Instituto Superior de Ciências Policiais e Segurança Interna

Elisabete Júlio Domingues

Aspirante a Oficial de Polícia

Dissertação de Mestrado Integrado em Ciências Policiais

XXVII Curso de Formação de Oficiais de Polícia

Os Ciberataques como um Novo Desafio para a Segurança: o *Hacktivismo*

Orientador:

Professor Doutor Felipe Pathé Duarte

Lisboa, 24 de abril de 2015

Instituto Superior de Ciências Policiais e Segurança Interna

Elisabete Júlio Domingues

Aspirante a Oficial de Polícia

Dissertação de Mestrado Integrado em Ciências Policiais

XXVII Curso de Formação de Oficiais de Polícia

Os Ciberataques como um Novo Desafio para a Segurança: o *Hacktivismo*

Orientador:

Professor Doutor Felipe Pathé Duarte

Dissertação apresentada ao Instituto Superior de Ciências Policiais e Segurança Interna, com vista à obtenção do grau de Mestre em Ciências Policiais, elaborada sob orientação do Professor Doutor Felipe Pathé Duarte.

Ao meu padrinho,
pelo exemplo.

Agradecimentos

A realização deste trabalho não teria sido possível sem o apoio de algumas pessoas, que, direta ou indiretamente, contribuíram para o resultado final do mesmo.

Dirijo uma palavra de apreço e gratidão à minha família e aos meus amigos, que nunca deixaram a base estremecer, apoiando-me sempre na realização dos meus sonhos e amparando as minhas quedas.

Aos meus camaradas do XXVII Curso de Formação de Oficiais de Polícia, pela camaradagem e apoio constantes nas adversidades encontradas durante a minha caminhada ao longo dos cinco anos de formação.

Ao Professor Doutor Felipe Pathé Duarte, pela sua orientação, que em muito contribuiu para o resultado final deste trabalho.

Um agradecimento especial ao Intendente Rui Moura, ao Tenente-Coronel Paulo Santos, ao Doutor Vitor Costa, ao Doutor Carlos Cabreiro, ao Doutor José Carlos Martins e ao Dirigente do Serviço de Informações de Segurança pela disponibilidade e pela riqueza das entrevistas que me cederam.

Quero ainda agradecer ao Instituto de Defesa Nacional, na pessoa do Coronel João Barbas, coordenador do II Curso de Cibersegurança e Gestão de Crises no Ciberespaço, por ter aceitado a minha candidatura para o curso, que se revelou um contributo indispensável para a sedimentação dos meus conhecimentos, no âmbito desta dissertação.

É fundamental, para mim, deixar uma palavra de apreço a algumas pessoas que me foram apoiando, dando sugestões e opiniões relativamente ao meu trabalho de investigação, sem as quais não teria sido possível alcançar os resultados conseguidos: Subintendente Élia Chambel, Comissário João Carvalho, Técnica em Informática Teresa Mendes, Coronel Luís Nunes, Comissário Nuno Silva, Subcomissário Nuno Ponciano, Subcomissário Sílvio Pires, Subcomissário Hermínio Costa, Chefe Anabela Machado, Agente Principal Jorge Carvalho, Coronel Fernando Freire e Doutor João Silva.

Agradeço a todos os que se revelaram sempre disponíveis e interessados em levar a bom porto este trabalho de investigação.

Resumo

Desde o final do século passado, as novas tecnologias da informação e comunicação têm apresentado uma evolução célere, originando uma mudança radical na forma como as pessoas se relacionam. O mundo transformou-se numa complexa teia de redes, cujos nós se encontram interligados. A sociedade em rede assume-se como uma realidade profícua em inovação e desenvolvimento, contudo, é também promotora de novos perigos e desafios, entre eles o cibercrime. A insegurança no ciberespaço, demonstrada pelo aumento de ciberataques, torna premente o estudo de ciberameaças, como o *hacktivismo*. As entidades governamentais, as Forças de Segurança e as grandes empresas são constantemente alvo de ciberataques, sendo que em Portugal têm vindo a ser recorrentes casos de instituições portuguesas que são vítimas de ataques desta índole. Neste estudo, procuramos perceber se o fenómeno *hacktivista* representa uma ameaça para as Forças de Segurança portuguesas. Assim, abordamos concetualmente o fenómeno do *hacktivismo*, analisando em concreto o fenómeno em Portugal. Para alcançar as respostas pretendidas recorremos ao método qualitativo, realizando entrevistas a especialistas e a responsáveis pela área da cibersegurança e fazendo uma análise a recortes de imprensa nacionais. Depois de submetidos a análise de conteúdo, os instrumentos permitem-nos perceber os contornos do fenómeno *hacktivista* nacional, bem como perceber a ameaça representada pelo *hacktivismo* para as Forças de Segurança.

Palavras-chave: *Hacktivismo*; Ciberataques; Cibersegurança; Cibercrime; Forças de Segurança.

Abstract

Since the end of last century, the new information and communication technologies have been on a speedy development, leading to a radical change in the way people relate themselves. The world has become a complex web of networks, whose nodes are interconnected. The network society is assumed as a useful reality in innovation and development, however it is also a promoter of new dangers and challenges, including cyber crime. Insecurity in cyberspace, shown by the increase of cyber attacks, makes urgent the study of cyber threats, as hacktivism. Government entities, the Security Forces and large companies are constantly cyberattacks target and, in Portugal, have been recurrent cases of Portuguese institutions who are victims of this kind of attacks. In this study, we try to see whether hacktivist phenomenon poses a threat to the Portuguese security forces. Thus, conceptually approach the phenomenon of hacktivism, analyzing in particular the phenomenon in Portugal. To achieve the desired answers we use the qualitative method by conducting interviews with experts and responsible for the area of cyber security and the analysis the national press clippings. After undergoing the content analysis, the instruments allow us to understand the contours of phenomenon in Portugal as well as realize the threat posed by hacktivism to the Security Forces.

Keywords: Hacktivism; Cyber Attack; Cybersecurity; Cybercrime; Security Forces.

Índice

Índice de Apêndices e Documentação Anexa

Lista de Siglas

APT – *Advanced Persistent Threats*

CEGER – Centro de Gestão da Rede Informática do Governo

CERT – *Computer Emergency Response Team*

CNCseg – Centro Nacional de Cibersegurança

COSI – Centro de Operações de Segurança Informática

CRP – Constituição da República Portuguesa

CSIRT – *Computer Security Incident Response Team*

DDoS – *Distributed Denial of Service*

DoS – *Denial of Service*

EC3 – *European Cybercrime Centre*

EM – Estados Membros

ENIAC – *Electronic Numerical Integrator Analyzer and Computer*

ENISA – Agência Europeia de Segurança de Redes e da Informação

EUA – Estados Unidos da América

Europol – Serviço Europeu de Polícia

FCCN – Fundação para a Computação Científica Nacional

FS – Forças de Segurança

FSS – Forças e Serviços de Segurança

GNR – Guarda Nacional Republicana

GNS – Gabinete Nacional de Segurança

IC – Infraestruturas Críticas

IDN – Instituto da Defesa Nacional

IoE – *Internet of Everything*

IP – *Internet Protocol*

IRC – *Internet Relay Chat*

ITU – *International Telecommunication Union*

MAI – Ministério da Administração Interna

MP – Ministério Público

OCS – Órgãos de Comunicação Social

ONU – Organização das Nações Unidas

OTAN – Organização do Tratado do Atlântico Norte

PJ – Polícia Judiciária

PSP – Polícia de Segurança Pública

RASI – Relatório Anual de Segurança Interna

RCTS – Rede Ciência, Tecnologia e Sociedade

SIRESP – Sistema Integrado de Redes de Emergência e Segurança de Portugal

SIS – Serviço de Informações de Segurança

SOC – *Security Operations Center*

TIC – Tecnologias da Informação e Comunicação

UE – União Europeia

WWW – *World Wide Web*

Introdução

Incidentes informáticos têm lugar com uma frequência diária, fruto de ataques de *hacktivistas*, encetados individualmente ou em grupo, que veem nas Forças de Segurança (FS) portuguesas um alvo apetecível. Mas será que o *hacktivismo* pode constituir uma ameaça para a Segurança?

As Tecnologias de Informação e Comunicação (TIC) têm apresentado, desde o final do século passado, uma evolução bastante célere, originando uma mudança radical na forma como as pessoas se relacionam. A *internet* tornou-se no motor desta mudança e o ciberespaço no novo palco da sociedade, onde a comunicação ocorre de forma constante.

As potencialidades deste novo espaço são imensas, sendo que a nível económico e social a sociedade beneficiou do fator de proximidade, tal como de economia de esforço e tempo. Todavia, no verso da moeda encontramos também fragilidades, visto que "as actividades criminosas (…) também se tornaram globais e informacionais, propiciando os meios para estimular a hiperactividade mental e os desejos proibidos" (Castells, 2011, p. 2). Deste modo, com a massificação da utilização da *internet,* são colocadas questões que se relacionam com a segurança das pessoas e das infraestruturas que dependem das TIC, pelo que se coloca o problema da *internet* ter uma dupla dimensão, ou seja, produz desenvolvimento e inovação, mas cria novos problemas, nomeadamente ao nível da segurança.

Esta nova ordenação da sociedade trouxe consigo um novo conjunto de conceitos modernos como o de ciberespaço, cibercrime, *hacktivismo*, *hackers*, os quais serão esmiuçados ao longo do presente trabalho. Contudo, permanecem entre nós conceitos tradicionais que sofreram uma mutação, como é o caso do conceito de segurança. Segundo Silva (2012), "a segurança hoje não pode ser contida por muros. As fronteiras físicas já não isolam e pouco significam" (p. 9), ou seja, assiste-se a uma alteração do conceito tradicional de segurança.

Na Era digital, a possibilidade de utilização das TIC para disseminar mensagens e realizar protestos de índole diversa converte o ciberespaço "numa ágora electrónica global onde a diversidade do descontentamento humano explode numa cacofonia de pronúncias" (Castells, 2007, p. 168). O *hacktivismo* é fruto desta alteração verificada na sociedade, uma vez que a *internet* provocou "uma mudança no panorama de mobilização e protesto" (Cardoso, 2014, p. 502).

O *hacktivismo* é considerado, no âmbito da presente dissertação, a combinação da política transgressiva da desobediência civil, com as novas técnicas e tecnologias de *hacking*[1], cujo propósito é alterar o normal funcionamento de *sites*, mas não o de causar graves danos (Denning, 1999). As instituições estatais, o setor bancário/financeiro e o setor empresarial simbolizam, nas palavras de Martins (2012), "um novo alvo a explorar e a abater" (p. 41). Recentemente, têm sido realizados ataques informáticos a *sites* e sistemas informáticos de algumas instituições governamentais portuguesas, nomeadamente às FS. Refira-se que o grupo *Anonymous* tem reivindicado vários ataques a *sites* governamentais e instituições de relevo (Pavia, 2012). A título de exemplo, este grupo terá, alegadamente, sido responsável pelo ataque à Procuradoria-Geral da República, em 2014[2].

Para Castells (2007), "não há dúvida de que a habilidade para obter uma informação crucial, contaminar as bases de dados ou criar desordem nos sistemas de comunicação-chave, se converteu numa arma importante no novo ambiente tecnológico" (p. 190). Desta forma, "a protecção das infraestruturas críticas de informação, tornou-se não só uma necessidade como um imperativo" (Caldas, 2011, p. 95).

Este trabalho de investigação versa a temática do fenómeno do *hacktivismo* e a inerente ameaça para a Segurança, inserindo-se no campo epistemológico das Ciências Policiais. Tratando-se de uma temática transversal, são ainda feitas algumas incursões no campo da Sociologia e da Ciência Política. A opção pelo tema deve-se tanto à sua atualidade como à relevância que assume no contexto da segurança portuguesa, uma vez que é essencial, para as instituições cuja missão passa por garantir a segurança, conhecer as ameaças existentes, para que melhor as possam evitar e prevenir. A este respeito, consideramos pertinente remeter para os ensinamentos de Sun Tzu (2009), o famoso estratega chinês, que refere na sua obra de referência, *A Arte da Guerra*, que "conhecer os outros e conhecer-se a si próprio em cem batalhas, nenhum perigo. Não conhecer os outros e conhecer-se a si próprio, uma vitória por cada derrota. Não conhecer os outros e não se conhecer a si próprio, em cada batalha, derrota certa" (p. 29). Torna-se, portanto, essenciais conhecer as nossas vulnerabilidades, mas sobretudo verificarmos qual a ameaça representada pelo *hacktivismo*.

O nosso problema passa, inevitavelmente, por saber se os ataques cometidos por *hacktivistas* representam ou não uma ameaça para a Segurança portuguesa, avaliando em

[1] Termo que designa o conjunto de técnicas informáticas que permitem a infiltração não autorizada em sistemas informáticos.
[2] Ver Apêndice J, sobre a análise realizada a recortes de imprensa, retirados da base de dados CISION.

concreto o caso das FS[3] − Polícia de Segurança Pública (PSP) e Guarda Nacional Republicana (GNR). Já que analisar todas as instituições com contributos no âmbito da Segurança do país se torna demasiado exaustivo, a nossa opção deve-se ao facto de serem estas as instituições que são frequentemente alvo deste tipo de ataques. Na nossa investigação procuramos dar resposta à seguinte pergunta de partida: O fenómeno *hacktivista* representa uma ameaça para as FS portuguesas?

O objetivo geral deste estudo é caracterizar o *hacktivismo*, com o propósito de apurar se o mesmo constitui ou não uma ameaça. Assim, é nosso intuito verificar quais os grupos que desenvolvem protestos sob forma de ciberataque, quais as suas pretensões, quais os tipos de ataques realizados com maior frequência, bem como quais as consequências dos mesmos. Em termos de objetivos específicos deste trabalho, procuramos apurar a representatividade do *hacktivismo* a nível nacional e quais os grupos envolvidos, definir a forma de organização e características dos ataques perpetrados e determinar quais as pretensões ou motivações dos grupos *hacktivistas.*

O trabalho encontra-se dividido em quatro capítulos, sendo o primeiro dedicado à contextualização da sociedade atual, onde fazemos uma breve apresentação da evolução da sociedade com base no aparecimento das tecnologias de relevo de cada época. De seguida, analisamos a sociedade em rede e, por último, caracterizamos o ciberespaço, nomeadamente no que concerne ao exercício da soberania na Era digital.

No segundo capítulo abordamos a cibersegurança como aspeto essencial e indispensável da sociedade atual. Começamos por abordar a evolução da cibercriminalidade, nomeadamente a nova criminalidade informática. Em seguida, distinguimos os conceitos de cibersegurança e ciberdefesa, indicando as iniciativas tomadas pela União Europeia (UE) no sentido de desenvolver a cibersegurança, mas também os esforços feitos por Portugal no que diz respeito à segurança do ciberespaço.

No terceiro capítulo damos especial destaque às ciberameaças, nomeadamente a ciberguerra, o ciberterrorismo, a ciberespionagem e o *hacktivismo*. Este capítulo é sobretudo dedicado ao *hacktivismo*, à sua origem, à sua forma de organização, aos tipos de *hacktivismo* existentes e à descrição dos ataques realizados com mais frequência.

[3] De acordo com Raposo (2006), FS são "corporações policiais que têm por missão assegurar a manutenção da ordem e segurança públicas e o exercício dos direitos fundamentais dos cidadãos, dispondo para o efeito de uma estrutura organizativa fortemente hierarquizada, especialmente habilitada para o uso colectivo de meios coercivos" (p. 49). Embora Raposo considere, neste âmbito, também a Polícia Marítima, no nosso trabalho optámos por estudar apenas a PSP e a GNR.

O quarto capítulo destina-se à análise da ameaça *hacktivista* no panorama português. Dedicamos uma parte para as características do *hacktivismo* em Portugal, verificando qual a sua representatividade, qual a sua forma de organização e quais os grupos mais envolvidos. Neste capítulo, projetamos um tipo de perfil de *hacktivista*, com base nos seus propósitos e nas suas capacidades. São indicados os motivos e as causas que levam as FS a ser um alvo recorrente destes ataques, e, por último, tentamos perceber se podemos considerar o fenómeno *hacktivista* uma ameaça para a Segurança.

Metodologia

De acordo com Sarmento (2013), "pode ser utilizado mais do que um método, para que sejam encontradas as respostas para a pergunta de partida da investigação" (p. 7), pelo que recorremos ao método descritivo e inquisitivo para alcançar as respostas pretendidas, o que torna mais sólidas a fundamentação e credibilidade dos dados analisados.

De forma a concretizar os objetivos do estudo, é construído um modelo de análise, assente numa base metodológica qualitativa, o que permite inferir se o *hacktivismo* representa ou não uma ameaça para a Segurança. Nas palavras de Sarmento (2013), "para que a informação recolhida no universo informacional seja fiável e os resultados da investigação sejam válidos, os instrumentos e métodos científicos utilizados devem ser apropriados" (p. 27). Neste sentido, são analisadas fontes primárias, concretamente entrevistas, que permitem "explorar um domínio e aprofundar o seu conhecimento" (Sarmento, 2013, p. 28), e secundárias, nomeadamente, bibliografia e recortes de imprensa.

Para proceder ao levantamento do estado da arte baseamo-nos numa análise bibliográfica, recorrendo a autores nacionais e internacionais. Face à escassez de bibliografia encontrada, recorremos a entrevistas exploratórias a especialistas e a responsáveis nesta área e nas FS alvo deste estudo. Recorremos à análise dos recortes de imprensa dos vários Órgãos de Comunicação Social (OCS), recolhidos na base de dados CISION[4], que contem todas as notícias regionais, nacionais e internacionais divulgadas.

As entrevistas semidiretivas desenvolvidas, após solicitação oficiosa (ver Apêndice A), foram realizadas presencialmente a profissionais que trabalham diretamente com a problemática abordada: Rui Moura, Intendente da PSP; Paulo Santos, Tenente Coronel da GNR; Vitor Costa, do Centro de Operações de Segurança Informática (COSI) da Secretaria Geral do Ministério da Administração Interna (SGMAI), já que é este organismo que

[4] Disponível em http://www.cision.com/pt/ (consultado em 2 de março de 2015).

monitoriza os incidentes de segurança detetados nas infraestruturas tecnológicas do Ministério da Administração Interna (MAI); José Carlos Martins, Diretor do Centro Nacional de Cibersegurança (CNCseg), que é a autoridade nacional competente em matéria de cibersegurança[5]; Carlos Cabreiro, da Polícia Judiciária (PJ), por ser este o órgão de polícia criminal responsável pela investigação dos crimes informáticos[6]; Dirigente do SIS[7] (Serviço de Informações de Segurança), que é o organismo responsável pela produção de informações cujo fito passa por garantir a segurança interna, prevenir a sabotagem, o terrorismo, a espionagem, entre outros[8]. Pretende-se, assim, uma conjugação de pontos de vista entre as várias entidades competentes na área estudada.

Tendo em conta que a imprensa é o reflexo da sociedade, já que Cruz (2014) refere que "os jornais são os diários da humanidade, contendo os registros dos principais acontecimentos de cada dia" (p. 3), decidimos analisar recortes de imprensa de OCS nacionais e regionais, através de uma pesquisa na base de dados CISION para podermos identificar os episódios que tiveram lugar em Portugal, bem como para verificar quais os grupos que desenvolvem os ataques. Para isso, foi solicitada autorização ao Departamento de Formação da Direção Nacional da PSP para aceder à conta do MAI da base de dados CISION (ver Apêndice B). Desta forma, realizou-se uma pesquisa pelo termo "*hacktivismo*" e "*hacker*", no período de 1 de janeiro de 2010 a 1 de março de 2015 (ver Apêndice J). A nossa opção deve-se ao facto de 2010 ser considerado o ano a partir do qual o *hacktivismo* começou a ganhar mais relevo. De acordo com Esteves (2012), "o «*hacktivismo*» tornou-se conhecido em finais de 2010, quando o grupo «*Anonymous*» iniciou uma série de ciber-ataques (…) contra grandes corporações que se recusaram a apoiar o *site Wikileaks*" (p. 45).

A informação será tratada através da análise de conteúdo, uma vez que esta "oferece a possibilidade de tratar de forma metódica informações e testemunhos que apresentam um certo grau de profundidade e de complexidade" (Quivy & Campenhoudt, 1998, p. 227). A partir de uma análise exploratória, pretende-se dar resposta aos objetivos específicos traçados (Sarmento, 2013).

[5] Nos termos da al. c) do n.º 1 do Art.º 2.º-A do Decreto-Lei n.º 3/2012, de 16 de janeiro, cuja última alteração foi introduzida pelo Decreto-Lei n.º 69/2014, de 9 de maio.
[6] Conforme previsto na al. l) do n.º 3 do Art.º 7.º da Lei n.º 49/2008, de 27 de agosto.
[7] No que concerne a este entrevistado, o mesmo exigiu o anonimato por motivos profissionais.
[8] Conforme previsto no Art.º 3.º da Lei n.º 9/2007, de 19 de fevereiro.

Capítulo 1 – A Sociedade Atual: uma Sociedade em Rede

1.1. A Evolução da Sociedade e a Inovação Tecnológica

A sociedade encontra-se em constante evolução, sendo que ao longo da História da Humanidade o ser humano, enquanto animal social e político, sempre procurou desenvolver e melhorar os seus mecanismos de comunicação. Essa característica foi abordada por Aristóteles (2000), filósofo grego, que no seu *Tratado da Política* afirma que o ser humano é um animal social por natureza. De facto, a comunicação sempre esteve presente na vida das pessoas, assim como continua a estar em tudo quanto fazemos. Podemos mesmo dizer que a comunicação evoluiu progressivamente ao longo dos anos e foi provocando alterações na sociedade e na forma como as pessoas se relacionam.

A relação entre a tecnologia, o ser humano e a sociedade tem vindo a ser explorada ao longo dos tempos. Neste sentido, podemos identificar três conceções sobre esta relação, nomeadamente a instrumental, a determinista e a construtivista. A conceção instrumental assenta na premissa de que a sociedade controla as tecnologias que cria, uma vez que as desenvolve baseando-se nos seus desejos, necessidades e ambições e para os objetivos por si determinados. Karl Marx, Charles Darwin e Nikolai Kondratiev contribuíram para a sedimentação desta teoria (Dias, 2014).

A perspetiva determinista assenta no pressuposto de que a influência das tecnologias na sociedade é determinante na vida dos indivíduos, podendo provocar consequências devastadoras que estes não têm sequer capacidade para imaginar. Esta perspetiva é defendida por autores como Max Weber, Martin Heidegger, Jacques Ellul, Lewis Mumford e Marshall McLuhan (Dias, 2014).

Por último, a conceção construtivista defende que existe um equilíbrio entre a sociedade e a tecnologia, já que a sociedade controla em parte a tecnologia que cria, sendo, inevitavelmente, afetada por ela. Todavia, é ao ser humano que cabe decidir como pretende ou não fazer uso das novas tecnologias. Foram intelectuais como Herbert Marcuse e Michel Foucault que contribuíram para a construção desta teoria (Dias, 2014).

1.1.1. Revoluções da sociedade

A evolução da comunicação e dos seus meios acompanhou e motivou o desenvolvimento da História tal como a conhecemos. Harold Innis e Marshall McLuhan,

pensadores da Escola de Toronto[9], defendem que a inovação tecnológica é promotora de mudança social (Dias, 2014). Marshall McLuhan realiza uma análise da História da Humanidade dividindo-a em quatro fases, tendo por base três evoluções tecnológicas que considera revolucionárias – a escrita, a imprensa e a eletricidade (Dias, 2014). Rodrigues (2010) apresenta uma evolução semelhante, identificando a existência de quatro revoluções da informação.

A origem da fala, considerada o primeiro sistema de informação a existir, remonta à génese da espécie humana. A primeira revolução da informação surge com a escrita, há cerca de 5000 anos. Para Druncker, a segunda revolução da informação surgiu com a criação do livro escrito, na China por volta de 1300 a.C. e 800 anos depois na Grécia (Rodrigues, 2010). Em meados de 1455, o alemão Johannes Gutenberg cria a prensa de tipos móveis, configurando a terceira revolução da informação. Esta permitia a impressão em massa, transformando de forma indelével a sociedade ocidental, através de maiores fluxos de informação e redução de custos inerentes à produção de publicações, o que permitia difundir a informação por grande parte da população (Rodrigues, 2010).

A partir do século XIX, outro momento marcante foi a revolução industrial, que se deveu em grande medida à utilização da máquina a vapor. Este contexto conduziu ao desenvolvimento de novas tecnologias, sendo que "as comuns comunicações escritas não conseguiram competir com a rapidez da transmissão de mensagens electrónicas, usadas nos meios interactivos da telegrafia e telefonia" (Rodrigues, 2010, p. 13). Na década 20 do século XX, o rádio ganhou protagonismo, sendo anos mais tarde substituído pela televisão. McLuhan refere que o início desta Era se deu com a criação do telégrafo em 1844. Contudo, o meio mais influente durante esta época foi, sem dúvida, a televisão (Dias, 2014).

A quarta revolução da informação inicia-se com a criação do computador, em 1946 nos Estados Unidos da América (EUA). Para Drucker, o computador representa o mesmo na sociedade da informação, do que representou a máquina a vapor durante a revolução industrial (Rodrigues, 2010). No entanto, a quarta revolução da informação não se limita à criação e utilização de computadores, mas prende-se, sobretudo, com a massificação da sua utilização e da capacidade de se interligarem em rede (Rodrigues, 2010). A segunda vaga da revolução informática surge com a *internet* e com a *World Wide Web* (WWW). Nas

[9] Corrente de pensamento sociológico, cuja origem remonta à primeira metade do séc. XX, baseando-se num conjunto de pensadores e intelectuais da Universidade de Toronto, que defendem que a inovação tecnológica é o motor da mudança na sociedade.

palavras de Rodrigues (2010), "a *internet* cresceu a um ritmo impressionante, atingindo uma escala gigantesca, mudando a forma de ver o mundo para sempre e ampliando as possibilidades de uso do computador como fonte de informação e comunicação" (p. 15). A *internet* transformou-se no motor de desenvolvimento da sociedade em rede, permitindo, de forma pioneira, a comunicação de muitos para muitos, num tempo definido e a uma escala planetária (Castells, 2007).

A expansão em larga escala da *internet* durante a última década do séc. XX deve--se, sobretudo, ao surgimento da banda larga e à generalização da utilização de computadores pessoais. Em consequência, houve um aumento desmesurado de informação, com um custo de acesso insignificante e com uma capacidade de alcance virtual mundial, causando novos problemas como os da sobrecarga da informação e da difusão do poder, para os quais nos alerta Nye (2012), quando afirma que " a disseminação da informação significa que o poder será distribuído de forma mais vasta e as redes informais vão minar o monopólio da burocracia tradicional" (p. 138).

No âmbito da ecologia dos *media*[10], Neil Postman e Paul Levision começam a defender uma nova Era, baseada na intensificação dos meios eletrónicos, a denominada Era digital (Dias, 2014).

1.2. A Sociedade em Rede

Criado o primeiro computador, o *Electronic Numerical Integrator Analyzer and Computer* (ENIAC), em 1946, e até à atualidade, as TIC apresentaram uma evolução bastante célere, originando uma mudança radical na forma como as pessoas se relacionam e se relacionarão no futuro, uma vez que todos os dias novas ferramentas tecnológicas surgem, fruto de um mercado cada vez mais competitivo. A este propósito, Castells (2011) refere que "uma revolução tecnológica, centrada nas tecnologias de informação, começou a remodelar, de forma acelerada, a base material da sociedade" (p. 1). Consequentemente, surgiu o conceito de "sociedade em rede", proposto por Manuel Castells, que, segundo este, é marcada pela:

> Convergência de três processos independentes: a revolução da tecnologia da informação; a crise económica do capitalismo e do estatismo e a sua reestruturação;

[10] A ecologia dos *media* é uma corrente de pensamento mais atual, que se inspira na Escola de Toronto.

> o apogeu dos movimentos socioculturais (…). A interacção entre estes processos e as reacções por eles desencadeadas fez surgir uma nova estrutura social dominante, a sociedade em rede, uma nova economia informacional/global, e uma nova cultura, a cultura da virtualidade real. (Castells, 2003, p. 458)

Para Castells (2007), uma rede é "um conjunto de nós interligados" (p. 15). Estas são hoje a base das relações humanas, isto porque a influência da *internet* lhes confere uma nova dimensão, convertendo-as em redes de informação (Castells, 2007).

Segundo Musso (2013), nos dois últimos séculos, as revoluções a que assistimos têm-se traduzido na construção de redes técnicas territoriais: a construção da rede de caminho de ferro (1780-1830), a construção da rede elétrica (1880-1930) e, por último, o aparecimento da *internet*, das telecomunicações e da tecnologia da informação (desde 1960). A rede é uma forma de organização que assume hoje uma importância fundamental:

> Uma nova divindade tende a prevalecer nos dias de hoje, uma divindade técnica, e a *Internet* é apenas uma das suas luminosas aparições: "a Rede". A figura de rede está a tornar-se ubíqua. Tudo é uma rede, ou até mesmo uma "rede de redes". A organização do dia-a-dia torna-se numa constante utilização de redes, uma procura pelo acesso ou conexão a redes elétricas ou eletrónicas, redes de comunicação e informação, redes urbanas, redes de transportes, etc., e encaixadas as suas densas teias cobrem todo o planeta. (Musso, 2013, p. 2)[11]

A organização em rede está associada ao conceito de interdependência verificada entre os nós. Esta característica da sociedade atual traz vantagens, mas também inconvenientes, uma vez que, quando exploradas, as vulnerabilidades de um nó da rede podem provocar consequências que facilmente se alastram, influenciando outros nós que à partida não se encontrariam vulneráveis.

As estruturas da sociedade revelam uma dependência relativamente às TIC, sendo que os serviços modernos se caracterizam pela utilização do interconectado método de produção, ou seja, todos dependem de uma infraestrutura de comunicação baseada na *internet*. De acordo com Castells (2011), "no novo modo informacional de

[11] Tradução livre da autora.

desenvolvimento, a fonte de produtividade encontra-se na tecnologia de produção de conhecimentos, de processamento de informação e de comunicação de símbolos" (p. 20).

A sociedade em rede é também caracterizada por uma mutação dos conceitos de tempo e espaço. Embora as teorias clássicas apontem para o facto de o tempo controlar o espaço, Castells (2011) refere que, na sociedade estabelecida em rede, o espaço domina o tempo: "o espaço de lugares múltiplos, espalhados, fragmentados e desconexos, exibe temporalidades diversas, desde o domínio mais primitivo dos ritmos naturais até à estrita tirania do tempo cronológico" (p. 601). Existe uma crescente interdependência entre organismos, instituições e pessoas, relacionada com a maior velocidade de fluxo comunicacional e informacional que, perante a ausência de fronteiras, não deixa espaço ou tempo para a análise do mesmo, provocando "um novo sentimento no homem que terminará por agir e operar no seio de um ambiente a uma velocidade superior àquela a que no passado se submetia" (Martins, 2012, p. 34). De facto, a utilização das TIC permite-nos vencer quer a distância, quer o tempo, alterando de forma indelével a nossa sociedade.

O processo de relacionamento cibernético distingue-se do relacionamento do mundo físico, uma vez que produz "a edificação de um imaginário com consequências reais e por vezes nefastas no mundo concreto" (Martins, 2012, p. 35), o que direta ou indiretamente irá condicionar o ser humano, esteja ou não integrado neste novo domínio da sociedade. Neste sentido, embora estejamos a falar de um mundo virtual, é preciso considerar a probabilidade de haver consequências prejudiciais no mundo físico, o que reforça a exigência de garantir a segurança no ciberespaço.

A sociedade está constantemente a aumentar a rede na qual se encontra alicerçada, sendo prova disso o aumento considerável do número de dispositivos a partir dos quais podemos aceder à *internet*, principalmente dos dispositivos móveis, como é o caso dos *smartphones* e *tablets*. Atualmente, discute-se o fenómeno da *Internet* das Coisas (*Internet of Everything* – IoE), um conceito criado no início do terceiro milénio por Kevin Ashton (2009). Se todos os nossos objetos pessoais estivessem ligados em rede, pudessem comunicar uns com os outros e ser ativados e geridos por meio informático isso iria poupar trabalho e tempo. De acordo com Ashton (2009), "precisamos de capacitar os computadores com os seus próprios meios de recolha de informação, para que eles possam ver, ouvir e cheirar o mundo por si mesmos, em toda sua glória aleatória" (para. 5).

A média de crescimento do número de utilizadores da *internet* tem aumentado mais de 300% por ano, desde a primeira década do séc. XXI, apresentando, em 2011, um total

de 2,2 biliões de utilizadores (Fernandes, 2014). Segundo a recente avaliação do Eurostat de 2014[12] acerca da utilização das TIC, foi possível apurar que a grande maioria dos europeus utiliza a *internet*. Contudo, importa referir que 18% dos mesmos nunca a utilizou[13] (Seybert & Reinecke, 2014). A Agenda Digital para a Europa[14] traçou o objetivo de aumentar a percentagem de pessoas que usam a *internet* regularmente (média de uma vez por semana) para 75% em 2015. Todavia, em 2013 a percentagem era já de 73% e estima-se que a meta seja atingida um ano antes do expectável. A média europeia de pessoas que utiliza a *internet* todos os dias ou quase todos os dias é de 68%, enquanto em Portugal o valor aponta para os 51% (Eurostat, 2014). O aumento do número de utilizadores da *internet* tem vindo a verificar-se, tendo apresentado um ritmo maior do que o esperado, o que fortalece a ideia de que o ciberespaço assume, cada vez mais, um papel relevante na vida das pessoas.

1.3. Ciberespaço

A sociedade em rede desenrola-se num novo espaço paralelo ao mundo físico – o ciberespaço. Este termo foi utilizado, pela primeira vez, em 1984 pelo escritor William Gibson na sua obra de ficção científica *Neuromancer* (Thill, 2011). Gibson descreveu de forma bastante próxima a nossa realidade atual. Contudo, convém relembrar que nessa altura a criação da *internet* era ainda bastante prematura, o que confere à sua obra maior admiração e interesse.

O ciberespaço é um novo ambiente onde as pessoas se relacionam e comunicam. Nesta nova dimensão realizam-se negócios, partilham-se experiências, constroem-se novas amizades, expressam-se opiniões e reflexões, entre outros aspetos que fazem parte integrante do nosso quotidiano. Para Fernandes (2012), pode considerar-se que o termo ciberespaço é "a rede global de infraestruturas de tecnologias de informação interligadas entre si, especialmente as redes de telecomunicações e os sistemas de processamento dos

[12] Esta avaliação relativa ao ano de 2013 é baseada nos resultados das respostas de um total de 150 427 agregados familiares, constituídos pelo menos por uma pessoa com idade entre os 16 e 74 anos, e 211 325 indivíduos de idade compreendida entre os 16 e os 74 anos da UE.

[13] O indicador relativo ao número de pessoas que nunca utilizaram a *internet* encontra o seu valor máximo na Roménia (39%), Bulgária (37%), Grécia (33%), Itália (32%) e Portugal (30%). Por outro lado, a Dinamarca, o Luxemburgo e os Países Baixos, apresentam valores de 3%, 4% e 5%, respetivamente (Seybert & Reinecke, 2014).

[14] A Agenda Digital para a Europa é uma das iniciativas da estratégia Europa 2020 que tem como objetivo a definição de um mercado único digital, de forma a daí retirar benefícios económicos e sociais sustentáveis. Sugere-se também a consulta de COM (2010) 245 final, sobre a Agenda Digital para a Europa, e da COM (2010) 2020, sobre a Estratégia para um crescimento inteligente, sustentável e inclusivo.

computadores" (p. 12). Todavia, o mesmo autor refere que de forma abrangente ciberespaço indica, hoje, algo relacionado com a *internet* ou ligado às suas práticas culturais e sociais.

Para Freire e Caldas (2013) o ciberespaço integra "inúmeros computadores interconectados, servidores, *routers, switches* e cabos mas é este emaranhado tecnológico que serve de suporte, tecnologicamente, às infraestruturas críticas (….) e a muitos serviços críticos" (p. 90).

Freire e Caldas (2013) defendem a existência de dois modelos que caracterizam o ciberespaço, um que inclui as infraestruturas e outro que as exclui. Num deles, é considerado como um local abstrato, onde as relações humanas acontecem, enquanto no modelo inclusivo o ciberespaço compreende várias camadas sobrepostas. Relativamente a este último, Libicki (2009) apresenta uma perspetiva de ciberespaço assente num modelo de três camadas: a física, a sintática e a semântica. A primeira camada corresponde ao *hardware*, ou seja, a parte física das TIC, considerado o suporte do ciberespaço. A camada sintática diz respeito ao *software* e protocolos que regulam o funcionamento de sistemas de computadores e redes. A camada semântica diz respeito à informação trocada, armazenada e processada pelo ser humano nos sistemas de computadores e redes.

O ciberespaço pode ser caracterizado como um espaço dinâmico, uma vez que está em constante evolução e as mudanças são frequentes e, muitas vezes, imprevisíveis. O acesso ao mesmo tem um custo irrelevante, pelo que está acessível à grande maioria da população. Tendo apenas por base as características indicadas, podemos verificar que o potencial deste espaço é enorme e o seu crescimento é constante, visto que surgem diariamente novas funcionalidades, assim como a velocidade de troca de informação aumenta constantemente[15]. Associada a esta elevada potencialidade está a vasta capacidade de processamento (procura, processamento e armazenamento de informação), bem como o caráter assimétrico (recursos e conhecimentos necessários). Uma característica deste espaço é o anonimato, já que é difícil determinar a identidade dos utilizadores. O facto de o ciberespaço estar estabelecido em rede permite que um elemento afetado contamine os

[15] A este respeito importa referir o recente fenómeno designado *appification*, ou seja, a utilização massiva de aplicações *mobile*, debatido na terceira edição da conferência *Privacidade, Inovação e Internet*, no dia 30 de janeiro de 2015. De acordo com Clara Guerra, consultora coordenadora da Comissão Nacional de Proteção de Dados, o fenómeno da *appification* deverá ser encarado como uma oportunidade, mas também como um desafio. Para aprofundar o tema sugere-se a consulta de http://www.apdsi.pt/index.php/news/871/191/3-Conferencia-Privacidade-Inovacao-e-Internet.html (consultado em 15 de fevereiro de 2015). Ainda sobre este tema, ver Anderson, C. & Wolff, M. (2010) *The Web Is Dead. Long Live the Internet*, que aborda a crescente substituição da WWW pelas aplicações.

restantes elementos da rede, enfatizando o caráter transversal e interdependente (Freire, Nunes, Acosta, & Rojas, 2013).

As potencialidades deste novo espaço são inimagináveis, pois permitem uma maior partilha de conhecimento e informação, encurtando as distâncias e incrementando a economia. Em contrapartida, podemos identificar um número idêntico de vulnerabilidades, relacionadas, sobretudo, com a dependência criada nas pessoas em torno da *internet* e das TIC, que origina uma excessiva utilização dos meios tecnológicos, potenciando o surgimento de novos perigos e ameaças, que possibilitam a exploração das vulnerabilidades dos sistemas informáticos. Como nos indica Castells (2011), "as actividades criminosas (…) também se tornaram globais e informacionais, propiciando os meios para estimular a hiperactividade mental e os desejos proibidos" (p. 2). Segundo Fernandes (2012), "a própria difusão da *internet* e a digitalização da economia geram novas dependências, vulnerabilidades e riscos: o mais óbvio é o da possibilidade de ciberataques a organismos públicos ou empresas privadas ou até de uma ciberguerra envolvendo, directa ou indirectamente, atores estaduais" (p. 17).

1.3.1. Soberania no ciberespaço

Na atualidade, tudo gira em torno da *internet* e sistemas da informação, em virtude de serem estes que acrescentam valor a empresas e organizações, apesar de também evidenciarem vulnerabilidades e atraírem ameaças. Neste sentido, Freire e Caldas (2013) afirmam que o ciberespaço constitui o "sistema «nervoso» de controlo de um país" (p. 90). As características do ciberespaço, anteriormente descritas, nomeadamente no que concerne à sua dimensão e à ausência de fronteiras, criam dificuldades ao Estado no exercício do seu poder soberano, já que se verifica "uma falta de perceção sobre a natureza e limites do ciberespaço, caracterizado pela indefinição de fronteiras tais como se conhecem na sua expressão física ou geográfica" (Freire et al., 2013, p. 16). De acordo com Nye (2012), o principal problema desta "era da informação global é que a maior parte das coisas está a acontecer fora de controlo, até mesmo dos estados mais poderosos" (p. 135).

A Era digital é marcada por uma utopia libertário-anárquica, segundo a qual o Estado não deveria intervir no ciberespaço, nem deteria qualquer poder no mesmo, devendo manter-se afastado deste (Fernandes, 2012). Esta teoria vai ao encontro de *Uma*

declaração de independência do ciberespaço[16], um manifesto de 1996, da autoria de John Parry Barlow. Neste manifesto, Barlow alude à liberdade do ciberespaço, defendendo a ausência do exercício de poder do Estado dentro deste mundo virtual. Para Barlow, a *internet* é "um espaço promissor de realização da utopia libertária, vendo a possibilidade de emergir no ciberespaço um «homem novo» e uma «civilização nova» à margem da «tirania» dos Governos" (Fernandes, 2012, p. 16). Contudo, não parece sensato haver uma certa ausência de regras, onde tudo é permitido, como se defendia nos primeiros anos da *internet*. A nossa sociedade passou a alicerçar-se nas TIC e, consequentemente, isso implica a existência de normas no ciberespaço de maneira a assegurar direitos, liberdades e garantias das pessoas, bem como a garantir a segurança das infraestruturas vitais da sociedade e das suas organizações.

É de salientar que o ideal de liberdade da *internet* e a ausência de intervenção do Estado não é uma imposição da tecnologia, mas sim fruto dos princípios inerentes às democracias ocidentais. Uma prova disso é o caso da "Grande *Firewall* da China", que o país tem utilizado internamente, com o objetivo de controlar e bloquear conteúdos considerados sensíveis (Fernandes, 2012). A opção ocidental referente à utilização da *internet*, como um espaço de liberdade, é uma opção social e política, não dependente da inevitabilidade inerente à tecnologia. Ou seja, o controlo ou não da *internet*, por parte das autoridades governamentais, depende de uma opção política, em concordância com o regime vigente em determinado Estado (Goldsmith & Wu, 2006, citado por Fernandes, 2012). Contudo, como afirma Cardoso (2014), continua a persistir alguma incerteza sobre a melhor forma de regular a *internet*, conciliando essa normalização com os interesses dos cidadãos.

O domínio das TIC, onde se insere a *internet*, é hoje considerado uma capacidade estratégica dos Estados, o que leva a Organização do Tratado do Atlântico Norte (OTAN)[17] a eleger o ciberespaço como um novo "*global common*"[18] – que, de acordo com Barry Posen (2003) são áreas que não pertencem a nenhum Estado, mas que permitem o acesso a grande parte do planeta – para além das tradicionais águas internacionais, do espaço aéreo internacional e do espaço exterior. Demchak e Dombrowski (2011) referem que se

[16] Disponível em https://projects.eff.org/~barlow/Declaration-Final.html (consultado em 15 de fevereiro de 2015).
[17] Na Cimeira de Lisboa da OTAN, em 2010, é feita a última revisão do seu Conceito Estratégico, passando a englobar as preocupações com as ciberameaças e os ciberataques. Para mais informação, aconselha-se a leitura do documento, disponível em http://www.nato.int/strategic-concept/pdf/Strat_Concept_web_en.pdf.
[18] Disponível em http://www.act.nato.int/globalcommons (consultado em 15 de fevereiro de 2015).

encontra em desenvolvimento uma tendência para os Estados afirmarem o seu poder soberano no ciberespaço, que consideram tratar-se de "uma tendência necessária e desejável" (p. 40). Os mesmos argumentam, ainda, que "uma ciberfronteira nacional é tecnologicamente possível, psicologicamente confortável, sendo também sistematicamente e politicamente gerível" (Demchak & Dombrowski, 2011, p. 40).

