realização deste trabalho constatou precisamente isso. Esta é ainda uma matéria envolta em secretismo, aqueles que poderiam dizer o que realmente se passa não o querem fazer, os interesse nacionais e económicos superam qualquer intenção.

Por isso foram sentidas dificuldades ao longo do trabalho em particular na recolha de bibliografia que abordasse o tema da ciberespionagem nas duas diversas vertentes. Foi obtida muita informação com origem na comunicação social, mas tal informção carece sempre de alguma credibilidade. No entanto com esforço o trabalho foi crescendo e chegou ao fim.

Pese embora as dificuldades encontradas a realização deste trabalho foi sem dúvida desafiante e chegar ao fim representa um objetivo alcançado.

Considero que o estudo sobre a ciberespionagem deve continuar a ser desenvolvido e aprofundado, em especial no que respeita à forma como esta pode ser enquadrada na estrutura nacional de cibersegurança.

BIBLIOGRAFIA

BESSA, Jorge S. – A Espionagem Económica. (em linha) [Consult. 8 de Maio 2014.]Disponível na Internet: http://www.fiescnet.com.br/senai/conhecimento/arquivos/anais/DraKira/EspionagemEconomica-JorgeBessa.pdf.

CARDOSO, Pedro - As Informações em Portugal- Instituto de Defesa Nacional, 2004.

CHALOU, George C. – The Secrets war : The Office Os Strategic Services in World War II – National Archives and Records Administration . ISBN 0-911333-91-6. 1992. Disponível na Internet: http://www.znaci.net/00001/294.pdf

COELHO, Carlos – 'Os Americanos Espiam a Europa?' – O Caso Echelon Dois Anos Depois – Notícias Editorial. ISBN 972-46-1522-7. Jan. 2004.

CORNISH, Paul - Chinese Cyber Espionage: Confrontation or Co-operation?- Professor of International Security, University of Bath. Abril 2012. (em linha) [Consult. 6 Junho 2014]. Disponível em : http://www.cityforum.co.uk/publications/5/pdf/chinese-cyber-espionage---3412-final.pdf.

CYBERSECURITY STRATEGY OF THE EUROPEAN UNION (CSEU): 'An Open, Safe and Secure Cyberspace' – European Commissiona - Joint Communicationa to the European Parliament, The Council, The European Economic and Social Committee and The Committee of the Regions. 2013.

DELOITTE - Cyber Espionage: The harsh reality of advanced security threats - Center for Security & Privacy Solutions. 2011.(em linha) [Consult. 29 Maio 2014]. Disponível na Internet: http://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/AERS/us_aers_cyber_espionage_07292011.pdf.

DETICA e CABINET OFFICE - The Cost of Cybercrime – A Detica Report in Partnership with the Office of Cyber Security and Information Assurance in the Cabinet Office – 2011.(em linha) [Consult. 22 Junho 2014]. Disponível na Internet: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf.

ENISA - Annual Incident Reports 2012, Analysis of Article 13a annual incident reports. Agosto de 2013. (em linha) [Consult. 3 Junho 2014]. Disponível na Internet: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports/annual-incident-reports-2012.

ENISA's ten security awareness good practices. 2009. (em linha) [Consult. 3 Julho 2014]. Disponível na Internet: http://www.enisa.europa.eu/media/multimedia/ar-files/covers/arprac/view.

FREIRE, V.; CALDAS A. – O ciberespaço: Desafios à Segurança e à Estratégia-Publicação Atena, Segurança Internacional: Perspetivas Analíticas nº 30. 2013. ISBN 978-972-27-2168-4, p. 81-151.

FREIRE, V.; CALDAS A. Cibersegurança: das Preocupações à Ação. Instituto da Defesa Nacional -Working Paper 2 / 2013. ISBN: 978-972-9393-26-6.

GARCIA, Francisco Proença – La Transfromation de la Inteligência. (Em linha) In Boletin de Informacion Nº313, Centro Superior de Estudios de La Defensa Nacional, Ministério de Defensa de España,2009.(em linha) [Consult. 18 Jun. 2014] Disponível na internet: http://www.defensa.gob.es/ceseden/Galerias/destacados/publicaciones/Boletines_de_Informacion/ficheros/BOLETIN_DE_INFORMACION_DEL_CESEDEN_313.pdf

Government of United Kingdom - Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyber Space. 2009. (em linha) [Consult. 04 Maio 2014].Disponível em http://www.official-documents.gov.uk/document/cm76/7642/7642.pdf.

Government of Canada - Canada's Cyber Security Strategy. 2010 (em linha) [Consultado em 04 Maio 2014]. Disponível na internet: http://www.publicsafety.gc.ca/prg/ns/cbr/_fl/ccss-scc-eng.pdf.

HERSH, Seymour M. – The Online Threat – Should we be worried about a cyber war?. 2010. (em linha) [Consult. 6 Maio 2014]. Disponível na Internet: http://www.newyorker.com/reporting/2010/11/01/101101fa_fact_hersh?currentPage=all.

IDN nº 12 - Estratégia da Informação e Segurança no Ciberespaço - Investigação conjunta IDN-CESEDEN – Instituto de Defesa Nacional – 2013. (em linha) [Consult. 11 Junho 2014]. Disponível na internet: http://www.idn.gov.pt/publicacoes/cadernos/idncaderno_12.pdf.