Nos dias de hoje, em que a competitividade da sociedade vê a grande quantidade de informação, trocada a uma velocidade elevada, como uma vantagem estratégica, devemos considerar também o fator da segurança como indispensável para assegurar a capacidade estratégica dos vários setores envolvidos. Desta forma, podemos considerar que "o ciberespaço constitui uma dimensão crítica do funcionamento normal da sociedade moderna, da sua segurança, da sua economia, dos seus negócios, etc." (Freire et al., 2013, p. 10).

Os líderes políticos, em concreto, vão ter de alargar a sua interpretação, pois a principal premissa da *internet* é a expansão do saber ao nível mundial e o "poder de influência localizar-se-á gradualmente no ciberespaço, onde o destino do mundo se irá concretizar através de quem detiver a capacidade de dominar a rede virtual" (Martins, 2012, p. 35). Este poder, definido por Nye (2012) como ciberpoder, consiste na "capacidade de obter resultados desejados através do uso de recursos informativos do ciberdomínio interligados a nível eletrónico" (p. 145). A difusão da informação significa que o poder vai ser distribuído e possivelmente as redes informais vão substituir "o monopólio da burocracia tradicional" (Nye, 2012, p. 138).

Capítulo 2 – A Segurança no Ciberespaço

No presente capítulo desenvolvemos a temática da segurança no ciberespaço. A utilização em massa das TIC originou o surgimento de novos fenómenos criminais – p. e. o acesso ilegítimo e a sabotagem informática – e promoveu a deslocação dos crimes tradicionais para o ciberespaço, como é o caso do crime de injúrias.

De acordo com Nunes (2012), a dependência relativamente ao ciberespaço de praticamente todos os domínios da vida "conduz ao surgimento de vulnerabilidades que têm de ser cuidadosamente analisadas e, se possível, solucionadas ou reduzidas" (p. 125). Neste seguimento, Nye (2012) refere que a *internet* foi criada para ser facilmente utilizada e não para a segurança, pelo que atualmente "a ofensiva tem vantagem sobre a defesa" (p. 147). Para contrariar a evolução destes novos fenómenos têm vindo a ser desenvolvidas estratégias, medidas e iniciativas que promovem a segurança no ciberespaço.

A OTAN[19], a Organização das Nações Unidas (ONU) e a *International Telecommunications Union* (ITU)[20] estão entre as organizações internacionais que se preocupam e têm contribuído para a construção de uma cultura relacionada com a cibersegurança. Contudo, no presente capítulo optámos somente por abordar o contexto europeu e nacional.

2.1. Cibercriminalidade

A cibercriminalidade, como o próprio nome nos indica, relaciona-se com a ocorrência de fenómenos criminais no contexto do ciberespaço, desenvolvidos através de meios informáticos. Ora, aqui incluem-se os crimes ditos tradicionais, mas também os novos crimes informáticos, que surgiram como consequência do uso das novas tecnologias e da *internet*. Uma vez que o termo cibercriminalidade não encontra definição legal no sistema jurídico português, recorremos à definição presente na Estratégia da União Europeia para a Cibersegurança (2013)[21]:

[19] Sobre as medidas tomadas pela OTAN, no âmbito da cibersegurança, consultar: http://www.nato.int/cps/en/natohq/ topics_78170.htm?selectedLocale=en (consultado em 28 de fevereiro de 2015).
[20] Para mais informação, consultar http://www.itu.int/en/action/cybersecurity/Pages/default.aspx (consultado em 28 de fevereiro de 2015).
[21] Aconselha-se a consulta de JOIN (2013) 1 final, sobre a Estratégia da União Europeia para a cibersegurança.

> A cibercriminalidade refere-se, geralmente, a um amplo leque de diferentes atividades criminosas que envolvem os computadores e os sistemas informáticos, quer como instrumentos quer como alvos principais. A cibercriminalidade inclui as infrações tradicionais, infrações relativas aos conteúdos e crimes respeitantes exclusivamente a computadores e sistemas informáticos. (p. 3)

A criminalidade respeitante somente a computadores e sistemas informáticos, ou seja, o crime informático, é a grande novidade, pois compreende um leque de tipos criminais que surgiram após a expansão das TIC. O crime informático encontra-se estatuído na Lei do Cibercrime, aprovada pela Lei n.º 109/2009, de 15 de setembro, sendo os crimes previstos os seguintes: falsidade informática (Art.º 3.º), dano relativo a programas ou outros dados informáticos (Art.º4.º), sabotagem informática (Art.º 5.º), acesso ilegítimo (Art.º 6.º), interceção ilegítima (Art.º 7.º) e reprodução ilegítima de programa protegido (Art.º 8.º).

O cibercrime é um fenómeno transnacional, sendo que o relatório do *European Police Office* (2014) refere que os ataques têm origem maioritariamente no exterior da UE. Esta transnacionalidade impõe uma maior coordenação e colaboração entre os Estados e as entidades com competência no âmbito da cibersegurança. Neste aspeto, podemos mencionar a Convenção do Cibercrime do Conselho da Europa como um importante passo na resposta à transnacionalidade do fenómeno, através da uniformização dos normativos legais no âmbito do cibercrime. A referida Convenção, transposta para o ordenamento jurídico português através da Lei do Cibercrime, foi assinada em Budapeste no ano de 2001 e prevê um conjunto de linhas jurídicas comuns a serem adotadas pelos Estados Membros (EM) no âmbito da cibercriminalidade. Nesta convenção é estabelecido um conjunto de infrações, nomeadamente contra a confidencialidade, integridade e disponibilidade de sistemas informáticos e dados informáticos (o acesso ilegítimo, a interceção ilegítima, a interferência em dados, a interferência em sistemas e o uso abusivo de dispositivos). Também nos refere infrações relacionadas com computadores (falsidade informática e burla informática), com o conteúdo (pornografia infantil) e com a violação de direitos de autor e direitos conexos.

O cibercrime está a crescer e a desenvolver-se em termos de dimensão e impacto, verificando-se uma maior sofisticação dos ataques, associada a um maior número e tipos

de ciberataques. Simultaneamente, o número de vítimas é cada vez maior e o prejuízo económico é evidente, de acordo com o European Cybercrime Centre (EC3)[22].

Como indica o relatório do *European Police Office* (2014):

> O advento da *Internet* das Coisas (IoE) combinado com o número crescente de utilizadores da *internet* cria globalmente uma plataforma alargada de ataque, novos vetores de ataque e mais pontos de entrada, incluindo métodos de engenharia social[23], para criminosos explorarem, tornando os terminais de segurança ainda mais importantes. (p. 11)

O novo fenómeno da IoE coloca novos desafios de segurança, uma vez que o cibercrime possivelmente também se irá expandir. Apesar da preocupação crescente face à cibercriminalidade, a regulação deste novo espaço ainda se encontra pouco desenvolvida, devido não só à prematuridade da temática, como à constante evolução das TIC, o que exige um acompanhamento permanente. Para Martins (2012), a realidade "leva-nos a observar o ciberespaço como um local não somente virtual e físico mas isento de regulamentação jurídica, onde os mais diversos crimes se podem manifestar" (p. 36).

Qualquer pessoa pode praticar factos ilícitos através de meios informáticos, que provocam resultados em qualquer parte do mundo virtual, o que "dificulta e muito determinar com exatidão o local onde foram praticados os factos ilícitos, quem os praticou e qual a Lei Penal e processual aplicável ao caso" (Simas, 2014, p. 27). O relatório do *European Police Office* (2014) indica a *anonymisation* como um fator para o crescimento do cibercrime, no sentido em que existem cada vez mais técnicas que permitem esconder a identidade. Assim, existem grandes dificuldades em identificar os suspeitos da prática de factos ilícitos no ciberespaço, o que em certa medida potencia a propagação da cibercriminalidade.

O *crime-as-a-service* é um fenómeno que também merece alguma preocupação. Trata-se de um modelo de negócio que disponibiliza e fornece serviços especializados em quase todo o tipo de cibercrime. Os grupos de criminalidade organizada tradicionais

[22] Disponível em https://www.europol.europa.eu/ec/cybercrime-growing (consultado em 1 de fevereiro de 2015).

[23] Estes métodos dizem respeito ao estudo dos alvos de maneira a apurar-se qual a melhor forma de atrair a confiança dos mesmos para conseguir determinado objetivo, que de outra forma não seria possível alcançar.

começam a recorrer a estes serviços, de maneira que no futuro se prevê uma maior sofisticação do tipo de crimes praticados (*European Police Office*, 2014).

2.2. Cibersegurança e Ciberdefesa

No passado, os conceitos de segurança e defesa encontravam-se bem definidos, sendo que a maioria dos Estados traçava uma linha bem demarcada de separação entre segurança interna e externa, tendo por fator diferenciador os perigos e ameaças que surgem dentro das fronteiras e os que advêm do exterior das mesmas, de forma que caberia às polícias e aos militares fazer-lhes face, respetivamente (Guedes & Elias, 2010). Apesar de existirem autores que contestam atualmente esta conceção, a verdade é que a grande maioria dos Estados continua a fazer uma distinção legal entre segurança e defesa. O caso português é um bom exemplo desta opção, que consagra na sua Constituição da República a segurança interna[24] e a defesa nacional[25], no sentido em que à primeira cabe garantir a segurança dentro de fronteiras e à segunda caberá impedir que as ameaças externas afetem o nosso país.

Atualmente, apesar da separação clássica entre segurança e defesa ainda predominar, os limites e áreas de atuação respeitantes à segurança interna e à defesa nacional confundem-se cada vez mais. Fernandes (2014) refere a este propósito que:

> A clássica manutenção da segurança e da ordem, ainda uma função central das forças e serviços de segurança, associada por natureza à defesa de um território perfeitamente definido, tende cada vez mais a ser substituída por uma manutenção da segurança desterritorializada. (p. 11)

O conceito de segurança assume, atualmente, novos contornos, tratando-se de um conceito passível de ser alterado com a evolução da sociedade, pois "a força gravitacional do espaço e do tempo impõe ajustes inerentes à volatilidade dos factores políticos, económicos e jurídicos conjugados com o contexto social e cultural" (Valente, 2013, p.

[24] O n.º 1, do Art.º 272.º da CRP refere que a Segurança Interna é garantida pela Polícia. Simultaneamente, o Art.º 1.º da Lei n.º 53/2008, de 29 de agosto, que aprova a Lei de Segurança Interna, define segurança interna como "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".

[25] O n.º 2, do Art.º 273.º da CRP refere que a "defesa nacional tem por objetivos garantir, no respeito da ordem constitucional, das instituições democráticas e das convenções internacionais, a independência nacional, a integridade do território e a liberdade e a segurança das populações contra qualquer agressão ou ameaça externas". O n.º 1, do Art.º 275.º da CRP refere que compete às Forças Armadas a defesa militar da República.

115). Os Estados modernos "tornaram-se demasiado pequenos para resolver os grandes problemas e demasiado grandes para resolver os pequenos" (Bell, 2000, citado por Elias, 2015, p. 5), ou seja, por um lado, assiste-se a uma delegação cada vez maior, por parte dos Estados, de competências ao nível da segurança noutras entidades públicas e privadas, por outro lado, há questões para as quais não encontramos resposta no seio de um Estado, assumindo destaque as entidades supranacionais. De acordo com Guedes e Elias (2010), "o conceito de «segurança» abarca agora a actuação e o empenhamento de instituições públicas mas e também de privadas, da sociedade local e da sociedade civil num sentido mais amplo" (p. 28). Se antes a segurança era uma competência do Estado, hoje em dia assistimos cada vez mais à sua privatização. Para além de haver um número crescente de instituições a oferecer serviços de segurança, temos também de considerar que muitas das Infraestruturas Críticas (IC), como o sistema da água ou da energia, dependem do setor privado, logo cabe a estes também assumir um papel ativo na demanda da cibersegurança (Bendiek, 2012).

Os problemas relacionados com a segurança tornaram-se globais e interdependentes, o que cria urgência na definição de soluções também elas globalizadas e interligadas (Fernandes, 2014). Face a estes problemas, os Estados veem-se numa situação de impotência, pelo que são obrigados a "integrarem alianças ou organizações internacionais para garantirem a sua própria segurança, pois não têm capacidade para, por si próprios, prevenir ou combater determinados fenómenos de origem externa ou interna" (Elias, 2015, p. 5).

A nova organização da sociedade coloca em evidência o crescente desaparecimento das fronteiras e, como tal, a dificuldade em definir aquilo que é externo e interno. Como é referido por Guedes e Elias (2010), "não mais fazem sentido as tradicionais e rígidas distinções conceptuais entre segurança interna e externa (…) uma não pode deixar de ser pensada e executada sem a outra" (p. 8). No mesmo sentido, Bigo (2001) considera que os conceitos de segurança interna e externa se aproximam cada vez mais, apontando fatores como a globalização, o fim do mundo bipolar e as migrações através das fronteiras como responsáveis por esta "fusão". Outro aspeto que torna os tradicionais conceitos de segurança e defesa mais próximos é a transnacionalidade das ameaças e dos riscos, que cada vez mais são partilhados (Fernandes, 2014). Bigo (2001) refere, ainda, que a teoria de que as polícias e o exército partilham os mesmos inimigos ganha cada vez mais apoio:

> Os limites das tarefas da segurança não são definidos através de uma clara opinião do que a segurança é (e do que não é). Eles não sabem onde é que a parte externa acaba e onde é que começa. Eles não sabem onde é que a segurança começa e onde a insegurança acaba. Como numa fita de Möbius, o interno e o externo estão intimamente ligados. (Bigo, 2001, p. 12)

Tal como no mundo físico, no ciberespaço torna-se complexo definirmos o que é cibersegurança e ciberdefesa e, neste âmbito, a linha que separa aquilo que é interno do que é externo é praticamente inexistente. O ciberespaço tem uma dimensão planetária e não conhece fronteiras, pelo menos no mundo ocidental. Contudo, Demchak e Dombrowski (2011) defendem que a existência de fronteiras virtuais no ciberespaço tornaria possível analisar esta questão com maior clareza.

Enquanto o conceito tradicional de segurança aponta no sentido das ameaças externas serem da competência da defesa e as internas da competência da segurança, no mundo virtual é bastante complicado verificar qual a origem das ameaças e, portanto, definir competências com esta base. Freire e Caldas (2013) referem que "delinquentes, *hackers*, terroristas ou Estados estarão decerto algures por detrás de um ciberataque mas não se pode determinar com exatidão se será uma questão de segurança ou assunto militar" (p. 91).

A cibersegurança pode ser definida, de acordo com a Estratégia da União Europeia para a cibersegurança (2013)[26], da seguinte forma:

> Precauções e ações que podem ser utilizadas para proteger o ciberespaço, tanto nos domínios civil como militar, contra ameaças decorrentes da independência das suas redes e infraestruturas informáticas ou que as possam danificar. A cibersegurança procura manter a disponibilidade e a integridade das redes e infraestruturas e a confidencialidade das informações nelas contidas. (p. 3)

Podemos então deduzir que a definição de cibersegurança da UE abarca o domínio civil e militar. Freire et al. (2013) apresenta-nos a definição de ciberdefesa como o conjunto de medidas de segurança destinadas a proteger as infraestruturas TIC contra

[26] Consultar JOIN (2013) 1 final, sobre a Estratégia da União Europeia para a cibersegurança.

ciberataques, que assumem forma de guerra cibernética, uma vez que se destina a perturbar os sistemas informáticos do adversário, sendo acompanhados de ataque de natureza física ou não.

De acordo com Bendiek (2012), a política de cibersegurança europeia deve ser estruturada a nível global e incluindo os vários *stakeholders*[27]. No entanto, isto coloca três principais problemas para os Governos democráticos, designadamente a dificuldade em delimitar o que é interno e o que é externo, a securitização (ou seja, prevalência das medidas de segurança face à liberdade) e a privatização da governação.

2.3. Cibersegurança na Europa

Hoje em dia, a economia prospera na mesma medida em que existe desenvolvimento e inovação tecnológica. A intensificação das TIC incrementa as ameaças e fragilidades dos sistemas informáticos, o que faz aumentar os números relativos ao cibercrime[28]. De acordo com a Comissão Europeia (2014), "a Europa está a atrasar-se em relação a outros países no que respeita às redes digitais rápidas, fiáveis e interligadas que sustentam a economia e estão presentes em todos os aspetos da nossa vida profissional e privada" (p. 3).

A Agenda Digital para a Europa, uma das iniciativas da Europa 2020, tem como objetivo estimular a economia europeia aproveitando os benefícios económicos e sociais sustentáveis decorrentes de um mercado único digital "para os negócios, para o trabalho, para o lazer, para a comunicação e para a expressão livre das nossas ideias" (p. 3)[29].

Podemos depreender, então, que o desenvolvimento do ciberespaço, como espaço social, político e económico é um objetivo da UE, de forma que é necessário garantir a segurança do ciberespaço para que o seu propósito seja cumprido. Neste sentido, a UE, desde o início do século XXI, mostra preocupação em desenvolver esforços no sentido de promover a cibersegurança.

A UE encara o tema da cibersegurança de uma perspetiva dualista. Por um lado, encoraja o setor privado a participar no processo, e, por outro, quando o problema assume contornos que colocam em causa a segurança nacional, é o Estado que tem o papel

[27] Parceiros ou partes interessadas.
[28] De acordo com o *site* oficial do EC3, um relatório recente sugere que o cibercrime provoca uma perda de 290 biliões de euros para as vítimas, no mundo, todos os anos, tornando o cibercrime mais rentável que o tráfico de droga mundial de marijuana, cocaína e heroína combinadas. Informação disponível em https://www.europol.europa.eu/ec/cybercrime-growing (consultado em 31 de janeiro de 2015).
[29] COM (2010) 245 final, sobre a Agenda Digital para a Europa.

principal. Uma característica da política de cibersegurança na UE é a pluralidade de atores envolvidos, que revela a natureza dinâmica da problemática, mas também a falta de clareza na delimitação de áreas de responsabilidade entre as instituições que tomam parte. Na prática, a UE apresenta uma política de cibersegurança assente num modelo *multi-stakeholder,* onde qualquer grupo especializado ou entidade estatal pode participar no processo político (Bendiek, 2012).

A cibersegurança é identificada, no Relatório de 2008 sobre a Execução da Estratégia Europeia de Segurança, como um dos principais desafios globais. Este relatório aponta também no sentido das economias modernas se encontrarem numa situação de dependência crescente face a IC, entre as quais a *internet*. Perante o exposto, é fácil perceber que uma maior dependência e interligação entre a sociedade e as TIC, associadas à proliferação de condutas ilícitas, requerem por parte da UE e dos EM novas medidas de segurança. Deste modo, têm sido feitos alguns esforços no sentido de promover a cibersegurança na UE. Concretamente, organismos como a Agência Europeia de Segurança de Redes e da Informação (ENISA)[30] e o EC3[31] têm desenvolvido alguns contributos no âmbito da cibersegurança.

A ENISA, criada em 2004[32], iniciou a sua atividade em 2005 com o objetivo de incrementar a segurança das redes e informações, tendo vindo a desempenhar um importante papel no âmbito da cibersegurança. Esta instituição tem desenvolvido a cooperação entre as diversas entidades na área da cibersegurança, facilitando a troca de informação e promovendo a partilha de boas práticas, tendo também um importante papel na sensibilização e formação na área da cibersegurança (Santos, 2014).

Uma nova instituição que tem garantido um importante contributo é o EC3, que é uma das mais recentes iniciativas da UE na luta contra o cibercrime. Este novo centro começou a funcionar em 2013, na sede da Europol (Serviço Europeu de Polícia), em Haia. Esta instituição pretende coordenar uma resposta concreta para a cibercriminalidade, constituindo-se como o ponto de informação ao nível do cibercrime, e garantir apoio e suporte aos EM.

---

[30] Para mais informação, consultar o *site* da ENISA: http://www.enisa.europa.eu/ (consultado em 15 de fevereiro de 2015).
[31] Para mais informação, consultar o *site* do EC3: https://www.europol.europa.eu/ec3 (consultado em 15 de fevereiro de 2015).
[32] Regulamento n.º 460/2004 do Parlamento Europeu e do Conselho.

Em 2001, é publicada uma Comunicação[33] acerca da segurança das redes e da informação, tendo como fito a proposta para uma abordagem de política europeia. Entre outras coisas, é realizada uma caracterização das ameaças à segurança no ciberespaço. Esta Comunicação define segurança das redes e da informação como "a capacidade de uma rede ou sistema da informação para resistir, com um dado nível de confiança, a eventos acidentais ou acções maliciosas" (p. 3). Os eventos e ações maliciosos referidos podem comprometer a disponibilidade, autenticidade, integridade e confidencialidade da informação armazenada ou transmitida, ou seja, um incidente de segurança informático poderá colocar em causa os princípios básicos da segurança da informação.

De acordo com a Comunicação suprarreferida, estes eventos maliciosos estão relacionados com interceção das comunicações, com o acesso não autorizado a computadores e redes informáticas, com perturbações do funcionamento da rede, com a utilização de *software* malicioso que altera ou destrói dados, com a possibilidade da falsa identificação maliciosa e de eventos ambientais e não intencionais.

Em 2006, é publicada uma Comunicação[34] que desenvolve a anterior, no sentido em que promove o diálogo, as parcerias e um maior poder de intervenção como essenciais para o desenvolvimento da segurança das redes e da informação. A segurança das redes e da informação depende do contributo de todos os interessados, nomeadamente da Administração Pública, de empresas e de utilizadores finais. É ressalvado, contudo, que o papel da Administração Pública será não só proteger a informação do setor público, mas também ser o exemplo a seguir, em termos de boas práticas.

Em 2009, desenvolvem-se mecanismos para a segurança e resiliência das IC de informação, através de uma Comunicação[35] que alerta para o facto das infraestruturas, serviços e redes TIC assumirem uma função indispensável para a economia e sociedade, bem como para o facto de estas serem utilizadas muitas vezes por outras IC. Nesta Comunicação, as infraestruturas, serviços e redes TIC são consideradas uma IC de Informação, uma vez que a sua perturbação ou destruição produziria um impacto grave nas funções vitais da sociedade (energia, transportes, saúde, segurança, entre outras). Neste sentido, é dado destaque aos ciberataques realizados às infraestruturas, redes e sistemas de informação, bem como a soluções relativas à resiliência dos mesmos.

---

[33] Consultar COM (2001) 298 final, sobre Segurança das redes e da informação.
[34] Consultar COM (2006) 251 final, sobre a Estratégia para uma sociedade da informação segura.
[35] Consultar COM (2009) 149 final, sobre proteção de IC de informação.

No mesmo ano de 2009, aquando da publicação do Programa de Estocolmo, um programa plurianual para o período de 2010 a 2014, a criminalidade informática foi considerada como prioridade política. Nos últimos anos é possível verificar que os desenvolvimentos são constantes, fruto de um enorme esforço, exigido pela rápida evolução do cibercrime.

A crescente preocupação da UE para com esta problemática traduziu-se, em 2013, na publicação de uma Estratégia da União Europeia para a Cibersegurança[36]. Segundo este documento estratégico, "a *internet* sem fronteiras e multicamadas tornou-se um dos mais poderosos instrumentos de progresso a nível mundial sem supervisão ou regulamentação governamental" (p. 3). Esta escassez ao nível da supervisão e regulamentação é extremamente perigosa para a segurança das pessoas, mas também das instituições, serviços e infraestruturas. Face a isso, a estratégia vem impulsionar a utilização e desenvolvimento do ciberespaço de forma aberta, segura e protegida. É realçado o papel das entidades privadas, no sentido em que a responsabilidade pela segurança deste novo espaço é também sua, pois detêm e exploram partes relevantes do novo espaço digital. A segurança é partilhada no ciberespaço por todas as partes interessadas, logo o Estado, o setor privado e cada um dos utilizadores são responsáveis pela segurança no espaço digital.

Na Estratégia de cibersegurança são apontadas cinco prioridades estratégicas. A primeira é garantir a resiliência do ciberespaço, estabelecendo a cooperação entre setor público e privado, por forma a combater ameaças e riscos de cariz transfronteiriço e definir a resposta a dar em questões de incidentes de emergência. A segunda prioridade estratégica prende-se com a redução drástica da cibercriminalidade, sendo que para isso é necessário que exista uma legislação rigorosa, capaz de produzir resultados. A cibercriminalidade tem visto os seus números aumentados, uma vez que é uma atividade lucrativa e, simultaneamente, representa um risco muito baixo, pois socorre-se do anonimato.

Relativamente à terceira prioridade estratégica, a mesma procurou desenvolver as capacidades no domínio da ciberdefesa, assentes no quadro da política comum de segurança e defesa. Os esforços devem concentrar-se na deteção de ameaças informáticas sofisticadas, na resposta e recuperação. De acordo com o documento estratégico mencionado, "perante ameaças multifacetadas, há que melhorar as sinergias entre as abordagens civil e militar na protecção dos ativos informáticos críticos" (p. 12).

[36] Consultar JOIN (2013) 1 final, sobre a Estratégia Europeia para a Cibersegurança.

No que diz respeito à quarta prioridade estratégica, a mesma procura o desenvolvimento de recursos industriais e tecnológicos para a cibersegurança. A tendência atual é adquirir produtos e serviços de TIC e soluções de segurança, destinados a IC, no exterior da Europa, o que provoca uma grande dependência face a estes. De acordo com a Estratégia Europeia para a Cibersegurança (2013), para além da dependência, importa garantir "que os componentes de *hardware e software* (…) sejam de confiança, seguros e garantam a protecção de dados pessoais" (p. 13). Neste sentido, há que promover o mercado único de produtos de cibersegurança. Por último, a quinta prioridade estratégica é estabelecer uma política internacional coerente em matéria de ciberespaço para a UE e promover os seus valores fundamentais.

Em suma, importa referir que perante um ciberespaço global, numa sociedade estabelecida em rede, sem fronteiras bem definidas, é essencial recorrer à cooperação entre as várias entidades responsáveis para fazer frente ao novo fenómeno da cibercriminalidade. De acordo com a Estratégia da UE para a cibersegurança, "os incidentes informáticos não se detêm nas fronteiras. Todos os intervenientes (…) devem assumir responsabilidades quer a nível nacional quer a nível da UE, e trabalhar em conjunto para reforçar a cibersegurança" (p. 19).

2.4. Cibersegurança em Portugal

Em Portugal existe "uma elevada taxa de penetração quer da utilização das TIC, quer da prestação de serviços em linha" (Santos, 2011, p. 77), o que significa uma "maior dependência dos cidadãos, das empresas e do próprio Estado relativamente às TIC e esta dependência representa, claramente, um desafio para a segurança nacional" (Santos, 2011, p. 77). O facto de nos encontrarmos dependentes das TIC aumenta os riscos inerentes à sua possível afetação por parte de atores nocivos, o que torna urgente a sedimentação de uma cultura de proteção destas infraestruturas.

Até meados da década de 90 do século XX, a cibersegurança não preocupava os decisores políticos. Os cidadãos portugueses com computador pessoal eram escassos e, para além disso, a informatização na Administração Pública só se verificou a partir dos finais da década de 90 do século XX, pelo que o conhecimento e o acesso à informação era muito pouco ou insuficiente para suscitar preocupações relativamente à segurança das redes (Santos, 2014). Contudo, hoje em dia é um tema central na nossa sociedade, uma vez que o ciberespaço assume uma dimensão vital para os cidadãos e para os Estados.

No ano de 2000, os elementos da Fundação para a Computação Científica Nacional (FCCN) depararam-se com um aumento de incidentes de segurança informática na Rede Ciência, Tecnologia e Sociedade (RCTS)[37], de modo que decidiram, à semelhança das congéneres europeias, criar uma equipa de resposta a incidentes de segurança informática, designada de *Computer Emergency Response Team* (CERT), que acabou por se transformar no CERT nacional (CERT.PT), em 2005 (Santos, 2014). O CERT.PT desempenhou um papel relevante na promoção de uma cultura de cibersegurança em Portugal. Este faz parte da rede nacional de *Computer Security Incident Response Team* (CSIRT), da qual fazem parte várias organizações públicas e privadas. Esta rede tem a missão de criar uma relação de confiança entre os vários CERT's e pessoas com responsabilidade no âmbito da informática, de maneira a incentivar a partilha de informação e boas práticas, mas também de recolher indicadores que permitam definir medidas pró-ativas e reativas de resposta a incidentes de segurança informáticos. Tem, ainda, a missão de criar instrumentos que permitam dar resposta a um cenário de incidente de segurança com grande dimensão. O CERT.PT forneceu um contributo indispensável para a cibersegurança nacional, já que "é um ponto de referência e de contacto que (…) tem vindo a garantir a interligação nacional à rede europeia de CSIRT e a desenvolver um esforço importante no levantamento de uma rede de CSIRT nacional" (Freire et al., 2013, p. 56).

O aumento de ataques lançados por atores hostis, em termos de número e impacto, tornou premente a intervenção do Estado em dar resposta a esta problemática, pelo que a Resolução do Conselho de Ministros n.º 12/2012, de 7 de fevereiro[38], veio estabelecer, no âmbito da implementação de uma Estratégia Nacional de Segurança da Informação, a criação de um CNCseg, a ser coordenado pelo Gabinete Nacional de Segurança (GNS). A Comissão Instaladora do CNCseg foi definida pela Resolução do Conselho de Ministros n.º 42/2012, de 13 de abril, sendo que a sua missão seria definir os moldes para a criação, instalação e operacionalização de um CNCseg.

Em 20 de junho de 2012, a Comissão Instaladora do CNCseg apresentou um relatório com os resultados apurados. Com este relatório concluiu-se que, face ao aumento de ciberataques dirigidos contra o setor privado, público e utilizadores finais das TIC, a

[37] Trata-se de uma rede de alto desempenho para instituições como Universidades, Laboratórios de Estado, Institutos Politécnicos, constituindo-se ainda como uma plataforma de experimentação em aplicações e serviços de comunicações.

[38] Este diploma aprova o Plano Global Estratégico de Racionalização e Redução de Custos com as TIC na Administração Pública.

cibersegurança era considerada uma prioridade nacional, devendo ser criada uma estrutura nacional de cibersegurança assente numa Estratégia Nacional de Cibersegurança. É também sugerida a criação de um Conselho Nacional de Cibersegurança, e de um Gabinete de Gestão de Crises, para fazer face a ciberincidentes de grande envergadura, que coloquem em causa as IC de informação. Este relatório defende os benefícios da cooperação internacional, bem como da colaboração entre as autoridades nacionais competentes em matéria de cibersegurança.

Como resultado deste relatório, foi realizada uma Proposta de Estratégia Nacional de Cibersegurança[39], que identificou como principal problema a enfrentar por Portugal nos próximos anos o aumento de ciberataques realizados contra IC (GNS, 2012, p. 1). A Proposta apresenta três finalidades que devem ser alcançadas por Portugal, designadamente garantir a segurança no ciberespaço, fortalecer a cibersegurança das infraestruturas nacionais e defender os interesses nacionais e a liberdade de ação no ciberespaço.

Quanto à garantia da segurança no ciberespaço: deve analisar-se a informação existente ao nível de ataques e ameaças, para estarmos preparados para intervir se necessário; devem ser desenvolvidos mecanismos de deteção de ataques, principalmente dos sistemas de informação do Estado e IC nacionais; o CNCseg deve ser equipado com sala de situação e meios humanos e materiais adequados; o Estado deverá ser capaz de fazer frente a qualquer crise, podendo inclusive isolar as redes; devem desenvolver-se as capacidades científicas, técnicas, industriais e humanas, de maneira a diminuir a dependência face a entidades externas; deve adaptar-se a legislação nacional face aos desenvolvimentos verificados a nível internacional; deve desenvolver-se a cooperação internacional; deve difundir-se a cultura de cibersegurança na população portuguesa.

Outra finalidade será fortalecer a cibersegurança das infraestruturas nacionais, reforçando a segurança das TIC nas redes e sistemas de informação governamentais, da Administração Pública e dos operadores das IC, de maneira a assegurar uma maior resiliência nacional.

Por último, para atingir a finalidade de defender os interesses nacionais e a liberdade de ação no ciberespaço propõe-se o desenvolvimento de tecnologias de segurança, de forma a garantir que as autoridades governamentais e atores relacionados

[39] Para mais informação, consultar documento original, disponível em http://www.gns.gov.pt/media/ 1247/PropostaEstrat%C3%A9gia NacionaldeCiberseguran%C3%A7aPortuguesa. Pdf (Consultado em 15 de fevereiro de 2015).

com gestão de crises consigam comunicar com confidencialidade, bem como defender a governação eletrónica do Estado e fortalecer mecanismos de cooperação nacional e internacional.

O CNCseg[40] iniciou a sua atividade em 7 de outubro de 2014. Contudo, Portugal ainda não detém uma estratégia formal para a cibersegurança nacional, o que torna as competências do CNCseg um pouco indefinidas, dificultando a sua atuação e, consequentemente, acentuando a insegurança no ciberespaço. O CNCseg tem como missão garantir a segurança do país na utilização do ciberespaço, de forma livre, confiável e segura. Tem como objetivos ainda desenvolver a cibersegurança nacional e promover a cooperação internacional, conjuntamente com as autoridades competentes, bem como desenvolver mecanismos capazes de detetar, reagir e recuperar de situações de ciberataques ou incidentes que coloquem em causa IC ou os interesses nacionais (n.º 2 do Art.º 2.º do Decreto-Lei n.º 69/2014, de 9 de maio).

As competências do CNCseg passam por: desenvolver mecanismos capazes de fazer face a incidentes de cibersegurança e ciberataques; estimular a formação e qualificação de recursos humanos; criar uma cultura de cibersegurança; exercer o poder de autoridade nacional competente; cooperar na manutenção da segurança dos sistemas de informação e comunicação e das IC nacionais; promover a cooperação entre os vários intervenientes responsáveis pela área da cibersegurança; estabelecer referenciais normativos; promover projetos de inovação e desenvolvimento na área da cibersegurança, entre outras (Art.º 2.º-A, do Decreto-Lei n.º 69/2014, de 9 de maio[41]).

Recentemente, o CNCseg acolheu o serviço do CERT.PT, com as atribuições de coordenação de resposta a incidentes de cibersegurança, envolvendo as entidades do Estado, os operadores de infraestruturas críticas e outras CSIRTs nacionais[42].

A criação de um Conselho Nacional de Cibersegurança e de um Gabinete de Gestão de Crises ainda não foi concretizado, como havia sido preconizado no Relatório da Comissão Instaladora para o CNCseg, o que reflete uma fragilidade encontrada na resposta a dar a incidentes de grande envergadura, caso os mesmos venham a ocorrer.

Simultaneamente, foi criado um Centro de Ciberdefesa. O Conceito Estratégico de Defesa Nacional, aprovado pela Resolução do Conselho de Ministros n.º 19/2013, de 21 de

---

[40] Para mais informação acerca do CNCseg, consultar o *site*: http://www.cncs.gov.pt/pagina-inicial/index.html (consultado em 10 de abril de 2015).
[41] O Decreto-Lei n.º 69/2014 de 9 de maio altera pela segunda vez o Decreto-Lei n.º 3/2012 de 16 de janeiro.
[42] Disponível em http://www.cncs.gov.pt/cert-pt/coordenacao-da-resposta-a-incidentes/ (consultado em 08 de abril de 2015).

março, preconiza a constituição de uma capacidade de ciberdefesa pelas Forças Armadas. Na mesma senda, a Reforma "Defesa 2020", de acordo com a Resolução do Conselho de Ministros n.º 26/2013, de 19 de abril, prevê o levantamento da capacidade de ciberdefesa nacional, assim como a criação de um Centro de Ciberdefesa[43].

A existência de dois centros levanta a questão de quem terá a competência para intervir em caso de ciberataque. A solução de coordenação poderia passar pela criação do Conselho Nacional de Cibersegurança. De acordo com Nunes (2012), considera-se que este órgão assumiria a função de coordenador entre as áreas de cibersegurança e de ciberdefesa do Estado. Face à dificuldade em identificar a origem do ataque, devemos concentrar-nos no efeito provocado, ou seja, a ciberdefesa apenas terá uma intervenção em caso de guerra, estado de sítio ou emergência e apenas em situações em que a capacidade de cibersegurança não consiga dar resposta[44]. De acordo com Nunes (2012), torna-se importante para Portugal "garantir a segurança e a defesa da Infraestrutura de Informação Nacional, encarando esta necessidade como um processo contínuo e sistémico de análise e gestão do risco social" (pp. 116-117).

Em suma, o futuro digital e a cibersegurança de Portugal passam "por um desafio coletivo e por uma partilha de responsabilidades que envolve, numa visão conjunta o governo, a administração pública, forças armadas e de segurança, empresas e cidadãos" (Nunes, 2012, p. 125).

[43] Aconselha-se a consulta da Orientação Política para a Ciberdefesa, prevista no Despacho n.º 13692/2013 de 28 de outubro.

[44] Solução apontada por um dos oradores do II Curso de Cibersegurança e Gestão de Crises no Ciberespaço, ministrado no Instituto da Defesa Nacional (IDN), decorrido ao abrigo das *Chatham House Rules.*

Capítulo 3 – *Hacktivismo* e outras Ciberameaças

Embora a existência de ciberataques remonte à origem da *internet* e, que de acordo com Anderson (2008), tenham começado a desenvolver-se na década de 80 do século XX, a verdade é que estes têm vindo a ganhar dimensão nos últimos anos. Por um lado, devido à crescente dependência das infraestruturas vitais face às infraestruturas TIC e, por outro, devido à evolução e inovação técnica, a qual é realizada com tal velocidade que não nos permite estar sempre conscientes das vulnerabilidades existentes, mas também porque simultaneamente são criadas novas ferramentas tecnológicas para desenvolver práticas ilícitas contra alvos específicos, com o objetivo de provocar prejuízo para os mesmos. Perante isto, existe já uma enorme preocupação por parte dos Estados[45] em desenvolver mecanismos capazes de fazer frente aos ciberataques contra os sistemas de informação e comunicação, nos quais assentam as IC da sociedade.

Neste capítulo são definidas e delimitadas as ameaças cibernéticas. Em concreto, é abordado o fenómeno *hacktivista*, os tipos de *hacktivismo* e os grupos conhecidos por desenvolverem ataques de protesto *online*. Abordamos ainda, de forma sucinta, os tipos de ataques desenvolvidos.

3.1. Ciberataques

Os computadores e sistemas informáticos são alvos de ataques diários encetados por *hackers*, sendo estes definidos como "um ator individual, dotado de um computador e das necessárias competências técnicas, [que] pode tornar inoperacionais as infraestruturas críticas dos países mais desenvolvidos do mundo" (Nunes, 2012, p. 117).

Moreira (2012) 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

[45] Vejam-se, por exemplo, as estratégias de cibersegurança desenvolvidas em 37 países, desde EM da UE a países como a Rússia ou os EUA, disponibilizadas no *site* do GNS: http://www.gns.gov.pt/new-ciberseguranca.aspx (consultado em 28 de fevereiro de 2015).

> mesmo espaço de emissão eletromagnética, bem como os próprios computadores, redes de computadores, sistemas e equipamentos. (p. 32)

Os ciberataques desencadeados contra a Estónia[46] e a Geórgia[47], em 2007 e 2008 respetivamente, marcaram de forma indelével a sociedade e despertaram as autoridades dos vários Estados para um novo problema derivado da sociedade em rede: a ameaça dos ciberataques e a vulnerabilidade da rede e sistemas de informação.

Os ciberataques à Estónia e à Geórgia assemelham-se em certo aspeto, uma vez que em ambas as situações os ciberataques ocorreram em simultâneo com outros conflitos existentes no mundo real, que rapidamente se alastraram ao ciberespaço. Nestes ciberataques não foi verificada qualquer inovação técnica, residindo a novidade nas proporções que tomaram. No caso da Estónia, provocaram danos ao nível financeiro, ao nível da imagem das empresas e perturbações na vida da população (p. e. no sistema de pagamentos e caixas automáticas). Por sua vez, na Geórgia foi afetado o sistema de informação do Governo, o que o prejudicou no desenvolvimento do conflito armado em que tomava parte (Santos, 2011).

Estes ataques provaram que os Estados também estão vulneráveis a ciberataques. Estes podem provocar consequências negativas e em larga escala na sociedade, o que torna urgente a definição de medidas para impedir que tal aconteça. De acordo com Freire e Caldas (2013), tornou-se claro, com estes casos, que os Estados têm de desenvolver mecanismos com vista a protegerem-se contra uma eventual tentativa de disrupção dos sistemas de informação das IC. Estes mecanismos terão de estar capacitados para "reduzir as vulnerabilidades àquelas ameaças e assegurar que disrupções no ciberespaço sejam raras, de curta duração, e que causem danos mínimos" (Freire & Caldas, 2013, p. 92).

---

[46] O Governo da Estónia pretendia deslocar um cemitério, considerado um memorial soviético da Segunda Grande Guerra Mundial, para um cemitério na periferia de Tallin. Contudo, esta decisão não foi consensual, uma vez que cerca de um quarto da população daquele Estado era russa. Foi esta a motivação para um conjunto de conflitos que se verificaram neste país e em simultâneo foram encetados ataques no ciberespaço. Estes ataques dirigiram-se aos *sites* do Governo, do Primeiro-ministro, do Ministério das Finanças e da polícia da Estónia. O pico dos ataques teve lugar nos dias 9 e 10 de maio, já que se comemorava a data em que a Rússia tinha derrotado a Alemanha na Segunda Guerra Mundial (Santos, 2011).

[47] O conflito que esteve associado à vaga de ciberataques que se verificaram em 2008 na Geórgia relacionou-se do com o conflito entre a Geórgia e a Federação Russa em relação ao território da Ossétia do Sul, que era considerado pela comunidade internacional parte integrante da Geórgia. Em 7 de agosto, a Geórgia desenvolve um ataque militar surpresa contra as forças separatistas daquele território. De imediato a Federação Russa agiu em defesa dos cidadãos russos que residiam naquele local e, embora a comunidade internacional em geral não reconhecesse a independência deste território, a Federação Russa reconhece em 26 de agosto a independência da Ossétia do Sul (Santos, 2011).

A crescente dependência da sociedade face às novas tecnologias conduz-nos às IC ou, também designadas, infraestruturas vitais como parte integrante da rede. Delas depende o bom funcionamento da sociedade, sendo que a sua alteração poderá provocar incalculáveis prejuízos para as instituições e para as pessoas. Uma IC é definida como:

> O elemento, sistema ou parte deste situado nos Estados – Membros que é essencial para a manutenção de funções vitais para a sociedade, a saúde, a segurança e o bem-estar económico ou social, e cuja perturbação ou destruição teria um impacto significativo num Estado-Membro, dada a impossibilidade de continuar a assegurar essas funções. (al. a) do Art.º 2.º da Diretiva 2008/114/CE do Conselho de 8 de dezembro de 2008) [48]

Tratando-se de uma rede global, que ultrapassa o espaço físico onde a IC se encontra sedeada, surge o conceito de Infraestrutura Crítica Europeia, ou seja, a infraestrutura que quando atingida pode provocar um impacto em pelo menos dois EM, conforme a al. b) do Art.º 2.º da Diretiva 2008/114/CE do Conselho, de 8 de dezembro de 2008[49].

As IC incluem os setores das instalações e redes de energia, das TIC, das finanças, da saúde, da alimentação, da água, dos transportes, da produção, do armazenamento e transporte de mercadorias perigosas e da administração. Estas são determinadas em função de três fatores: o alcance (a extensão geográfica), a magnitude (o grau do impacto ou da perda, em função do impacto no público, dos efeitos económicos, da incidência ambiental, da interdependência entre IC e dos efeitos políticos) e os efeitos no tempo (o período temporal afetado)[50]. A gestão das IC afeta tanto o setor público como o privado, uma vez que estão interligados e a sua crescente dependência face às TIC poderá proporcionar um ataque em cadeia, pelo que a cooperação e a união de esforços é fundamental neste âmbito.

De acordo com Bejarano (2011), é muito improvável que uma IC seja afetada durante um longo período temporal apenas com recurso a ciberataques, já que as IC foram desenhadas para poderem falhar e serem novamente iniciadas, de forma que o objetivo não

---

[48] A Diretiva 2008/114/CE foi transposta para o quadro jurídico português através do Decreto-Lei n.º 62/2011 de 9 de maio, que define o conjunto de procedimentos de identificação e proteção das infraestruturas necessárias para a saúde, a segurança e bem-estar económico e social da sociedade no que concerne, somente, aos sectores da energia e dos transportes.

[49] Ver COM (2006) 786 final, sobre o Programa Europeu de Proteção de IC.

[50] Ver COM (2004) 702 final, sobre a Proteção das IC no âmbito da luta contra o terrorismo.

deverá ser a perfeição do sistema, mas sim uma boa gestão de crises. De acordo com Freire e Caldas (2013), mesmo o caso do *Stuxnet*[51] não provocou consequências profundas, o que não quer dizer que o assunto deva ser desprezado, uma vez que um ciberataque poderá "paralisar temporariamente o comércio e fazer duvidar a confiança dos consumidores nos mercados financeiros e nos instrumentos dos Governos" (p. 93).

É importante, todavia, estarmos preparados para cenários desse tipo, pois numa sociedade estabelecida em rede "o risco a que estão sujeitas as IC subsiste como um dos pontos mais preocupantes" (Freire et al., 2013, p. 25). Desta forma, é essencial que se definam procedimentos e planos de contingência para fazer face a crises no ciberespaço.

De acordo com o Relatório *Global Risks* 2015 publicado pelo *World Economic Forum,* os ciberataques são um dos riscos globais com maior probabilidade de acontecer, enquanto o colapso nas infraestruturas críticas de informação é referido como um dos riscos globais com maior impacto, logo a seguir à crise da água, à propagação de doenças infeciosas, às armas de destruição maciça, ao conflito entre Estados, à falha de adaptação à mudança climática e ao choque de preço na energia.

3.2. Ciberameaças

A sociedade em rede, embora muito promissora em termos sociais e económicos, agrega também um conjunto de novas ameaças, que restringem a liberdade das pessoas no ciberespaço e que colocam em causa as infraestruturas do Estado[52]. Neste sentido, importa elencar as várias ciberameaças que têm vindo a multiplicar-se no ciberespaço e distingui-las do *hacktivismo*, que é, em concreto, a ciberameaça privilegiada no nosso estudo.

No Relatório Anual de Segurança Interna (RASI) respeitante ao ano de 2013, considera-se que os riscos e as ameaças associadas ao ciberespaço, nomeadamente o *hacktivismo*, a espionagem e o terrorismo, são ameaças globais à segurança. O mesmo documento reforça ainda que "Portugal não ficou imune a tentativas de infiltração de sistemas informáticos do Estado, ocorridas no contexto de campanhas internacionais,

[51] *Stuxnet* é um vírus muito sofisticado que se instala no sistema operativo e controla os sistemas remotos de uma forma autónoma. O *Stuxnet* terá aparentemente infectado cerca de 60.000 computadores, principalmente no Irão, mas também terá atingido a Índia, Indonésia, China, Azerbaijão, Coreia do Sul, Malásia, Estados Unidos, Reino Unido, Austrália, Finlândia e Alemanha. Este vírus continua a espalhar-se na *internet*, embora já tenham sido encontradas soluções de segurança para o combater. Alegadamente, este vírus poderá ter atingido as centrais nucleares de Natanz no Irão (Farwell & Rohozinski, 2011).

[52] A ciberameaça é já considerada uma das temáticas alvo de estudo por parte do SIS. Ver em http://www.sis.pt/ciberameaca.html (consultado em 08 de fevereiro de 2015).

aparentemente visando o acesso a informação privilegiada" (p. 32). Embora o nosso país seja afetado por ciberataques, continuam a persistir dificuldades em identificar a origem e natureza dos mesmos, pois mesmo o *Internet Protocol* (IP)[53] de origem pode ser mascarado, não sendo possível verificar em concreto quem realiza o ataque, nem mesmo precisar se foi um ataque de natureza interna ou externa, o que dificulta a investigação criminal e a consequente responsabilização destas práticas[54].

Uma ameaça à segurança das TIC pode ser considerada "qualquer circunstância ou evento passível de explorar, intencionalmente ou não, uma vulnerabilidade específica num sistema de TIC, resultando numa perda de confidencialidade[55], integridade[56] e disponibilidade[57] da informação manipulada ou da integridade ou disponibilidade do sistema" (Centro Criptológico Nacional, 2006, citado por Freire et al., 2013, p. 22). Estas ameaças podem ter origem em desastres naturais, origem industrial, erros ou falhas não intencionais e podem estar relacionadas com ataques deliberados. Estes ataques deliberados merecem a nossa atenção já que elevam o nível de risco a que os sistemas estão sujeitos.

De acordo com Freire et al. (2013), as ameaças podem ser agrupadas nas seguintes categorias: cibercrime, ciberterrorismo, ciberespionagem, ciberguerra e *hacktivismo*. Na primeira categoria de cibercrime o autor inclui as ameaças centradas na obtenção de benefício económico mediante a utilização de ações ilegais, dando o exemplo de fraude bancária. Contudo, não concordamos em pleno com esta categoria, uma vez que consideramos cibercrime como todo o tipo de crime realizado com recurso a meios informáticos, pois mesmo os ataques informáticos de terroristas e espiões, por exemplo, podem constituir cibercrime, de acordo com a definição da Estratégia da União Europeia para a cibersegurança.

O conceito de ciberterrorismo foi cunhado por Barry Collin, na década de 80 do século XX, como a convergência do ciberespaço com o terrorismo (Collin, 1997). Porém, podemos considerar que até ao momento este conceito é meramente teórico, uma vez que nunca se verificou um ciberataque com fins terroristas. Todavia, essa hipótese não pode ser

[53] Código numérico identificativo de cada máquina conectada à *internet*.
[54] Conforme entrevista a Vitor Costa, em Apêndice C.
[55] Princípio da segurança da informação, segundo o qual a informação está acessível apenas às pessoas que têm autorização para tal (FCCN, 2005).
[56] Princípio da segurança da informação, de acordo com o qual a informação e os métodos de processamento devem ser rigorosamente salvaguardados (FCCN, 2005).
[57] Reflete-se na garantia de que a informação necessária para os utilizadores autorizados deve estar disponível, sempre que tal seja necessário (FCCN, 2005).

colocada de parte. Freire e Caldas (2013) afirmam que a probabilidade de ocorrência de um ataque com um impacto elevado é baixa, mas se acontecer pode provocar efeitos disruptivos, pelo que é uma hipótese que deve ser contemplada pelos Estados. De acordo com Argomaniz (2014), "os grupos terroristas têm explorado até agora a *internet* e outras tecnologias informáticas e *software* não como arma (também denominado ciberterrorismo), mas como instrumento de apoio para as suas ações no mundo físico" (p. 3), ou seja, a *internet* assume um papel importante para os terroristas, mas em termos de treino, propaganda e radicalização. Os ciberataques apresentam características que poderiam ser atrativas para os terroristas como a disponibilidade das ferramentas, a possibilidade de o alvo poder ser atacado à distância, a facilidade em manter o anonimato ou o grande impacto que possivelmente poderia originar. Contudo, a ausência do drama e da teatralidade que são essenciais para a propaganda da sua ação podem justificar a falta de interesse dos grupos terroristas no recurso a ciberataques (Argomaniz, 2014).

A ciberespionagem é, segundo Silva (2014), um conceito que evolui da tradicional espionagem, sendo considerada a "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" (p. 18). Entre os objetivos deste tipo de ciberameaça está a vantagem competitiva entre Estados ou empresas e a obtenção de vantagem económica pela venda da informação (Santos, 2014). No ciberespaço, qualquer um pode sentar-se em frente a um computador e aceder a grandes quantidades de informação de forma rápida e muitas vezes sem consequências (Armstrong, 2013).

Também o conceito de ciberguerra tem estado em cima da mesa para discussão. A ciberguerra consiste em "conduzir, e preparar-se para conduzir, operações militares de acordo com os princípios da informação" (Arquilla, 1993, p. 30). De acordo com Freire e Caldas (2013), a ciberguerra é o conflito entre duas ou mais nações ou diferentes partes de uma nação tendo como campo de batalha o ciberespaço. As guerras são como têm sido sempre, sendo que o objetivo continua a ser o de atingir o adversário e as suas forças armadas, não causando danos desnecessários (Howard, 2006).

A distinção relativa aos conceitos de ciberterrorismo, ciberguerra, ciberespionagem e *hacktivismo* reside sobretudo no campo das motivações e intenções. Para fazer uma análise das ameaças que podem afetar cada infraestrutura é necessário apurar qual a origem das mesmas, bem como os atores responsáveis. De acordo com Freire et al. (2013), as motivações inerentes a estes podem estar relacionadas com benefícios económicos (p. e.

cibercriminosos, espiões industriais e pessoal interno), vantagens táticas ou competitivas em termos militares ou empresariais (p. e. os espiões industriais e nações), motivações políticas (p. e. *hacktivistas* e terroristas), destruição ou dano (p. e. terroristas e nações) e fama ou vingança (p. e. *hacktivistas* e funcionários).

De acordo com Freire et al. (2013), os ciberataques podem distinguir-se em função do seu nível de organização: simples, organizados, *Advanced Persistent Threats* (APT), ataques coordenados de grande escala e ciberataques coordenados com ataques físicos. Os ataques simples são pouco ou nada organizados, realizados por uma pessoa ou várias, mas sem qualquer tipo de organização, apresentando um impacto médio-baixo. Quando falamos de ataques organizados estamos a falar de um ataque coordenado por um número significativo de pessoas organizadas. O impacto destes ataques é médio, dependendo muito dos objetivos pretendidos. No que diz respeito às APT, são ameaças desenvolvidas por pessoas com elevadas capacidades técnicas, com um alvo específico e que permanecem ao longo do tempo na rede. Estes têm uma precisão muito elevada, sendo a possibilidade de ocorrerem alta e o impacto de tal ameaça pode inclusive ser bastante forte. Os ataques coordenados de grande escala são organizados por uma nação ou organização e envolvem um múltiplo número de atores e neste curso o impacto pode vir a ser elevado ou muito elevado. Os ciberataques coordenados com ataques físicos são os ataques que envolvem um maior nível de coordenação, implicando a combinação de ataques em diferentes dimensões, com uma precisão exata, de maneira que são considerados de impacto extremamente elevado (Freire et al., 2013).

Embora seja possível distinguir as ciberameaças em termos teóricos, torna-se muito difícil fazê-lo na prática. De acordo com o ponto de vista de Martins (2012), o ciberespaço é atualmente um "mundo dos rostos invisíveis" (p. 40). Neste mundo onde o anonimato toma lugar, é bastante difícil identificar a origem das ameaças, bem como definir quais as verdadeiras intenções dos indivíduos que as desenvolvem.

De acordo com Klimburg e Tirmaa-Klaar (2011), "o principal problema na separação de ciberataques em categorias baseadas em autores como «criminosos», «terrorista» e «soldado» é que de facto estas próprias identidades podem ser fluidas e ambíguas" (p. 5), isto é, é difícil identificar qual o fenómeno cibernético que tem lugar quando ocorre um ciberataque, uma vez que os mesmos acabam por ser um tanto ambíguos. De acordo com Anderson (2008), o protesto *online* irá aumentar, mas manter-se-á provavelmente desorganizado. Os ataques que chamam a atenção da imprensa

perderão interesse e será necessário desenvolver ataques que causem maior impacto e consecutivamente mais interesse dos *media*.

3.3. O *Hacktivismo*

Embora o *hacktivismo* não seja a ciberameaça mais frequente, é aquela que apresenta uma maior atenção mediática, sendo que os ataques a *sites* governamentais ou empresas privadas, onde são deixadas mensagens de protesto, têm vindo a ser recorrentes nos últimos anos (Santos, 2014).

O fenómeno do *hacktivismo* começou a ganhar relevo nos finais de 2010, quando um grupo, designado *Anonymous*, começou a desenvolver alguns ciberataques, por vezes organizados, contra instituições de relevo que recusaram o apoio ao *site Wikileaks*[58] (Esteves, 2012, p. 45). O *site Wikileaks* tornou-se, então, tema de debate devido à disponibilização de vários documentos confidenciais dos EUA, por parte de Julian Assange, colocando em causa as relações diplomáticas norte-americanas com outros países. Os defensores da liberdade de expressão e de acesso à informação insurgiram-se nessa altura a favor do *site Wikileaks*, realizando "bloqueios a *sites* de pagamentos eletrónicos que, como o Visa/Mastercard e o PayPal, tinham recusado processar donativos a favor do *Wikileaks*" (Cardoso, 2012, p. 3). A partir deste episódio o fenómeno tem vindo a ganhar alguma dimensão, embora a sua história remonte à génese da própria *internet*.

O termo *hacktivismo* deriva da palavra *hacker*, termo utilizado pela primeira vez na década de 50 do século XX, pelo *Massachusetts Institute of Technology*[59]. *Hacker* designava, então, alguém com interesse pela área da informática. De acordo com a referida definição, *hacker* seria uma pessoa capaz de *hackear*, verbo derivado do inglês "*to hack*" que designa "o acto de alterar alguma coisa, que já está pronta ou em desenvolvimento, deixando-a melhor" (Rodrigues, 2010, p. 31). No fundo, era o que acontecia com os especialistas na área da informática, que procuravam melhorar constantemente a rede, explorando para isso as suas falhas ou imperfeições. Lévy (1984) considera que, entre os primeiros entusiastas das novas tecnologias, um *hack* era uma ação que transparecia

[58] *Wikileaks* é uma organização sem fins lucrativos, que tem por objetivo partilhar informação, por vezes confidencial, com a comunidade digital. Trata-se de uma organização que apela à liberdade de expressão e de liberdade de publicação dos *media.* Para mais informação sobre a *wikileaks,* consultar: https://wikileaks.org/About.html (Consultado em 12 de fevereiro de 2015).

[59] Instituto universitário de referência, localizado em Cambridge, nos EUA. Para mais informação consultar: http://web.mit.edu/ (consultado em 27 de fevereiro de 2015).

inovação, estilo e técnica, sendo que as pessoas se autodenominavam *hackers* com grande orgulho. Contudo, após o aparecimento e massificação dos meios de comunicação social, este termo começou a ser utilizado vulgarmente para definir os "infractores da lei do mundo digital" (Rodrigues, 2010, p. 31). Este foi o motivo que conduziu os *hackers* originais, que partilhavam um certo sentimento de ofensa, a criar o conceito de *cracker* para definir os "invasores de computadores (…) programadores maliciosos e ciberpiratas que agem com o intuito de violar ilegal ou moralmente sistemas cibernéticos" (Santos et al., 2007, citado por Rodrigues, 2010, p. 31).

Atualmente, Gelbstein (2012) define *hacker* como:

> Uma pessoa que contorna as medidas de segurança de um sistema informático. Os que têm a intenção de perturbação ou outras atividades maliciosas são muitas vezes referidos como "*Black Hat Hackers*" ou "*Crackers*". Aqueles que usam as suas habilidades para identificar vulnerabilidades, com ou sem o consentimento dos proprietários dos sistemas são chamados de "*White Hat Hackers*" ou "*Hackers* Éticos". (p. 143)

Os *hackers* podem ser divididos em três grupos distintos: *white hats, black hats e grey hats* (Arnone, 2005). Os w*hite hats* ou os *hackers* éticos são aqueles que utilizam as suas capacidades técnicas para encontrar falhas nos sistemas, no âmbito da legalidade. Segundo Martins (2012), são *hackers* que protegem o sistema e não traduzem em crime as suas ações, como fazem os *black hats*. Estes últimos são considerados *hackers* criminosos, sem ética e maliciosos, que de acordo com Rodrigues (2010) "descobrem falhas de segurança e criam *exploits*[60] para explorá-las. Agem para obter retorno financeiro, ou porque simplesmente gostam do que fazem" (p. 32). Os *gray hats* apresentam características de ambos, ou seja, embora tenham conhecimentos e ética do *hacker* original, por vezes utilizam as suas capacidades para ações maliciosas (Arrone, 2005).

Os *hackers* desenvolvem a sua atividade "num mundo paralelo à realidade diária do ser humano no qual a sua motivação expressa um sentimento de revolta em nome de uma causa" (Martins, 2012, p. 41). Deste modo, os *hackers* desenvolvem a sua atividade no

[60] *Exploits* são programas, normalmente, utilizados por *hackers*, que exploram vulnerabilidades conhecidas nos sistemas.

ciberespaço, mas as suas motivações podem estar associadas a eventos relacionados com o mundo físico.

No que respeita à definição de *hacktivismo*, a mesma é apresentada por Denning (1999) como a combinação do ativismo político com o *hacking* de computadores. Assim, o *hacktivismo* combina a política transgressiva da desobediência civil com as novas técnicas e tecnologias de *hackers* de computadores, sendo o seu principal objetivo alterar o normal funcionamento de *sites*, não tendo, todavia, o intuito de causar graves danos (Denning, 1999). A definição de Esteves (2012) vai ao encontro de Denning (1999), uma vez que também analisa o termo *hacktivismo* em duas perspetivas, nomeadamente o ativismo, que diz respeito à ação militante, tendo como objetivo alcançar um propósito político ou social, e o *hacking*, que respeita a infiltração não autorizada em sistemas informáticos. Samuel (2004), por sua vez, define *hacktivismo* como "o uso não-violento de ferramentas digitais, ilegal ou legalmente, na prossecução de fins políticos" (p. 2), tratando-se portanto de um meio poderoso de protesto no espaço digital, para promoção ideias e convicções.

Samuel (2004) considera que embora os conceitos de *hacktivismo*, ativismo *online*, desobediência civil, *hacking* e ciberterrorismo se aproximem, eles podem ser distinguidos, pelo que a autora faz uma delimitação bastante precisa entre estes conceitos (ver Anexo A). O *hacktivismo* caracteriza-se por recorrer a atividade legais, mas também ilegais, o que o faz diferir do ativismo *online* (por exemplo *sites* pelos direitos dos animais ou antiglobalização), que não compreende a existência de ações ilegais, ou seja, não transgride a Lei. Quanto à tradicional desobediência civil, distingue-se do *hacktivismo* na medida em que apresenta como campo de ação o mundo real e não o ciberespaço. O *hacking* relaciona-se com o *hacktivismo*, existindo porém um afastamento entre ambos, uma vez que os *hacktivistas* julgam que as suas capacidades podem ser utilizadas a favor do bem social comum, ao contrário do que acontece com o *hacking*, que apresenta um propósito meramente destrutivo. O *hacktivismo* tem um caráter não violento e assenta a sua ação no respeito pelos direitos humanos, distinguindo-se do ciberterrorismo, que é causador de danos provocados em seres humanos.

Segundo Anderson (2008), o fenómeno *hacktivista* relaciona-se com o apoio a causas anarquistas, ativistas e movimentos de protesto. As motivações para estes crimes informáticos politicamente motivados incluem protestos relacionados com a antiglobalização, direitos dos animais, movimentos operários, alimentos geneticamente modificados, movimentos antiguerra ou problemas ambientais (Anderson, 2008).

Simmel (1968, citado por Krauth, 2012) defende que determinados padrões de interação produzem grupos sociais gerados por partilha de objetivos e experiências de vida comuns – hoje em dia assistimos à formação destes grupos no ciberespaço. Os *hacktivistas* são pessoas que partindo da sua individualidade e singularidade foram capazes de construir locais culturais e políticos no ciberespaço – "a terra de empoderamento de indivíduos" (Jordan, 1999, citado por Krauth, 2012, p. 28), ou seja, a *internet* permite que os indivíduos aumentem o seu poder, sendo que por vezes um só indivíduo é capaz de provocar graves danos nos sistemas informáticos, como forma de protesto relativamente a algum tema que lhe seja sensível.

Estas pessoas recorrem muitas vezes ao humor para chamar a atenção dos *media* e são pessoas que se orgulham do seu poder tecnológico. A característica crucial do *hacktivismo* é a possibilidade de um indivíduo poder agir individualmente, ao contrário do que ocorre no mundo real, onde apenas as ações com elevado número de participantes têm projeção. Para Samuel (2004) "a possibilidade de ações individuais parecem ser uma das atrações do «*hacking*» em geral, e do *hacktivismo* em particular" (p. 50). Outra característica associada ao *hacktivismo* é o anonimato, já que no ciberespaço a comunicação pode ser anónima.

A possibilidade do *hacktivismo* atravessar fronteiras é outra característica importante deste fenómeno reivindicativo. Embora o ativismo transnacional tenha vindo a assumir uma importância crescente nos últimos anos, continua a ser uma exceção no contexto da participação política.

No *hacktivismo*, a prática de ações transnacionais é tanto ou mais frequente do que aquelas que ocorrem dentro das fronteiras, e acresce ainda a dificuldade em distinguir os dois (Samuel, 2004). A mesma autora faz ainda uma distinção entre o *hacktivismo* nacional, multinacional e internacional. O primeiro ocorre quando um *hacktivista* tem como alvo o Governo, uma empresa ou uma organização do seu próprio país. O *hacktivismo* multinacional ocorre quando *hacktivistas* se unem e desenvolvem um ataque para além fronteiras, cujo alvo comum se situa a nível nacional ou multinacional. O *hacktivismo* internacional ocorre quando *hacktivistas* de um país desenvolvem um ataque dirigido a um Governo, empresa ou organização de outro país, ocorrendo em paralelo com conflitos internacionais que tomam lugar no espaço real ou físico (frequentemente denominada de ciberguerra).

As vítimas são, por norma, indivíduos, instituições ou organismos que se encontram numa posição vulnerável:

> O Estado, as suas instituições, o sector empresarial ou a banca simbolizam um novo alvo a explorar e a abater por representar um motivo de desafio para quebrar os sistemas de segurança ou uma forma de transmitir a revolta contra as políticas definidas ou um meio para denunciar as violações dos direitos humanos. (Martins, 2012, p. 41)

Para Castells (2007) "não há dúvida de que a habilidade para obter uma informação crucial, contaminar as bases de dados ou criar desordem nos sistemas de comunicação-chave, se converteu numa arma importante no novo ambiente tecnológico" (p. 190), e desta forma "a protecção das infraestruturas críticas de informação, tornou-se não só uma necessidade como um imperativo" (Caldas, 2011, p. 95).

3.4. Tipos de Ataques

Os grupos de *hacktivistas* "transportam as tácticas do activismo convencional *off-line* para o ciberespaço, numa tentativa de chamar a atenção (…) para a sua causa, tirando partido da cobertura mediática que a excentricidade e, por vezes, a espectacularidade que os seus métodos proporcionam" (Santos, 2011, p. 27), ou seja, um ataque bem-sucedido para um grupo *hacktivistas* é aquele que tem visibilidade e mediatismo. Os *hacktivistas* recorrem a uma combinação entre os ciberataques e a projeção mediática para prosseguirem os seus propósitos, que são muitas vezes roubar informação para colocar a organização numa posição constrangedora ou provar o seu mau funcionamento (Anderson, 2008). Verifica-se que apesar de terem vindo a aumentar em termos de número e sofisticação, a verdade é que não têm vindo a provocar uma alteração significativa no funcionamento operacional das redes ou sistemas. Todavia, a atenção mediática dada pelos *media* pode intensificar os efeitos de um ataque. De acordo com Anderson (2008), os ataques *hacktivistas* "podem rapidamente ganhar a atenção dos *media*, de modo que, mesmo quando o ataque atual tem pouco impacto operacional numa organização, a cobertura mediática associada cria um problema mais significativo para a vítima" (p. 7).

Os grupos *hacktivistas* disponibilizam informação antes, durante e após o ataque, o que coloca a vítima do ataque numa posição ingrata perante a comunicação social, que acaba por transmitir globalmente uma imagem negativa da mesma.

Os ataques *hacktivistas* mais comuns apresentados por Samuel (2004) são os *site defacements* (invasão de *sites*), os *site redirects* (redirecionamentos de *site*), os ataques de negação de serviço (*Denial of Service* - DoS), o roubo de informação, o roubo de informação e distribuição, as *site parodies*, a sabotagem virtual, os *sit-ins* virtuais e o desenvolvimento de *software*.

Os *site defacements* consistem na substituição de uma página *web* por outra ou na alteração do seu conteúdo, com algum tipo de mensagem, que é frequentemente uma mensagem política. Os *site redirects* consistem num ataque a um servidor, de maneira a mudar o endereço de um *site* para que os seus visitantes sejam automaticamente conduzidos para um *site* alternativo, normalmente um que critica o *site* que foi alvo de ataque.

O ataque DoS é uma forma comum e bastante eficaz de provocar danos *online*. Trata-se de um ataque realizado por muitos utilizadores ou por meio de computadores hospedeiros de determinado vírus que são remotamente canalizados para aceder a um *site*. Este ataque esgota o acesso e quebra o sistema que está a ser alvo do ataque ou torna-o lento.

O roubo de informação consiste em desenvolver um ataque a uma rede privada com vista a retirar informação. Para os *hacktivistas* este ataque visa ridicularizar o alvo, mais do que obter a informação. O mesmo já não se poderá dizer de outros atores como é o caso dos espiões.

A sabotagem virtual consiste em atividades *online* destinadas a manipular ou danificar as tecnologias da informação do alvo. Este ataque inclui a criação de vírus ou *worms*, tipo de *software* que se programa automaticamente e que vai distribuir mensagens ou sabotar sistemas.

Os *sit-ins* virtuais consistem em vários utilizadores consultarem uma página ao mesmo tempo, estando constantemente a recarregá-la, de maneira a ocuparem a rede. O sucesso desta tática depende do número de participantes. A exigência de haver um grande número de pessoas reais a participarem neste ataque é o que diferencia do DoS, que pode ser feito por uma simples pessoa, com acesso a vários computadores.

As *site parodies c*onsistem em imitar determinada página de um alvo em termos de aparência e endereço, de maneira que possa ser facilmente confundido com o do alvo.

O desenvolvimento *de software* ilegal é considerado *hacktivismo* se for utilizado para fins políticos. No fundo, são ferramentas criadas e distribuídas livremente na rede, que podem ser utilizadas por qualquer um.

3.5. Tipos de *Hacktivismo*

Samuel (2004) identifica três tipos de *hacktivismo*: *political cracking*, *performative hacktivism e political coding*. Estes tipos distinguem-se pela sua origem (*hacker-programmer* ou artist-activist) e pela sua orientação (transgressiva ou *outlaw*). Quanto à origem, a cultura *hacker-programmer* deriva da cultura da *internet*, que remonta à sua origem e se relaciona com a ética *hacker*[61], enquanto a segunda, denominada *artist-activist*, deriva dos movimentos revolucionários contemporâneos. Existe uma espécie de conflito entre as duas perspetivas: os *hacker-programmers* veem frequentemente os *artist-activists* como ignorantes, descuidados com as infraestruturas da *internet* e como tecnicamente incompetentes, enquanto os *artists-activists* costumam descrever os *hackers-programmers* como demasiado cuidadosos com os computadores e como tecnologicamente elitistas (Samuel, 2004). Quanto à orientação, os tipos de *hacktivismo* podem ser de tipo transgressivo ou *outlaw*. A orientação *outlaw* é claramente ilegal, enquanto a transgressiva desafia a Lei, mas não assume uma gravidade semelhante.

3.5.1. Political cracking

O political cracking é desenvolvido por indivíduos originários dos *hacker-programmers* e com uma orientação "*outlaw*", isto é, recorrem fundamentalmente a formas ilegais de *hacktivismo*. Embora este tipo seja o mais frequente, não é o que apresenta maior número de participantes.

Estes indivíduos recorrem a ataques como o *site defacements, redirects, DoS*, roubo de informação e sabotagem. Trata-se de um tipo de *hacktivismo* que recorre a atividades ilegais utilizadas para alcançar objetivos políticos. Uma característica deste tipo é o

[61] A cultura *hacker* está associada à ética *hacker* cujos princípios são: toda a informação deve ser gratuita e o poder deve ser descentralizado; os *hackers* devem ser julgados pelas suas ações de *hacking* e não por critérios como raça, idade ou posição social; todos podem criar arte e beleza através de um computador; os computadores podem tornar a vida melhor (Lévy, 1984).

anonimato, uma vez que trabalham sozinhos ou em grupos muito pequenos, sendo difícil distinguir um ataque individual de um ataque em grupo, ou seja, "um único *cracker* pode experienciar um elevado grau de eficácia política por alterar ou redirecionar um *site*, provavelmente atraindo uma grande atenção dos *media*" (Samuel, 2004, p. 52). Embora abarque o *hacktivismo* nacional, internacional e multinacional, o mais comum é o internacional.

3.5.2. Performative hacktivism

O performative hacktivism é praticado por *hacktivistas* com origem nos *artist-activist* e têm uma orientação transgressiva. Embora desenvolvam a sua atividade no âmbito da legalidade, muitas vezes têm necessidade de desenvolver alguns *softwares* ilegais para tornar mais eficiente a sua estratégia.

Este tipo de *hacktivismo* baseia-se no tradicional teatro político, com recurso a técnicas de *hacking* para fins políticos. O termo *performative* relaciona-se com o termo performance, ou seja, representação teatral, uma vez que muitas das pessoas que desenvolvem este tipo vêm do mundo do espetáculo ou das artes e veem o *hacktivismo* como uma forma de expressão de arte política. O *performative hacktivism* deriva dos movimentos revolucionários contemporâneos, de maneira que os principais motivos para protesto são a globalização, a luta pela libertação, pelos direitos humanos e contra o poder corporativo (Samuel, 2004). As suas táticas mais comuns são os *site parodies* e *virtual sit-ins*, formas de *hacktivismo* que assentam na tradição teatral de protesto político. O sucesso destes ataques é diretamente proporcional à intensidade da reação provocada: "o *performative hacktivism* é muito orientado para os olhos do público, e veem as suas atividades como uma forma de desafiar a dominação, corporativa e dos *media*, do discurso público" (Samuel, 2004, p. 73).

3.5.3. Political coding

O *political coding* tem origem nos *hacker-programmers*. Contudo, a sua orientação é mais transgressiva do que *outlaw*, já que estes *hacktivistas* atuam na zona da legalidade ambígua do desenvolvimento de *software* político. Este tipo de *hacktivismo* consiste na utilização de capacidades tecnológicas pelos *hackers*, para fins de contestação política. Muitos destes *hackers* começaram como *programmers* ou *crackers*, mas desenvolveram a sua atividade no sentido do *political coding*. Estes refletem um ponto de vista de

cyber-libertarian, ou seja, uma ideologia que se relaciona com a defesa dos direitos individuais e, especialmente, dos direitos *online*, dedicando-se sobretudo a assuntos relacionados com a comunidade *hacker*. Estes indivíduos utilizam as suas capacidades técnicas para fins de contestação política (Samuel, 2004).

Capítulo 4 – Caracterização da Ameaça *Hacktivista* no Panorama das Forças de Segurança Portuguesas

Neste capítulo pretendemos analisar o fenómeno *hacktivista* em Portugal e, concretamente, verificar qual a sua influência no âmbito das FS portuguesas. Para alcançar o objetivo traçado identificamos os grupos que têm desenvolvido ataques em Portugal, as suas características, pretensões e verificamos qual o impacto nas FS.

O ciberespaço é considerado "um meio para a promoção e disseminação de discursos e perspetivas do mundo" (Freire & Caldas, 2013, p. 104), pois cada vez mais as pessoas expressam a sua opinião no ciberespaço como forma de intervir ativamente na sociedade.

4.1. *Hacktivismo* em Portugal

Muita tem sido a discussão em torno dos ataques *hacktivistas*. Em Portugal, os mesmos já se verificaram e vemos o seu reflexo de forma recorrente nos OCS, o que, consequentemente, faz com que cada vez mais as autoridades portuguesas demonstrem preocupação relativamente a este tema. Com alguma regularidade, vemos notícias que retratam casos de ataques desenvolvidos por *hacktivistas* contra *sites* governamentais ou ligados às FS[62].

Segundo Vitor Costa[63], o *hacktivismo* é "uma realidade em Portugal" e existem eventos ligados a este fenómeno com uma frequência diária. Nesta continuidade, José Carlos Martins[64] justifica que se verificou uma alteração espacial do conflito do mundo físico para o virtual, sendo que "hoje em dia é difícil não visualizarmos conflitos que não tenham expressão no ambiente ciber". De acordo com Esteves (2012), o *hacktivismo* é "um fator de risco para a segurança e a fiabilidade das comunicações e dos sistemas de informação sobre os quais assenta o funcionamento da nossa sociedade pública e privada, transformando-a numa «infraestrutura crítica» nacional" (p. 47).

A maioria dos entrevistados, no âmbito desta dissertação, reconheceu que o *hacktivismo* é um fenómeno significativo em Portugal. Contudo, parece não ter havido um

[62] Conforme a análise de recortes de imprensa em Apêndice J.
[63] Conforme entrevista em Apêndice F.
[64] Conforme entrevista em Apêndice H.

aumento dos casos. Rui Moura[65] indica que o "potencial impacto que pode ter ao nível político, social, económico e criminal" são fatores que proporcionam que o *hacktivismo* seja um fenómeno relevante na nossa sociedade. Porém, o impacto mediático pode por vezes ultrapassar os danos provocados nos sistemas, uma vez que a credibilidade da instituição é colocada em causa.

Paulo Santos[66] refere que a evolução deste fenómeno na sociedade portuguesa se deve, essencialmente, ao desenvolvimento da cidadania digital, que, segundo este, é talvez a principal motivação para a realização de ciberataques. De acordo com Vitor Costa[67], houve um aumento acentuado dos incidentes de segurança, no caso concreto do MAI, em outubro e novembro do ano de 2011, período durante o qual o COSI esteve "constantemente sob alvo de ataque de *hackers"*[68]. Este pico relacionou-se com manifestações em que a PSP teve necessidade de intervir, havendo no COSI da SGMAI "uma reação quase imediata" e "direta" em termos de aumento do número de incidentes. Pode apontar-se, portanto, para a existência de uma relação entre os eventos que têm lugar no mundo físico e os ataques *hacktivistas* que se processam no ciberespaço. Honorato (2013)[69] refere que durante o mês de setembro de 2012 houve alguns momentos, como o Conselho de Estado (22 e 23 de setembro), a manifestação na Assembleia da República (24 de setembro) e as declarações do Primeiro-Ministro (24 de setembro), durante os quais se assistiu a um aumento exponencial de acessos a páginas do Governo.

O *hacktivismo* surgiu em Portugal sensivelmente a partir de 2011, de acordo com o Dirigente do SIS[70], e desde então houve já algumas situações relacionadas com este fenómeno em Portugal. Com base na análise dos recortes de imprensa analisados (ver Apêndice J), foi possível identificar alguns acontecimentos, que estão alegadamente relacionados com o *hacktivismo*, nomeadamente em setembro de 2011 o grupo *LulzSec* terá atacado o *site* das Finanças, tendo provocado a lentidão do mesmo. No mesmo mês, o grupo terá desenvolvido um ataque contra o SIS, o Partido Social Democrata (PSD), o Partido Socialista (PS), o Partido do Centro Democrático e Social (CDS-PP), entre

[65] Conforme entrevista em Apêndice D.
[66] Conforme entrevista em Apêndice E.
[67] Conforme entrevista em Apêndice F.
[68] Este episódio esteve na origem da implementação do COSI (ver entrevista a Vitor Costa em Apêndice F).
[69] Intervenção feita por Manuel Honorato, representante da CEGER (Centro de Gestão da Rede Informática do Governo), em 12 de setembro de 2013, no seminário internacional "*Cyber Security: na action to establish the national cyber security center*".
[70] Conforme entrevista em Apêndice I.

outros[71]. Em novembro de 2011, foi realizado um ataque ao *site* do sindicato nacional da carreira de Chefes da PSP, tendo sido divulgados dados pessoais e confidenciais (patentes, telefones e endereços eletrónicos) de 107 elementos da PSP. O ataque foi assumido pelo grupo *LulzSec* Portugal, o qual justificou no *Twitter* que a ação era uma resposta à ação de agentes provocadores infiltrados na manifestação de dia 24 de novembro. Em dezembro de 2011, o grupo *Luzleaks* terá desenvolvido um ataque contra o Ministério da Economia[72].

Durante o mês de novembro de 2012, o grupo *LulzSec* Portugal terá dirigido um ataque contra o Banco de Portugal e contra o Parlamento, tendo deixado os seus *sites* inacessíveis durante horas. Em abril de 2013, o grupo *SideKingdom12* terá convocado uma operação que deixou indisponíveis os *sites* do PSD, PS, CDS-PP, do Governo, da PSP e da GNR. Alegadamente, o objetivo seria o protesto contra as medidas de austeridade[73].

Em abril de 2014, terá sido divulgada uma lista com os contactos de dois mil procuradores do MP, no âmbito da operação "Apagão Nacional". Os *sites* da Procuradoria-Geral da República, da Procuradoria-Geral Distrital de Lisboa ficaram inoperacionais durante o dia 25 de abril. Em maio do mesmo ano, o *Sidekingdom* 12, um subgrupo do grupo *Anonymous* Portugal, terá divulgado uma lista de 300 veículos policiais descaracterizados, utilizados em operações de trânsito pela PSP e GNR. Em agosto de 2014, o Grupo *Anonymous* Portugal desenvolveu uma operação designada "Novo Sangue", contra o Banco de Portugal e o Novo Banco, tendo divulgado mais de 200 *emails* destas instituições[74].

Relativamente a fevereiro de 2015, os *Anonymous* Portugal terão desenvolvido um ataque à Comissão de Carteira Profissional de Jornalistas, onde tiveram acesso a mais de 470 mil documentos e 322 *emails* e *passwords* de jornalistas e juízes. O ataque foi desenvolvido pelo *hacker Outsiderz Arcainex*, que opera nos Grupos *Hackers Street*, *SideKingdom12* e *OutsideTheLaw*. Em 26 de fevereiro de 2015 teve lugar a operação C4R3T0S (Caretos) da PJ, que resultou na detenção de sete pessoas do Grupo *Anonymous* Portugal[75]. Esta operação contribuiu para a moderação deste fenómeno[76].

---

[71] Como resultado desta ação terá sido publicado um vídeo, que incentiva à revolta da população portuguesa, contra a corrupção. Disponível em https://www.youtube.com/watch?v=-QUhfMf6J78.
[72] Conforme consta na análise dos recortes de imprensa em Apêndice J.
[73] *Idem.*
[74] *Idem.*
[75] *Idem.*
[76] Ver entrevistas em Apêndice H e I.

Os dados, aos quais tivemos acesso[77], relativamente aos incidentes de segurança registados no COSI da SGMAI em 2014[78], apontam no sentido de terem sido contabilizados 6810 *tickets*[79], sendo os incidentes mais reportados o *exploit attempt*[80], o *malware distribution*[81] e o *system infection*[82]. De acordo com a taxonomia do CERT.PT[83], os eventos podem ser inseridos nas seguintes classes: disponibilidade, fraude, *malware*, recolha de informação, segurança da informação e tentativa de intrusão[84]. O *malware* foi o grande vetor de ataque ocorrido em 2014 embora a maioria destes incidentes de segurança tenha ocorrido em dispositivos móveis ou tenham sido automaticamente mitigados pelos sistemas de segurança da SGMAI. As tentativas de intrusão resultaram em tentativas de exploração de vulnerabilidades. Os ataques contra a disponibilidade dos sistemas informáticos foram os que causaram maior impacto na largura de banda larga, assumindo especial relevância, neste âmbito, os *Distributed Denial of Service* (DDoS) e os DoS.

De acordo com o mesmo relatório, os EUA espoletaram o maior número de incidentes de segurança (40 %), devido à sua dimensão, facilidade para alugar servidores virtuais e ao facto de existirem diversos servidores comprometidos. Cerca de 26 % dos incidentes de segurança verificados na SGMAI tem origem em Portugal[85].

Os ataques *hacktivistas* podem provocar várias consequências, nomeadamente a nível económico, social, político e de segurança. Estes ataques poderão colocar em causa a confiança depositada pelos cidadãos nas instituições vítimas destes grupos, como realça Paulo Santos[86], mas também a identificação de vulnerabilidades e influência de outras pessoas com determinados ideais são situações que poderão acontecer. Para Vitor Costa[87], as consequências dependem do tipo de ataque em causa, podendo ser o roubo de informação, a indisponibilização de serviços ou a alteração da informação. No caso das FS é importante considerarmos, desde logo, que um ataque deste calibre irá afetar a confiança

[77] Ver Tabela 1, disponível em Anexo B.
[78] Pedido de colaboração em Apêndice C),
[79] *Reports* de incidentes para análise. Desde finais de 2013 que o COSI da SGMAI utiliza uma ferramenta interna de *ticketing* orientada para a resposta a incidentes de segurança, designada RTIR. Para mais informação consultar: https://bestpractical.com/rtir/ (consultado em 29 de março de 2015).
[80] Tentativa de exploração de uma determinada vulnerabilidade no sistema (FCCN, 2012).
[81] Distribuição de *malware*, ou seja, a infeção de um ou vários sistemas com um tipo de *software* malicioso (FCCN, 2012).
[82] Infeção de sistema informático.
[83] Em Portugal existe uma taxonomia publicada pelo FCCN que é adotada pelas entidades que fazem parte da rede CSIRT's.
[84] Ver Gráfico 1, disponível em Anexo B.
[85] Ver Gráfico 2, disponível em Anexo B.
[86] Conforme entrevista em Apêndice E.
[87] Conforme entrevista em Apêndice F.

que os cidadãos depositam nestas instituições, tratando-se de uma consequência simbólica, contudo, de grande importância. Por conseguinte, Rui Moura[88] indica que poderá estar em causa o sentimento de segurança das pessoas, bem como a desregulação social.

De acordo com o Dirigente do SIS[89], o *hacktivismo* apresenta uma tendência para se manter estável, sendo que os grupos vão aparecendo e os agentes vão mudando.

4.2. Grupos *Hacktivistas* em Portugal

A complexa teia de redes do ciberespaço não permite definir e delimitar com certeza quais os grupos *hacktivistas*. Sabemos, contudo, que um dos seus propósitos é a propaganda mediática de modo a tornarem visíveis as suas causas, pelo que muitas vezes o próprio grupo assume o ataque, seja no momento do ataque, por exemplo fazendo referência no *site* que é alvo, ou em manifestações nas redes sociais. Apesar disto, muitas vezes não é possível apurar a identidade das pessoas que fazem parte do mesmo, o que torna as investigações criminais levadas a cabo pela PJ[90] dificilmente concretizáveis, acabando por possibilitar o anonimato. Neste sentido, Carlos Cabreiro[91] refere que "na *internet* cada vez mais está a haver ferramentas e subterfúgios que tendem a anonimização da nossa conduta (…) e que nos obrigam a ter outros mecanismos de recolha de prova".

Os *hacktivistas* conhecem-se através das plataformas digitais e, regra geral, não se conhecem pessoalmente, toda a organização e comunicação é feita por este meio. De acordo com Carlos Cabreiro[92], "a união que possam fazer transparecer nas suas ações apenas se limita ao conhecimento virtual e feito via plataforma informática". Quanto ao perfil do *hacker*, pode dizer-se que se trata muitas vezes de jovens em idade escolar, que estão inseridos num contexto familiar desestruturado e apresentam problemas de sociabilização e integração na sociedade[93]. Existe outro grupo constituído por adultos, com mais algum conhecimento da realidade que os rodeia, que estão descontentes com alguma questão política ou social, o que os leva a desenvolver estes ataques.

---

[88] Conforme entrevista em Apêndice D.
[89] Conforme entrevista em Apêndice I.
[90] Órgão de Polícia Criminal com competência no âmbito do crime informático e praticado com recurso a tecnologia informática de acordo com a al. l) do n.º 3 do Art.º7.º da Lei da Organização de Investigação Criminal, aprovada pela Lei n.º 49/2008, de 27 de agosto, cuja última alteração foi introduzida pela Lei n.º 34/2013, de 16/05.
[91] Conforme entrevista em Apêndice G.
[92] *Idem.*
[93] Conforme entrevista a Dirigente do SIS em Apêndice I.