KASPERSKY – Special report 'Who's Spying on You?', 2013. (em linha) [Consult. 25 Junho 2014]. Disponível na Internet: http://media.kaspersky.com/en/business-security/kaspersky-cyber-espionage-whitepaper.pdf?icid=en_GL:ent-gallery

KOSTADINOV, Dimitar – "Cyber Exploitation". 2013 – (em linha) [Consult. 6 Maio 2014]. Disponível na Internet: http://resources.infosecinstitute.com/cyber-exploitation/.

LIN, Herbert S. - Offensive Cyber Operations and the Use of Force. Journal of National Security Law&Policy [Vol. 4: 63-86]. 2010. (em linha)[Consult. 6 Maio 2014]. Disponível na Internet: http://jnslp.com/wp-content/uploads/2010/08/06_Lin.pdf.

MCAFEE – Economic Impact of Cybercrime and Cyber Espionage – Centre for Strategic and International Studies, Julho de 2013. (em linha) [Consult. 20 Junho 2014]. Disponível na Internet: http://www.mcafee.com/sg/resources/reports/rp-economic-impact-cybercrime.pdf

MOREIRA, João M. D. – O Impacto do Ciberespaço como Nova Dimensão nos Conflitos - Boletim Ensino | Investigação nº 13, Novembro 2012, Capítulo 2, p. 27-50. (em linha) [Consult. 08 Abril 2014]. Disponível na Internet: http://www.iesm.pt/cisdi/boletim/Artigos/Artigo_2.pdf.

NATÁRIO, Rui – O Combate ao Cibercrime: Anarquia e Ordem no Ciberespaço- Revista Militar N.º 2541 - Outubro de 2013. Disponível na internet: http://www.revistamilitar.pt/artigo.php?art_id=854 – 27/06/2014.

NATO Cooperative Cyber Defence Centre of Excellence, International Group of Experts at the Invitation - The Tallinn Manual on the International Law Applicable to Cyber Warfare – Cambridge University. 2013. (em linha) [Consult. 7 Maio 2014]. Disponível na Internet: http://nuclearenergy.ir/wp-content/uploads/2013/11/tallinn_manual.pdf.

NATIONAL STRATEGY USA - The National Strategy to Secure Cyberspace – Fev. 2003. (em linha) [Consult. 30 Junho 2014]. Disponível na internet: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf.

OCDE - Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies. 2012. (em linha) [Consult. 3 Julho 2014]. Disponível na Internet: http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf.

OFFICE OF THE NATIONAL COUNTERINTELLIGENCE EXECUTIVE – Foreign Spies Stealing US Ecnomic Secrets in Cyberspace – Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009. 2011.

OPHARDT, Jonathan A. – Cyber Warfare and the Crime of Agression: The Need for Individual Accountability on Tomorrow's Battlefield. Duke Law & Technology Review, Nº3. 2010. (em linha) [Consult. 7 Maio 2014]. Disponível na Internet: http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1198&context=dltr.

Proposta da Estratégia Nacional de Cibersegurança - (em linha) [Consult. 08 Junho2014]. Disponível na internet: http://www.gns.gov.pt/media/1247/PropostaEstratégiaNacionaldeCibersegurançaPortuguesa.pdf.

PURSER, Steve – Standards for Cyber Security – European Unit network and Information Security Agency (ENISA). IOS Press, 2014. (em linha) [Consult. 21 Junho 2014]. Disponível na internet: http://www.enisa.europa.eu/publications/articles/standards-for-cyber-security.

RASI – Relatório Anual de Segurança Interna – Governo de Portugal. 2013.(em linha) [Consult. 7 Maio 2014] Disponível na internet: http://www.portugal.gov.pt/media/1391220/RASI%202013.pdf

SACRAMENTO, António, Tenente-Coronel – Enquadramento da Segurança das Comunicações. Revista Militar, *Nº2449/2450,* (Fevereiro/Março 2006). (em linha) [Consult. 7 Maio 2014]. Disponível na Internet: http://www.revistamilitar.pt/artigo.php?art_id=60.

SANTOS, José L. – 'Contributos para uma melhor Governação da Cibersegurança em Portugal' – 2011, Lisboa.(em linha) [Consult. 7 Maio 2014] Disponível na Internet: http://run.unl.pt/bitstream/10362/7341/1/Santos_2011.PDF.

SOCTA – EU Serious and Organized Crime Threat Assessment, 2013 – Europol. (em linha) [Consult. 7 Maio 2014] Disponível na internet https://www.europol.europa.eu/sites/default/files/publications/socta2013.pdf.

SYMANTEC Internet Security Threat Report - Trends for 2010 -Volume 16, Abril 2011. (em linha) [Consult. 02 Julho 2014]. Disponível na internet: https://www4.symantec.com/mktginfo/downloads/21182883_GA_REPORT_ISTR_Main-Report_04-11_HI-RES.pdf.

TAVARES, Enéias F. – "Otelo – O Mouro de Veneza, de Shakespeare: Crítica e Tradução Literária". Universidade Federal de Santa Maria (UFSM, RS, Brasil). 2007, p. 23. (em linha) [Consult. 28 Abril 2014]. Disponível na Internet: http://www.dbd.puc-rio.br/shakespeare/pdfs/dissertacaoEneiasTavares.pdf.

TZU, Sun – A Arte da Guerra. Lisboa: Editorial Futura, 1974.

VERIZON – Data Breach Investigations Report. 2014. (em linha) [Consult. 31 Maio 2014]. Disponível na Internet: http://www.verizonenterprise.com/DBIR/.

WHITE HOUSE - Cyberspace Policy Review. Assuring a Trusted and Resilient Information and Communications Infrastructure. 2009.Disponível em http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf. (em linha) [Consult. 04 Maio 2014].