O que estes grupos pretendem, de acordo com Carlos Cabreiro[94], é "fazer ouvir a sua voz (…) contra uma determinada causa ou contra uma determinada realidade". Vitor Costa[95] defende que os grupos *hacktivistas* pretendem visibilidade, pois "dizer que o *site* da PSP ou a rede do MAI esteve em baixo ou obter uma informação dos agentes da PSP ou GNR tem sempre visibilidade". Pode ter a ver com o descontentamento das pessoas relativamente a alguma situação, de acordo com o relatório do COSI da SGMAI (2014), sendo as causas dos grupos *hacktivistas* principalmente políticas e relacionadas com a defesa dos direitos humanos. No caso dos jovens, fazem-no "para se promoverem dentro do grupo de amigos"[96], pois muitas vezes o que pretendem é sentir-se realizados e mostrar que são bons a fazer alguma coisa, "na maior parte dos casos eles não têm muito bem a noção do que fazem"[97].

Uma característica dos grupos portugueses é atacar *sites* desprotegidos e explorar vulnerabilidades. Planeiam os ataques em IRC's (*Internet Relay Chat)* e *chatrooms*, não assumem a sua identidade e utilizam *nicknames*. Os *hacktivistas* portugueses recorrem às ferramentas disponibilizadas *online* para realizar os ataques, ou seja, "não fabricam programas à medida, mas utilizam aqueles que estão disponibilizados na rede"[98]. Quanto às pessoas que assumem a organização e liderança deste tipo de iniciativas, são muitas vezes pessoas pouco especializadas tecnicamente, dedicando-se à realização de comunicados e à divulgação das ações a desenvolver, sendo que muitas vezes "aqueles que têm mesmo competências técnicas muito especializadas não têm noção que eles são dos mais competentes e especializados no grupo, pensam que são pessoas que sabem pouco e que estão só a ajudar outros que sabem mais"[99].

Estes grupos fazem propaganda para conseguir reunir seguidores nas redes sociais, de maneira a conferir mais algum impacto e dimensão aos seus ataques dirigidos contra alvos previamente estudados. De acordo com Paulo Santos[100], os *hacktivistas* "trabalham a engenharia social, ou seja, estudam os alvos e constroem soluções através das redes sociais". Com base em dados disponibilizados pelo COSI da SGMAI, é possível verificar

[94] Conforme entrevista em Apêndice G.
[95] Conforme entrevista em Apêndice F.
[96] Conforme entrevista a Dirigente do SIS em Apêndice I.
[97] *Idem.*
[98] Conforme entrevista a Paulo Santos em Apêndice E.
[99] Conforme entrevista ao Dirigente do SIS em Apêndice I.
[100] Conforme entrevista em Apêndice B.

que muitas vezes estes grupos disponibilizam informação relacionada com as suas ações nas redes sociais.

Segundo o COSI da SGMAI, durante o ano de 2014 foi possível identificar um novo grupo de *hacktivistas*, o *Worldmach1n3*. Estes intitulam-se como um grupo *hacktivista* independente na sua página do *facebook*[101]. Para além de muitas publicações que incentivam ao ataque a vários *sites* governamentais, encontram-se também disponíveis tutoriais, por exemplo, o de como fazer um ataque de *SQL Injection*[102] para principiantes[103]. Na mesma página encontramos referência à operação *OPDOWNPSP*, cujo alvo foi a PSP, no dia 1 de janeiro de 2014. Todavia, esta operação não despertou a atenção dos *media*, à exceção do *Tugaleaks*[104] que noticiou o ocorrido[105]. De acordo com este último, a motivação para os ataques prende-se com o negócio realizado de aquisição de *drones* para a PSP.

O grupo *LulzSec*[106], um grupo internacional, com representatividade em Portugal (*LulzSec* Portugal), é um dos mais referenciados nas notícias analisadas[107]. Alegadamente, as ações deste grupo fizeram-se notar mais a partir de 2011 quando se propuseram a invadir alguns sistemas, chegando mesmo a divulgar dados de elementos da PSP de Chelas[108], como resposta à ação da PSP na manifestação do dia 24 de novembro. A lista disponibilizada continha postos, patentes, endereços eletrónicos, números de telefone. Indignados com a atuação política e dos governantes, estes recorreram aos ataques informáticos para mostrarem o seu desagrado.

Os *Sud0H4k3rs* são um grupo que luta pela liberdade de expressão global, contra a corrupção governamental e corporativa e pelos direitos humanos. *Luzleaks* surge em dezembro de 2012, para denunciar a corrupção do país. Para além destes grupos, consideramos pertinente referir ainda outros cuja referência encontrámos na nossa análise

---

[101] Disponível em https://www.*facebook*.com/worldmach1n3 (consultado em 28 de fevereiro de 2015).
[102] Técnica designada de *Structured Query Language* (SQL) *Injection* aproveita-se de falhas e vulnerabilidades dos sistemas com vista à manipulação ou leitura de dados de uma determinada base de dados. É desenhada especificamente para invadir aplicações e roubar dados (FCCN, 2012).
[103] Disponível em https://www.*facebook*.com/worldmach1n3/timeline (consultado em 28 de fevereiro de 2015).
[104] Órgão de comunicação social *online*, que divulga frequentemente notícias de ataques informáticos e outros, um pouco à semelhança do Wikileaks. O seu diretor Rui Cruz foi um dos detidos na operação Caretos da PJ de 26 de fevereiro.
[105] Disponível em http://www.tugaleaks.com/psp-drones-ataque-informatico.html (consultado em 28 de fevereiro de 2015).
[106] Consultar o *facebook* dos *LulzSec*, disponível em https://www.*facebook*.com/Contingent.86 (consultado em 28 de fevereiro de 2015).
[107] Conforme análise de recortes de imprensa em Apêndice J.
[108] *Idem.*

dos recortes de imprensa[109]: *Anonymous Squad* n.º 666; *AntiSecPT*; *Team Whit3* Portugal; *Hackers Street*; *SideKingdom*12; *OutsideTheLaw*.

Embora tenhamos identificado algumas referências a estes grupos, não consideramos relevante para o presente trabalho caracterizar cada um deles. Em primeiro, porque a informação disponível é reduzida e pouco credível. Em segundo, porque muitas vezes estes grupos confundem-se, não se caracterizam individualmente, mediante a apresentação de determinadas características. Contudo, consideramos pertinente abordar em pormenor o grupo *Anonymous*, já que é o que apresenta maior mediatismo e o que parece ter uma atividade mais recorrente.

4.2.1. O grupo *Anonymous*

O grupo que tem vindo a gerar maior polémica é o *Anonymous*[110], um conjunto de *hacktivistas* que protagonizou ataques mediáticos. Este grupo não tem nenhum líder, organizam-se, recrutam e coordenam as suas ações em fóruns de conversação, como o *4chan*[111], e em redes sociais (Imperva, 2012). Embora sejam, maioritariamente, jovens e adolescentes, sobretudo nos EUA, as suas campanhas são suportadas por pessoas de todas as idades e em vários países. Tornaram-se famosos devido ao ataque à Igreja da Cientologia em 2008[112], começando a protagonizar com regularidade campanhas e ataques noutros domínios (Aguilar, 2010).

De acordo com o relatório da Imperva (2012), uma empresa de segurança informática, conclui-se que os *Anonymous* realizam dois tipos de ataques. Em primeiro lugar temos os reativos, quando a motivação para o ataque está noutro incidente, por exemplo, quando o *MasterCard* e *Visa* negaram apoio à *Wikileaks*, os *Anonymous*

[109] Conforme análise de recortes de imprensa em Apêndice J.
[110] *Site* oficial https://anonops.com/ (consultados em 28 de fevereiro de 2015).
[111] Fórum norte-americano de discussão e partilha de imagens. Disponível em https://www.4chan.org/ (consultado em 28 de fevereiro de 2015).
[112] Em janeiro de 2008 é feita a primeira aparição pública dos *Anonymous*, com a publicação de um vídeo no *youtube* intitulado "*Message to Scientology*" (Disponível em https://www.*youtube*.com/watch?v= JCbKv9yiLiQ). Tudo começou quando foi divulgado um vídeo de Tom Cruise no *Youtube* sobre a Igreja da Cientologia. Alegando violação de direitos de autor, a igreja solicitou ao *Youtube* que retirasse o vídeo, contudo, esta atitude não colheu concordância entre a comunidade *hacker*, defensores da liberdade de acesso à informação. Fruto desta situação teve início o projeto *Chanalogy*, foram desenvolvidos ataques cibernéticos, mas também ações de protesto no mundo físico contra a Igreja da Cientologia (Gutiérrez, 2012).

iniciaram a operação *Payback*[113]. Em segundo lugar, os pró-ativos, que se desenvolvem quando o grupo afirma que irá desencadear um ataque, sendo estes menos comuns.

No relatório acima indicado, a Imperva, fazendo uma análise de um ataque desenvolvido durante 25 dias no ano de 2011, descreve as três fases de desenvolvimento do ataque: a primeira fase (dia 1 a 18) é a do recrutamento e comunicação através das redes sociais e divulgação de vídeos no *youtube*, na qual tentam de algum modo justificar o ataque e convencer as pessoas; a segunda fase (dia 19 a 22) é a do reconhecimento e aplicação do ataque, em que cerca de 10 a 15 *hackers* exploram as vulnerabilidades do *site*, de maneira a tentar obter dados; quando a segunda fase não é bem conseguida, passam à terceira fase (dia 23 a 25), na qual tem lugar o DDoS, um ataque desencadeado com a ajuda das pessoas sem competências técnicas.

Os *Anonymous* utilizam métodos convencionais de *hacking* como *Havij*[114] e *SQL Injection*, sendo a sua principal inovação a criação de *sites* que realizam ataques DoS. Neste grupo estão envolvidos dois grupos de pessoas: um de *hackers* especializados, normalmente em menor número e com competências técnicas elevadas; outro de leigos, que pode já envolver dezenas ou centenas de voluntários, constituído por pessoas sem grande capacidade técnica, cujo papel é realizar DDoS (Imperva, 2012).

O seu lema é "nós não perdoamos, nós não esquecemos, esperem-nos". Utilizam simbolicamente a máscara do filme *V de Vingança*, produzido pelos irmãos Wachowski, em 2006, inspirando-se em Guy Fawkes, que conspirou para explodir o Parlamento britânico no ano 1605 (Gutiérrez, 2012). Este grupo globalizou-se e hoje desenvolvem ações em todo o mundo. Em Portugal, por exemplo, este grupo já tem alguma representação[115] e é talvez o mais mediático. Os grupos no *facebook* relativos aos *Anonymous* são imensos, parece que é uma tendência que se multiplicou. A título de exemplo, ficam algumas páginas de *facebook* relacionadas com este grupo, concretamente

[113] Em dezembro de 2010, a operação foi desenvolvida com recurso a DDoS, que incidiram sobre a *PayPal*, *Visa*, *MasterCard*, entre outros.
[114] Ferramenta de exploração de vulnerabilidades dos sistemas do tipo SQL.
[115] *Blog* oficial http://*Anonymous*pt.*Blogs*pot.pt/ e *facebook* https://www.*facebook*.com/*Anonymous*PORTUGAL (consultados em 7 de março de 2015).

os *Anonymous*PT*Hackers*[116], os *Shadow Elite_ Anonymous*[117] e os *Anonymous Legion* Portugal[118].

4.2.2. "Operações" coordenadas

As operações desencadeadas, no ambiente informático, pelos grupos de hacktivistas têm vindo a desenvolver-se nos últimos anos. A questão que se coloca neste momento é perceber qual a capacidade que têm estes grupos para concretizar um ataque que desencadeie consequências nas FS. As ferramentas para a realização de ataques encontram-se *online* e acessíveis a qualquer pessoa, havendo mesmo tutoriais que explicam e ensinam os mais inexperientes. De acordo com Vitor Costa[119], "este tipo de ataques está ao dispor de qualquer cidadão. É só a pessoa procurar na *internet*, as ferramentas, os métodos, os grupos e começar a participar. Estes grupos (…) [fazem] *workshops* de como fazer os ataques", o que nos leva a considerar que a ideia de um ataque não seja assim tão inexequível e longínqua quanto se julga.

Contudo, de acordo com o Dirigente do SIS as capacidades globais são baixas, sendo que por vezes existem algumas pessoas que dão nas vistas pela sua competência, mas o que acontece é que "a perceção e o impacto da ameaça é claramente superior à efetiva capacidade que eles têm"[120]. No caso português, os *hacktivistas* recorrem sobretudo à exploração de vulnerabilidades básicas dos sistemas, o que, de acordo com o mesmo entrevistado, não demonstra grande capacidade técnica por parte dos mesmos.

Neste sentido, para que o ataque produza os efeitos desejados é necessário muitas vezes haver uma coordenação entre as pessoas envolvidas, recorrendo à propaganda feita para operações que se pretendem desenvolver. Embora as novas tecnologias tenham afastado as pessoas e a sua forma de interação se tenha alterado, não podemos dizer que não exista organização nestes grupos. Estes estruturam-se através de redes sociais, como o *facebook* ou *twitter*[121], e utilizam-nos para divulgarem as ações perpetradas.

---

[116] *Facebook* disponível em https://www.*facebook*.com/*Anonymous*PT*Hackers (*consultado em 28 de fevereiro de 2015).
[117] *Facebook* disponível em https://www.*facebook*.com/pages/Shadow-elite_-*Anonymous*-Portugal/276532535857658?fref=ts (consultado em 28 de fevereiro de 2015)
[118] *Facebook* disponível em https://www.*facebook*.com/*Anonymous*LegionPt?fref=ts (consultado em 28 de fevereiro de 2015).
[119] Conforme entrevista em Apêndice C.
[120] Conforme entrevista a Dirigente do SIS em Apêndice F.
[121] De acordo com entrevista a Paulo Santos e Vitor Costa, em Apêndice B e C, respetivamente.

De acordo com os dados disponibilizados pelo COSI da SGMAI, tiveram lugar em 2014 algumas operações que foram acompanhadas por este organismo. A Operação "Valquíria", promovida pelos *Anonymous* Portugal e pelo *Shadow Elite* onde apelavam à não votação nas eleições legislativas de 2015. Os motivos prendem-se com o protesto contra o sistema democrático português, a corrupção e a constituição de elites políticas, a favor de uma maior representatividade e participação do povo. Esta operação foi acompanhada por alguns vídeos de propaganda[122].

A operação "*Stop Corruption Part 1"* foi uma operação promovida em fevereiro por elementos do *Team Whit3* Portugal contra *sites* do Governo através de DDoS[123].

"RiosAoCarmo" foi uma operação promovida pelos *AnonymousLegionPt*[124] para o dia 24 de abril de 2014, que previa um ataque DDoS[125]. Na lista de alvos disponibilizada na rede[126] é feita referência a *sites* de partidos políticos como o PS e PSD.

Por último, a operação "*System Failed"*, promovida em junho de 2014 por *AnonymousLegionPt* e *SUD0H4K3RS*[127] contra bancos portugueses e entidades políticas relacionadas. Esta operação foi acompanhada por um vídeo de propaganda[128].

4.3. As Forças de Segurança: um Alvo Apetecível

A PSP e GNR têm missões semelhantes, que passa por assegurar a legalidade democrática, garantir a segurança interna e os direitos dos cidadãos, conforme previsto nas suas Leis Orgânicas[129]. A PSP é uma FS uniformizada, armada e organizada hierarquicamente (Art.º 1.º da Lei n.º 57/2007 de 31 de agosto), enquanto a GNR é uma FS de natureza militar, com elementos organizados num corpo especial de tropas (Art.º 1.º da Lei nº 63/2007 de 6 de novembro).

---

[122] Vídeo de propaganda disponível em https://www.*youtube*.com/ watch?v= 1RE2ee1fQ5A (consultado em 28 de fevereiro de 2015).
[123] Evento disponível em https://www.*facebook*.com/events/397504820385327/permalink/ 400247450111 064/ (consultado em 28 de fevereiro de 2015).
[124] *Facebook* disponível em https://www.*facebook*.com/*Anonymous*LegionPt (consultado em 28 de fevereiro de 2015).
[125] Disponível em http://pastebin.com/63uxSyfd (consultado em 28 de fevereiro de 2015).
[126] Disponibilizada em http://pastebin.com/tT24ngbu (consultado em 28 de fevereiro de 2015).
[127] *Facebook* disponível em https://www.*facebook*.com/SUD0H4K3RS (consultado em 28 de fevereiro de 2015).
[128] Disponível em https://www.*youtube*.com/watch?v=YFq8_cDtxE8 (consultado em 28 de fevereiro de 2015).
[129] A Lei n.º 57/2007 de 31 de agosto, que aprova a Lei Orgânica da PSP e a Lei n.º 63/2007 de 6 de novembro, que aprova a Lei Orgânica da GNR.

De acordo com Vitor Costa, os incidentes de segurança nas FS são recorrentes e acontecem praticamente todos os dias[130]. Para Rui Moura[131], as FS são um potencial alvo dos grupos *hacktivistas* "pelo valor intangível que tem a informação residente na PSP e GNR [e] pelo impacto que pode causar na sociedade a inoperação da PSP e GNR derivada de um ataque". Já Paulo Santos[132] considera que os principais alvos destes grupos são os *sites* governamentais e não tanto as FS. De acordo com este entrevistado, "o cidadão tem confiança nas FS e considera que os *sites* destas são meramente instrumentais, pelo que não motivam a execução de ataques contra as mesmas, a não ser que apresentem fragilidades brutais em termos tecnológicos".

O Dirigente do SIS afirma que as FS "têm sido sempre um alvo em reação a eventos do mundo real"[133], ou seja, foram alvo de ataques *hacktivistas* em resposta a episódios que motivaram os *hacktivistas* a contestar. De acordo com o mesmo, a GNR não é um alvo tão assíduo pois a "maior parte desses eventos não acontecem na área da GNR", isto é, o contacto direto com o cidadão, exigindo, por vezes, situações de maior demonstração de força, provoca insatisfação e revolta por parte dos cidadãos.

Existe uma relação entre as situações que são relatadas pela imprensa, em que é construída uma perceção nas pessoas, conduzindo-as a manifestarem o seu desagrado. De acordo com Elias (2015), "as novas tecnologias são utilizadas como meio de subversão e de desinformação, sobretudo em acções de deslegitimação da actuação da Polícia e da Justiça após manifestações mais mediáticas" (p. 18). Com o surgimento dos novos *media*, motivada pelo desenvolvimento da *internet*, também a formação da opinião pública se alterou. Hoje em dia, qualquer um pode expressar-se no ciberespaço, sendo que estes novos contornos da sociedade permitem que, por vezes, pessoas passem a assumir certos factos como realidade, quando muitas vezes não o são[134].

Os *hacktivistas* veem nas FS uma representação do poder do Estado, e por vezes realizam ações contra estas, mas com o propósito de atingir o próprio Estado, descredibilizando-o. De acordo com Esteves (2012), o Sistema de Segurança Interna é um

---

[130] Conforme entrevista em Apêndice C.
[131] Conforme entrevista em Apêndice A.
[132] Conforme entrevista em Apêndice B.
[133] Conforme entrevista em Apêndice F.
[134] Veja-se o caso do vídeo que se tornou viral de um menino que, fingindo-se de morto, salva uma menina de baixo de disparos de armas de fogo, na Síria. O vídeo tornou-se notícia, foi transmitida por vários OCS por todo o mundo, tornou-se viral e foi assumido como verdadeiro, quando se veio a constatar que afinal o vídeo não era real, mas fruto de uma campanha publicitária para um filme. Este exemplo, bem como este assunto, foram abordados no II Curso de Cibersegurança e Gestão de Crises no Ciberespaço do IDN, decorrido ao abrigo das *Chatham House Rules*.

alvo especialmente visado pelo "simbolismo de autoridade que representa e pela sensibilidade e reserva que as matérias manuseadas implicam" (p. 47), nomeadamente as Forças e Serviços de Segurança (FSS).

Ainda outra razão identificada poderá ser a visibilidade que é dada à mensagem dos *hacktivistas* quando o alvo é as FS. Para Vitor Costa, o que os *hacktivistas* pretendem é visibilidade e "dizer que o *site* da PSP ou a rede do MAI esteve em baixo ou obter uma informação dos agentes da PSP ou GNR, tem sempre visibilidade".

Importa salientar que estes grupos gerados *online*, para além dos ciberataques que desenvolvem, também transportam a sua mensagem de protesto e indignação para o mundo físico, fazendo manifestações, também elas, mediáticas (Elias, 2015). Neste sentido, importa também às FS manterem uma monotorização atenta das redes sociais, para antever possíveis situações de desordem pública e atentados à paz e à tranquilidade pública.

4.4. *Hacktivismo*: uma Ameaça à Segurança?

Tendo em conta a caracterização dos grupos *hacktivistas* realizada, torna-se fulcral neste momento percebermos se o fenómeno *hacktivista* tem características que o tornam uma ameaça à Segurança e, em concreto, às FS. De acordo com Argomaniz (2014):

> A utilização perniciosa do ciberespaço chegou até nós sem aviso prévio, teve um período de gestação muito curto, e apenas nos últimos anos é que nós atingimos um nível onde o problema se tornou suficientemente sério para merecer a atenção das autoridades. (p. 5)

Segundo Abel Couto (1988), uma ameaça é "qualquer acontecimento ou acção (em curso ou previsível) que contraria a consecução de um objectivo e que, normalmente, é causador de danos, materiais ou morais" (p. 329). As ameaças podem ser consideradas naturais ou intencionais. Neste âmbito, torna-se relevante explorar as ameaças intencionais, de maneira que devem ser considerados três requisitos para que a mesma se verifique: a intenção (desejos e expetativas), a capacidade (recursos e tecnologias) e a oportunidade, ou seja, a relação existente entre fatores que permitam a concretização dos objetivos (p. e. fatores ambientais, sociopolíticos, entre outros) (Torres, 2009). Couto (1988) considera que "a avaliação das intenções é mais incerta, vaga e insegura, exigindo uma penetrante análise dos interesses nacionais e dos objectivos específicos em jogo (p. 329).

A valoração das ameaças é uma missão principalmente atribuída aos serviços de informações, sendo a sua principal preocupação a componente intenções, cuja informação é cada vez mais acessível através da *internet*, o que exige um acompanhamento atento do ciberespaço (Torres, 2009). Neste sentido, o Dirigente do SIS refere, a propósito do *hacktivismo,* que "neste momento a ameaça é moderada pelo potencial da ameaça mas reduzida pela ação dos grupos atualmente identificados, porque esses foram contidos no âmbito da operação da PJ"[135]. Assim, a última operação da PJ contribuiu para dissuadir os indivíduos que fazem estes ataques e, por isso, considera-se que se trata de uma ameaça reduzida. Contudo, o potencial dos danos que pode provocar, tornam o *hacktivismo* uma ameaça moderada.

Quanto à intenção, os *hacktivistas* pretendem expressar a sua opinião sobre determinado assunto, sob forma de protesto ou contestação, utilizando técnicas de *hacking*, para chamarem a atenção dos *media*. Essas técnicas de *hacking* podem atingir os *sites* ou os sistemas das FS, alterando-os, tornando-os mais lentos, inacessíveis ou mesmo extraindo-lhes informação.

Quando analisamos os ciberataques desencadeados contra as FS portuguesas, percebemos que dificilmente se consegue antever a motivação ou o fenómeno que proporcionou a ocorrência de tal ataque. A verdade é que é muito difícil verificar qual a origem dos ciberataques, pois embora se consiga saber o IP de origem, hoje em dia, é já possível esconder a sua proveniência[136].

Quanto à capacidade, sabemos que qualquer um que tenha interesse em aprender, consegue fazê-lo através da *internet*. Não são raros os casos de tutoriais que explicam como fazer um ciberataque[137]. Quanto à oportunidade, hoje em dia, resume-se a ter uma máquina com acesso à *internet*, de acordo com Nunes (2012), nos ataques feitos com recurso às TIC, utilizam-se meios "relativamente baratos, fáceis de contrabandear, praticamente indetetáveis e difíceis de correlacionar" (p. 117).

Neste sentido, é possível indicar o *hacktivismo* como uma possível ameaça à Segurança, o que é também demonstrado nas entrevistas realizadas, nas quais todos os intervenientes consideraram o fenómeno uma ameaça efetiva à Segurança. De acordo com Rui Moura[138], por exemplo, deve-se aos "potenciais impactos que a concretização das

[135] Conforme entrevista em Apêndice F.
[136] De acordo com Vitor Costa, cuja entrevista se encontra em Apêndice C.
[137] Conforme entrevista a Vitor Costa em Apêndice F.
[138] Conforme entrevista em Apêndice A.

ações *hacktivistas* podem ter ao nível da Segurança [porque] revestem-se de um elevado grau de produção de danos, cuja recuperação/reposição da normalidade pode ser muito onerosa (tempo e dinheiro) para a Segurança". Nas palavras de Vitor Costa[139], temos de considerar o *hacktivismo* como uma ameaça pois, atualmente, as FS utilizam estas ferramentas digitais no seu dia a dia e, a partir do momento em que exista uma intrusão nas infraestruturas do MAI, poderá ser colocada em causa a estabilidade dos seus sistemas de informação ou tornar indisponíveis as aplicações utilizadas pelas FS. Carlos Cabreiro[140] defende a perspetiva de que além de disruptivos, estes ataques *hacktivistas* podem colocar em causa a informação das instituições, pelo que considera que são "uma ameaça contra a segurança do Estado ou contra a segurança dos cidadãos a partir do momento em que as suas instituições são atacadas".

Um ataque deste género pode, concretamente, causar consequências no desempenho da missão das FS e Vitor Costa[141] reitera que, logo que os sistemas centrais sejam afetados, a missão das FS pode sair prejudicada, uma vez que atualmente estas instituições utilizam muito as ferramentas e aplicações tecnológicas, pelo que se "uma ação destas se for bater no sítio certo de forma eficiente pode afetar as FS". De acordo com Carlos Cabreiro[142], "depende do impacto que esse ataque tiver porque se afetar setores vitais, como por exemplo, a informação que estiver no âmbito das FS" pode provocar consequências nefastas. Na possibilidade de se verificar um ataque *hacktivista* contra as infraestruturas das FS, Paulo Santos[143] considera que "pode ter um efeito catastrófico, podendo provocar um alarme social brutal", uma vez que o cidadão não espera que instituições credíveis, como a PSP e GNR, partilhem informações erradas. Por outro lado, José Carlos Martins[144] refere que um ciberataque pode mesmo colocar em causa a operacionalização das FS. Viana (2012) chama a atenção para o facto de, em Portugal, a *internet* ser a base de comunicação entre FS, Forças Armadas, Serviços de Informações e Governo. Neste sentido, importa recordar que a rede SIRESP sustenta a comunicação entre FS no terreno e se essa for afetada vai dificultar a atuação e a proatividade das FS, o que possivelmente representará uma dificuldade no desempenho da sua missão[145].

---

[139] Conforme entrevista em Apêndice C.
[140] Conforme entrevista em Apêndice D.
[141] Conforme entrevista em Apêndice C.
[142] Conforme entrevista em Apêndice D.
[143] Conforme entrevista em Apêndice F.
[144] Conforme entrevista em Apêndice H.
[145] Conforme entrevista a Vitor Costa, em Apêndice F.

Face à ocorrência de ciberataques é essencial fazer-se uma gestão do risco adequada para antecipar os possíveis ataques que podem ter lugar no ciberespaço contra os sistemas de informação. De acordo com Torres (2009), o risco pode ser considerado "a probabilidade de uma determinada ameaça explorar com sucesso uma vulnerabilidade potencial do sistema, resultando um determinado impacte num activo crítico para a missão e objectivos e uma empresa, instituição ou Estado" (p. 50).

Independentemente das medidas de segurança que se adotem, torna-se praticamente impossível anular o risco de concretização de uma ameaça. Na opinião de Carlos Cabreiro[146], "em matéria de segurança informática costuma-se dizer que não há uma segurança total e não há sistemas 100% seguros". Por mais esforço que se faça para o diminuir, uma parte do risco permanece inalterável. De maneira que o objetivo não deverá ser uma estratégia de eliminação do risco, uma vez que simplesmente não é possível eliminá-lo, mas antes uma estratégia baseada na previsão de cenários possíveis, para que os riscos sejam previamente calculados e os procedimentos e planos de contingência desenvolvidos (Torres, 2009).

De acordo com o Dirigente do SIS[147], ainda há muito trabalho a fazer no que diz respeito a vulnerabilidades dos sistemas, bem como do ponto de vista da cibersegurança. Faz também referência à dificuldade em construir capacidades operacionais para fazer frente a *hackers* especializados e com competências sólidas e desenvolvidas, uma vez que o investimento que é preciso fazer em cibersegurança não é proporcional ao que é necessário para desenvolver ciberataques, já que "uma pessoa bem formada que saiba, com *skills*, com computador portátil e poucos recursos económicos consegue produzir um grande efeito". Segundo Paulo Santos, "só se combate o *hacktivismo* com colaboração e coordenação entre instituições responsáveis e com competência no âmbito da cibersegurança".

Por último, Silva (2014) faz uma sugestão interessante que se relaciona com a criação de equipas vermelhas, como acontece no Reino Unido, com o propósito de detetar vulnerabilidades fazendo uma avaliação rigorosa da organização. Uma possibilidade avançada passaria também pela contratação de *hackers* éticos, o que no nosso entender seria benéfica para as organizações, pois de forma proactiva seria possível combaterem as ameaças encontradas.

[146] Conforme entrevista em Apêndice D.
[147] Conforme entrevista em Apêndice F.

Conclusão

A sociedade em rede elegeu o ciberespaço como o novo espaço predominante e que liga as pessoas a uma escala planetária. Este possibilita tornar os processos comunicacionais e de interação mais rápidos e eficientes, conferindo à economia um espaço privilegiado para se desenvolver e prosperar.

Para além do fluxo de informação, o crime desloca-se para o espaço digital e tem vindo a aumentar e a desenvolver-se em termos de sofisticação. Concretamente, o *crime-as-a-service* tem vindo a ganhar terreno, tratando-se de um fenómeno preocupante. A par de uma criminalidade tradicional que tem agora um novo meio para se desenvolver, surge o crime informático, relacionado estritamente com computadores e sistemas informáticos. Para reduzir drasticamente o fenómeno do cibercrime, considerado como uma prioridade estratégica para UE, é necessário que exista um suporte legislativo rigoroso, capaz de produzir resultados práticos e eficientes. Contudo, não basta que cada Estado autonomamente tome medidas e prossiga um caminho sem a cooperação de outros atores políticos. Face a esta realidade, torna-se essencial promover mecanismos de cooperação interestatais, de forma a garantirmos a segurança no espaço digital.

Na atualidade, a segurança torna-se num conceito mais alargado e complexo. As fronteiras diluíram-se e já não somos capazes de separar os conceitos de segurança e defesa como o fazíamos, já que as ameaças são comuns e partilhadas, devido ao seu caráter transnacional. As ameaças multiplicam-se no espaço digital e tornaram-se transversais aos vários setores da sociedade. Os conflitos deixam de ser locais para chegarem a qualquer parte do mundo e a resposta para este problema está certamente na cooperação entre as várias entidades nacionais com competência no âmbito da cibersegurança, mas também na cooperação internacional.

O *hacktivismo* é encarado como um novo desafio para as instituições e especialmente, no caso das FS, um ataque *hacktivista* pode provocar consequências nefastas, que podem influenciar inclusive o desempenho das suas missões, sendo portanto considerado uma ameaça real, no sentido em que para Couto (1988) esta é caracterizada por contrariar os objetivos da organização, produzindo, por norma, danos materiais e/ou morais.

As FS recorrem, cada vez mais, às TIC no desempenho da sua atividade, sendo importante relembrar que, por exemplo, para comunicarem no terreno recorrem à rede

SIRESP. Ora, as consequências que um ataque desta índole pode ter para as FS passam pela alteração da informação ou pelo roubo de dados que, quando mediatizado pelos OCS, pode provocar a descredibilização da instituição afetada. Em último caso, poderá mesmo provocar sentimento de insegurança e desregulação social.

As capacidades de concretização de um ataque pelos grupos *hacktivistas*, por norma, são baixas, pois os mesmos recorrem a ferramentas disponíveis na rede e não são muito inovadores em matéria de *hacking*, tirando proveito da exploração de vulnerabilidades já existentes. No que diz respeito à oportunidade, qualquer pessoa a partir de um computador com acesso à rede e com algum conhecimento ou vontade de aprender a partir da informação disponibilizada na rede é capaz de desenvolver um ciberataque, e esse facto torna-se preocupante para as FS.

Concluímos, portanto, que o *hacktivismo* é uma ameaça para a Segurança, uma vez que pode colocar em causa a segurança da informação, das infraestruturas e das pessoas, reunindo para isso os critérios da intenção, da capacidade e da oportunidade. O *hacktivismo* é, igualmente, considerado uma ameaça moderada pelo seu potencial. Todavia, não sendo possível evitar que a ameaça aconteça, há que ser feita uma gestão do risco adequada pelas instituições, definindo-se procedimentos, objetivos, prioridades e planos de contingência, de modo a anteciparmos as respostas eficazes para um eventual ataque.

Tendo em conta que as FS são um alvo preferencial destes grupos de *hacktivistas*, torna-se premente estudar esta ameaça, bem como as vulnerabilidades existentes nas nossas infraestruturas de comunicação e informação, por forma a estarmos preparados para um eventual ataque. Quanto aos objetivos específicos, concluímos que o *hacktivismo* tem alguma representatividade em Portugal, já que verificamos alguns ataques recentes e com alguma importância mediática. No que diz respeito aos elementos envolvidos, em Portugal, constatamos a existência de referências a grupos distintos, todavia, os que assumem maior relevância são o *Anonymous* e o *LulzSec*. Estes grupos organizam-se através da *internet*, sobretudo por meio das redes sociais e desenvolvem a sua atividade com base no anonimato.

Quanto ao perfil do *hacktivista*, podemos verificar que os grupos são constituídos por pessoas de todas as idades. No caso dos jovens o objetivo passa sobretudo pelo desafio e pelo reconhecimento no seu círculo relacional, enquanto no caso dos adultos o objetivo é sobretudo de contestação ou protesto. Para alcançar estes objetivos desenvolvem ataques

com vista a causar um dano sobretudo reputacional na instituição alvo do ataque. Assim, nesta distinção etária verificamos que existe um grupo de pessoas mais especializadas e outro de pessoas com poucas capacidades técnicas, mas que têm competências noutros domínios, concretamente em relações públicas, estabelecidas com vista a angariar simpatizantes. Os ataques desenvolvidos por estes grupos são variados, sendo seu objetivo atrair atenção mediática para as suas causas e, por isso, recorrem muitas vezes a ataques que possam colocar as instituições numa situação constrangedora e vulnerável.

Concluímos, também, que parece existir uma relação entre eventos do mundo físico e o aumento do número de ciberataques, o que deixa transparecer a ideia de que as pessoas recorrem ao *hacktivismo* para expressar o seu protesto e indignação perante uma situação que consideram inaceitável.

Apesar de conseguirmos distinguir, no plano teórico, as ameaças presentes no ciberespaço, na prática, torna-se difícil identificarmos qual a promotora de determinado ataque, uma vez que o ciberespaço possibilita o anonimato. Desta forma, no que concerne a ameaças presentes no ciberespaço, é essencial a existência de sinergias entre entidades públicas e privadas, no âmbito da partilha de informação, conhecimento e eliminação das vulnerabilidades.

É premente que se construa uma cultura de cibersegurança em Portugal para fazer face ao aumento do número de ciberataques. Os recém-criados CNCseg e o Centro de Ciberdefesa representam já um importante avanço nesse sentido. Contudo, a inexistência de um Estratégia Nacional de Cibersegurança é algo que se continua a verificar e que necessita de ser alterado. O atraso em aprovar esta estratégia traz inconvenientes, pois existem problemas e dificuldades que vão surgindo à medida que o ciberespaço se desenvolve. O caráter dinâmico do ciberespaço impõe-nos uma atualização constante e uma decisão rápida, sob pena de, quando aplicadas, as medidas se encontrarem já desatualizadas, de modo que a adoção de uma Estratégia Nacional de Cibersegurança é determinante e essencial para o combate eficaz ao *hacktivismo*.

A criação de um CNCseg e de um Centro de Ciberdefesa coloca-nos a questão de quem terá competência para agir em situações de ciberataques. Ora, a competência para intervenção da segurança ou da defesa deve residir não no campo da origem da ameaça como tradicionalmente acontecia, mas no campo do impacto e da dimensão do ataque. Assim, uma resposta adequada seria a constituição do Conselho Nacional de Cibersegurança e de um Gabinete de Gestão de Crises, capazes de fazer face a incidentes

de segurança informáticos de grande envergadura. A construção de uma cultura de cibersegurança em Portugal requer que todos os responsáveis assumam uma parte interveniente no processo. Deste modo, é essencial que se perceba que também as FS têm um papel fundamental neste âmbito e este trabalho de investigação pretende ser um contributo nesse sentido.

Uma das principais limitações para a realização deste trabalho foi a escassez de bibliografia encontrada, pelo que tentámos contornar o problema recorrendo a entrevistas realizadas a especialistas e a responsáveis no âmbito estudado. Recorremos também a recortes de imprensa e informação disponível nas redes sociais, uma vez que a informação que pretendíamos – concretamente no que diz respeito aos eventos que ocorreram em Portugal no âmbito do *hacktivismo* e aos grupos *hacktivistas* envolvidos – não nos foi cedida pelas instituições em causa, por se tratar de uma matéria delicada, sendo esta última, um entrave importante para um maior e melhor conhecimento da temática abordada.

Terminado o trabalho de investigação a que nos propusemos, surgem-nos algumas temáticas que consideramos relevantes para estudos futuros. O cibercrime apresenta-se como um tema inovador de relevância inegável, que carece de investigação. Percebemos que os ciberataques levados a cabo têm várias motivações intrínsecas, as quais merecem um estudo aprofundado, pelo que consideramos relevante o estudo da ciberespionagem e da utilização das TIC pelos grupos terroristas. Seria importante estudar o papel da PSP no âmbito da cibersegurança, concretamente no que concerne à sensibilização e prevenção do crime *online*, tendo em conta o Projeto *Internet* Segura, do qual são parceiras as FS.

Por último, de maneira a sedimentar uma cultura de cibersegurança nas FS, sugerimos a criação de uma linha de investigação na área da cibersegurança no Instituto Superior de Ciências Policiais e Segurança Interna, uma vez que se trata de um tema de importância extrema e atual, que carece de estudo e no qual a PSP deve ter um papel ativo.

Lista de Referências

Bibliografia

Aristóteles, (2000). *O Tratado da Política* (2ª ed.). Lisboa: Publicações Europa-América.

Bigo, D. (2001). Security(s): Internal and external, the möbius ribbon. In M. Albert, D. Jacobson, & Y. Lapid (Eds.), *Identities, borders, orders* (pp. 91-116). Retirado de http://guessoumiss.files.wordpress.com /2011/08/identities-borders-orders.pdf.

Cardoso, G. (2014). *Os Media na Sociedade em Rede* (2ª ed.). Lisboa: Fundação Calouste Gulbenkian.

Castells, M. (2003). *O fim do milénio – A era da informação: Economia, sociedade e cultura* (Vol. 3). (A. Figueiredo, & R. Espanha, Trads.). Lisboa: Fundação Calouste Gulbenkian.

Castells, M. (2007). *A galáxia internet: Reflexões sobre internet, negócios e sociedade* (2ª ed.). (R. Espanha, Trad.). Lisboa: Fundação Calouste Gulbenkian.

Castells, M. (2011). *A Sociedade em rede - A era da informação: Economia, sociedade e cultura* (4ª ed., Vol. 1). (A. Lemos, C. Lorga, & T. Soares, Trads.). Lisboa: Fundação Calouste Gulbenkian.

Cavelty, M. D. (2012). The Militarisation of Cyber Security as a Source of Global Tension. In Möckli, Daniel, Wenger, Andreas (Eds.), *Strategic Trends Analysis* (pp. 103-123). Retirado de http://papers.ssrn.com/sol3/ papers.cfm?abstract_id =2007043

Couto, A. C. (1988). *Elementos de Estratégia: Apontamentos para um curso.* Lisboa: Instituto de Altos Estudos Militares.

Cruz, L. (2014). *O repórter como historiador do tempo presente: notas sobre a relação entre jornalismo e memória social* (Trabalho final, Rio de Janeiro, Escola de Comunicação da UFRJ). Retirado de https://www.academia.edu/8274541/ O_rep%C3% B3rter_como_historiador_do_tempo_presente_notas_sobre_a_rela %C3%A7%C3%A3o_entre_jornalismo_e_mem%C3%B3ria_social

Denning, D. E. (1999). Activism, hacktivism, and cyberterrorism: The internet as a tool for influencing foreign policy. In J. Arquilla, & D. Ronfeldt (Eds.), *Networks and netwars: The future of terror, crime, and militancy* (pp. 239–288). Retirado de

http://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch8.pdf

Dias, P. (2014). *Viver na sociedade digital: Tecnologias digitais, novas práticas e mudanças sociais.* Cascais: Princípia Editora, Lda.

Fernandes, J. (2014). *Os desafios da segurança contemporânea: Estado, identidade e multiculturalismo.* Lisboa: Pedro Ferreira-Artes Gráficas, Lda.

Gibson, W. (1984). *Neuromancer*. (A. Boyd, & L. Nahodil, Trads.). Retirado de http://www.libertarianismo.org/livros/wgneuromancer.pdf.

Guedes, A. M., & Elias, L. (2010). *Controlos remotos: Dimensões externas da segurança interna em Portugal.* Coimbra: Edições Almedina, SA.

Lévy, P. (2000). *Filosofia world: O mercado o ciberespaço, a consciência.* (C. Brito, Trad.). Lisboa: Instituto Piaget.

Lévy, S. (1984). *Hackers: Heroes of the Computer revolution.* Retirado de http://www.temarium.com/wordpress/wp-content/documentos/Levy_S-*Hackers*-Heroes-Computer-Revolution.pdf

Nye, J. S. (2012). *O futuro do poder*. (L. Santos, Trad.). Maia: Temas e Debates.

Pavia, J. F. (2012). Ameaças à segurança internacional: De acordo com o novo conceito estratégico da NATO aprovado em Lisboa, em 2010. In E. Correia, & R. Duque (Eds.), *O poder político e a segurança* (pp. 191-200). Lisboa: Fonte da Palavra.

Quivy, R., & Campenhoudt, L. (1998). *Manual de investigação em ciências sociais* (2ª ed.). (J. Marques, M. Mendes, & M. Carvalho, Trads.). Lisboa: Gradiva.

Raposo, J. (2006). *Direito Policial I*. Lisboa: Almedina.

Rodrigues, P. (2010). *Segurança informática de redes e sistemas* (Dissertação de Mestrado, Vila Real, Universidade de Trás-os-Montes e Alto Douro). Retirado de https://repositorio.utad.pt/bitstream/10348/747/1/MsC_pebrodrigues.pdf

Samuel, A. (2004). *Hacktivism and the future of political participation.* (Tese de Doutoramento, Cambridge, Harvard University). Retirado de http://www.alexandra samuel. com/dissertation/pdfs/Samuel-Hacktivism-entire.pdf

Santos, D. (2014). *A cibersegurança em Portugal: A ação política nacional em matéria de cibersegurança* (Dissertação de Mestrado). ISCTE, Lisboa.

Santos, J. (2011). *Contributo para uma melhor governação da cibersegurança em Portugal* (Dissertação de Mestrado). Universidade Nova de Lisboa, Lisboa.

Santos, L., Bravo, R., & Nunes, P. (2012). Protecção do ciberespaço: Visão analítica. In C. Guedes Soares, A. P. Teixeira, & C. Jacinto (Eds.), Riscos, *segurança e sustentabilidade* (pp. 163-176). Lisboa: Edições Salamandra.

Sarmento, M. (2013). *Metodologia científica: Para a elaboração, escrita e apresentação de teses*. Lisboa: Universidade Lusíada Editora.

Silva, N. (2012). *Cibersegurança: A Europol e Interpol face à cibercriminalidade* (Dissertação de Mestrado). Instituto Superior de Ciências Policiais e Segurança Interna, Lisboa.

Silva, S. (2014). *A Ciberespionagem no contexto português* (Dissertação de Mestrado). Academia Militar, Lisboa.

Simas, D. (2014). *O cibercrime* (Dissertação de Mestrado). Universidade Lusófona de Humanidades e Tecnologias, Lisboa.

Torres, J. (2009). *Terrorismo islâmico: Gestão dos riscos para a segurança nacional.* Lisboa: Centro de Investigação e desenvolvimento em Direito.

Tzu, S. (2009). *A arte da guerra*. Cascais: Vogais & Companhia.

Valente, M. M. (2013). *Segurança: Um tópico jurídico em construção*. Lisboa: Âncora Editora.

Fontes bibliográfica periódicas

Aguilar, L. J. (2010, dezembro). Introducción. Estado del arte de la ciberseguridad. *Cuadernos de Estrategia*, *149*, 13–49. Retirado de http://www.cni.es/comun/recursos/descargas/Cuaderno_IEEE_149_Ciberseguridad.pdf

Anderson, C., & Wolff, M. (2010, agosto) The web is dead. Long live the internet. *Wired magazine.* Retirado de http://www.wired.com/2010/08/ff_webrip/all/1

Argomaniz, J. (2014, setembro). European Union responses to terrorist use of the internet. *Cooperation and Conflict.* doi:10.1177/0010836714545690

Armstrong, I. (2013, novembro). Moving on up. *SC magazine*, *24*(11), 4. Retirado de http://media.scmagazine.com/documents/59/sc_can_1113_14740.pdf

Arnone, M. (2005, outubro). White hat, gray hat, black hat. *The business of federal technologie*. Retirado de http://fcw.com/Articles/2005/10/03/White-hat-gray-hat-black-hat.aspx?Page=3

Arquilla, J., & Ronfeldt, D. (1993). Cyberwar is coming!. *Comparative Strategy*, *12*(2), 23–60. Retirado de http://www.rand.org/content/dam/rand/pubs/reprints/2007/_RP223.pdf

Ashton, K. (2009, junho 22). That 'internet of things' thing. *RFID Journal*. Retirado de http://www.rfidjournal.com/articles/pdf?4986

Bejarano, M. (2011). Alcance y ámbito de la seguridad nacional en el ciberespacio. *Cuadernos de Estrategia*, *149*, 49−82. Retirado de http://dialnet.unirioja.es/descarga/articulo/3837251.pdf

Caldas, A. (2011). Uma Estratégia Nacional de Cibersegurança. *Segurança e Defesa*, *16*, 94–98.

Cardoso, R. (2012). Os piratas, a nuvem e a política. *Courrier Internacional*, *191*, 3.

Collin, B. (1997, março). The future of cyberterrorism. *Crime & Justice International,13.* Retirado de http://www.cjimagazine.com/archives/cji4c18.html?id=415

Demchak, C., & Dombrowski, P. (2011). Rise of cybered Westephalian Age. *Strategic Studies Quarterly*, *5*(1), 32–61. Retirado de http://www.au.af.mil/au/ssq/2011/spring/demchak-dombrowski.pdf

Esteves, P. (2012, maio). Hacktivismo, transpondo a fronteira entre a liberdade de expressão e o cibercrime. *Segurança e Defesa*, *21*, 45–47.

Farwell, J., & Rohozinski, R. (2011). Stuxnet and the future of cyber war. *Survival, 53*(1), 23–40. doi:10.1080/00396338.2011.555586

Fernandes, J. (2012). Utopia, liberdade e soberania no ciberespaço. *Nação e defesa*, *133*, 11–31.

Freire, F. V., & Caldas, A. (2013). O Ciberespaço: Desafios à Segurança e à Estratégia. *Atena, 30*, 90–168.

Freire, F. V., Nunes, V., Acosta, O., & Rojas, E. (2013). Estratégia da informação e segurança no ciberespaço. *Cadernos do IDN*, *12*.

Gelbstein, E. (2012). Protecting critical information infrastructures. *Nação e defesa*, *133*, 128–146.

Gutiérrez, B. (2012). Anonymous, a explosão do enxame. *Cadernos Adenauer XIII*, *3*, 135–148. Retirado de http://www.kas.de/wf/doc/9309-1442-5-30.pdf

Hampson, N. (2012). Hacktivism: A new breed of protest in a networked world. *Boston College International & Comparative Law Review*, *35*(2), 511–542.

Howard, M. (2006). A long war. *Survival*, *48*(4), 7–14. Retirado de http://www.iiss.org/-/media/Silos/Survival/2006/Survival--Global-Politics-and-Strategy-Winter-2006/48-4-01-Howard/ 48-4-01-Howard.pdf

Krauth, A. (2012, julho). Anonymous in portmanteaupia. *Social Alternatives, 31(2), 27–33*. Retirado de EBSCO.

Martins, M. (2012). Ciberespaço: Uma nova realidade para a segurança internacional. *Nação e defesa*, *133*, 32–49.

Mendonça, A. (2012). Diplomacia, tecnologia e informação. *Nação e defesa*, *133*, 50–58.

Moreira, J. M. (2012, novembro). O impacto do ciberespaço como nova dimensão nos conflitos. *Boletim de Ensino*, *13*, 27–50. Retirado de http://www.iesm.pt/cisdi/boletim/Artigos/Artigo_2.pdf

Nunes, P. V. (2012). A definição de uma Estratégia Nacional de Cibersegurança. *Nação e defesa*, *133*, 113–127.

Posen, B. R. (2003). Command of the commons: The military foundation of U.S. hegemony. *International Security*, *28*(1), 5–46. Retirado de http://web.mit.edu/ssp/people/posen/commandofthecommons.pdf

Thill, S. (2011, março 17). March 17, 1948: William Gibson, father of cyberspace. *Wired magazine*. Retirado de http://www.wired.com/2011/03/0317cyberspace-author-william-gibson-born/

Viana, V. R. (2012) Editorial. *Nação e defesa*, *133*, 5–7.

Relatórios e outros Documentos Institucionais

Anderson, K. (2008). *Hacktivism and politically motivated computer crime*. Retirado do *site* da Encurve, LLC: http://www.aracnet.com/~kea/Papers/Politically%20Motivated% 20Computer%20Crime.pdf

Bendiek, A. (2012) *European cyber security policy.* Retirado do *site* de German Institute for International and Security Affairs: http://www.swp-berlin.org/fileadmin/contents/ products/research_papers/2012_RP13_bdk.pdf

Comissão Instaladora do CNCseg (2012). *Relatório da Comissão Instaladora do Centro Nacional de Cibersegurança.*

European Police Office (2014). *The Internet Organised Crime Theat Assessment (iOCTA)*. Retirado de https://www.europol.europa.eu/ec3

Eurostat. (2014). *Information society statistics at regional level.* Retirado de http://ec.europa.eu/eurostat/statistics-explained/index.php/Information_society_ statistics_at_regional_level

FCCN. (2005). *Estrutura Nacional de Segurança da Informação (ENSI).*Retirado de https://www.fccn.pt/fotos/editor2/Seguran%C3%A7a/CERT/PolSegRCTS1112/ensi_politica_de_seguranca_da_informacao_da_entidade.pdf

FCCN. (2012). *Taxonomia comum para a rede Nacional de CSIRTs.* Retirado de http://www.cncs.gov.pt/cert-pt/documentos/

GNS. (2012). *Proposta de Estratégia Nacional de Cibersegurança.* Retirado de http://www.gns.gov.pt/media/1247/PropostaEstrat%C3%A9giaNacionaldeCiberseguran%C3%A7aPortuguesa.pdf

Imperva. (2012). *Imperva's hacker intelligence summary report: The anatomy of an Anonymous attack*. Retirado de http://www.imperva.com/docs/ HII_The_Anatomy _of_an_Anonymous_Attack.pdf

Klimburg e Tirmaa-Klaar (2011). *Cybersecurity and cyberpower: Concepts, conditions and capabilities for cooperation for action within the EU.* Retirado do site da UE: http://www.europarl.europa.eu/RegData/ etudes/etudes/join/2011/433828/EXPO-SEDE_ET(2011)433828_EN.pdf

Lewis, J. A. (2005). *Computer espionage, Titan Rain and China.* Retirado do *site* do Center for Strategic and International Studies: http://csis.org/files/media/csis/pubs/051214_ china_titan_rain.pdf

Libicki, M. C. (2009). *Cyberdeterrence and cyberwar.* Retirado do *site* da Rand Corporation: http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_ MG877.pdf

Secretaria-Geral do Ministério da Administração Interna (2015). *Relatório de Segurança COSI SGMAI 2014.*

Seybert, H., & Reinecke, P. (2014). *Half of Europeans used the internet on the go and a fifth saved files on internet storage space in 2014*. Retirado do *site* do Eurostat: http://ec.europa.eu/eurostat/statistics-explained/index.php?title=*Internet*_and_cloud_services_-_statistics_on_the_use_by_individuals

Sistema de Segurança Interna. (2014). *Relatório anual de Segurança Interna 2013.* Retirado de http://www.portugal.gov.pt/pt/documentos-oficiais/20140401-rasi-2013.aspx

União Europeia. (2008). *Relatório sobre a Execução da Estratégia Europeia de Segurança. Garantir a Segurança num Mundo em Mudança*. Retirado de http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/pt/reports/104638.pdf

World Economic Forum. (2015). *Global risks 2015.* Retirado de http://www.weforum.org/reports/global-risks-report-2015

Simpósios, Conferências e Cursos

Elias, L. (2014, outubro). *Dimensões securitárias na contemporaneidade.* Lição inaugural apresentada na Abertura Solene do Ano Letivo 2014/2015 do Instituto Superior de Ciências Policiais e Segurança Interna, Lisboa.

Guerra, C. (2015, janeiro). Mobilidade e appification: oportunidade ou desafio?. In *Privacidade, Inovação e Internet.* Conferência promovida pela APDSI, Lisboa.

Honorato, M. (2013, setembro) Ameaças, vulnerabilidades e pressões nos sistemas governamentais. In *Cyber Security: an action to establish the national cyber*

security center. Seminário promovido pelo GNS e pela AFCEA, Lisboa. Retirado de http://www.afceaportugal.pt/2013/eventos/Amea%C3%A7as,_Vulnerabilidades_e_Riscos_nos_Sistemas_Governamentais_%28GNS_-_AFCEA_-_12SET2013%29.pptx

IDN (2015, março). II Curso de cibersegurança e gestão de crises no ciberespaço. Lisboa.

Musso, P. (2013, junho). *Network Ideology: From saint-simonianism to the internet.* Paper apresentado na Conferência da Sociedade para a Filosofia e Tecnologia, Lisboa.

Documentos oficiais dos órgãos da União Europeia

COM (2001) 298 final (Segurança das redes e da informação: Proposta de abordagem de uma política europeia).

COM (2004) 702 final (Proteção das infraestruturas críticas no âmbito da luta contra o terrorismo).

COM (2006) 251final (Estratégia para uma sociedade da informação segura).

COM (2006) 786 final (Programa Europeu de Proteção das Infraestruturas Críticas).

COM (2009) 149 final (Proteger a Europa contra os ciberataques e as perturbações em grande escala: melhorar a preparação, a segurança e a resiliência).

COM (2010) 2020 (sobre uma estratégia para um crescimento inteligente, sustentável e inclusivo).

COM (2010) 245 final (Agenda Digital para a Europa).

COM (2010) 245 final (Uma Agenda Digital para a Europa).

Comissão Europeia. (2014). *Compreender as políticas da União Europeia: Agenda Digital para a Europa.*

Conselho da Europa. (2001). Convenção sobre o cibercrime.

Conselho Europeu. (2009). *Programa de Estocolmo: Uma Europa aberta e segura que sirva e proteja os cidadãos*.

Diretiva 2008/114/CE, do Conselho de 8 de dezembro de 2008, relativa à identificação e designação das infraestruturas críticas europeias e à avaliação da necessidade de melhorar a sua proteção.

Diretiva n.º 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção de pessoas singulares, no que diz respeito ao tratamento dos dados pessoais e à livre circulação desses dados.

JOIN (2013) 1 final (Estratégia da União Europeia para a cibersegurança: um espaço aberto, seguro e protegido).

Legislação

Constituição da República Portuguesa.

Lei n.º 67/98, de 26 de outubro. *Diário da República*, 1.ª Série, n.º 247, 5536-5546. Assembleia da República. (Lei da Proteção de Dados Pessoais. Transpõe para a ordem jurídica interna a Diretiva n.º 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de outubro de 1995).

Lei n.º 9/2007, de 19 de fevereiro. *Diário da República*, 1.ª Série, n.º 35, 1238-1252. Assembleia da República. (Estabelece a orgânica do Secretário-Geral do Sistema de Informações da República Portuguesa, do Serviço de Informações Estratégicas de Defesa e do Serviço de Informações de Segurança).

Lei n.º 49/2008, de 27 de agosto. *Diário da República*, 1.ª Série, n.º165, 6038-6042. Assembleia da República. (Aprova a Lei da Organização de Investigação Criminal).

Lei n.º 53/2008, de 29 de agosto. *Diário da República*, 1.ª Série, n.º 167, 6135-6141. Assembleia da República. (Aprova a Lei de Segurança Interna).

Lei n.º 109/2009, de 15 de setembro. *Diário da República*, 1.ª Série, n.º 179, 6319-6325. Assembleia da República. (Aprova a Lei do Cibercrime, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de fevereiro).

Lei n.º 34/2013, de 16 de maio. *Diário da República*, 1.ª Série, n.º 94, 2921-2942. Assembleia da República. (Estabelece o regime do exercício da atividade de segurança privada e procede à primeira alteração à Lei n.º 49/2008, de 27 de agosto,

no concernente às competências da Polícia Judiciária em matéria de investigação criminal).

Decreto-Lei n.º 62/2011, de 9 de maio. *Diário da República*, 1.ª Série, n.º 89, 2624-2627. Ministério da Defesa Nacional. (Estabelece os procedimentos de identificação e de proteção das infraestruturas essenciais para a saúde, a segurança e o bem-estar económico e social da sociedade nos setores da energia e transportes e transpõe a Diretiva n.º 2008/114/CE, de 8 de dezembro).

Decreto-Lei n.º 3/2012, de 16 de janeiro. *Diário da república*, 1.ª Série, n.º 11, 174-177. Presidência do Conselho de Ministros. (Aprova a orgânica e o quadro de pessoal dirigente do GNS, estabelecendo as suas atribuições e competências).

Decreto-Lei n.º 69/2014, de 9 de maio. *Diário da República*, 1.ª Série, n.º 89, 2712-2719. Presidência do conselho de Ministros. (Aprova a orgânica do GNS, estabelecendo os termos do funcionamento do CNCseg).

Resolução do Conselho de Ministros n.º 12/2012, de 7 de fevereiro. *Diário da República*, 1.ª série, n.º 27, 596-605. (Aprova as linhas gerais do plano global estratégico de racionalização e redução de custos com as TIC na Administração Pública).

Resolução do Conselho de Ministros n.º 19/2013, de 21 de março. *Diário da República*, 1.ª Série, n.º 67, 1981-1995. Presidência do Conselho de Ministros. (Aprova o Conceito Estratégico de Defesa Nacional).

Resolução do Conselho de Ministros n.º 26/2013, de 19 de abril. *Diário da República*, 1.ª Série, n.º 77, 2285-2289. Presidência do Conselho de Ministros. (Aprova as linhas de orientação para a Reforma «Defesa 2020»).

Resolução do Conselho de Ministros n.º 42/2012, de 13 de abril. *Diário da República*, 1.ª Série, n.º 74, 1925-1926. Presidência do Conselho de Ministros. (Cria a Comissão Instaladora do CNCseg).

Despacho n.º 13692/2013, de 28 de outubro. *Diário da República*, 2.ª Série, n.º 208, 31976-31979. Ministério da Defesa Nacional. (Determina a publicação da diretiva iniciadora com a orientação política para a ciberdefesa).

Webgrafia

http://projects.eff.org/~barlow/Declaration-Final.html

http://annops.com/

http://cert.pt/

http://pastebin.com/

http://web.mit.edu/

http://wikileaks.org/

http://www.act.nato.int/globalcommons

http://www.apdsi.pt/

http://www.cision.com/pt/

http://www.cncs.gov.pt/cert-pt/

http://www.enisa.europa.eu/

http://www.gns.gov.pt/

http://www.gns.gov.pt/new-ciberseguranca.aspx

http://www.itu.int/

http://www.nato.int/

http://www.sis.pt/

http://www.tugaleaks.com/

https://bestpractical.com/

https://www.europol.europa.eu/

https://www.europol.europa.eu/ec3

https://www.facebook.com

https://www.youtube.com/

Apêndices

Apêndice A – Pedidos de colaboração para Entrevistas

MINISTERIO DA ADMINISTRAÇÃO INTERNA
POLÍCIA DE SEGURANÇA PÚBLICA
INSTITUTO SUPERIOR DE CIÊNCIAS POLICIAIS E SEGURANÇA INTERNA
DIRECÇÃO DE ENSINO
SECRETARIA ESCOLAR

Exmo. Senhor
Eng.º Vítor Costa
Secretaria Geral do Ministério da Administração Interna
Rua S. Mamede, n.º 23
1100-553 Lisboa

S/Referência	S/Comunicação	N/Referência	Data
		45/SECDE/2015	2015-01-20
		Processo:	
		Classificador: 080.10.02	

Assunto: PEDIDO DE COLABORAÇÃO EM TRABALHO DE DISSERTAÇÃO DE MESTRADO INTEGRADO EM CIÊNCIAS POLICIAIS

1. O Curso de Mestrado Integrado em Ciências Policiais (CMICP), no 5.º ano - Estágio - compreende a elaboração de uma dissertação/trabalho de projeto que deverá, obrigatoriamente, incidir sobre um tema das áreas científicas de Ciências Policiais, Ciências Jurídicas, Ciências Sociais e Humanas e/ou Ciências de Desenvolvimento e Adaptação Motora.

2. Neste sentido, a Aspirante a Oficial de Polícia Elisabete Júlio Domingues irá realizar o seu estudo numa daquelas áreas científicas subordinado ao tema "O fenómeno hacktivista: Uma ameaça à segurança interna?", do qual é Orientador o Prof. Doutor Felipe Pathé Duarte.

3. Deste modo, solicita-se a V.ª Ex.ª a concessão de uma entrevista, tendo por objetivo a obtenção de informação relevante para o trabalho.

4. A necessidade da aplicação da entrevista prende-se com o facto de vir a constituir um capítulo essencial à elaboração da dissertação, sustentando todo o trabalho de investigação realizado.

5. Mais se informa V.ª Ex.ª que a Aspirante a Oficial de Polícia Elisabete Domingues se compromete ao dever de confidencialidade e anonimato, relativamente aos dados recolhidos, fora do âmbito do seu trabalho académico.

Com os melhores cumprimentos

O Diretor
Pedro José Lopes Clemente
Superintendente

135573
Pagina1/1

R. 1º de Maio, nº3 1349-040 Lisboa Tel.: 213613900 Fax: 213610535
www.iscpsi.pt | iscpsi@psp.pt

MINISTERIO DA ADMINISTRAÇÃO INTERNA
POLÍCIA DE SEGURANÇA PÚBLICA
INSTITUTO SUPERIOR DE CIÊNCIAS POLICIAIS E SEGURANÇA INTERNA
DIRECÇÃO DE ENSINO
SECRETARIA ESCOLAR

Exmo. Senhor
Diretor do Centro Nacional de Cibersegurança
Gabinete Nacional de Segurança
Rua da Junqueira, nº. 69
1300 – 342 Lisboa

S/Referência	S/Comunicação	N/Referência	Data
		43/SECDE/2015	2015-01-19
		Processo:	
		Classificador: 080.10.02	

Assunto: PEDIDO DE COLABORAÇÃO EM TRABALHO DE DISSERTAÇÃO DE MESTRADO INTEGRADO EM CIÊNCIAS POLICIAIS

1. O Curso de Mestrado Integrado em Ciências Policiais (CMICP), no 5.º ano – Estágio - compreende a elaboração de uma dissertação/trabalho de projeto que deverá, obrigatoriamente, incidir sobre um tema das áreas científicas de Ciências Policiais, Ciências Jurídicas, Ciências Sociais e Humanas e/ou Ciências de Desenvolvimento e Adaptação Motora.

2. Neste sentido, a Aspirante a Oficial de Polícia Elisabete Júlio Domingues irá realizar o seu estudo numa daquelas áreas científicas subordinado ao tema "O fenómeno hacktivista: Uma ameaça à segurança interna?", do qual é Orientador o Prof. Doutor Felipe Pathé Duarte.

3. Deste modo, solicita-se a V.ª Ex.ª a concessão de uma entrevista, tendo por objetivo a obtenção de informação relevante para o trabalho.

4. A necessidade da aplicação da entrevista prende-se com o facto de vir a constituir um capítulo essencial à elaboração da dissertação, sustentando todo o trabalho de investigação realizado.

135573
Pagina1/2

R. 1º de Maio, nº3 1349-040 Lisboa Tel.: 213613900 Fax: 213610535
www.iscpsi.pt | iscpsi@psp.pt

MINISTERIO DA ADMINISTRAÇÃO INTERNA
POLÍCIA DE SEGURANÇA PÚBLICA
INSTITUTO SUPERIOR DE CIÊNCIAS POLICIAIS E SEGURANÇA INTERNA
DIRECÇÃO DE ENSINO
SECRETARIA ESCOLAR

Exmo. Senhor
Diretor do Centro Nacional de Cibersegurança
Gabinete Nacional de Segurança
Rua da Junqueira, nº. 69
1300 – 342 Lisboa

S/Referência	S/Comunicação	N/Referência	Data
		43/SECDE/2015	2015-01-19
		Processo:	
		Classificador: 080.10.02	

Assunto: PEDIDO DE COLABORAÇÃO EM TRABALHO DE DISSERTAÇÃO DE MESTRADO INTEGRADO EM CIÊNCIAS POLICIAIS

1. O Curso de Mestrado Integrado em Ciências Policiais (CMICP), no 5.º ano – Estágio - compreende a elaboração de uma dissertação/trabalho de projeto que deverá, obrigatoriamente, incidir sobre um tema das áreas científicas de Ciências Policiais, Ciências Jurídicas, Ciências Sociais e Humanas e/ou Ciências de Desenvolvimento e Adaptação Motora.

2. Neste sentido, a Aspirante a Oficial de Polícia Elisabete Júlio Domingues irá realizar o seu estudo numa daquelas áreas científicas subordinado ao tema "O fenómeno hacktivista: Uma ameaça à segurança interna?", do qual é Orientador o Prof. Doutor Felipe Pathé Duarte.

3. Deste modo, solicita-se a V.ª Ex.ª a concessão de uma entrevista, tendo por objetivo a obtenção de informação relevante para o trabalho.

4. A necessidade da aplicação da entrevista prende-se com o facto de vir a constituir um capítulo essencial à elaboração da dissertação, sustentando todo o trabalho de investigação realizado.

135573
Pagina1/2

R. 1º de Maio, nº3 1349-040 Lisboa Tel.: 213613900 Fax: 213610535
www.iscpsi.pt | iscpsi@psp.pt

5. Mais se informa V.ª Ex.ª que a Aspirante a Oficial de Polícia Elisabete Domingues se compromete ao dever de confidencialidade e anonimato, relativamente aos dados recolhidos, fora do âmbito do seu trabalho académico.

Com os melhores cumprimentos

O Diretor

Pedro José Lopes Clemente
Superintendente

135573
Pagina2/2

R. 1º de Maio, nº3 1349-040 Lisboa Tel.: 213613900 Fax: 213610535
www.iscpsi.pt | iscpsi@psp.pt

MINISTERIO DA ADMINISTRAÇÃO INTERNA
POLÍCIA DE SEGURANÇA PÚBLICA
INSTITUTO SUPERIOR DE CIÊNCIAS POLICIAIS E SEGURANÇA INTERNA
DIRECÇÃO DE ENSINO
SECRETARIA ESCOLAR

Exmo. Senhor
Intendente Rui Filipe Resende Melo Coelho de Moura
Diretor do Gabinete de Estudos e Planeamento da DN/PSP
DN/PSP - Largo da Penha de França, 1
1199 - 010 Lisboa

S/Referência	S/Comunicação	N/Referência	Data
		64/SECDE/2015	2015-01-27
		Processo:	
		Classificador: 080.10.02	

Assunto: PEDIDO DE COLABORAÇÃO EM TRABALHO DE DISSERTAÇÃO DE MESTRADO INTEGRADO EM CIÊNCIAS POLICIAIS

1. O Curso de Mestrado Integrado em Ciências Policiais (CMICP), no 5.º ano - Estágio - compreende a elaboração de uma dissertação/trabalho de projeto que deverá, obrigatoriamente, incidir sobre um tema das áreas científicas de Ciências Policiais, Ciências Jurídicas, Ciências Sociais e Humanas e/ou Ciências de Desenvolvimento e Adaptação Motora.

2. Neste sentido, a Aspirante a Oficial de Polícia Elisabete Júlio Domingues irá realizar o seu estudo numa daquelas áreas científicas subordinado ao tema "O fenómeno hacktivista: Uma ameaça à segurança interna?", do qual é Orientador o Prof. Doutor Felipe Pathé Duarte.

3. Deste modo, solicita-se a V.ª Ex.ª a concessão de uma entrevista, tendo por objetivo a obtenção de informação relevante para o trabalho.

4. A necessidade da aplicação da entrevista prende-se com o facto de vir a constituir um capítulo essencial à elaboração da dissertação, sustentando todo o trabalho de investigação realizado.

O Diretor

Pedro José Lopes Clemente
Superintendente

135573
Pagina1/1

R. 1º de Maio, nº3 1349-040 Lisboa Tel.: 213613900 Fax: 213610535
www.iscpsi.pt | iscpsi@psp.pt

MINISTERIO DA ADMINISTRAÇÃO INTERNA
POLÍCIA DE SEGURANÇA PÚBLICA
INSTITUTO SUPERIOR DE CIÊNCIAS POLICIAIS E SEGURANÇA INTERNA
DIRECÇÃO DE ENSINO
SECRETARIA ESCOLAR

Exmo. Senhor
Dr. José Maria de Almeida Rodrigues
M.I. Diretor Nacional da Polícia Judiciária
Polícia Judiciária - Rua Gomes Freire, s/n
1169 - 007 Lisboa

S/Referência	S/Comunicação	N/Referência	Data
		47/SECDE/2015	2015-01-20
		Processo:	
		Classificador: 080.10.02	

Assunto: PEDIDO DE COLABORAÇÃO EM TRABALHO DE DISSERTAÇÃO DE MESTRADO INTEGRADO EM CIÊNCIAS POLICIAIS

1. O Curso de Mestrado Integrado em Ciências Policiais (CMICP), no 5.º ano - Estágio - compreende a elaboração de uma dissertação/trabalho de projeto que deverá, obrigatoriamente, incidir sobre um tema das áreas científicas de Ciências Policiais, Ciências Jurídicas, Ciências Sociais e Humanas e/ou Ciências de Desenvolvimento e Adaptação Motora.

2. Neste sentido, a Aspirante a Oficial de Polícia Elisabete Júlio Domingues irá realizar o seu estudo numa daquelas áreas científicas subordinado ao tema ''O fenómeno hacktivista: Uma ameaça à segurança interna?'', do qual é Orientador o Prof. Doutor Felipe Pathé Duarte.

3. Deste modo, solicita-se a concessão de uma entrevista a manter com um elemento, dessa Polícia Judiciária, especializado na matéria em apreço, a designar por V. Ex.ª.

4. A necessidade da aplicação da entrevista prende-se com o facto de vir a constituir um capítulo essencial à elaboração da dissertação, sustentando todo o trabalho de investigação realizado.

135573
Pagina1/2

R. 1º de Maio, nº3 1349-040 Lisboa Tel.: 213613900 Fax: 213610535
www.iscpsi.pt | iscpsi@psp.pt

5. Mais se informa V.ª Ex.ª que a Aspirante a Oficial de Polícia Elisabete Domingues se compromete ao dever de confidencialidade e anonimato, relativamente aos dados recolhidos, fora do âmbito do seu trabalho académico.

Com os melhores cumprimentos

O Diretor

Pedro José Lopes Clemente
Superintendente

135573
Pagina2/2

R. 1º de Maio, nº3 1349-040 Lisboa Tel.: 213613900 Fax: 213610535
www.iscpsi.pt | iscpsi@psp.pt

MINISTERIO DA ADMINISTRAÇÃO INTERNA
POLÍCIA DE SEGURANÇA PÚBLICA
INSTITUTO SUPERIOR DE CIÊNCIAS POLICIAIS E SEGURANÇA INTERNA
DIRECÇÃO DE ENSINO
SECRETARIA ESCOLAR

Exmo. Senhor
Coronel de Artilharia, Eng.º Geógrafo Luís Nunes
Guarda Nacional Republicana
Comando Geral da Guarda Nacional Republicana
Largo do Carmo, s/n
1200 - 092 Lisboa

S/Referência	S/Comunicação	N/Referência	Data
		46/SECDE/2015	2015-01-20
		Processo:	
		Classificador: 080.10.02	

Assunto: PEDIDO DE COLABORAÇÃO EM TRABALHO DE DISSERTAÇÃO DE MESTRADO INTEGRADO EM CIÊNCIAS POLICIAIS

1. O Curso de Mestrado Integrado em Ciências Policiais (CMICP), no 5.º ano – Estágio - compreende a elaboração de uma dissertação/trabalho de projeto que deverá, obrigatoriamente, incidir sobre um tema das áreas científicas de Ciências Policiais, Ciências Jurídicas, Ciências Sociais e Humanas e/ou Ciências de Desenvolvimento e Adaptação Motora.

2. Neste sentido, a Aspirante a Oficial de Polícia Elisabete Júlio Domingues irá realizar o seu estudo numa daquelas áreas científicas subordinado ao tema ''O fenómeno hacktivista: Uma ameaça à segurança interna?'', do qual é Orientador o Prof. Doutor Felipe Pathé Duarte.

3. Deste modo, solicita-se a V.ª Ex.ª a concessão de uma entrevista, tendo por objetivo a obtenção de informação relevante para o trabalho.

4. A necessidade da aplicação da entrevista prende-se com o facto de vir a constituir um capítulo essencial à elaboração da dissertação, sustentando todo o trabalho de investigação realizado.

135573
Pagina1/2

R. 1º de Maio, nº3 1349-040 Lisboa Tel.: 213613900 Fax: 213610535
www.iscpsi.pt | iscpsi@psp.pt

5. Mais se informa V.ª Ex.ª que a Aspirante a Oficial de Polícia Elisabete Domingues se compromete ao dever de confidencialidade e anonimato, relativamente aos dados recolhidos, fora do âmbito do seu trabalho académico.

Com os melhores cumprimentos

O Diretor

Pedro José Lopes Clemente
Superintendente

135573
Pagina2/2

R. 1º de Maio, nº3 1349-040 Lisboa Tel.: 213613900 Fax: 213610535
www.iscpsi.pt | iscpsi@psp.pt

Apêndice B – Pedido de Acesso a Base de Dados CISION

MINISTERIO DA ADMINISTRAÇÃO INTERNA
POLÍCIA DE SEGURANÇA PÚBLICA
INSTITUTO SUPERIOR DE CIÊNCIAS POLICIAIS E SEGURANÇA INTERNA
DIRECÇÃO DE ENSINO
SECRETARIA ESCOLAR

Exmo. Senhor
Diretor Nacional Adjunto para a Unidade Orgânica de Recursos Humanos
(Departamento de Formação)

S/Referência	S/Comunicação	N/Referência	Data
		308/SECDE/2014	2014-10-09
		Processo:	
		Classificador: 080.10.02	

Assunto: PEDIDO DE COLABORAÇÃO EM TRABALHO DE DISSERTAÇÃO DE MESTRADO INTEGRADO EM CIÊNCIAS POLICIAIS

1. O Curso de Mestrado Integrado em Ciências Policiais (CMICP), no 5.º ano – Estágio – compreende a elaboração de uma dissertação/trabalho de projeto que deverá, obrigatoriamente, incidir sobre um tema das áreas científicas de Ciências Policiais, Ciências Jurídicas, Ciências Sociais e Humanas e/ou Ciências de Desenvolvimento e Adaptação Motora.

2. Neste sentido, a Aspirante Elisabete Júlio Domingues irá realizar o seu estudo numa daquelas áreas científicas que abordará as notícias relativas a ataques informáticos, levadas a cabo por grupos *hacktivistas*, tendo como alvo as forças e serviços de segurança, do qual é Orientador o Prof. Doutor Felipe Pathé Duarte.

3. Deste modo, solicita-se a V.ª Ex.ª a necessária autorização para a consulta daqueles dados na base CISION do Núcleo de Imprensa e Relações Públicas.

4. A necessidade da consulta prende-se com o facto de vir a constituir um capítulo essencial à elaboração da dissertação, sustentando todo o trabalho de investigação realizado.

5. Mais se informa V.ª Ex.ª que a Aspirante a Oficial de Polícia Elisabete Domingues se compromete ao dever de confidencialidade e anonimato, relativamente aos dados recolhidos, fora do âmbito do seu trabalho académico.

Com os melhores cumprimentos,

O Diretor

Pedro José Lopes Clemente
Superintendente

135573
Pagina1/1

R. 1º de Maio, nº3 1349-040 Lisboa Tel.: 213613900 Fax: 213610535
www.iscpsi.pt | iscpsi@psp.pt

Apêndice C – Pedido de Relatório de Segurança ao COSI da SGMAI

MINISTERIO DA ADMINISTRAÇÃO INTERNA
POLÍCIA DE SEGURANÇA PÚBLICA
INSTITUTO SUPERIOR DE CIÊNCIAS POLICIAIS E SEGURANÇA INTERNA
DIRECÇÃO DE ENSINO
SECRETARIA ESCOLAR

Exmo. Senhor
Dr. Carlos Palma
M.I. Secretário-geral da Secretaria-geral do Ministério da Administração Interna
Secretaria-geral da Administração Interna
Rua S. Mamede n.23
1100-553 Lisboa

S/Referência	S/Comunicação	N/Referência	Data
		15/SECDE/2015	2015-01-09
		Processo:	
		Classificador: 080.10.02	

Assunto: PEDIDO DE COLABORAÇÃO EM TRABALHO DE DISSERTAÇÃO DE MESTRADO INTEGRADO EM CIÊNCIAS POLICIAIS

1. O Curso de Mestrado Integrado em Ciências Policiais (CMICP), no 5.º ano – Estágio – compreende a elaboração de uma dissertação/trabalho de projeto que deverá, obrigatoriamente, incidir sobre um tema das áreas científicas de Ciências Policiais, Ciências Jurídicas, Ciências Sociais e Humanas e/ou Ciências de Desenvolvimento e Adaptação Motora.

2. Neste sentido, a Aspirante a Oficial de Polícia Elisabete Júlio Domingues irá realizar o seu estudo numa daquelas áreas científicas subordinado ao tema "O fenómeno *hacktivista*: Uma ameaça à segurança interna?", do qual é Orientador o Prof. Doutor Felipe Pathé Duarte.

3. Deste modo, solicita-se a V.ª Ex.ª a necessária autorização para o acesso aos relatórios mensais, elaborados na sequência de incidentes informáticos verificados nas infraestruturas da Polícia de Segurança Pública, Guarda Nacional Republicana e Serviço de Estrangeiros e Fronteiras.

4. A necessidade do acesso a tais documentos prende-se com o facto de vir a constituir um capítulo essencial à elaboração da dissertação, sustentando todo o trabalho de investigação realizado.

135573 R. 1º de Maio, nº3 1349-040 Lisboa Tel.: 213613900 Fax: 213610535
www.iscpsi.pt | iscpsi@psp.pt

5. Mais se informa V.ª Ex.ª que a Aspirante a Oficial de Polícia Elisabete Domingues se compromete ao dever de confidencialidade e anonimato, relativamente aos dados recolhidos, fora do âmbito do seu trabalho académico.

Com os melhores cumprimentos

O Diretor

Pedro José Lopes Clemente
Superintendente

135573
Página2/2

R. 1º de Maio, nº3 1349-040 Lisboa Tel.: 213613900 Fax: 213610535
www.iscpsi.pt | iscpsi@psp.pt

Apêndice D – Entrevista a Rui Moura

A presente entrevista insere-se no âmbito da dissertação de mestrado para obtenção do grau de mestre no Mestrado integrado em Ciências Policiais, ministrado no Instituto Superior de Ciências Policiais e Segurança Interna (ISCPSI).

O título provisório da dissertação é "O *Hacktivismo*: Uma análise aos ciberataques dirigidos contra as Forças de Segurança", sendo orientador da mesma o Professor Doutor Felipe Pathé Duarte.

Pretende-se com esta dissertação estudar o fenómeno *hacktivistas* em Portugal e, em concreto, analisar os ataques realizados às Forças de Segurança, no sentido de determinar quais são os tipos de ataques efetuados, quais os grupos envolvidos e quais as pretensões destes grupos, de maneira a determinar se o fenómeno constitui ou não uma ameaça para a Segurança.

Local: Direção Nacional da Polícia de Segurança Pública, Lisboa
Data: 16 de fevereiro de 2015
Cargo/Posto: Intendente da Polícia de Segurança Pública

Guião

1. **Tendo em conta a evolução do *hacktivismo*, considera que atualmente este fenómeno é significativo em Portugal? Porquê?**

Sim, pela sua quantidade de eventos, pela disputa/competição que se gera no seio deste tipo de pessoas, pelo mediatismo causado nos/pelos OCS e pelo potencial impacto que pode ter ao nível político, social, económico e criminal.

Em relação à evolução não sei se há aumento de casos. O que sei é que não tem havido grande mediatização nos OCS, o que não significa que não tenha existido evolução do fenómeno.

2. **Considera o *hacktivismo* uma ameaça à Segurança? Porquê?**

Não discutindo conceptualmente se o *hacktivismo* é uma ameaça ou um meio de concretização da ameaça, considero que sim. Porque os potenciais impactos que a concretização das ações *hacktivistas* podem ter ao nível da Segurança revestem-se de um

elevado grau de produção de danos, cuja recuperação / reposição da normalidade pode ser muito onerosa (tempo e dinheiro) para a Segurança.

3. Considera que Portugal está devidamente protegido contra os ciberataques?

Não sei. Sei que recentemente foi criado o CNCseg. Sei que existe uma proximidade colaborativa muito forte entre o centro, as universidades e os "operadores tecnológicos". Sei que Portugal é um dos países que não tem uma estratégia de cibersegurança aprovada formalmente.

4. Quais as possíveis consequências de um ataque *hacktivista*?

Diretas: consequências económicas, sociais, políticas, e de segurança. Indiretas: sentimento de segurança, desregulação social, e em último caso, soberania do País, das instituições, das famílias.

5. Como se caracterizam, organizam e o que pretendem os grupos de *hacktivistas* (traçar perfil)?

Não sei como se caracterizam e organizam. Sei que têm sofisticadíssimas formas de contacto entre si; sei que podem pretender uma ou várias finalidades:

a) ataque genérico a IC (nacionais/europeias);
b) ataque específico a setores de atividade (banca, seguros, saúde, transportes, energia, segurança, justiça, ….);
c) ataque específico a entidade ou pessoa.

Sistematicamente o que se pretende é:

a) um resultado específico (alvo e consequências conhecidas) – efetuar um apagão energético nacional;
b) um resultado não conhecido mas "pensado" na sua ação – negação de serviços *online*;
c) um resultado aleatório.

6. Considera que as Forças de Segurança (PSP e GNR) são um alvo potencial para grupos *hacktivistas*?

Claro que sim. Pelo valor intangível que tem a informação residente na PSP e GNR. Pelo impacto que pode causar na Sociedade a inoperação da PSP e GNR derivada de um ataque.

7. Poderá um ataque informático contra as infraestruturas das Forças de Segurança afetar a sua missão? Em que sentido?

Sim. No sentido de negar o acesso às tecnologias e à informação, uma vez que o GEP [Gabinete de Estudos e Planeamento] tem a sua informação maioritariamente em suporte digital.

Apêndice E – Entrevista a Paulo Santos

A presente entrevista insere-se no âmbito da dissertação de mestrado para obtenção do grau de mestre no Mestrado integrado em Ciências Policiais, ministrado no Instituto Superior de Ciências Policiais e Segurança Interna (ISCPSI).

O título provisório da dissertação é "O *Hacktivismo*: Uma análise aos ciberataques dirigidos contra as Forças de Segurança", sendo orientador da mesma o Professor Doutor Felipe Pathé Duarte.

Pretende-se com esta dissertação estudar o fenómeno *hacktivistas* em Portugal e, em concreto, analisar os ataques realizados às Forças de Segurança, no sentido de determinar quais são os tipos de ataques efetuados, quais os grupos envolvidos e quais as pretensões destes grupos, de maneira a determinar se o fenómeno constitui ou não uma ameaça para a Segurança.

Local: Comando Geral da Guarda nacional Republicana, Lisboa
Data: 16 de fevereiro de 2015
Cargo/Posto: Tenente Coronel da Guarda Nacional Republicana

Guião

1. **Tendo em conta a evolução do *hacktivismo*, considera que atualmente este fenómeno é significativo em Portugal? Porquê?**

O *hacktivismo* é um fenómeno que merece a atenção da Guarda Nacional Republicana. A *internet* é um fenómeno global e o *hacktivismo* é um fenómeno que tem vindo a evoluir, sobretudo devido ao desenvolvimento da cidadania digital, que possivelmente é a principal motivação para a ocorrência de ciberataques. O grupo *Anonymous* é talvez é o mais representativo em Portugal. Dele fazem parte dois grupos distintos de pessoas: o primeiro é constituído por jovens, que realizam ataques não muito organizados, uma vez que também não têm ideias muito bem formadas acerca da realidade que os rodeia, realizam ataques por uma questão de competição entre pares. O outro grupo é constituído por adultos, maioritariamente com formação (licenciados), que têm mais alguns conhecimentos técnicos e têm já uma ideia formada sobre o mundo, bem como uma perspetiva crítica enraizada e promovida também pela cidadania digital, quando realizam

ataques fazem-no por questões de protesto ou contestação política. Estes *hacktivistas* portugueses fazem uso de ferramentas digitais que encontram *online*, não têm por hábito criar ferramentas à medida, os ataques normalmente são bem-sucedidos pelas vulnerabilidades encontradas nos sistemas. Dentro do grupo *Anonymous* ainda se destaca um grupo, mais especializado e organizado, denominado *Sidekingdom*. Sobretudo importa atentar que muitas vezes estes grupos querem somente expressar a cidadania digital, pelo que cabe também à polícia perceber qual o seu propósito e ir ao seu encontro, uma vez que para nos protegermos temos de conhecer o inimigo.

2. Considera o *hacktivismo* uma ameaça à Segurança? Porquê?

Sim. Pode colocar em causa a tranquilidade e ordem pública.

3.Considera que Portugal está devidamente protegido contra os ciberataques?

Portugal está a construir o seu caminho nesse sentido, está a trabalhar na definição de estratégias. Concretamente já temos um CNCseg e um Centro de Ciberdefesa. Mas também já existe um enquadramento europeu, nomeadamente uma estratégia de cibersegurança que deve ser considerada por todos os EM, inclusive por Portugal. O fenómeno *hacktivistas* é global, a origem de um ataque pode ser nacional ou transnacional, de maneira que só se combate o *hacktivismo* com colaboração e coordenação entre as instituições responsáveis e com competência no âmbito da cibersegurança, o que não tem vindo a ser prática habitual em Portugal.

4. Quais as possíveis consequências de um ataque *hacktivistas*?

Um ataque deste tipo poderá principalmente afetar a confiança que a população deposita nas instituições, mas também, influenciar outras pessoas com determinados ideais ou opiniões, ridicularizar o poder político, identificar fragilidades dos sistemas informáticos. Há quem defenda a existência de *hacktivistas* extremistas, como é o caso dos nossos vizinhos espanhóis, neste caso podemos tomar como exemplo por exemplo a alteração de um *site* que indique as condições de trânsito, que em último caso poderá colocar em causa a segurança. O que os *hacktivistas* pretendem é primeiro reconhecimento e conseguir influenciar o poder político (cidadania digital). A "exfiltração" de dados também poderá ser uma das possíveis consequências de um ataque *hacktivistas*.

5. Como se caracterizam, organizam e o que pretendem os grupos de *hacktivistas* (traçar perfil)?

Estes grupos atacam *sites* desprotegidos e exploram fragilidades, o que é uma característica dos grupos portugueses, já que mais do que atacar visam explorar as vulnerabilidades existentes. Planeiam os seus ataques em IRC's e *chat*rooms, muitas vezes encontram-se mesmo não se conhecendo. Uma característica peculiar é que não usam os seus nomes próprios, mas utilizam *nicknames*, recorrendo ao anonimato. Não fabricam programas à medida, mas utilizam aqueles que estão disponibilizados na rede. Neste âmbito, importa destacar duas teorias que se enquadram perfeitamente neste fenómeno: a teoria da aprendizagem diferencial e a teoria das oportunidades. Enquanto a primeira diz respeito ao facto de o crime se aprender, sendo a *internet* um importante veículo de aprendizagem, a segunda diz respeito ao facto de o crime ocorrer onde existe oportunidades criadas para a sua prática, ora a *internet* é um mar de oportunidades, sendo mais facilmente cometido o delito. Trata-se de jovens e adultos (licenciados e que realizam ataques mais estruturados) que recorrem ao *facebook* e ao *twitter* para fazer a sua propaganda, angariar seguidores e planear operações. Importa ainda referir que estes indivíduos trabalham a engenharia social, ou seja, estudam os alvos e constroem soluções através das redes sociais.

6. Considera que as Forças de Segurança (PSP e GNR) são um alvo potencial para grupos *hacktivistas*?

O principal alvo destes grupos são os *sites* governamentais e não tanto as FS. No entanto, ultimamente estes grupos têm estado mais focados naquilo que está a ocorrer no mundo. É a Guarda que gere o *site* oficial, pelo que vamos tendo maior conhecimento das vulnerabilidades existentes. Neste sentido, segundo é do nosso conhecimento, não tem havido um ataque massivo aos *sites* da Guarda. O cidadão tem confiança nas FS e considera que os *sites* destas são meramente instrumentais, pelo que não motivam a execução de ataques contra as mesmas, a não ser que apresentem fragilidades brutais em termos tecnológicos. Contudo, vivemos num mundo em constante evolução e a realidade dos ataques de hoje pode não ser a de amanhã, a cidadania digital pode alterar o rumo das coisas a qualquer momento e importa sempre lembrar que os nossos vizinhos espanhóis já falam em *hacktivismo* extremista.

7. Poderá um ataque informático contra as infraestruturas das Forças de Segurança afetar a sua missão? Em que sentido?

Pode ter um efeito catastrófico, podendo provocar um alarme social brutal. Ora quando estamos a falar de instituições credíveis, nas quais o cidadão deposita a sua confiança, espera-se que as mesmas não partilhem informações erróneas. Essa situação poderá ter efeitos nefastos para as FS. Daí que se justifiquem as regras restritas em termos de segurança informática.

Apêndice F – Entrevista a Vitor Costa

A presente entrevista insere-se no âmbito da dissertação de mestrado para obtenção do grau de mestre no Mestrado integrado em Ciências Policiais, ministrado no Instituto Superior de Ciências Policiais e Segurança Interna (ISCPSI).

O título provisório da dissertação é "O *Hacktivismo*: Uma análise aos ciberataques dirigidos contra as Forças de Segurança", sendo orientador da mesma o Professor Doutor Felipe Pathé Duarte.

Pretende-se com esta dissertação estudar o fenómeno *hacktivistas* em Portugal e, em concreto, analisar os ataques realizados às Forças de Segurança, no sentido de determinar quais são os tipos de ataques efetuados, quais os grupos envolvidos e quais as pretensões destes grupos, de maneira a determinar se o fenómeno constitui ou não uma ameaça para a Segurança.

Local: Instalações da Secretaria Geral do MAI no Tagus Parque, Lisboa
Data: 19 de fevereiro de 2015
Cargo/Posto: Responsável no Centro de Operações de Segurança Informática da Secretaria Geral do Ministério da Administração Interna

Guião

1. **Tendo em conta a evolução do *hacktivismo*, considera que atualmente este fenómeno é significativo em Portugal? Porquê?**

Hoje em dia a questão do *hacktivismo* é uma realidade em Portugal, ou seja, nós todos os dias temos eventos, nem que seja nas redes sociais a anunciar determinados eventos. No caso concreto do MAI, com muita frequência, temos algumas ações praticamente diárias, mas há incidentes com muita frequência. Temos alguns alvos entre as Forças que colhem maior preferência do que outras, a PSP tem mais adeptos digamos do que as restantes, mas abrange quase todos os *sites*.

Em termos de RNSI, entidade responsável pela parte tecnológica do MAI, publica a maioria dos *sites* para a *internet* dos diversos organismos, não só os *sites* institucionais, mas também as próprias aplicações e serviços que são disponibilizados. Quanto à evolução, penso que já tivemos um período mais crítico: os anos de 2011 e 2012 foram os anos mais

complicados, em que houve um aumento significativo, ultimamente tem havido alguns incidentes, todavia não com o peso e dimensão que houve nessa altura. Em 2011 foi o ano em que houve uma situação mais complicada, em finais de outubro e no mês de novembro tivemos constantemente sob alvo de ataque de *hackers* durante esse período, o que levou à implementação deste COSI, que digamos que é o SOC (*Security Operations Center*) do MAI, para nos prepararmos para este tipo de ataques. As ações tiveram a ver, na altura, com manifestações realizadas, em que a PSP intervinha e nós víamos aqui [no COSI] a reação quase imediata, ou seja, nós tínhamos conhecimento da notícia de uma manifestação, por exemplo, em que a PSP tinha agido de forma mais forte e depois isso refletia-se nos ataques ao *site* da PSP, havia uma relação direta com o aumento do número de ataques. Havia alguns elementos do próprio grupo de *Anonymous* portugueses, alguns identificados, que realizaram algumas ações, sendo que na altura fizemos a participação à PJ, como é normal, entretanto em relação a essas ações de 2011, recebemos este ano a comunicação de que os processos foram arquivados.

Quando refere as redes sociais, é porque fazem o acompanhamento do que se passa nestas?

Uma das ações que a equipa faz é acompanhar os canais sociais, ou seja, desde IRC's, todo o tipo de *chat*, *facebooks*, tudo a partir do qual se possa obter informação na *internet* e acompanhar e tentar perceber se há algumas ações.

De acordo com o *modus operandi*, que já está definido em termos do grupo *Anonymous*, eles anunciam inicialmente nessas redes sociais, ou seja, nos IRC's e *facebooks*, as ações que vão tomar e é aí que eles começam por divulgar e comunicar entre eles. Depois usam canais privados de *chat* para comunicar entre eles e houve alturas em que conseguimos "infiltrar-nos" e simular ser um deles e chegámos a participar nesses canais de *chat*, em que eles diziam que iam fazer agora o ataque e nós estávamos preparados para lhe responder, era de imediato. É também uma das ações que fazemos, é acompanhar todo esse tipo de informação que é divulgada, para tentar de uma forma proativa agir.

2. Considera o *hacktivismo* uma ameaça à Segurança? Porquê?

Sim, podemos considerar que o *hacktivismo* poderá ser uma ameaça. Isto porque nós temos aqui na nossa infraestrutura muitos dos sistemas na nossa rede sistemas de informação que dão apoio à segurança interna. Desde que possa existir uma intrusão ao

nível da nossa infraestrutura poderá pôr-se em causa esses sistemas de informação ou até pode não ser uma questão de intrusão, mas de negação do serviço em que indisponibiliza o sistema às Forças que hoje em dias usam as aplicações para o seu dia a dia, até para comunicação muitas vezes entre as Forças. Nesse aspeto, podemos considerar que, de certa forma, poderá ser uma ameaça. Aliás temos de considerar uma ameaça, temos de estar sempre precavidos e atentos para aquilo que possa vir a acontecer e tentar minimizar ao máximo qualquer intervenção destas e é por isso que tem sido feito um investimento forte desde 2012 nesta área da segurança no MAI. Não só em termos de recursos mas em termos de plataformas, em termos de criar novas barreiras, sem que o serviço em si fique em causa. Temos tentado elevar ao máximo o nível de segurança.

3. Considera que Portugal está devidamente protegido contra os ciberataques?

Na minha opinião, em termos gerais, penso que não. A maioria das infraestruturas não estão preparadas, ou seja, muitas vezes são infraestruturas que não têm grande preocupação na componente segurança, a grande preocupação está na funcionalidade do serviço, ou seja, ter o serviço disponível, sem a mínima preocupação ao nível da segurança, isso muitas das vezes traz alguns dissabores. No caso do MAI, neste momento, tenho a garantia de que somos uma referência para a Administração Pública em termos de segurança da informática.

Temos uma equipa a trabalhar 24 x 7 que vê todo o fluxo de informação que anda na rede e ao mínimo alerta vai analisar e ver se é um possível ataque ou um falso positivo e após o discernimento dessa situação faz o procedimento, ou escala ou apenas reporta que houve um incidente e que foi considerado falso positivo. No caso de um ataque é escalado e temos protocolos definidos consoante o tipo de ataques de que temos conhecimento e estão identificadas determinadas ações a executar e medidas a tomar.

4. Quais as possíveis consequências de um ataque *hacktivistas*?

As consequências destes ataques são variadas, depende do tipo de ataque, se for um ataque do tipo de negação de serviço, (DOS, DDOS), ou seja, esgotar os recursos em termos de sistemas ou de comunicações, isso é o mais frequente que temos tido, temos tido também alguns tipo de ataques de tentativa de intrusão como os *SQL Injection* e os *defacements*, ou seja, para a questão do MAI, qualquer um destes tipos de ataque que tenha sucesso é muito complicado. Para nós o principal aspeto é salvaguardar a informação,

preferimos interromper o serviço em caso de haver um possível ataque que ponha em causa a nossa infraestrutura e que a mesma não esteja preparada ou que saibamos que possa haver uma situação de intrusão ou de obtenção de alguma informação interna. Preferimos interromper o serviço do que garantir que o serviço se mantenha ativo, portanto para nós a questão da informação é muito mais importante do que a disponibilização do serviço, não temos qualquer problema em desligar os acessos aos sistemas se a segurança da informação estiver em causa. As possíveis consequências são portanto o roubo de informação, a indisponibilização dos serviços e a alteração da informação, uma vez que da mesma forma como retiram também podem introduzir essa informação, ou seja estamos sujeitos a isso. Nós temos feito um trabalho no sentido de o evitar, mas temos a noção que não estamos cem por cento seguros e estamos sempre a tentar melhorar, de forma a acompanhar novos métodos que vão surgindo. Estes tipos de ataques vão evoluindo e as técnicas vão se aperfeiçoando ao longo do tempo e nós temos de ir ajustando e evoluindo dessa forma a nossa proteção da rede, ora isto é um bocado a história do polícia e do ladrão.

Já aconteceu muitas vezes terem de interromper o serviço para garantirem a segurança da informação?

Sim já aconteceu algumas vezes. Já tivemos de parar os acessos à rede por não estarem reunidas as condições para garantir que a segurança da informação interna seja mantida. Já fizemos isso, na totalidade, uma hora no máximo. Pontualmente, alguns serviços já têm ficado durante toda a noite inacessíveis. Uma das coisas que fazemos é: muitos desses ataques vêm de *providers* internacionais, ou seja, em termos nacionais ainda não há muitas plataformas que disponibilizem as ferramentas que os *hackers* usam tipo serviço de *VPN [Virtual Private Network]*, as *bootnets*, muitas delas são com origem em IP*'s* internacionais, muitas vezes pedimos o barramento dos acessos internacionais aos nossos *sites*. Isso é feito com alguma frequência. Agora cada vez menos porque no último ano, por exemplo, não tivemos tido muitos incidentes desse género, mas é uma coisa que fazemos se entendermos que existe razão para isso e temos informados os nossos utilizadores (FS e todos os outros serviços do MAI), que em caso da segurança estar em causa, é interrompido o serviço.

Acha que as Forças de Segurança estão devidamente sensibilizadas para este problema?

Na sua globalidade penso que não, porque a interação que temos é muito pouca com as nossas Forças internas, é mais com as entidades externas ao MAI, ou seja, quando há incidentes ou há previsão de haver incidentes, trabalhamos muito mais com entidades externas ao MAI do que com as áreas de investigação da PSP ou GNR, não tem havido até hoje muita preocupação nesse sentido, mas no futuro penso que venha a melhorar.

O que acha que pode ser diferente?

Podia haver uma interação maior. Sabemos que a PSP tem um departamento de investigação assim como a GNR, em que muitas das vezes têm alguma informação e que essa informação podia ser trocada. Nós de certa forma informamos através daqueles relatórios mensais, para a GNR ou qualquer outra força, enviamos os relatórios mensais, o que se passou o que houve, no momento em que está a haver algum incidente, se o incidente chegar a uma determinada escala que possa causar impacto entramos em contacto com as forças a comunicar que poderá haver uma interrupção do *site* ou da aplicação que está disponibilizada, relativa à força em questão, mas não temos um trabalho digamos de *back office,* preventivo, não há um trabalho conjunto, não há uma comunicação. Temos mais troca de experiências e de informação com outras entidades, por exemplo, com o Ministério da Justiça, com o CEGER, dentro da Administração Pública temos alguma troca de informação e experiências. Dentro do MAI isso infelizmente não acontece.

5. Como se caracterizam, organizam e o que pretendem os grupos de *hacktivistas* (traçar perfil)?

A informação que nos é passada, em termos do perfil do tipo, da personalidade do *hacker* é que muitas vezes são jovens, em idade escolar, ao nível do secundário, mas isto é na generalidade. Pode haver uma ou outra situação em que sejam já pessoas mais adultas se calhar com menos conhecimentos na área tecnológica, mas descontentes com o que se passa na sociedade.

Este tipo de ataques está ao dispor de qualquer cidadão. É só a pessoa procurar na *internet*, as ferramentas, os métodos, os grupos e começar a participar, estes grupos de anónimos na altura dos ataques faziam *workshops* de como fazer os ataques, eles faziam o

curso do "abc" de como perceber, muitas vezes têm ferramentas já desenvolvidas e que qualquer pessoa acede ao *site*, basta pôr lá o endereço de destino e a aplicação desenvolve o ataque. Na grande maioria de quem faz essas ações, ou seja, jovens ainda em idade escolar, muitos deles utilizam ferramentas que são utilizadas por especialistas que as desenvolvem, pessoas com certo grau académico mais evoluído, com mais uns anos, mas muitos deles é com ferramentas que já são desenvolvidas para o efeito, ou seja, na *internet* pode-se procurar e obter informação para realizar o ataque e depois como o fazer e que tipo de ferramentas utilizar para ajudar a fazer o ataque.

O que eles pretendem muitas das vezes é a visibilidade, porque dizer que o *site* da PSP ou a rede do MAI esteve em baixo ou obter uma informação dos agentes da PSP ou GNR, tem sempre visibilidade. Eu acho que principalmente, no caso do MAI, é que apareça nas notícias e alguma visibilidade. Isto acontece mais para pôr em causa a infraestrutura, porque isto muitas vezes tem a ver com o descontentamento das pessoas em termos do contexto atual em que vivemos e muitas vezes as pessoas demonstram o seu desagrado desta forma, outras vezes é por simples brincadeira, estamos a falar, muitas vezes, de idades entre 16 ou 17 anos, que não têm muitas preocupações em termos sociais, muitas vezes é porque os amigos fazem, e para se promoverem dentro do grupo de amigos, outras vezes são experiências que fazem porque se trata da idade da experiência. Muitas vezes não acho que tenham a noção quando fazem estas ações do impacto que isto vai ter. Isto foi-nos relatado em alguns casos pela PJ, que muitas vezes acontece identificarem um ou dois indivíduos e quando entram lá em casa é um miúdo nessa fase etária, os pais estão na sala a ver televisão, o miúdo esta no quarto a fazer estas brincadeiras e os pais ficam muito surpreendidos. Este é o *feedback* que tenho tido. Nós fazemos a participação à PJ e depois não temos *feedback* em relação à investigação criminal que é feita, mas muitas vezes em conversa é dentro deste perfil mais ou menos o que é feito, ou seja, há um grupo de *hacktivistas* ferranhos e que muitos deles têm conhecimentos tecnológicos e desenvolvem as ferramentas para ser utilizadas depois pela maioria, que eles "recrutam" e que disponibilizam para um grupo de pessoas sem conhecimentos informáticos, mas aquilo é como uma simples aplicação que é usada para despoletar esses ataques.

6. Poderá um ataque informático contra as infraestruturas das FS afetar a sua missão? Em que sentido?

Sim, desde que os sistemas centrais sejam afetados poderá afetar a missão das Forças, porque as Forças, hoje em dia, utilizam muitas ferramentas que são disponibilizadas pela parte da infraestrutura tecnológica, aplicações, até de georreferenciação, e uma ação destas se for bater no sítio certo de forma eficiente pode afetar as FS.

Por exemplo vamos supor, as FS têm a rede SIRESP [Sistema Integrado de Redes de Emergência e Segurança de Portugal] para comunicar entre elas, quando estão no terreno, ora se esse sistema for afetado e temos de pensar que poderá ser afetado, é um dos princípios básicos da segurança é que não estamos totalmente protegidos, isso poderá pôr em causa a ação, vamos supor que há uma manifestação em frente à Assembleia da República, por norma as FS têm um camião com uma antena do rádio SIRESP para as FS naquela zona comunicarem entre elas, se deixarem de ter essa comunicação porque o sistema do SIRESP foi afetado, ou seja houve uma ação que interferiu com o sinal que é dado naquela zona por aquela antena e impossibilitar a comunicação entre os agentes das várias FS isso vai complicar a ação dessa Força no local.

O controlo da rede SIRESP não esta na minha área, mas é feita em parte aqui, outra parte é feita por um dos operadores das comunicações. Para prosseguir um ataque o computar tem de estar preparado para comunicar na rede rádio, pode interferir embora, neste momento, a rede SIRESP tenha um grau de segurança de certa forma elevado, mas como tudo na vida não podemos dizer que é 100 % segura, portanto não é fácil, mas nesta questão dos *hackers* e dos ataques cibernéticos, se for feito um ataque, se for um especialista, uma pessoa com bastante conhecimento na matéria, essa pessoa pode ao fim de algum tempo chegar ao seu objetivo, não são é feitos de um dia para o outro, pode levar meses, por vezes até mais que um ano a fazer várias tentativas, a ver onde pode ir ou não, mas pode acontecer.

7. Tendo em conta que no ciberespaço as fronteiras são praticamente inexistentes, em que medida é possível identificar se a origem dos ataques é interna ou externa?

Nós conseguimos saber o *provider* utilizado, ou seja, se o *provider* que o utilizador está a utilizar é interno ou externo, que é o endereço IP que nos chega cá inicialmente, mas isso pode ser mascarado, ou seja, posso estar aqui em Portugal e estar a usar um operador

da China, dos Estados Unidos, da Holanda para fazer uma ação de ataque a um *site* aqui em Portugal. Portanto não temos a garantia de 100 % da origem do IP que nos chega cá: pode ser um IP nacional ou internacional, mas não ser a origem concreta de quem está a fazer o ataque.

É possível verificar se o IP é mascarado ou não?

Sim, normalmente vamos ver e percebemos quando estão a utilizar os serviços que disponibilizam as ditas *VPN bootnets*, são muitas vezes IP's de empresas que fornecem o serviço. Vamos ver e está associado a empresas que disponibilizam o serviço VPN que permite que utilizador mascare o seu IP de origem e isso dá-nos a entender que não é aquele o IP real de quem está a fazer o ataque. Numa situação dessas o que fazemos é: esses *sites,* normalmente, têm um endereço de *email* para reportar os problemas e fazemos isso, reportamos os problemas, enviamos um *email*, reportamos o problemas e muitas vezes eles próprios desabilitam o serviço, outras vezes não nos ligam nenhuma ao *email*, mas quando são ataques internacionais é mais complicado. Nesse caso, recorremos muitas vezes ao nosso CSIRT português que tem canais de comunicação com CSIRT de outros países e que é um meio de comunicação de forma de identificar e eliminá-lo e temos outro canal que é a PJ, em que utilizamos a sua rede de investigação e ação para tomar as providências necessárias, ou seja, muitas vezes os IP's que nos chegam cá são o início de um rasto, que temos ainda de perceber e analisá-lo. É isso que faz a equipa do Centro de Operações de Segurança aqui do MAI. Uma das ações no momento do ataque é perceber a origem do ataque, de quem é, se aquilo vem de algum IP associado a um serviço que disponibiliza acessos remotos ou se é alguém que inadvertidamente ou ingenuamente está a usar o seu próprio acesso direto para fazer o ataque, isso hoje em dia é muito raro porque, como disse há pouco, na *internet* há muitos tutoriais de como fazer os ataques, portanto a pessoa não precisa de ter conhecimentos tecnológicos para saber como o fazer, basta ver a informação, seguir passo a passo o que lá vem e consegue fazer um ataque. Uma das recomendações que muitas vezes dão é mascarar e esconder o IP de origem.

8. Quais os tipos de ataques informáticos que ocorrem com mais frequência?

Com mais frequências é os DDoS com *Injection* ataque, as tentativas de *defacement, SQL Injection,* basicamente é o que temos tido com mais frequência. O *fishing* por *email*, também é um dos ataques mais frequentes que temos, por exemplo, agora anda

aí uma campanha de *fishing* associada a *Microssoft*, que está aí a fazer uns contactos como se fosse a *Microssoft* para obter informação.

Seria possível um *hacker* realizar um ataque ciberterrorista?

Sim, pode. Hoje em dia, por exemplo, o sistema de distribuição da água está executada no sistema informático, ou seja, se esse sistema for alvo de algum ataque ou intrusão ou alguém se apoderar desse sistema pode prejudicar, com o sistema da luz é a mesma coisa. Todos aqueles serviços básicos, ou seja, a distribuição da água, da luz, do gás, do dia a dia, podem ser comprometidos num ciberataque, porque todos eles têm tecnologia informática, por isso, podem ser alvo de um ataque e com isso haver impacto no cidadão. Nas telecomunicações, por exemplo, mandarem a baixo o sistema de um operador, por exemplo, da eletricidade.

Há algum protocolo com as Forças Armadas no caso de haver um conjunto de ataques derivado de um conflito internacional?

Isso existe, já estamos a um outro nível, se nos encontrarmos numa situação de calamidade, de estado de sítio, a defesa entra em ação, são eles já que tomam conta da segurança interna. Mas isso é já num outro âmbito. Está a ser desenvolvido o CNCseg, que terá mais a ver com a questão da defesa nacional, depois há o Centro de Ciberdefesa, que está na competência do Ministério da Defesa Nacional, que tem como principal ação o ataque aos *hackers* que possam estar a desenvolver ataques, ou seja, deteção e contra-ataque a esses elementos, mas neste momento ainda estão em fase de implementação. Pela informação que tenho, ainda estão numa fase inicial.

Nós qui do MAI iremos participar, pelo menos no CNCseg, estamos a trabalhar em conjunto com o GNS, que é a entidade que está com essa competência e seremos um dos *inputs* de informação para esse tipo de cibersegurança, a ideia é esse centro ter a informação do que se está a passar ao nível nacional, o objetivo é recolher informação tanto dos centros tecnológicos da Administração Pública, da banca, da indústria, das várias áreas da sociedade portuguesa e, com isso, terem noção do impacto e da abrangência que possa ter determinado tipo de ataque, mas ainda estamos a aguardar que isso seja colocado em produção.

Apêndice G – Entrevista a Carlos Cabreiro

A presente entrevista insere-se no âmbito da dissertação de mestrado para obtenção do grau de mestre no Mestrado integrado em Ciências Policiais, ministrado no Instituto Superior de Ciências Policiais e Segurança Interna (ISCPSI).

O título provisório da dissertação é "O *Hacktivismo*: Uma análise aos ciberataques dirigidos contra as Forças de Segurança", sendo orientador da mesma o Professor Doutor Felipe Pathé Duarte.

Pretende-se com esta dissertação estudar o fenómeno *hacktivistas* em Portugal e, em concreto, analisar os ataques realizados às Forças de Segurança, no sentido de determinar quais são os tipos de ataques efetuados, quais os grupos envolvidos e quais as pretensões destes grupos, de maneira a determinar se o fenómeno constitui ou não uma ameaça para a Segurança.

Local: Direção Nacional da Polícia Judiciária, Lisboa
Data: 9 de março de 2015
Cargo/Posto: Coordenador de Investigação Criminal

Guião

1. **Tendo em conta a evolução do *hacktivismo*, considera que atualmente este fenómeno é significativo em Portugal? Porquê?**

Nesta questão da evolução do *hacktivismo* o que se pode dizer é o seguinte: de facto com a utilização massiva dos meios tecnológicos e da informática transportou-se para este tipo de redes e plataformas, um conjunto de ações que eram só levadas a cabo em atividades de rua, nós aqui não investigamos concretamente a parte do ativismo, mas sim as situações que envolvem a prática de crimes informáticos e que por influência e com base nas notícias que estes grupos dão, também estão colados aos grupos de ativismo.

Tem vindo a aumentar mais como plataforma de comunicação, isto é, os meios de telecomunicações, processamento, tudo o que é *internet*, redes sociais, etc. Ou seja, estou a falar de interação de grupos e não de ciberataques, porque aí não podemos ligar-nos à palavra ativismo, de facto nós temos tido ataques informáticos, mas aí reduzem-se à criminalidade informática, ou são intrusões, ou crimes de acesso ilegítimo, podem não

estar associados à parte do *hacktivismo* como nós ouvíamos. Isto é, podem estar ou não, o facto é que utilizam muitas vezes estes ataques como propaganda de *hacktivismo* é só isso que aparece associado ao *hacktivismo*. Trata-se de um fenómeno significativo em Portugal como o é em toda a parte do mundo, porque felizmente não estamos à margem das tecnologias, somos um país com um índice de penetração de tecnologias bastante interessante e eu diria que dos países com mais penetração em termos informáticos e por isso não podemos estar e não ficamos à margem de qualquer outro país. Estas ações e este tipo de atos cometidos no seio das redes informáticas, também acontecem em Portugal ao mesmo nível e com a mesma percentagem de utilização de meios informáticos de qualquer outro país. Quando se fala em *hacktivismo* não se pode associar aos ciberataques. Deriva uma coisa da outra, mas não é por fazer determinado ataque a uma instituição que seja um *hacktivista*, podemos exclusivamente estar a falar de pessoas com motivação exclusivamente patrimonial que só querem o lucro, não têm por trás qualquer outra intenção. Quando fazemos a investigação deste tipo de crimes também investigamos o fenómeno que está por detrás, mas grande parte da criminalidade informática acaba por não ter associado a ela essa motivação de *hacktivismo*, mas outro tipo de motivações, de lucro, satisfação pessoal, o desafio, é mais nessa ordem de ideias. Não ligo, de maneira nenhuma, tudo o que é crimes informáticos a tudo o que é *hacktivismo*, há uma franja de crimes que lança, a bandeira do *hacktivismo* como fator de ataque, mas não é, na sua maioria, o que estamos a investigar. Quando estamos a falar deste tipo de ataques, eu não gosto muito de lhe chamar ataques, porque o que eles praticam efetivamente são crimes e nós entramos, por isso, noutra linguagem, mas estaremos a falar dentro dessa motivação a parte do *hacktivismo* poderá significar 10 % talvez [dos casos investigados], é o número que avanço pela perceção que tenho. A maioria de ataques que ocorrem são os que têm fins patrimoniais.

2. Considera o *hacktivismo* uma ameaça à Segurança? Porquê?

É com certeza, vou-me só referir ao *hacktivismo* praticado nas redes informáticas, porque além de ser de facto disruptivo, na forma como podem fazê-lo, podem pôr em causa a informação do Estado, podem assumir e ter conhecimento de determinada informação, que pode constituir até segredo de Estado e, portanto, é uma ameaça contra a segurança do Estado ou contra a segurança dos cidadãos a partir do momento em que as suas instituições são atacadas.

3. Considera que Portugal está devidamente protegido contra os ciberataques?

Em matéria de segurança informática, costuma-se dizer que não há uma segurança total e não há sistemas 100% seguros, daí que também o Estado e Portugal não seja uma exceção. O que se tem assistido é à criação de um conjunto de infraestruturas que permitem que se vá começando a ter uma estrutura de segurança que possa corresponder e responder a este tipo de fenómenos: o recém-criado CNCseg, a aposta que a PJ tem feito no combate ao cibercrime, a perceção que se faz ter na sociedade para que isto seja um tema que possa ser incluído na cultura de segurança, na cultura dos menores, na cultura dos jovens, é com certeza um motivo que nos desafiará a todos para percebermos que também a utilização das novas tecnologias, das plataformas de *internet* e outras redes podem mexer com a segurança dos cidadãos, mas Portugal tem feito o seu caminho naturalmente na proteção das infraestruturas, na proteção da segurança da informação.

4. Quais as possíveis consequências de um ataque *hacktivistas*?

Podem ser várias as consequências, nós temos tido exemplos disso, há situações que se ficam pela impossibilidade de acesso aos serviços, quando estamos a falar de ataques DDoS. Mas podem-se também configurar outro tipo de ataques em que existe um acesso à informação privada e de instituições públicas, que tem grande valor em termos de informação, por isso, as consequências são sempre relativas e podem, para uma determinada instituição, constituir uma base de trabalho porque é esse o *core business* da instituição. Outra coisa será essas instituições em que, vamos dar um exemplo: imagine um ataque informático a uma estrutura do Estado, onde existe informação cadastral dos cidadãos, que se possa vir a perceber que um determinado registo que estava feito em meu nome, passou a estar no nome de outro. Esta alteração com certeza tem uma consequência verdadeiramente devastadora para a organização de um país. Entramos pelos princípios fundamentais, ou seja, aqueles cinco chavões da segurança da informação: autenticidade, disponibilidade, integridade. Entramos por aí e aí as consequências serão com certeza muito mais gravosas.

5. Como se caracterizam, organizam e o que pretendem os grupos de *hacktivistas* (traçar perfil)?

Mais uma vez entramos pela motivação que está por trás desta gente que se dedica à prática destes crimes, aqueles que invocam o *hacktivismo*, a motivação é essa: o *hacktivismo*. Processam a sua atividade e esta atividade maléfica, digamos assim, sobre a *internet* e sobre os sistemas de informação com a bandeira do *hacktivismo*. Outros haverá, e aí podem não entrar dentro do campo dos *hacktivistas*, mas sim dos cibercriminosos exclusivamente, que são aqueles que têm motivações extra *hacktivismo*, económicas, patrimoniais, satisfação. O que eles pretendem é fazer ouvir a sua voz, o *hacktivismo* passa por causas que essas pessoas defendem, naturalmente o que querem passar para a parte da informática. É precisamente a mesma mensagem do *hacktivismo*, do protesto contra uma determinada causa ou contra uma determinada realidade. Em termos organizativos, se estiverem ligados à realidade, à parte denominada ativista denotam alguma organização porque se encontram, são pessoas que se conhecem, quando estamos a falar da parte da informática pode não haver esse elemento do conhecimento. A união que possam fazer transparecer nas suas ações apenas se limita ao conhecimento virtual e feito via plataforma informática. Pode haver organização, mas o conceito de rede organizada se calhar não a conseguimos transpor.

6. Poderá um ataque informático contra as infraestruturas das Forças de Segurança afetar a sua missão? Em que sentido?

Pode com certeza. Como lhe digo depende do impacto que esse ataque tiver porque se afetar setores vitais, como por exemplo, a informação que estiver no âmbito das FS. É esse o exemplo típico da capacidade que este tipo de ataques informáticos pode ter sobre as FS.

7. Qual o balanço que faz da investigação dos crimes relacionados com ciberataques?

O balanço que faço é o seguinte: Algumas dificuldades específicas relacionadas com a investigação. Portugal tem vindo a aderir ao normativo, no sentido de uniformizar a legislação que existe a nível europeu, a ciberconvenção, por exemplo, é um caso desses, para além dos países da Europa também outros países como o Canadá e os EUA, aderiram à ciberconvenção, isto trás um benefício enorme quando estamos a falar da possibilidade de classificar o mesmo tipo de facto da mesma forma em várias partes do mundo, até

porque é isso que a *internet* nos exige, que é que sejamos uniformes na forma de pensar este tipo de fenómenos e Portugal tem vindo a aderir a essas possibilidades de investigação, tem aderido também a novos meios de obtenção de prova, nomeadamente, ações encobertas, interceções telefónicas, as próprias pesquisas informáticas que estão previstas na Lei da Criminalidade informática, fazem com que Portugal não esteja de nenhuma forma atrasado em termos de investigação, há naturalmente apostas que têm de ser feitas, clarificações, ultrapassar algumas dificuldades na obtenção de prova, mas estamos a fazer o nosso caminho e o balanço que faço é extremamente positivo, na sua maioria conseguimos percecionar realidades que estão envolvidas e fazer com que possamos propor a acusação das pessoas que praticam este tipo de crimes. A maioria deles, em Portugal, são mais portugueses do que estrangeiros, mas também existem autores de crimes praticados em Portugal que têm nacionalidade estrangeira.

Mas esses crimes são realizados a partir do estrangeiro ou de dentro do país?

Aí entram outros mecanismos de responsabilização e que tem a ver com a aplicação da Lei penal no espaço e sempre que é necessário essa cooperação, em termos policiais existe uma excelente cooperação, entre as unidades de investigação de criminalidade informática, as nossas e de outros países, fazemos também parte de grupos de trabalho muito ativos da própria EUROPOL e INTERPOL, que facilitam este tipo de troca de informação e que fará com que, em termos legais, de acordo com os nossos requisitos possamos "perseguir" aqui estrangeiros que cometem crimes em Portugal e prestando o apoio possível a outros países e recebendo-o. Para isso, é necessário haver a uniformização de procedimentos, a própria Lei e a ciberconvenção é exemplo disso, porque veio munir os Estados de uma legislação muito idêntica em termos da perseguição penal, porque quando estou a falar de um crime de acesso ilegítimo, eu tenho a certeza que em França e na Alemanha, quando eu falo de acesso ilegítimo também eles sabem do que estamos a falar e também temos lutado na criação de uma taxonomia comum, porque nesta área da informática estamos ajudados por um léxico próprio e importa que cada um tenha a perceção do que fala quando estamos a falar de um ataque de DDoS ou outro, todos saibamos.

A taxonomia que utilizamos é em parte a do CERT.PT, a taxonomia já foi um trabalho que tivemos com o CERT e foi aí que tentámos logo em Portugal criar uma taxonomia porque aquele trabalho é conjunto entre nós e o CERT.PT, agora mesmo a nível

europeu em ações comuns, em planos de ação que estamos a ter em grupos de trabalho da EUROPOL, estamos a fazer essa tentativa uniformização da taxonomia, que vai um pouco ao encontro à taxonomia que é disponibilizada no CERT.

Os contornos das investigações nacionais e estrangeiras são os mesmos?

Existem especificidades, não é com certeza a mesma coisa porque temos de ir buscar outro tipo de informação que vamos buscar noutro crime onde não necessitamos de esse meio de obtenção de prova, por exemplo na *internet*, mas quais são as dificuldades que estão aqui envolvidas: primeiro a transnacionalidade, porque estamos a falar da possibilidade de alguém, mesmo através de Portugal, estar a cometer um crime, cuja comunicação passou para outro país no mundo e, daí poder surgir desde logo essa questão da transnacionalidade. O percurso do *iter criminis*[148] também é feito em vários territórios se for necessário porque eu não tenho a certeza quando estou a falar daqui para o Brasil se a minha comunicação não foi feita através dos EUA ou outro país, tudo depende das disponibilidades de redes. Em termos internos as dificuldades estão quase sempre relacionadas com determinação de origem de uma comunicação, porque o que sustenta a *internet* são as comunicações e o objetivo principal de um investigador será sempre determinar de onde é que partiu determinada comunicação, por onde é que foi e qual foi o destino, para nós percebermos a causa e o efeito das coisas. Na *internet*, cada vez mais, está a haver ferramentas e subterfúgios que tendem a anonimização da nossa conduta ou de quem queira praticar factos, com certeza que isso serão dificuldades acrescidas que fazem já alguma diferença e que nos obrigam a ter outros mecanismos de recolha de prova, não nos cingirmos tão só aquela parte da comunicação, aquele ato em si, mas temos de fazer uma análise mais diversificada da atuação de uma determinada pessoa, se chegarmos à pessoa. Mas há situações de facto às quais não se consegue chegar, porque estamos a falar da impossibilidade, por exemplo, de um número de telefone que eu adquiri, num supermercado, os chamados pré pagos, e que eu não tenho qualquer possibilidade de identificação porque foi descartado e nada o liga à pessoa.

[148] Expressão latina que designa "caminho do crime".

8. Quais as principais dificuldades na investigação deste tipo de crimes?

As dificuldades são essas. E depois também a grande tecnicidade e a grande dificuldade que existe em tecnicamente ir acompanhando a realidade, porque o que hoje é a realidade amanhã já não é e a evolução ultrapassa-nos um pouco.

Como se processa a coordenação com outras instituições?

Aqui ao nível de coordenação nós temos efetivamente que de ter uma atuação coordenada. Estamos a falar é de uma criminalidade que é da competência exclusiva da PJ, e que grande parte de toda a informação nos chega. Em todo o caso é evidente que tem de haver uma excelente coordenação quer com o CNCseg agora, até porque se torna necessário haver essa proximidade e intercâmbio de informação que é a perceção de segurança e também nos casos concretos. Nós aqui, lidamos com crimes com situações concretas que urge responder, embora tenhamos uma missão importante no âmbito da prevenção criminal quando lidamos com casos concretos temos de nos cingir aos casos concretos e a cooperação que tiver de existir existirá, não existindo qualquer quebra de coordenação em relação ao que é o objetivo do Estado no combate ao cibercrime.

Apêndice H – Entrevista a José Carlos Martins

A presente entrevista insere-se no âmbito da dissertação de mestrado para obtenção do grau de mestre no Mestrado integrado em Ciências Policiais, ministrado no Instituto Superior de Ciências Policiais e Segurança Interna (ISCPSI).

O título provisório da dissertação é "O *Hacktivismo*: Uma análise aos ciberataques dirigidos contra as Forças de Segurança", sendo orientador da mesma o Professor Doutor Felipe Pathé Duarte.

Pretende-se com esta dissertação estudar o fenómeno *hacktivistas* em Portugal e, em concreto, analisar os ataques realizados às Forças de Segurança, no sentido de determinar quais são os tipos de ataques efetuados, quais os grupos envolvidos e quais as pretensões destes grupos, de maneira a determinar se o fenómeno constitui ou não uma ameaça para a Segurança.

Local: Presidência do Conselho de Ministros, Lisboa
Data: 3 de março de 2015
Cargo/Posto: Diretor do Centro Nacional de Cibersegurança

Guião

1. **Tendo em conta a evolução do *hacktivismo*, considera que atualmente este fenómeno é significativo em Portugal? Porquê?**

Sendo Portugal um país, de alguma forma, de brandos costumes, obviamente que o *hacktivismo* tem algum significado em Portugal, na medida e na razão do seu tamanho, da sua grandeza, da sua afirmação. Obviamente que é um fenómeno significativo que tem vindo, cada vez mais, (focando um pouco na sua componente ciber) a ter uma maior expressão, resultado e fruto de que hoje em dia todos e quaisquer tipos de conflitos têm um palco de atuação diferente que tinham no passado. Se no passado tínhamos conflitos que se resolviam no mundo físico, os conflitos atualmente estão a passar cada vez mais do mundo físico para o mundo virtual. Os conflitos, sejam eles quais forem, podem ser conflitos pessoais, conflitos institucionais ou conflitos sociais, e o que tem acontecido é passar de um palco físico para um palco virtual, ou seja, utiliza-se o ciberespaço para fazer a gestão de conflitos, é uma realidade nova e que cada vez mais tem vindo a acontecer, portanto

hoje em dia é difícil não visualizarmos conflitos que não tenham expressão no ambiente ciber, é praticamente impossível. Levando isto ao máximo conseguimos até focar isto às vezes em questões até pessoais, quando duas pessoas de alguma forma se desentendem, nós sabemos, um chega a casa " o que é que este tipo faz, o que é que não faz….". Pode não resultar em nada mas há aqui um novo mundo para investigar, para saber, para perceber. Tanta informação que depois permite atuar de alguma forma, pode resultar numa difamação, na obtenção de uma informação ou, até quem sabe, num crime. Relativamente ao *hacktivismo* em si, recentemente tivemos uns acontecimentos novos, na semana passada, tivemos 7 pessoas que foram detidas, no âmbito de processos de *hacktivismo* também e, de alguma forma, agora vão acalmar as coisas em Portugal durante mais uns tempos, mas possivelmente será sol de pouca dura, porque volta outra vez estes movimentos e estes grupos, nomeadamente, o grupo dos *Anonymous* e outros.

A própria detenção deles pode levar a reações quer sejam elas reações internas mas também muito reações internacionais. A nível interno isto criou aqui um momento de medo nestes grupos que se retraíram um pouco e enquanto estiver na memória vai criar uma retração mas depois passa, na parte internacional esta retração não existe quando muito até existe outra coisa diferente que é a solidariedade. Houve elementos que foram detidos, nós somos solidários com eles, vamos agora executar ações. Até ver, isto aconteceu há pouco tempo, uma semana quase, passou uma semana e as coisas estão relativamente calmas mas eu creio que sim, que lá para a frente que iremos voltar a ter novas manifestações. Portanto, em concreto, é um fenómeno significativo, não podemos de forma alguma abandoná-lo nem podemos de forma alguma menosprezá-lo, porque hoje em dia os conflitos levam a isto. Todas as áreas de intervenção quer quando falamos em *hacktivismo* podemos estar a falar das áreas de crime de cibercrime todas as áreas de intervenção cada vez mais atentas e mais ativas porque obviamente vamos ter, à medida que vamos andando para frente, mais conflitos e vai haver um desenrolar de maiores conflitos e vai haver necessidade de maior atuação por parte das entidades que lidam com estas matérias, nomeadamente a PJ, outros órgãos de informação e mesmo o CNCseg, obviamente, portanto é um fenómeno significativo e que irá continuar.

Considera que o número de ciberataques ligados ao *hacktivismo* tem vindo a aumentar?

Tem vindo a aumentar e a tendência é que continue a aumentar. Obviamente que as instituições vão criando mecanismos para diminuir mas eu penso que em virtude de não só conhecimento mas também das capacidades destes próprios grupos, que são grupos que têm muitos (e provou-se agora nestas detenções) jovens envolvidos, vem criar aqui algumas apetências que levam a que estes tipos de ataques continuem a acontecer e até de alguma forma tenhamos sempre fenómenos destes com alguma intensidade.

Obviamente que estas instituições como o CNCseg, a PJ e outras instituições terão que ter capacidade para contrariar este fenómeno, por um lado através de uma prevenção sensibilização junto da sociedade civil, dos cidadãos, das empresas das IC, da Administração Pública, por outro lado, com medidas concretas que diminuam a exposição ao risco dos sistemas ou serviços vitais de informação ou das infraestruturas criticas com aplicação de sistemas concretos, de alguma forma também com medidas que permitam monitorizar a atividade no ciberespaço português que consiga possibilitar uma possível antecipação nos ataques. Criar aqui alguns mecanismos de mitigação de redução que sejam dissuasores dos *hacktivistas* mas também que consigam numa ótica de continuação de serviços e numa ótica de combate ao cibercrime.

2. Considera o *hacktivismo* uma ameaça à Segurança? Porquê?

Obviamente que sim. Porque conforme disse há pouco estes conflitos que hoje em dia são gerados, que se disputam muitas vezes no ciberespaço, têm objetivos muito concretos. Nós podemos ter *hacktivistas* que decidem atacar, por exemplo, IC, vamos falar de duas infraestruturas muito críticas, que muitas vezes nós não temos a perfeita noção delas, desde logo tudo o que tenha a ver com o ramo da energia, que uma paragem de um serviço deste pode deixar Portugal simplesmente parado, porque não funciona, porque nada funciona sem energia. Por outro lado, um serviço como a água, o simples facto de deixar uma desconfiança de que houve qualquer coisa, um ataque, às infraestruturas das águas, sejam elas quais forem, que possa pôr em dúvida o consumo da água leva a um estado de quase paranoia nos cidadãos. Nós vimos uma coisa recente há pouco tempo que foi o caso da Legionella em Vila Franca de Xira, em que as pessoas já nem sequer bebiam água da torneira, ficaram semanas sem tomar banho. Um fenómeno muito pequenino mas que tem a ver com a água, porque a Legionella resultava do vapor de água mas as pessoas

já nem sequer bebiam água fria, que não faz vapor. As pessoas ficaram em estado de alerta, e cria um estado de paranoia e isto pode criar problemas sérios relativamente à segurança nacional.

Mas quando fala aqui em interromper a energia, por exemplo, é possível fazê-lo a longo prazo?

Não sabemos o que é possível. Podemos estar a falar de sistemas, até porque esta avaliação não está completa e não sabemos se um ataque a uma IC que tenha a ver com a energia não pode criar constrangimentos graves.

Não sei se se recorda há uns anos atrás, houve um apagão enorme provocado por uma cegonha. Se for ao *Google* e fizer umas pesquisas, apagão, EDP e cegonha. Houve há uns anos atrás um apagão que deixou, eu não tenho a certeza se foi o país todo, mas pelo menos parte do país às escuras. Depois isto foi justificado, nunca se soube, (pelo menos eu não tenho essa informação) com uma cegonha que expôs um sistema de eletricidade e aquilo parou, e de repente tudo parou. Imagine que há um sistema qualquer de controlo de estações elétricas de subestações, seja o que for, que é comprometido e que o atacante decide deitar abaixo as estações ou de alguma forma corromper a informação de forma que o sistema normal não funcione e podemos ter um problema aqui grave como falta de energia, como falta de energia em hospitais, mesmo que tenham geradores e coisas do género tem uma limitação e noutras áreas que pode criar problemas sérios à Segurança Nacional. Obviamente que há outras áreas críticas, desde logo as infraestruturas e serviços vitais de informação do Estado, sejam impostos, a justiça, a segurança social. Imagine que os sistemas da segurança social, por exemplo, são comprometidos e naquele mês todos os pensionistas, porque os sistemas foram comprometidos, a informação foi corrompida houve roubo de informação, e naquele mês não é possível pagar a pensão a ninguém, isto cria um problema, agora imagine todos os reformados e todos os pensionistas, de repente naquele mês, não tem dinheiro e não se consegue reativar o sistema, não se consegue pôr os sistemas a funcionar qual é o impacto disto tudo na sociedade? Digo isto, mas podemos falar da saúde, imagine que os sistemas da saúde, os sistemas onde todos nos estamos inscritos – o SNS – tem um problema qualquer um colapso qualquer e se perdem os nossos dados, os nossos dados passam a estar disponíveis na *Internet* que são pessoais. Isto são problemas que são muito complicados temos que ter alguma atenção com eles, muita atenção com eles e que ver e contribuir todos, desde logo, enquanto cidadãos até ao Estado,

contribuir para a segurança e cibersegurança nacional. É um trabalho que começa em nós, enquanto cidadão, e acaba no Estado, enquanto Estado de direito.

3. Quando falamos em *hacktivismo*, podemos falar em cibersegurança e ciberdefesa? Onde termina um e começa o outro?

É verdade, está a ser criado um Centro de Ciberdefesa e existe um CNCseg. No entanto, eu confesso que há um chavão, há um conceito, isto tem muito a ver com a definição de conceitos, há um conceito que para mim é um conceito único e totalmente abrangente que é a cibersegurança e a cibersegurança é um chapéu que abrange tudo o que é segurança do ciberespaço, segurança de ciberespaço são todas as valências. O CNCseg não se pode confundir com a cibersegurança. Isto aqui é a minha forma de ver as coisas. Quando falamos de Cibersegurança estamos a falar de um chapéu, ciberdefesa é uma componente da cibersegurança. Isto para tentar traduzir de uma forma mais clara si. Num estado normal, em que alguém compromete ou ataca um *site* ou faz um *defacement* a um *site* qualquer de uma instituição isto é um problema de cibersegurança normal. Quando esse ataque, esse *defacement* ou essa tentativa de intrusão pode causar riscos que possam pôr em causa a soberania nacional estamos a entrar num capítulo que já é de defesa, ou seja, temos a componente de cibersegurança normal, ou seja, temos o chapéu de cibersegurança mas quando entremos no capítulo em que precisamos de componentes ofensivas de resposta entramos numa área que é de ciberdefesa. Esta é a forma como eu consigo alinhar as coisas no chapéu da cibersegurança.

Ciberdefesa só num caso em que estamos envolvidos num conflito internacional ou seja no âmbito da defesa?

Há um conceito que é muito utilizado que é ciberdefesa defensiva e ciberdefesa ofensiva. Ciberdefesa defensiva é cibersegurança, a cibersegurança é defender, ao fim ao cabo é estar sempre protegidos, é termos sempre prevenção. Quando passamos para uma componente ofensiva ou que impliquem estados de sítios, estados de guerra, seja o que for, que não são tempo de paz, estamos a falar em ciberdefesa. Ou seja, quando é que começa um e termina o outro? A cibersegurança começa sempre, dependendo do enfoque do *hacktivismo* e do resultado das ações podemos entrar na componente ciberdefesa. Estes dois polos de ciberdefesa e cibersegurança têm algumas dificuldades de cruzamento, principalmente porque existem Centros de ciberdefesa e cibersegurança.

Qual é que é a relação existente?

Tanto um como outro são centros recentes. Centro cibersegurança tem 6 meses e ciberdefesa tem se calhar três. É uma relação muito recente, mas estamos a trabalhar na relação, na cooperação e o objetivo é que haja total cooperação entre os dois não faz sentido que seja de outra forma. A cibersegurança é um chapéu muito mais amplo, a atividade do CNCseg é uma atividade muito focada e muito consagrada, até pelas atribuições que tem para as IC, para a Segurança Nacional, no que diz respeito a Estados a IC, cidadão e depois temos uma componente onde entramos em matérias militares, comando e controlo, CNO's, e quando entramos em estados que podem ser estados de emergência, estados de sítio, estados de guerra, seja o que for, entramos numa componente mais ofensiva em que a ciberdefesa obviamente toma conta das operações.

4. De que forma se processa a coordenação da cibersegurança nacional entre as várias instituições responsáveis?

A coordenação operacional nas áreas da cibersegurança, nomeadamente, na parte mais concreta no que respeita à resposta de incidentes é uma incumbência clara do CNCseg. Tudo o que tenha a ver com gestão de incidentes, reporte de incidentes, reporte de vulnerabilidades, toda a parte operacional de cibersegurança que é proteger os serviços, que é preventivamente garantir que os serviços estão disponíveis, garantir as três componentes de segurança: integridade, disponibilidade e confidencialidade, garantir três níveis fundamentais. A coordenação é feita pelo CNCseg, com os vários parceiros e atores. Obviamente que na sociedade civil não existe grandes planos para que se possa fazer coordenação, no entanto existe rede nacional de CSIRT's, que são centros de resposta a incidentes. Esta rede nacional é uma entidade privada, autónoma criada de uma forma *ad hoc* e que tem representantes de vários organismos e várias entidades privadas, públicas e que partilha neste universo, não só informação mas partilham tipologias, taxonomias, de forma que, por exemplo, alguém está a receber um ataque, seja ele de *fishing*, *defacement*, numa conta qualquer na Vodafone partilha a esta comunidade: "atenção estou a ser alvo de uma atividade de *fishing* preparem-se que pode-vos acontecer o mesmo" esta rede funciona como um canal que partilha sinergias e que permite divulgar uma série de informação. Esta é uma rede *ad hoc*, na qual o CNCseg também está inserido, não é coordenador desta rede, permitiu que os privados criassem algo privado, e não criando o chapéu de papão do Estado, que chega coordena e faz. É uma rede informal na qual o centro também está e

obviamente que o centro através deste canal, enquanto entidade coordenadora, também dá as suas orientações e instruções para esta entidade porque é a entidade coordenadora nacional e tem que assumir esse papel. Relativamente ao Estado, o CNCseg é a entidade coordenadora e tem que assumir perante as Entidades do Estado e perante as IC esse papel, no sentido de conseguir coordenar toda a parte operacional de gestão de resposta a incidentes e prevenção de incidentes. Esse é o papel que estamos a desempenhar neste momento, este é um processo evolutivo, começámos as nossas atividades a 7 de outubro do ano passado mas a coordenação estará assegurada dessa forma. Estamos a tentar capacitar alguns organismos do Estado de forma a estarem preparados para responder a estes desafios, estamos a tentar capacitá-los, quer a nível tecnológico quer a nível de recursos humanos, para podermos responder a essas necessidades. Relativamente aos vários atores que têm de alguma forma ligações e estão dependentes do CNCseg na questão da cibersegurança nós temos obviamente um papel coordenação e colaboração, nomeadamente, quando falamos da PJ na área de cibercrime. Nós temos a nossa própria orgânica, claro que qualquer incidente somos obrigados a compartilhar e a comunicar com a parte do cibercrime, temos ligações com ciberterrorismo, com o ciberativismo, com a parte da espionagem, portanto todas estas identidades depois conseguem com certeza identifica-la, sejam elas a PJ, sejam elas as próprias FS, nós fazemos colaboração e coordenação com todas. Como estamos numa fase de construções de equipa, construção de centro, estamos a estudar os melhores mecanismos para conseguir de uma forma ágil e rápida não só termos, não sei se serão elementos de ligação operacional, serão menos informais que permitam a coordenação e comunicação rápida entre as instituições todas. É um processo que nós sabemos que demora um pouco porque temos que ganhar a confiança junto destas instituições apesar de existirmos por Lei, há aqui uma base que é a confiança e que estamos a ganhá-la, e que, de alguma forma, sendo nosso papel de entidade coordenadora nesta matéria temos de transmitir e ganhar confiança para conseguirmos com todos trabalhar. Depois há outras entidades que também estão envolvidas nisto, desde logo a maior parte do setor das comunicações sejam os service *providers* sejam as entidades reguladoras para as comunicações, para a energias, para outras entidades, nós vamos criar aqui este núcleo que nos permite coordenar tudo de alguma forma nesta ótica essencialmente da gestão de incidentes na parte da prevenção, na parte da sensibilização, que é uma forte aposta nossa e que, de alguma forma, nós vamos ter que trabalhar.

5. Considera que Portugal está devidamente protegido contra os ciberataques?

Devidamente protegido não. Acho que encontramos algumas lacunas, quer na Administração Pública, ou seja, no Estado, quer também nas IC. A resposta é não estamos devidamente protegidos. Esse é um trabalho que nós pretendemos fazer quer com as entidades do Estado quer com as IC, que é levantar um conhecimentos sobre o estado de cada uma dessas entidades para de alguma forma ajudar a contribuir para a segurança dos seus sistemas, é um trabalho que fazemos neste momento. Neste momento, sobre as entidades do Estado estamos a conhecer o negócio, a sua atuação, a sua visão da parte toda da segurança, estamos a fazer esse levantamento, mas já identificamos algumas.

Não diria só em termos de vulnerabilidade dos sistemas, muitas vezes levantamentos são vulnerabilidades processuais e de governação, identificámos aqui algumas falhas, algumas lacunas das várias instituições. Neste momento, é um levantamento muito mais do conhecimento das instituições, do negócio, dos processos críticos de negócio e do que é que está a ser feito para proteger esses processos críticos e aí é que nós temos algumas dúvidas da robustez da proteção dos processos críticos desses negócios e, de alguma forma, achamos que não está, sei que tem sido feito um trabalho de há uns anos a esta parte, mas é preciso criar também consciencialização, para os decisores sejam eles gestores públicos, sejam privados, dos riscos que correm em não estarem devidamente protegidos ou salvaguardados para os ciberataques sendo que obviamente eles irão acontecer sempre por muitas pretensões que se tenham, mas tudo o que seja mitigado é um ganho para o país. Neste momento achamos que ainda não existe capacidade suficiente, as próprias entidades, na eventualidade de ter um ciberataque, muitas delas não conseguem fazer uma despistagem de como as coisas acontecerem, há aqui uma necessidade de capacitar as entidades para conseguirem fazer um levantamento de quais foram os processos utilizados, de como as coisas aconteceram, portanto há um trabalho que tem de ser feito junto das instituições, nomeadamente as do Estado, infraestruturas críticas, de forma a que não só conheçam a realidade do negócio, conheçam a realidade do risco que tem sobre o negócio, a análise de risco bem equacionada, bem realizada, para perceberem qual é a exposição que têm e perceberem qual o nível de criticidade e de risco a que estão expostos e, de alguma forma, terem a noção real do estado atual relativamente à proteção contra ciberataques.

6. Quais as possíveis consequências de um ataque *hacktivistas*?

As consequências de um ataque *hacktivista* podem ser diversas, podem ser questões em que coloca em causa a segurança nacional, a soberania nacional até, muitas vezes pode ter consequências de credibilidade, pode ser um ataque a um órgão do Governo que possa descredibilizar esse órgão, portanto pode provocar a falência de um sistema, tem vários tipos de ataque, segurança nacional, roubo de informação

Considera possível haver um ataque ciberterrorista?

Os termos confundem-se. Utilizando o termo ciber dá para tudo. A questão do ciberterrorismo em primeira instancia está na parte montante que tem a ver com a questão que nós vemos hoje em dia está na parte do recrutamento. Todo este processo de "recrutamento de negócio" é feito no ciberespaço. Logo aí temos uma componente de educação e sensibilização que tem de ser trabalhada mas é possível que numa fase final o ciberterrorismo possa ter implicações muito graves, que possa inclusivamente causar mortes causar danos materiais, de vidas isso pode acontecer. Imagine que um ataque terrorista consegue entrar num hospital e consegue desligar sistemas digitais de saúde na sala de cuidados intensivos, não conheço suficientemente os centros hospitalares, é um trabalho que também estamos a fazer, mas isto pode causar mortes ou qualquer ataque a qualquer infraestrutura ou sistema público possa causar disrupção de serviço, ou mais que isso, também não conheço o sistema ferroviário totalmente mas imagine, o controlo do sistema rodoviário que passa pelo controlo de linhas, isto pode no extremo causar vítimas mortais e danos materiais.

Até hoje, não tem acontecido nada neste sentido, mas é importante que Portugal esteja atento e mais é importante que esteja numa fase de prevenção, de monotorização, de perceber de alguma forma o que está a acontecer, perceber se existem manifestações estranhas, perceber se existem ações que não era expectável estarem a acontecer, perceber se existem comunicações que talvez não devessem estar a acontecer no ciberespaço e que estão. Eu penso que será muito por aí a aposta no ciberterrorismo.

7. Como se caracterizam, organizam e o que pretendem os grupos de *hacktivistas* (traçar perfil)?

Obviamente que não temos ainda os dados que nos possam levar a este tipo de conclusões. De alguma forma sabemos que muitos deles são jovens, que são curiosos, que

se colocam nestas matérias, das tecnologias da informação, que investigam e tentam perceber e depois gostam de algum forma de ganhar troféus e apresentar troféus mas estes não são os maus, estes chateiam, incomodam, mandam *site*s a baixo, fazem *defacements*, mas por trás destes há os que querem fazer espionagem, que querem roubar informação, os que querem de alguma forma ter controlo sobre a informação.

Estava a falar em questões mais concretas de detenções que foram feitas recentemente, questões muito mais profundas relacionadas com crime organizado, que é algo muito mais preocupante, com ataques de Estados, com obtenção de informação por parte de estados, ultimamente tem havido alguns ataques que são realizados por ferramentas que são construídas por Estados para obter informações a outros Estados.

Crime organizado, a ciberespionagem, a espionagem feita por Estados, por parte da espionagem industrial, na utilização de *bootnets* que estão controláveis, a própria venda de serviços de ataques que alguém controla, por exemplo, uma *bootnet* que está no meu computador está sempre no meu computador e depois vende este serviço para que alguém desenvolva um ataque com intuito de tirar informação, roubar informação. Obviamente que há aqui uma coisa importante que é a continuidade das operações, ou seja, se o *site* ou o serviço de *internet* de uma organização pública foi abaixo vai-se retomar o serviço mas depois há que ver o que isso provocou, se houve roubo de informação, se houve penetração dos sistemas, há aqui várias situações que têm de ser ponderadas. Não temos aqui um perfil definido. Os nossos serviços operacionais vão ser ativados, a parte de resposta a incidentes e monotorização, a partir de 16 março, até agora temos estado a trabalhar na casa, a montar as infraestruturas e toda a parte tecnológica, está tudo montado vai ser ativado a partir dessa data. Depois começamos a perceber de forma mais clara de qual o perfil dos atacantes, de que forma é que os ataques se efetuam. Até à data, temos o que de senso comum vamos percebendo, o que obtemos de fontes abertas, o conhecimento que temos da nossa experiência passada, porque todos nós lidamos com a questão da cibersegurança, dos ataques, dos *defacements*, dos DoS, com estas questões todas que envolvem a cibersegurança, nessa altura teremos mais informações para dar do que agora. Por outro lado, alguma informação dessa de perfis conseguia obter junto de outras instituições como o SIS ou a PJ, era bom ter o enquadramento todo.

8. Poderá um ataque informático contra as infraestruturas das Forças de Segurança afetar a sua missão? Em que sentido?

Diria que sim. Se as FS não se conseguirem operacionalizar temos um ataque às FS. Eu não conheço em detalhe os sistemas de informação das FS, mas o que conheço não tenho dúvidas de que pode causar um problema à atuação das FS, porque de alguma forma também têm uma dependência dos sistemas de informação, basta que no extremo exista o comprometimento de um sistema de informação crítico, não sei se os vossos serviços de informações assentam sobre sistemas de informação, mas eu penso que sim, basta que esses sistemas estejam comprometidos, que tenham informações não íntegras, haja um comprometimento de informações que lá estão, haja informação erradas de alguma forma, ou seja, sem integridade para que as Forças possam perder um pouco a sua capacidade de reação, porque a sua base de conhecimento é uma base de conhecimento errada.

As FS têm acesso a sistemas de informação, que podem ser comprometidos e ter informações falsas e comprometer a operação, porque a informação não é verdadeira, até os próprios sistemas de comunicação podem ser comprometidos. É uma preocupação que acho que tem de ser uma preocupação grande em relação às FS, por outro lado, há ações que não são de comprometimento efetivo da operação, mas ações de comprometimento da credibilidade e essas às vezes têm um impacto ainda maior e tem acontecido, aconteceu há pouco tempo, quando saíram uma série de agentes cá para fora, isso compromete uma instituição, para já expõe as pessoas e compromete segurança na instituição. Uma FS que deixa sair cá para fora os nomes dos agentes, os dados dos agentes, tira credibilidade, a confiança é a base de tudo, portanto, se eu enquanto cidadão deixo de ter confiança na PSP ou outra Força qualquer, há aqui um aspeto que não funciona tão bem, a cidadania não funciona, eu não confio, não é um caso que vai fazer com que deixe de confiar, mas vai quebrar a credibilidade. As FS têm obrigatoriamente que ter uma credibilidade muito forte, porque nós cidadãos apoiamo-nos nas FS, na proteção das FS. Eu não tenho dúvidas em dizer que sim, um ciberataque pode por em causa não só a operacionalização mas também muito a credibilidade da instituição. Muitas vezes é quase tão importante a credibilidade quanto a operacionalização. Nós vemos isto em algumas instituições, nomeadamente, em instituições financeiras que lidam com o nosso dinheiro dificilmente manifestam um ataque, eles no princípio até quando desaparecia o dinheiro eles repunham o dinheiro. Se eu souber que o meu banco está a ser alvo de ataques eu não ponho lá o meu dinheiro. Se eu souber que a PSP que é a Força que me protege, pelo menos aqui na cidade de Lisboa, a

primeira a quem vou recorrer, é uma FS que menospreza a segurança da sua informação, não diz respeito ao agente, porque eu confio no agente que é uma pessoa, mas a instituição em si perde credibilidade. Recordo-me, por exemplo, há uns anos atrás, 5, 6, 7 anos saiu a lista de todos os homens do SIS ou do SIED, saiu cá para fora com os nomes todos, isto por causa de uns cartões de livre-trânsito que estavam a ser pedidos na Presidência do Conselho de Ministros, isto é uma questão muito grave, tirou uma série de credibilidade. Eu acho que, garantidamente, um ciberataque que possa não só parar as operações ou colocar o funcionamento das operações de uma forma deficiente, obviamente que pode acontecer por outro lado pode criar um problema de credibilidade às instituições.

Acha que a PSP e a GNR são alvos preferenciais para os *hacktivistas*?

São alvos, não do crime organizado, mas destes grupos de desafio, que são estes miúdos. A segurança está nas FS, se eu conseguir fazer algo contra as FS, é um alvo muito apetecido, sem dúvida nenhuma, FS, Governo, todas as instituições que de alguma forma teriam de mostrar credibilidade são alvos apetecíveis, portanto este tipo de criminosos o que fazem é mostrar a um alvo que tem uma exposição muito grande que conseguem, há aqui relacionada uma parte de orgulho e autoestima destes indivíduos.

Apêndice I – Entrevista a Dirigente do SIS

A presente entrevista insere-se no âmbito da dissertação de mestrado para obtenção do grau de mestre no Mestrado integrado em Ciências Policiais, ministrado no Instituto Superior de Ciências Policiais e Segurança Interna (ISCPSI).

O título provisório da dissertação é "O *Hacktivismo*: Uma análise aos ciberataques dirigidos contra as Forças de Segurança", sendo orientador da mesma o Professor Doutor Felipe Pathé Duarte.

Pretende-se com esta dissertação estudar o fenómeno *hacktivistas* em Portugal e, em concreto, analisar os ataques realizados às Forças de Segurança, no sentido de determinar quais são os tipos de ataques efetuados, quais os grupos envolvidos e quais as pretensões destes grupos, de maneira a determinar se o fenómeno constitui ou não uma ameaça para a Segurança.

Local: Academia Militar (polo da Amadora)**,** Lisboa
Data: 27 de março de 2015
Cargo/Posto: Dirigente do Serviço de Informações de Segurança

Guião

1. **Tendo em conta a evolução do *hacktivismo*, considera que atualmente este fenómeno é significativo em Portugal? Porquê?**

Do ponto de vista da avaliação da ameaça é uma ameaça moderada. Neste momento depois da operação da PJ de 26 de fevereiro, a denominada operação caretos, que atingiu aquilo que se julga ser um núcleo central dos agentes desta ameaça conhecidos e pela análise que se faz da pouca adesão a sequelas na sequência dos ataques, em eventos convocados para depois dos ataques, i. e. a adesão que tiveram. Neste momento, a ameaça é moderada pelo potencial da ameaça, mas reduzida pela ação dos grupos atualmente identificados, porque esses foram contidos no âmbito da operação da PJ.

Este é um fenómeno que existe em Portugal sensivelmente a partir de meados de 2011, que se tornou público e que se tornou notório a partir de meados de 2011, teve uma grande expressão pela sua surpresa a partir de novembro e dezembro de 2011. No início de dezembro de 2011 houve mesmo jornais que abriram com uma capa em que falavam em

golpe de estado informático. Nessa altura, provavelmente, estávamos todos pouco preparados para lidar com este tipo de ações. Acho que houve aqui um processo de aprendizagem, hoje globalmente está toda a gente mais preparada.

Eu acho que é um fenómeno que vai sempre ocorrer, vai ter tendência para se manter mais ou menos estável, os grupos vão aparecer, vão desaparecer e os agentes vão mudando, se calhar neste momento estamos eu diria na terceira ou quarta geração depois de 2011, ou seja, já houve duas ou três levas de grupos atuando mais ou menos no mesmo setor, mas que se foram sucedendo uns aos outros, não quer dizer que haja ligação entre eles, portanto essa é uma característica.

Qual foi o motivo que teve por trás do aparecimento do *hacktivismo* em 2011?

Deveu-se a um conjunto de fatores significativos. Primeiro porque era uma ameaça que estava latente, uma ameaça que estava identificada como uma possibilidade pelo menos diria eu desde o ano 2003 ou 2004, identificada como uma ameaça potencial, ainda não estavam criadas as condições para que ela pudesse acontecer. Esta foi a primeira vez em que se conseguiram estruturar grupos, que conseguiram levar a cabo ações com causas próprias, o problema que havia anteriormente é que havia grupos daquilo que eram as dinâmicas dos movimentos sociais e de causas externas à cultura *hacker* que pretendiam mobilizar pessoas com capacidades para as causas que não eram deles. Este foi o momento em que à volta da liberdade de informação, da transparência da informação que são as causas próprias da cultura *hacker*, portanto aqueles princípios elencados por Steven Lévy, no livro, *Hackers: Heroes of the Computer Revolution*, no qual o autor enumera um conjunto de princípios que ele denomina a ética *hacker*, esse conjunto de princípios que são aquilo que norteiam esta subcultura não estavam presentes antes, a emergência dos movimentos como o *Anonymous* que carrega muito esta subcultura, dos movimentos *occupy*, na decorrência disso do *LulzSec* veio fazer emergir este tipo. Claro que pode haver outras coisas que também potenciam isso toda esta ideia dos *winslow blowers*, a Bradley Manning ou se preferirmos a Chelsea Manning, aquele soldado que roubou aqueles ficheiros e depois mudou de nome e transformou-se numa mulher, mais recentemente o caso Snowden, acabam por ser ocorrências do mesmo tipo de movimento que propugna a liberdade de informação, uns prosseguem vias mais físicas de obter os dados, ou seja o Snowden teve de prosseguir uma via física, estar dentro do sistema para sacar os dados, outros fazem-no de uma forma mais remota, mas a cultura que premeia isto é a mesma.

Depois surgiram também outras questões, mas não se pode dizer que tenha sido a crise e a austeridade, porque essas já vinham de antes, mas se nós olharmos para as causas que advinham do mundo físico são precisamente as mesmas causas que entroncam nesta cultura, ou seja a causa da corrupção, da transparência, dos políticos limpos, são o mesmo tipo de causas que são advogadas na ética *hacker*, ou seja os *hackers* encontraram aqui finalmente uma comunhão entre aquilo que são os seus ideias e as causas que derivam dos movimentos e portanto esse é um momento crítico, se calhar noutros países começou mais cedo, se calhar o *Anonymous* vem de 2008, 2009, 2007. Aqui a expressão foi nessa altura.

Mas acha que existe uma relação entre ativistas e *hacktivistas*?

Dito com essa generalização não. Se é altamente provável que haja uma comunhão entre os mascarados dos *Anonymous* e os que advogam ser *Anonymous* neste mundo do *online*, neste mundo do *hacktivismo*, sim. Se nós podemos dizer que a generalidade dos movimentos sociais que contestam têm existência no mundo do *hacktivismo* não.

Então o *hacktivismo* não é uma evolução do ativismo tradicional?

Não é uma evolução do ativismo tradicional. Há aliás uma tese muito interessante de uma senhora chamada Alaxandra Samuel, uma tese de Harvard, que explica bem qual a diferença entre os movimentos sociais clássicos e os movimentos sociais *hacktivistas*, portanto não há uma evolução. Os movimentos sociais desejavam isso, ou seja, sempre desejaram ter uns piratas para fazer umas coisas, mas os piratas nunca se deixaram ir nas causas dos movimentos sociais, os piratas vão nas suas próprias causas, nas causas que acham que entroncam nas suas próprias causas, pode é haver uma coincidência, o que se passou em 2011 foi haver essa coincidência, mas nem eles se misturam muito, se olharmos para aquilo que são as plataformas que houve, por exemplo, nas acampadas em Espanha, nós não costumamos encontrar pessoas dos *Anonymous*, mas nas grandes manifestações de massas sim, mas quando olhamos para as plataformas organizadores não. Eles não fazem parte dos novos movimentos sociais, eles têm uma coisa própria deles.

2. Considera o *hacktivismo* uma ameaça à Segurança? Porquê?

Sim é uma ameaça à segurança interna. Depois é uma questão de graduação do dano, mas isso depende das capacidades.

Quais são as capacidades?

Depende das capacidades que tenham do ponto de vista técnico de cada um. O que temos encontrado são capacidades globais baixas, por vezes há uma ou outra pessoa que, em cada momento, tem um papel mais relevante, a perceção e o impacto da ameaça é claramente superior à efetiva capacidade que eles têm, porque como é uma matéria que é impossível de explicar em meia dúzia de carateres de jornais é muito fácil dizer "foi um grande ciberataque" ou "há ciberataques por todo lado". Cria uma falsa noção de comprometimento de sistemas por parte das pessoas e as pessoas não têm noção graduação da escala de dano, ficam sempre com a ideia de que está tudo a saque, portanto é uma coisa que é muito técnica e há a exploração de vulnerabilidades que são muito básicas no sistema, se isso é um grande feito do ponto de vista *hacking* não é, as vulnerabilidades é que estão muito presentes. Outra coisa, que acontece com muita frequência, é que, reiteradamente, são os mesmos *site*s que são atacados várias vezes e há vários exemplos disso, há um conjunto de *site*s que são uns 10 ou 15 que estão constantemente a ser atacados porque vai-se lá, concerta-se e repõe-se a situação que os *site*s tinham e não se resolve o problema da segurança, eles voltam a ter as mesmas vulnerabilidades, limpa-se a imagem, limpa-se o texto que foi comprometido e repõe-se o *site* tal como ele estava e o comprometimento continua lá, voltam a usá-lo a ser divulgado o ataque e isso é uma coisa que temos visto com grande recorrência.

Poucas ferramentas, muitas ferramentas feitas de downloads feitos, pouca capacidade de utilizar ferramentas em cadeia para coisas inovadoras, de vez em quando há um ou outro indivíduo que se destacam por terem mais talento e por conseguirem fazer coisas novas de uma maneira geral estamos ao nível daqueles *Script Kiddie* que conhecem uma ou duas ferramentas e exploram o que essas ferramentas podem fazer.

3. Considera que Portugal está devidamente protegido contra os ciberataques?

Eu acho que há muito trabalho a fazer do ponto de vista das vulnerabilidades, há muito trabalho a fazer do ponto de vista da cibersegurança, é preciso criar um corpo de profissionais de cibersegurança, é preciso que a cibersegurança faça parte dos próprios sistemas, eu acho que há muito trabalho a fazer. Se do ponto de vista da investigação criminal, do conhecimento das coisas, dos serviços informações, no que diz respeito ao *hacktivismo,* já ficou provado que se consegue dar resposta, se estamos a falar de outro tipo de ciberataques com outros atores, profissionais e sofisticados, ainda temos muita

capacidade para construir. Quando falamos em ciberataques o leque é muito muito grande, nos atores Estado é muito complicado, nos atores *black hats hackers*, profissionais, pessoas que sabem o que estão a fazer é muito complicado termos capacidade, se há meio em que há uma ameaça muito assimétrica, em que a quantidade de investimento que é preciso fazer para fazer frente ao ataque é completamente irrisório face à quantidade de investimento que é preciso fazer para a segurança porque uma pessoa bem formada que saiba, com *skills*, com computador portátil e poucos recursos económicos consegue produzir um grande efeito e para responder a esse efeito é preciso fazer um investimento desproporcional em segurança. E, portanto, é pior do que atacar as Torres Gémeas com X-atos nos aviões, portanto quando nos pensamos no 11 de setembro, foi feito com o quê? Com x-atos e, portanto, isso é o cúmulo da sofisticação é usar poucos meios com um efeito muito grande. Com X-atos é muito mais sofisticado do que usar uma bomba. E este é o problema das ciberameaças, é que se utilizam meios baratos, acessíveis a qualquer um e o que é preciso é ter um elevado conhecimento. E com meios baratos e acessíveis a qualquer um indivíduo dotado de elevado conhecimento rapidamente consegue mobilizar as ferramentas que precisa na *Internet* ou construi-las ele próprio se tiver capacidade para isso e o investimento que temos de fazer em investigação criminal, recolha de prova, cooperação internacional é claramente desproporcional ao dano que um único indivíduo pode causar.

4. Quais as possíveis consequências de um ataque *hacktivistas*?

Até agora as consequências têm sido relativamente baixas. Quando estamos no domínio da negação de serviço, dos DDoS, o que nos temos é um dano reputacional, ou seja, as instituições que são atingidas sofrem o dano reputacional de terem os seus *site*s atingidos, apesar de não comprometerem. Por exemplo deitarem o *site* do Governo a baixo não provoca dano nenhum porque passados poucos minutos a informação volta a estar toda no ar conforme estava, não foi nada roubado, o que causa é dano reputacional por o Governo não ter tido o *site* no ar e cria uma falsa sensação de insegurança porque para quem está a ler isto e diz que o *site* foi deitado a baixo… na maior parte dos casos os *websites* são posters, isto significa que a informação que neles esta contida é informação pública, que podia ser afixada num edital numa cidade, é comunicável ao público, é informação que as pessoas consomem igual a um poster, não há sistemas suportados, na maior parte dos casos não há sistemas suportados nos *site*s que têm sido atacados. Esse é o

problema, por exemplo, da negação de serviço passa-se mais com o portal social da PSP. Quando começam ataques esse, por exemplo, é desligado ao tráfego internacional para prevenir alguma coisa, outra coisa tem a ver com os SQL *Injection* e com os *servers*, em que na realidade são efeitos que só se produzem do lado do cliente, eles capturam uma imagem a dizer que aquilo aconteceu, mas nunca ninguém teve acesso aquilo, portanto, é quase uma fabricação. Nos *defacements* com acesso ao servidor, eles precisam de ir lá colocar um ficheiro e substituir um ficheiro, aí depende do tipo de informação que as informações, tenham ou não o cuidado de guardar nos servidores que suportam os sistemas web. Portanto, aí se tudo correr bem e se o servidor servir só para afixar o *poster* isso é um problema. Outra coisa diferente são os SQL *Injection*, nomeadamente, em sistemas que tenham *login's* de utilizadores e *passwords* mal protegidos e que possam conter outro tipo de informações, que foi o que aconteceu no caso da PGR, não era propriamente um *site*, mas um sistema, em que eles tiveram acesso e aí sim informação é comprometida. Muita da informação que é comprometida e que é levada ao público em muitos casos essa informação não resulta do comprometimento remoto através de rede, eu lembro-me por exemplo de ter sido publicado dois casos diferentes ambos envolvendo a PSP: um foi uma lista completa do dispositivo da Esquadra de Chelas, isto foi em 2011, isso aí claramente que teve de vir de um computador que foi para arranjar ou não foi comprometido sistema nenhum, alguém passou aquela informação aos indivíduos que estavam a fazer o ataque. Outra coisa foi o sindicato das carreiras de chefe em que esse foi particularmente grave por violação de direitos fundamentais e de liberdade de expressão e de direitos sindicais em que foi um problema de higiene informática, quem administrava aquele *site,* periodicamente devia ir limpar a base de dados que suportava o formulário em que as pessoas deixavam até queixas contra as chefias, esse caso foi particularmente grave, aí sim foi por SQL *Injection* e por se ter conseguido ter acesso aos campos da base de dados que suportava aqueles formulários. Se periodicamente tivessem ido lá limpar não tinha acontecido. Estes são os tipos de vulnerabilidades que vão acontecendo, são graves, em alguns casos muito graves e nas situações mais graves, concretamente, a divulgação de dados de procuradores do MP, no dia 25 de abril de 2013, essa foi a situação em que se agiu do ponto de vista da investigação criminal de forma mais decisiva, não por acaso, porque essa foi particularmente grave e era um sistema único em que era mais fácil obter prova e onde houve a decisão mais rápida, não era um mero DDoS, não era só aquela coisa

de se juntar 50 pessoas para se mandar a baixo. Também temos de analisar isto consoante a escala de dano e os ataques são todos diferentes.

5. Como se caracterizam, organizam e o que pretendem os grupos de *hacktivistas* (traçar perfil)?

Eles comunicam através do mundo virtual organizam se em volta desses meios de comunicação, são muito poucas pessoas, nem sempre se conhecem no espaço real, se bem que isso é uma coisa que sempre chamos que acontecia, não são todos, alguns conhecem-se no mundo real. A base de cada um dos grupos, porque há muitos grupos *Hackers Streets*, *Anonymous*, *Anonymous* Margem Sul, os *sud0h4ck3rs*, enfim cada grupo tem na base sempre pessoas que se conhecem entre si, outras conhecem-se do mundo *online* vão comunicando nos seus sítios de comunicação próprio primeiro no IRC's, depois passaram muito por alguns servidores de comunicação de jogos, os *team speakers*, mas eles também não são particularmente bons em encriptação, por exemplo, em construir coisas próprias, é assim tudo muito juvenil, vão combinando operações, vão combinando alvos, vão combinando coisas que querem executar e fazer.

Como é que se caracterizam? Tipicamente estamos a falar de jovens, bastante jovens, eu diria entre os 16 e os 22 ou 23 anos, às vezes um ou outro pode ser mais velho mas quando é mais velho é mais próximo dos 40 aos, há um *gap* muito grande, a base dos grupos são muito jovens e daí as varias gerações, porque as pessoas perdem o interesse, é muito impulsivo e muito à volta disto, as pessoas que têm sito identificadas tem mais ou menos este perfil.

No que diz respeito ao perfil individual, o que temos reparado, com a exceção de um único caso, estamos sempre a falar de jovens provindos de lares muito desestruturados, com graves problemas de socialização e graves problemas de desempenho escolar, não é que não sejam muito inteligentes, a maior parte deles são, mas os graves problemas de socialização e isso leva a um mau desempenho escolar, graves problemas, ao nível da prostituição, do próprio agregado, seja prostituição violência doméstica, divórcios, outra situação que leva ao desenraizamento, há de tudo, há casos de tutela por parte de avós, indivíduos que estão mesmo em regime de tutela de menores, há muitas situações de desenraizamento que são, por exemplo, indivíduos que nasceram no estrangeiro e que vieram ainda jovens do estrangeiro para Portugal mas não se conseguiram adaptar desde logo na escola. Não se conseguiram adaptar no ambiente familiar, ou que nasceram em

Portugal foram com os pais ainda jovens com a experiência de emigração que correu mal, os pais voltaram e eles não conseguem adaptar-se, enfim depois também o ambiente familiar joga e não se conseguem adaptar ao ambiente escolar, portanto há situações sociais muito complicadas. Nisto aqui, enfim quando digo com a exceção de um único caso é que há uma situação que não é nada assim. Mas este não é o paradigma, o paradigma é sempre ou nascido na Suíça, na França, nos EUA em África do Sul e depois vieram para cá porque os pais tiveram na Suíça, no Benlux. Tem tudo influência disto.

O que pretendem é um sentido de realização, ou seja, realizarem-se, conseguirem ser bons a fazer alguma coisa e demonstrarem um bocadinho que são capazes de fazer certas coisas, junto de amigos ou assim. É mais a questão do desafio do que do protesto político porque em entrevistas com eles na maior parte dos casos eles não têm muito bem a noção do que fazem.

Há muitas vezes a reação de verem uma coisa no jornal, por exemplo, reações contra a PSP, tipicamente, é divulgada nos meios sociais, e auto incentivam se a atacar a PSP, não há ali verdadeiramente […] são jovens com falhas graves de cultura geral e noções de cidadania, mas não quer dizer que não existam lá pessoas adultas com grande noção do que estão a fazer mas que têm outro papel, têm um papel mais de comunicações, de fazer os comunicados, comunicar para fora, pensar por eles, dar entrevistas. As pessoas que lideram e organizam esses ataques são mais os adultos não especializados em coisas técnicas, são especializados em escrever comunicados. Muitas vezes eles julgam que na maior parte dos casos aqueles que têm mesmo competências técnicas muito especializadas não têm noção que eles são dos mais competentes e especializados no grupo, pensam que são pessoas que sabem pouco e que estão só a ajudar outros que sabem mais.

6. Considera que as Forças de Segurança (PSP e GNR) são um alvo potencial para grupos *hacktivistas*?

Têm sido sempre um alvo em reação a eventos do mundo real, todas as entidades são sempre alvo em função de acontecimentos do mundo real. Por exemplo, a PGR foi alvo porque apareceu uma série de artigos a dizer que a Procuradoria não investigava a corrupção, a PSP foi e é alvo quando existem situações de ordem pública em que existem indivíduos que se queixam da forma como a PSP exerceu as suas funções de ordem pública, a GNR, por exemplo, raramente é visada porque a maior parte desses eventos não acontecem na área da GNR. Por exemplo, o SIS é visado quando aparece no jornal que o SIS foi falar e já identificou não sei quantos e aí sim eles atacam. É basicamente por coisas

que são reportadas na imprensa, não quer dizer que aconteçam, mas são reportadas, ou que há uma determinada ou é construída uma determinada perceção na imprensa ou nas redes sociais que é uma coisa que é mais imediata.

7. Poderá um ataque informático contra as infraestruturas das Forças de Segurança afetar a sua missão? Em que sentido?

No contexto do *hacktivismo* até agora não me parece. Poderá um ataque informático afetar as infraestruturas das FS, sim. Um ataque *hacktivista*, o tipo de *hacktivismo* que temos, dirigido contra as infraestruturas das FS, pode afetar? Não me parece, porque tem uma escala baixa e uma intensidade baixa, mas um ataque informático dirigido conduzido por profissionais pode. Depende sempre do que estivermos a falar, por exemplo, o sistema estratégico de informação. Aí sim, porque a dependência hoje em dia desse tipo de ferramenta é muito elevada.

Acha que esse sistema pode ser afetado?

Não conheço a infraestrutura de suporte do SEI para dizer, mas sim, se eles soubessem que uma coisa dessas existia e se soubessem como detetá-la e encontrá-la, mas eles não têm bem a noção disso. Agora um ator profissional que o queira fazer, já é mais complicado.

Apêndice J – Tabela de notícias analisadas

Pesquisa pela palavra "*hacktivismo*"

Data	Meio	Nome	Autor	Título	Observações
12/12 /2010	Imprensa	Correio da Manhã	Paulo Querido	*Hacktivismo* e Mudança	- Referência ao caso Assange e *Wikileaks*.
29/06 /2013	Imprensa	Expresso	Micael Pereira	*Hacktivistas* uma nova casta de heróis	- Grupos: *Anonymous*, *LulzSec* e *Anonymous* Squad nº666 - Caso de Assange e *Wikileaks*; - Referência a Rui Cruz e ao *site Tugaleaks*: "o fenómeno *hacktivismo* fez-se notar mais «a partir de 2011, quando os *LulzSec* Portugal invadiram quase todos os sistemas a que se propuseram» e «divulgaram inclusive dados de agentes da PSP de Chelas»"; *Anonymous Squad* nº666: "lançou uma lista de *site*s de câmaras municipais e do Governo como alvos para ataques XSS, o Cross-*site scripting*, uma técnica que permite roubar informação colocada num *site* por utilizadores e assim ter acesso às bases de dados associadas ao *site*"; A forma mais popular de *hacktivismo* são os DDoS; - Referência à Primavera Árabe; Caso Snowden.
02/07 /2014	*Internet*	Computer World.pt	João Nóbrega	"*Hacktivismo*" é preocupação (…) CEGER	- Referência ao atraso de Portugal no âmbito da cibersegurança; A contestação social manifestada através de ciberataques, ou «*hacktivismo*», é uma das principais preocupações do EGER
03/12 /2014	Imprensa	Diário de notícias	Rute Coelho	*Hackers*: os ativistas que obrigam a PJ a vigiar os *site*s do Estado	- Grupos: *Anonymous* e *SUDOH4KERS*; Perfil *hacktivista*: entre 20 e 40 anos; craques de computadores ou não, engenheiros, informáticos, gestores de sistemas; "já acederam a dados reservados de magistrados do Ministério Público, a dados confidenciais de polícias, a páginas do Estado que deveriam ser invioláveis. Publicaram nesses *site*s propaganda e símbolos de luta social"; - Associados a datas históricas importantes como o 25 de abril ou o 1 de maio, ou escândalos como o BPN ou BES.; - Operações: operação "Novo Sangue" traduziu-se num ataque ao Banco de Portugal e ao Novo Banco (puseram a descoberto 200 *emails* com contactos das duas instituições para que os cidadãos pudessem reclamar contra a intervenção do Estado no BES"; - *SUDOH4KERS*: a sua motivação é a "defesa da ideia global de liberdade de expressão"; "forma de nos insurgirmos contra a corrupção governamental e corporativa e [de lutarmos] pela defesa dos direitos humanos e dos animais"; - "O nosso grupo ter deitado a baixo uma rede inteira de escolas (…) a invasão ao *site* da Procuradoria-Geral da República (…) operações *Megaupload* (…) operações contra o regime egípcio, contra a Síria ou Israel, e do envolvimento de toda a comunidade *Anonymous* na Primavera Árabe"; "o *hacktivismo* nada mais é do que uma forma de protestar. É defender o acesso à informação como um direito fundamental"
01/02 /2015	Imprensa	ITChannel	Sónia Gomes da Silva	Segurança: Um novo paradigma	- Casos de espionagem: *Symantec* (descobriu a existência de ataques contra governos europeus através do *Regin* (um *software* malicioso que tem espiado indivíduos, governos, investigadores, empresas, telecomunicações e infraestruturas); - Conflito entre Rússia e Ucrânia, como gerador de ciberataques; Ataques de *malware* sofisticado denominado *Heartbleed* contra sistemas de controlo de centenas de empresas de energia na Europa e nos EUA (comprometeu *websites*, lojas *online*, aplicações de segurança, etc.); Caso de uma cadeia hospitalar dos EUA que anunciaram roubo de 4,5 milhões de dados clínicos de pacientes;

					- Ataques a JP Morgan, eBay, Sony Pictures (paralisada durante uma semana), entre outras provocaram as seguintes consequências: colocaram em causa a reputação e geraram prejuízos de elevada gravidade; - "O grupo *Anonymous* reivindicou uma série de ataques contra *site*s de organismos públicos – divulgando nomes e números de telemóveis dos procuradores públicos – e de entidades privadas – EDP, BES, Barclays e Banif"; - "Tal como nos telemóveis, os problemas advêm do *spyware* e esse reside nas aplicações e não das redes de telecomunicações"; - Aplicações desenvolvidas na saúde, em meios hospitalares e na vida rodoviária, onde os *hackers* podem ser um problema.
26/02 /2015	*Internet*	Computer World.pt	Pedro Fonseca	Sete detidos, 14 arguidos e 24 buscas em operação C4R3T05	- O MP deteve sete pessoas no âmbito da chamada operação "C4R3T05" (Caretos), pela PJ no dia 26 de fevereiro, para a investigação de diversos ataques informáticos; constituídos 14 arguidos; efetuadas 24 buscas domiciliárias investigação visa ataques informáticos a servidores dos *site*s do Ministério Público, da PJ, do Conselho Superior da Magistratura, da EDP e da Comissão da Carteira Profissional de Jornalista, estando em causa crimes de acesso ilegítimo, de dano informático, de sabotagem informática e de associação criminosa; - Os ciberataques têm "um efeito erosivo sobre a confiança dos cidadãos nas estruturas nacionais da rede *Internet*, prejudicando a sua credibilidade, nível de segurança e funcionamento regular, bem como comprometendo uma maior e mais segura adesão aos serviços nas redes de informação, processamento e comunicação". - Nas sete pessoas (um autor de sexo feminino) em detenção, com idades entre os 17 e os 40 anos e das regiões de Lisboa e Porto; - "Entre as entidades atacadas por elementos do grupo encontram-se o Serviço de Informações e Segurança, Procuradoria-Geral Distrital de Lisboa, PSP, GNR, vários ministérios, quase todos os bancos e, até, o Patriarcado de Lisboa".
26/02 /2015	*Internet*	Económico *Online*	Lígia Simões	Autor do *site TugaLeaks* é um dos sete detidos em operação contra crime informático	- Sobre a operação "C4R3T05" (Caretos) da PJ; Referência a Rui Cruz; O ataque em 3 de Fevereiro, à CCPJ "poderá ter permitido a visualização e eventual cópia/reprodução de documentos digitalizados" na sua plataforma informática. A notícia deste ataque tinha sido divulgada no mesmo dia pelo *site Tugaleaks*, que atribuiu a sua autoria ao coletivo de *hackers Anonymous* Portugal. - Na sequência deste ataque "vários *emails* e *passwords* de juízes e jornalistas" teriam sido já divulgados - Presumíveis autores, um deles de sexo feminino, têm idades compreendidas entre os 17 e os 40 anos de idade, vivem nas áreas metropolitanas de Lisboa e Porto; Os ataques mais graves culminaram na divulgação de dois ficheiros com dados de agentes da polícia. Um dos ficheiros, retirado de computadores governamentais, divulgou o posto, *email*, nome e número de telefone de 107 agentes da PSP. O outro, retirado dos computadores de um sindicato, continha informação de 67 polícias, em muitos casos incluindo a morada. A ação foi apresentada como uma represália pelos incidentes entre manifestantes e polícia, em S. Bento, na greve geral de 24 de Novembro.

Pesquisa pela palavra "*hacker*"

Data	Meio	Nome	Autor	Título	Observações
30/11 /2010	Imprensa	Diário de Notícias	Lumena Raposo	Os segredos diplomáticos que estão a fragilizar os EUA	Caso *Wikileaks* de Julian Assange;
25/02 /2011	Imprensa	Diário de Notícias	Helena Tecedeiro	Assange recebe extradição sem pestanejar e recorre	Caso *Wikileaks*.
30/11 /2011	Imprensa	O Primeiro de Janeiro	S/A	Ataque informático amanhã	- Ataque ao *site* do Sindicato Nacional da Carreira de Chefes da PSP; O grupo de piratas informáticos *LulzSec* Portugal divulgou no dia 26 de novembro dados pessoais e confidenciais de pelo menos 107 elementos da PSP de três esquadras (14.ª, 16.ª e 38.ª) da zona de Chelas, em Lisboa; - A *LulzSec* justificou no *Twitter* que a ação foi uma "resposta aos ataques de mais de 50 'agentes provocadores' infiltrados na manifestação [do dia 24]". A lista contém postos, patentes, telefones e endereços eletrónicos. Este grupo já foi protagonista de outros ataques, nos últimos meses, aos *site*s do MAI, PSP, SIS, PDS, CDS, PS, parlamento, RTP, Sapo e Portal das Finanças; - O *LulzSec* Portugal afirma que vai juntar-se ao *Anonymous* Portugal para dar início à operação *#AntiSecPT*, inspirada numa ideia igual a nível internacional. O principal motivo da operação é os incidentes com a polícia ocorridos durante o dia da greve geral.
06/12 /2011	Imprensa	O diabo	João Filipe Pereira	SIS e PJ no encalço dos piratas da net	- O grupo *LulzSec* já conseguiu aceder a *emails* e palavras-chave de membros de partidos políticos e fizeram publicar uma lista de nomes de agentes da PSP com os seus contactos; - O último ataque (com mais de 100 elementos) deveu-se à detenção de um elemento estrangeiro "por agentes à paisana durante a greve geral"; - Têm como objetivo "lutar contra a corrupção, o grupo de atacantes anónimos tem alargado a sua acção tendo mesmo participado nas várias manifestações que se têm realizado no País"; Querem "acabar com este sistema onde os pobres são cada vez mais pobres" Alguns membros do *LulzSec* encontram-se indignados com a atuação política dos governantes portugueses e os ataques são a forma de demonstrar o seu desagrado. Não dão a cara devido às consequências com a polícia e porque querem continuar a ser um grupo de anónimos, sem líder ou representante. - Segundo os mesmos as ações irão continuar, sendo cada uma delas "pensada e debatida nos fóruns do grupo" Nestes fóruns é ensinada a forma de realizar ataques. A grande maioria dos piratas não se conhece e querem que continue assim; Grande parte dos mesmos concentra-se na Grande Lisboa.
08/12 /2011	*Internet*	Jornal de Notícias *online*	Daniela Espírito Santo e Manuel Molinos	Ataques de piratas decididos numa sala de *chat*	- Temas como o capitalismo, a corrupção e a falência da democracia são debatidos por *hacktivistas*; "partilham-se "armas" para usar contra *websites* vulneráveis. (…) há tempo para dar aulas de segurança e ataque aos "*newbies*" (mais novos)"; A sala de *chat* dos *AntiSecPT*, que têm reclamado vários ataques, encontra-se no IRC; Referência a um ataque para o dia seguinte: "pretendem deixar uma mensagem a quem governa: o povo tem voz e quer revolução"; - Ex-*hacker* e consultor de segurança acredita, que o grupo é «demasiado descentralizado. Na essência,

					não há grupo, mas sim uma ideia, um conceito. Nada mais»"; O mesmo considera improvável que os ataques tenham ligação internacional, mas os "ideais de base parecem ser os mesmos e resultam de "muita desinformação"; Referência ao capitalismo, como motivo para realização de ataques; "Estes jovens estão a tentar fazer algo popular. No fundo, as pessoas gostam de aparecer nas revistas e na TV e a carreira de ativista é bastante aliciante" para o mesmo estes grupos não têm filiação política ou pouco percebem do assunto; Ricardo Lafuente acredita que a "postura politicamente activa" dos ataques tem paralelo com o que sucede no estrangeiro. Considera que é errado encarar este grupo como "*white hat*" ou "*black hats*" pois o método usado nos ataques escapa a tal distinção. "O objectivo é político e propagandista", servindo os ataques para enviar uma "mensagem de crítica e denúncia da actual situação política e económica em Portugal. A "forte motivação ideológica demonstrada nas mensagens" descarta, para Lafuente, "a hipótese de isto ser um passatempo". - O *AntiSecPT*, "entopem" um *site* até o tornarem inoperacional, invadindo as páginas e deixando mensagens; "Existem inúmeras ferramentas *online*, bem como tutoriais disponíveis no *Youtube* e páginas que explicam o que fazer". Parecem ser autodidatas, mas trabalhar (ou estudar) em áreas relacionadas com programação. São maioritariamente novos, mas parece haver gente de idades variadas; - Surgiu no dia 5 de dezembro de 2012 um novo movimento, o Lusitânia *Leaks* (ou *Luzleaks*) que reivindicou um ataque à página do Ministério da Economia; "Segundo os *Luzleaks*, o objectivo não é ganhar fama (não querem "magoar ninguém") mas sim dar a conhecer «as raízes da corrupção do nosso país»"; As páginas da PGR e de uma associação da PSP foram os ataques que mais provocaram preocupações, uma vez que foram retirados documentos confidenciais. Foram alvo de ataques os ministérios da Economia, da Educação, o PS, o PSD, o Banco de Portugal, SIS, Finanças e *Freeport* entre outros; O movimento *AntiSecPT* continua a apelar ao ataque em massa do dia seguinte. Os responsáveis da operação apelaram a que sejam guardados mais documentos pirateados para divulgação nestes dias.
05/12/2012	*Internet*	Computer World.pt	Pedro Fonseca	Mais de 1250 *site*s portugueses vandalizados desde Março	- "Entre 6 de Março e 3 de Dezembro, mais de 1250 *site*s registados no domínio .pt foram vandalizados, com modificações não autorizadas efectuadas nas páginas Web (também conhecida por "*defacement*")"; - "No caso do pseudónimo "gr0un" constam, desde 5 de Novembro, os "*defacement*s" aos Governos Civil de Santarém e Coimbra, Provedor de Justiça, Águas de Portugal, câmaras municipal de Caminha e Serpa, Sindicato Nacional da Carreira de Chefes da PSP, PSD de Setúbal e de Lisboa e ainda o *site* do Freeport"; "Em nome de "c0ldc0d3r", foram registados ataques ao Sindicato Independente dos Agentes de Polícia, Escola Superior de Saúde do Instituto Politécnico de Viseu, Iniciativa para a Infância e Adolescência (do Ministério da Solidariedade e Segurança Social) e ainda a Junta de Freguesia do Telhado, no Fundão. Um terceiro elemento, "sl0wb", não tem quaisquer registos em seu nome"; Nenhum deles faz parte do "Top 25" dos autores de "*defacement*s" a *site*s nacionais registado no *Zone-H*.
12/02/2013	*Internet*	*TugaLeaks Online*	S/A	Ataque aos Hospitais da Universidade de Coimbra remete utilizadores para (…)	- Ataque realizado aos HUC, pode estar com: "Aumentos na saúde As taxas moderadoras aumentaram em 2013 bem como aumentaram os cortes que o OE 2013 e o Governo fazem na saúde."

29/03 /2013	Imprensa	Correio dos Açores	S/A	Relatório alerta para potencial crescimento (…)	Sobre RASI 2013
04/05 /2013	Imprensa	Expresso	S/A ver *email*	IRS e IVA usam tecnologia insegura	Vulnerabilidades do sistema Java, utilizado pelo IRS e IVA; Recomendação do CERT.PT para não utilizar o mesmo.
20/06 /2013	Imprensa	O crime	R.C.	*Hacker* canadiano apanhado com imagens de pedofilia	Ryan Cleary, um *hacker* de 21 anos, membro do grupo internacional *LulzSec* foi preso por ter sido encontrado com imagens pedófilas dentro do seu computador;
25/06 /2013	*Internet*	*TugaLeaks Online*	S/A	*Hacker* "Barack_11" ataca 22 *site*s Portugueses e coloca dados no Pastebin	"sncc-psp.com: o Sindicato Nacional da Carreira de Chefes da PSP tem *user* e *passwords online* mas também IP's, sendo fácil descobrir um IP da PSP pertencente ao Ministério da Administração Interna"
29/06 /2013	Imprensa	Expresso	Micael Pereira	*Hacktivistas* uma nova casta de heróis	Já descrito na pesquisa feita para a palavra *hacktivismo*
01/07 /2013	Imprensa	Exame infromát.	S/A	*Site* do cidadão vence *password* dourada 2013	"Depois do ataque ao *site* do Cartão do Cidadão, o *hacker hack_addicted.pt* revelou *passwords* de altas patentes do Estado": Pedro Passos Coelho, Paulo Portas e José Seguro.
12/07 /2013	Imprensa	Sol	Sónia Graça	Burlas com cartões disparam	"As fraudes com cartões de crédito estão a aumentar a olhos vistos"; "Os *site*s da China, por exemplo, requerem mais cuidado"
18/07 /2013	Imprensa	People Ware *Online*	S/A	Como manter o Mac seguro do *Malware*	- "O *malware* tem adquirido os mais variados figurinos, com o objectivo de atrair as vítimas e apoderar-se dos seus dispositivos. As "técnicas tradicionais" mais conhecidas já não funcionam, pois as defesas criadas pelas empresas de segurança, os antivírus e *anti-spyware*, conseguem detectar e prevenir tais ataques de uma forma eficaz. Nesse sentido, damos conta que os ataques estão agora mais refinados, assentando em técnicas de engenharia social, criando assim uma proximidade/intimidade com o utilizador". - O *Ransomware* é uma ameaça informática tem vindo a ser uma prática muito comum. O *Ransomware*, também considerado com "sequestradores digitais", são *trojans* que, após invadirem as máquinas, impedem o acesso a várias funcionalidades e até a informação. Para voltar a aceder a esses conteúdos, o atacante pede ao utilizador um valor monetário para que este volte a "resgatar" a informação. "Em Portugal, este tipo de *malware* emitia um aviso/ultimato, em nome (supostamente) da PSP, como, caso não seja feito um pagamento. Em Portugal foram muitas as pessoas que cederam e acabaram por pagar tal "resgate". Dinheiro que vai para o *hacker* que desenvolveu este "mecanismo" de engenharia social não presencial.
18/07 /2013	*Internet*	Sol *online*	Catarina Guerreiro	Burlas com cartões de crédito disparam	Sobre burlas com catões de crédito.
20/07 /2013	*Internet*	FX Tech *Online*	S/A	*Ransomware*: quando os *hackers* encriptam o disco e "raptam" o PC	- "*Malware*, *Phishing*, *Rootkits* e *Trojans* estão entre os ciberataques mais conhecidos. Contudo, há um tipo de ameaça que tem vindo a ganhar mais protagonismo: o *Ransomware*." - Em Portugal, a ameaça surgiu em nome da PSP, o que forçou as próprias autoridades a publicarem no seu *site* oficial um alerta aos cidadãos para não caírem na armadilha. A PSP dava, inclusive, instruções de como desbloquear o computador".

01/08/2013	Imprensa	PCGuia	Márcia Campana, Gustavo Dias e Ricardo Durano	Guerra Digital	- Fugas de informação em destaque devido ao caso *Wikileaks* e Edward Snowden. - "Mais recentemente assistimos às revelações de Snowden, que veio colocar em causa o programa PRISM"; Um relatório dos EUA aponta os *hackers* chineses como "os mais activos e persistentes do mundo da espionagem económica"; - Referência ao *Stuxnet*: um "vírus informático descoberto em 2010 que detém a capacidade de atacar alvos selecionados com a precisão de um míssil telecomandado", "acredita-se que terá surgido de uma parceria entre norte-americanos e israelitas", "O *Stuxnet* espalha-se pela rede como um vírus qualquer". Quando algum computador infectado entra em contacto com o alvo do *Stuxnet* através de uma rede, o vírus entra em acção", "Assumiu o controlo das válvulas que regulam a entrada de urânio na central nuclear de Natanz no Irão. O *Stuxnet* conseguiu atrasar o programa nuclear iraniano em pelo menos dois anos", "O *Stuxnet* é capaz de reprogramar *softwares* baseandos no padrão Scala. Um ataque bem-sucedido pode parar uma fábrica, uma central nuclear ou uma rede de energia. Também é possível utilizar o *Stuxnet* para causar acidentes, como explodir uma unidade de processamento de urânio."
08/08/2013	Imprensa	O Crime	Rui Cruz	'*Hackers*' lançam ofensiva em Portugal	- Várias instituições portuguesas, incluindo a PSP e PJ tiveram "os endereços de *email*, profissionais e pessoais, de vários responsáveis plasmados em todo o mundo" - "Os responsáveis por este ataque são subgrupos de *hackers* que pertencem ao grupo '*Anonymous*'" - "A marca registada destes piratas informáticos é a máscara do personagem 'V de Vingança' criada por Guy Fawkes", "Afirmam lutar por Portugal através da *Internet*, expondo dados e alterando *websites*" - Há grupos organizados na rede social *Facebook*, que ensinam a fazer ciberataques, fornecendo dicas de programação para utilizadores experimentados na área informática; - "Comum a todos os ataques foi a colocação '*online*' da imagem do grupo de *hackers Team Whit3* Portugal'". De acordo com um *hacker*: "o Estado 'nunca estará seguro' às mãos dos piratas informáticos. 'Por muitas ferramentas que usem, o elo mais fraco é sempre o factor humano"
09/08/2013	Imprensa	Sol	Margarida Davim	*Hackers*: à caça dos pedófilos na *internet*	Comunidade de *hackers* pertencentes ao grupo *Anonymous* Portugal supervisionam fóruns e redes sociais para encontrar pedófilos.
15/08/2013	Imprensa	O crime	S/A	Açorianos sequestram em estação de rádio	Caso de dois sequestradores de uma rádio, ameaçaram-no com uma arma de *paintball* para que passasse uma mensagem de cariz político. Os sequestradores identificaram-se como pertencentes ao grupo *Anonymous*.
01/09/2013	Imprensa	ITChannel	S/A	"Sequestro" de PC's está a aumentar	*Ransomware* – tipo de *software* malicioso que os cibercriminosos usam para obter dinheiro das vítimas depois de encriptarem os dados do disco rígido do computador e bloquearem o acesso do proprietário ao sistema. Este tipo de *malware* é cada vez mais popular em todo o mundo. "Em Portugal a ameaça surgiu em nome da Polícia de Segurança Pública, o que forçou as próprias autoridades a publicarem no seu *site* oficial um alerta aos cidadãos para não caírem na armadilha"
12/09/2013	Imprensa	O Mirante		Pré-campanha agitada em Ourém	Telemóvel de candidato clonado para envio de mensagens ameaçadoras. As mensagens estavam assinadas por *Hacker* JSD.

26/11 /2013	Imprensa	Público		Ana Gomes e mais cinco deputados europeus vítimas de pirataria informática	- Ataque informático ao Parlamento Europeu. - "O pirata não é identificado, teve acesso a 'dezenas de milhares de *emails*, documentos confidenciais, cadernos de endereços, agendas, correspondências profissionais mas também privadas. "Segundo o Mediapart, a intenção do *hacker* – qualificada por este de 'natureza política' – foi provar a fragilidade do sistema informático do PE." - "O pirata terá contado ao Mediapart que a devassa das 13 caixas de *email* foi uma 'brincadeira de crianças' para a qual apenas precisou de um computador 'de gama baixa' com acesso sem fios à *internet* (*wifi*) mais 'alguns conhecimentos que toda a gente pode encontrar na *internet*'
06/12 /2013	Imprensa	Jornal de Santo T	Mário Ferreira	Do passado… do presente. Piratas informáticos	- Sobre fenómenos como ciberespionagem, *hacktivismo*. Artigo generalista.
01/01 /2014	Imprensa	Jornal de Notícias	A. Soares e A.F. Sousa	Piratas inventam programa para saquear multibancos	Ataques informáticos a ATM
11/01 /2014	Imprensa	Expresso	Rui Gustavo e Micael Pereira	Prédios do BES roubados *online*	- Referência a um ataque ao BES cuja consequência foi a passagem de alguns imóveis do BES para uma empresa, que não existe de facto; "Os contornos de aparente pura provocação do incidente com o sistema informático do Registo Predial – sem ter havido aparentemente o objetivo de ganhar dinheiro do desvio de mais de 100 propriedades do Banco Espírito Santo – remetem para o universo de sucessivos ataques que a comunidade de *hackers* portuguesa tem vindo a fazer desde o início da crise" - "A luta contra a corrupção e contra os interesses das grandes corporações tem sido o cavalo de batalha dos *hackers*" - "No verão, várias células portuguesas do movimento *hacktivistas Anonymous* tinham participado numa série de ataques informáticos a bancos nacionais, no contexto de uma operação mundial batizada de *#OPBanksters*" - "Mas há dois argumentos fortes a favor da inocência do movimento de *hackers*. O primeiro é que o incidente no Registo Predial não foi reivindicado. Porque se movem por razoes políticas, os *hackers* têm por hábito fazer publicidade dos seus ataques. Muitas vezes até os anunciam com antecedência. (…) O segundo argumento é que este tipo de ataques não é comum nos *hackers* portugueses (…) Os *hackers* portugueses têm optado por usar as suas habilidades para ações menos graves" - "Além de deitarem abaixo, com uma preferência especial para partidos políticos e algumas grandes empresas, têm feito *defacement*es, em que acedem ao conteúdo de *site*s para mudar a sua aparência e colocarem imagens e textos provocadores. O mais longe que foram, na Operação *Banksters* (…) foi explorarem uma vulnerabilidade no banco Santader Totta, que poderia permitir uma injeção de SQL, um tipo de ataque que dá acesso a bases de dados"
21/02 /2014	Imprensa	A voz de Chaves	S/A	GNR levou lições sobre segurança na *internet* às (…)	A GNR e a *Microsoft* Portugal promoveram no dia 11 de fevereiro, no âmbito do Dia Europeu da *Internet* Mais Segura cerca de 700 ações de sensibilização e formação.
11/04 /2014	Imprensa	Diário de notícias	Valentina Marcelino	Resposta a ciberataques custa 2 milhões por ano	- O Governo aprovou no dia anterior a constituição de um CNCseg; - Portugal foi alvo de um ataque ao Ministério dos Negócios estrangeiros por *hackers* chineses. Os ataques foram feitos através de envio de *emails*; - Em novembro de 2012, o grupo *LulzSec* dirigiu um ataque contra o Banco de Portugal e o Parlamento.

					As suas páginas deixaram de estar acessíveis durante horas. O ataque foi descrito no *Twitter*. - Em abril do ano anterior o grupo *SideKingdom12* convocou os *hackers* que quisessem participar numa operação que deixou indisponíveis os *site*s do PSD, PS e CDS-PP, do Governo, da PSP e da GNR. A ação foi contra as medidas de austeridade - Em agosto de 2011 foi detetado um ataque de "cavalos de troia" brasileiros codificados contra a banca de Portugal. "estes ataques informáticos 'envolvem o uso de *phishing* e de ficheiros executáveis que vão roubar os dados das vítimas'"
06/05 /2014	Imprensa	Jornal de Notícias	Alexandra Lopes	Piratas exigem resgate a empresa em *bitcoin*s	- Um empresário "viu-se obrigado a ceder às exigências e a pagar pouco mais de um *bitcoin* e meio – a cotação oficial anda nos 314 euros por cada *bitcoin* – para resgatar os ficheiros da empresa" - "O *bitcoin* é uma moeda virtual que foi introduzida em 2009 nas transações *online*. Permite transferências anónimas, sem a interferência de qualquer banco"; "As transações em *bitcoin*s são transmitidas em códigos para manter as informações anónimas. Para as fazer, basta instalar um *software* próprio, criar uma carteira virtual e passar a fazer parte da rede." - Referência ao *Ransomware*
06/05 /2014	*Internet*	Notícias ao m(…)	S/A	Empresa paga a ´*hacker*´ para recuperar ficheiros próprios	Um empresário de Famalicão pagou 500 euros em *bitcoin*s para poder ter acesso aos ficheiros da própria empresa a um *hacker*.
06/05 /2014	*Internet*	Wintech *Online*	S/A	PJ recomenda cuidado na abertura de ficheiros	- Referência ao caso do empresário de Famalicão. - "No caso da pornografia, o esquema é o seguinte: abre-se uma janela *pop-up* com os emblemas da PJ ou da PSP e uma mensagem a pedir para pagar uma multa, ficando o computador bloqueado. As pessoas pensam que estão a infringir, temendo que o *site* visitado tenha pornografia infantil, por exemplo, ficam amedrontadas e os mais incautos pagam, sem denunciar."
08/05 /2014	*Internet*	Diário Digit(…)	S/A	Ponte de Lima: Pirata informática emite filme p (…)	" Um painel publicitário eletrónico colocado no centro da vila de Ponte de Lima, em Viana do Castelo, começou a passar filmes pornográficos na passada segunda-feira, para choque dos transeuntes."
08/05 /2014	*Internet*	I *online*	Pedro Rainho	Pirata informático passa pornografia em painel Tur(…)	Relativo aos filmes pornográficos passados num painel turístico em Ponte de Lima.
08/05 /2014	Imprensa	Jornal de Notícias	Márcio Silva	Filmes pornográficos nos painéis do turismo	Relativo ao caso dos filmes pornográficos num painel turístico em Ponte de Lima.
08/05 /2014	*Internet*	Jornal de Not (…)	Márcio Silva	Pornografia nos painéis do turismo de Ponte de Lima	Relativo ao caso de filmes pornográficos em painel de turismo em Ponte de Lima.
08/05 /2014	*Internet*	Notícias ao M(…)	S/A	Pirata põe a rodar filme pornográfico em painel (…)	Relativo ao caso de filmes pornográficos em painel de turismo em Ponte de Lima.
08/05 /2014	*Internet*	Sol *online*		*Hacker* exibe pornografia em painel turístico em Ponte (…)	Relativo ao caso de filmes pornográficos em painel de turismo em Ponte de Lima.
08/05 /2014	*Internet*	TVI 24 *online*	A.M.	«Piratas» ataca painel de turismo com ponografia	Relativo ao caso de filmes pornográficos em painel de turismo em Ponte de Lima.
08/05 /2014	*Internet*	Wintech *Online*	S/A	Painéis de turismo de Ponte de Lima passaram filmes (…)	Relativo ao caso de filmes pornográficos em painel de turismo em Ponte de Lima.

09/05 /2014	Imprensa	Algarve resident	S/A	'*Anonymous*' Portugal targets police forces	O grupo *anonymous* Porugal divulgou uma lista de 300 veículos descaracterizados utilizados em operações de trânsito. Trata-se de um subgrupo denominado *Sidekingdom12.* Referência à operação *national blackout*
09/05 /2014	*Internet*	TVI 24 *online*	A.M.	Pornografia em Ponte de Lima bateu recordes na *Internet*	Relativo ao caso de filmes pornográficos em painel de turismo em Ponte de Lima.
10/05 /2014	Imprensa	Correio da (…)	A.C.	Autoridades procuram '*hacker*'	Relativo ao caso de filmes pornográficos em painel de turismo em Ponte de Lima.
10/05 /2014	Imprensa	Jornal de Notícias	Cristiano Pereira	"Foi uma sátira que não pretendeu ofender ninguém"	- Em declarações o "pirata" de Ponte de Lima afirma tê-lo feito apenas para se divertir. Trata-se de alguém com conhecimentos acima da média na área da informática; A invasão foi feita através de um *software* (por ele designado banalíssimo): o *Team viewer*: utilizado para gerir os mesmos à distância.
12/05 /2014	*Internet*	Diário Atual On	S/A	GNR esteve no terreno com operação "Sete dias com (…)	Programa de sensibilização "*Internet* Mais Segura" da GNR.
16/05 /2014	Imprensa	A voz de Chaves	S/A	GNR esteve no terreno com operação "Sete dias com (…)	Programa de sensibilização "*Internet* Mais Segura" da GNR.
23/05 /2014	Imprensa	Expresso	Rui Gustavo e Micael Pereira	Ataque ao BES foi falha de segurança	- Não foi possível chegar aos autores do ataque ao BES. É difícil encontrar um rasto. - Referência ao grupo *Anonymous*: "O cenário é menos grave, ainda assim, em relação aos ataques sucessivos e muito mediáticos a alguns *site*s públicos por parte do movimento ativista *Anonymous*, que recentemente divulgou uma lista com os contactos de dois mil procuradores do MP.
01/06 /2014	Imprensa	Exame Informática	Hugo Séneca	*Anonymous* reivindicam ataque à PGR com HEARTBLEED	- A operação "Apagão Nacional" provocou a publicação de contactos pessoais de 2000 magistrados. No dia 1 de maio registaram-se tentativas de ataque, porém os gestores dos *site*s do Estado já se encontravam alerta; Deixaram inoperacionais os *site*s da PGR, da PGDL e do SIMP durante o dia 25 de abril.
31/07 /2014	Imprensa	Reconquista	J. Furtado e Cruz	Serviços negam pirataria na informática	Possível ataque em serviços de saúde negado.
23/08 /2014	*Internet*	Wintech *Online*	João Fernandes	Banco de Portugal e Novo Banco são atacados pelos «*Anonymous*»	- "Grupo *hacker Anonymous* atacaram esta sexta-feira os servidores onde estão alojados os *site*s do Banco de Portugal, do Novo Banco e do Ministério da Agricultura"; "Numa ação a que chamaram Operação Novo Sangue , os piratas informáticos conseguiram obter o acesso a mais de 200 *emails* do Banco de Portugal e do Novo Banco (antigo BES) tendo-os divulgado, posteriormente, na *internet*." - "Em relação ao Ministério da Agricultura, os *hackers* divulgaram 2700 dados de pessoal pertencente à instituição pública nomeadamente *emails*, nomes, *passwords*, contatos telefónicos e profissionais, números de identificação fiscal e respetivos vencimentos."; "Na página de *Facebook* dos *Anonymous* Portugal, os *hackers* dão conta de que estes 200 *emails* estão à disposição dos cidadãos para que estes, querendo, reclamem."
26/09 /2014	Imprensa	Negócios	Ana Torres Pereira	Ainda seremos donos do nosso passado?	Sobre vulnerabilidade da *icloud* ou nuvem. Dispositivos móveis e vulnerabilidades associadas.
15/10 /2014	*Internet*	Imagens de Marca.pt	S/A	Marcas vão passar a comunicar nas camisolas da NBA	*Dropbox* alvo de ciberataques.

25/01 /2015	*Internet*	FilmSpot *Online*	S/A	Odyssey (2015)	Sobre filme.
28/01 /2015	*Internet*	Bola *online*	S/A	Rádio cristã vítima de ataque	"A Hope FM, uma conhecida estação de rádio cristã do Quénia, foi vítima de um ataque na terça-feira à noite, passando a transmitir, durante cerca de três horas, versos islâmicos, antes de sair do ar."
03/02 /2014	*Internet*	Gazeta do Rossio	S/A	*Anonymous* Portugal ataca Comissão da Carteira Profissional de Jornalistas	- "Os piratas informáticos *Anonymous* Portugal reivindicaram hoje um ataque à página da *internet* de CCPJ. Os *hackers* afirmam terem acesso a mais de 470 mil documentos da comissão e copiado 322 *emails* e *passwords* de jornalistas e juízes". Algumas dessas informações foram publicadas no *site* do *Pastebin*; O ataque foi reivindicado através do *site Tugaleaks*, que diz ter falado com o *hacker Ousiderz Arcainex*, este opera nos grupos *Hackers Street*, *SideKingdom12* e *OutsideTheLaw*"
03/02 /2015	*Internet*	Sapo *Online*	S/A	Obama quer mais 14 mil milhões de dólares para (…)	Investimento dos EUA no combate ao cibercrime.
05/02 /2015	Imprensa	Açoriano Oriental	S/A	Tribunal de Tóquio condena '*hacker*'	Homem condenado pela criação de um vírus que enviou a terceiros, em Tóquio.
05/02 /2015	Imprensa	Visão	S/A	Jornalistas na mira de *hackers*	- Ataque à base de dados da CCPJ. Ataque reivindicado pelo coletivo *Anonymous* Portugal no *Tugaleaks*. Este ataque permitiu a visualização de mais de 470 mil documentos, bem como *emails* e *passwords* de jornalistas; O *hacker Ousiderz Arcainex* declarou que usou apenas cinco letras "admin" para aceder.
16/02 /2015	*Internet*	PT Jornal *online*	Sérgio Meireles	Aliança internacional de *hackers* roubou mais de 900 milhões de euros a bancos	- "Este tipo de ataques baseia-se no '*phishing*', onde são desviados dados dos utilizadores ou empresas através da monitorização fraudulenta dos respetivos computadores. - Um dos bancos vidados perdeu em 'ataques eletrônicos', cerca de 9 milhões de euros. Ainda há bem pouco tempo, foi revelada uma nova técnica de ataque por parte de *hackers*. Esta nova forma de ataque consiste na programação de uma caixa ATM, para que esta liberte dinheiro a uma hora programada pelo *hacker* para que este possa ser levantado."
26/02 /2015 1	*Internet*	Portugal residente *online*	Michael Bruxo	Police arrest seven in connection with *hacker* group ´*Anonymous* Portugal´	- Sete pessoas foram detidas pela PJ suspeitas de fazerem parte do grupo *Anonymous* Portugal nas áreas metropolitanas de Lisboa e Porto. Os suspeitos encontravam-se na faixa etária entre os 17 e os 40 anos e estão acusados de inúmeros crimes. Um dos detidos é Rui Cruz, fundador do *Tugaleaks;* O código da operação da PJ é "C4R3T0S" (Caretos); O *Anonymous* Portugal existe desde 2011 e é responsável por um grupo de ciberataques, como os encetados contra o MP, a PSP e a GNR. Informação confidencial foi retirada através da *internet*, por exemplo o caso da divulgação das 300 matrículas de viaturas descaracterizadas da polícia utilizadas em operações de trânsito.
27/02 /2015	*Internet*	Portugal Resident *Online*	Michael Bruxo	UPDATE: *Hackers* strike back and demand release of arrested	Um dia depois das detenções de 7 indivíduos pela PJ, outro grupo conhecido como *Sudoh4k3rs* exigiu a sua libertação imediata, dirigindo um ciberataque ao *site* da universidade de Lisboa. Os *hackers* acederam o sistema da universidade e retiraram *passwords* que garantem o acesso à página da administração do *site*; *Sudoh4k3rs* descrevem-se como *hacktivistas* que se opõem aos Governos corruptos e pretendem servir a população.

Documentação Anexa

Anexo A – Os limites do *hacktivismo.*

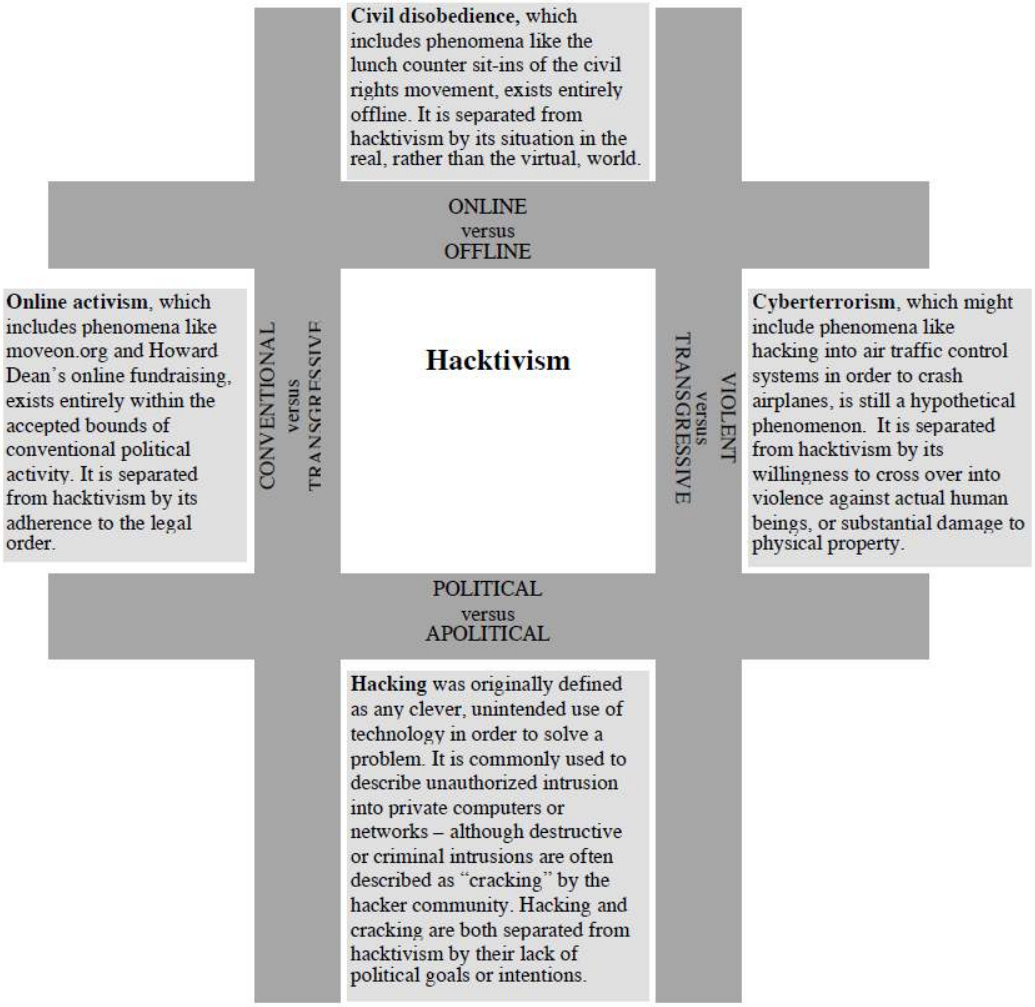

Figure 1. The boundaries of hacktivism

Fonte: Samuel, A. (2004). Hacktivism and the future of political participation. (Tese de Doutoramento). Cambridge: Harvard University.

Anexo B – Incidentes de Segurança informática no COSI da SGMAI

Tipo de Evento	N.º Tickets abertos
Exploit attempt	1915
Malware Distribuition	1410
System Infection	422
System Scan	389
Sql injection attempt	370
Data Leak	364
Unauthorized resource use	260
Network Scan	244
XSS atempt	222
Tool based DoS/DDoS/DRDoS	222
File inclusion attempt	122
Flood	100
System unauthorized access	77
C&C	72

Tabela 1 - Top 14 dos incidentes reportados pela ferramente RTIR no COSI da SGMAI. Fonte: Relatório de Segurança do COSI SGMAI 2014.

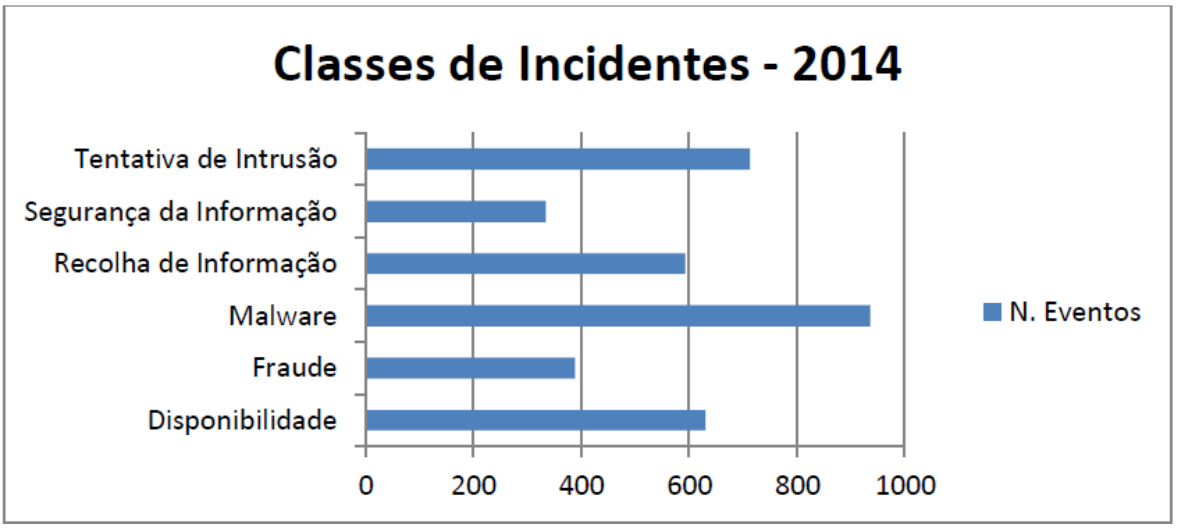

Gráfico 1- Classes de incidentes mais verificados no ano de 2014, na SGMAI. Fonte: Relatório de Segurança do COSI SGMAI 2014.

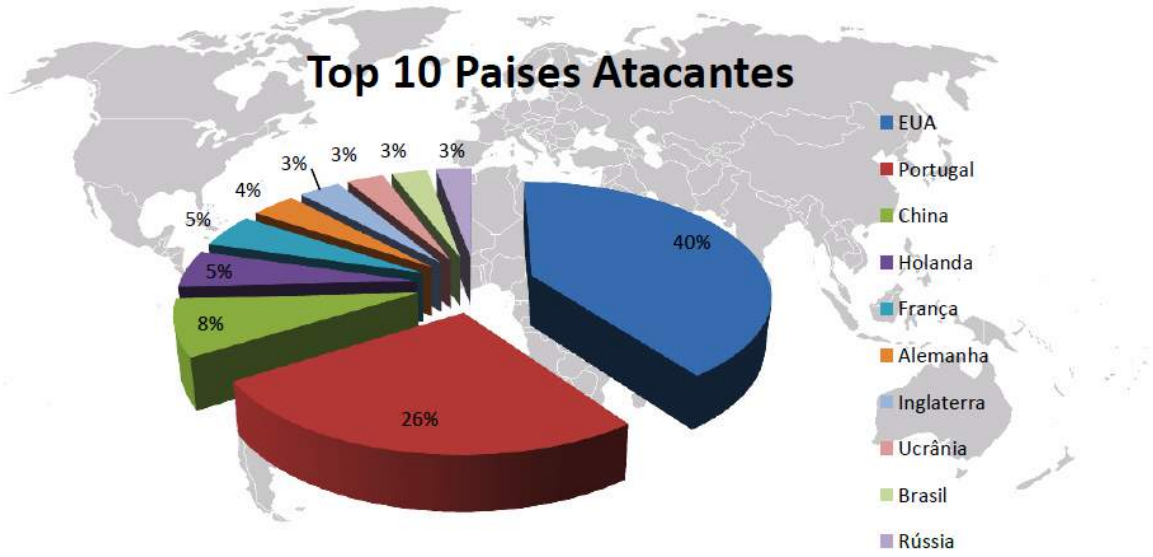

Gráfico 2 - Top dos 10 países de onde são originários os incidentes de segurança verificados no ano de 2014 no COSI da SGMAI. Fonte: Relatório de Segurança do COSI SGMAI 2014.