ACADEMIA MILITAR

Departamento de Estudos Pós-Graduados

Mestrado em Guerra de Informação

Estudo da criptomoeda

- Análise aos desafios de substância criminal

Projeto de investigação para a obtenção do grau de Mestre em
GUERRA DA INFORMAÇÃO

Lisboa, 2018

ACADEMIA MILITAR

Mestrado em Guerra de Informação

Estudo da criptomoeda

- Análise aos desafios de substância criminal

Projeto de investigação para a obtenção do grau de Mestre em GUERRA DA INFORMAÇÃO

Orientando: João Nuno Ferreira Gaspar

Orientador: Professor (Doutor) Bruno Alexandre Marques

Co-orientador: Professor Paulo Miguel Mendes Santos

Lisboa, 2018

AGRADECIMENTOS

Uma palavra de apreço a todos aqueles que contribuíram diretamente para esta investigação. Com destaque para todos aqueles que se disponibilizaram para gentilmente contribuir e enriquecer o estudo com o seu conhecimento, nomeadamente aos entrevistados CAlm Gameiro Marques, Mário Valente, Inspetor-chefe Rogério Bravo, Paulo Moniz, *Riclas*, José Pereira e Inspetor Carlos Cabreiro, aos professores orientadores Prof. Dr. Bruno Marques e Professor Paulo Miguel Santos e à própria Academia Militar de Lisboa que me formou e simultaneamente me despertou para os desafios tecnológicos que se avizinham influenciando a minha forma de pensar o futuro.

Sem se terem apercebido contribuíram também indiretamente para o culminar desta etapa os meus colegas, a minha família, os meus irmãos e amigos. Uma palavra especial ao meu Amigo António Mil-Homens com quem refleti horas a fio sobre as temáticas aqui abordadas e que sem dúvida me deu ânimo, estímulo e solidez de raciocínio para desempenhar a tarefa a que me propus.

Agradecer à própria tese que me obrigou a superar-me e a questionar. A procurar mais além quando a resposta parecia ser difícil de encontrar. A acreditar que dedicação e esforço acrescidos dão aso a resultados melhores. E a perceber que a exigência em colocar-me no patamar mais alto daquilo que acredito poder conseguir alcançar, me pode guiar ao sucesso.

Resta-me ainda agradecer à minha Mãe, em quem me inspiro para traçar o meu caminho, todos os dias. A ti dedico o meu esforço, assim como todas as metas que espero atingir. O meu sucesso será sempre o teu. Obrigado!

RESUMO

Pese embora a evolução tecnológica tenha melhorado a qualidade do dia-a-dia da sociedade, este fenómeno compreende significativos desafios a quem nele está inserido, não se tratasse de uma evolução que, paralelamente, engloba também entidades terroristas e criminosos que dela tiram partido. O progresso das ferramentas tecnológicas trouxe formas inovadoras para mover, armazenar e liquidar fundos através de mecanismos nem sempre transparentes ou monitorizáveis, tal como acontece com as criptomoedas que recentemente começaram a desempenhar um papel importante no que à consumação de crimes no, ou através do ciberespaço diz respeito. Infelizmente, o ritmo através do qual o ciberespaço se vai instalando na vida dos cidadãos e nos processos das empresas fez esquecer certas questões relacionadas com a segurança e que seriam fundamentais na prevenção da exploração de vulnerabilidades por parte de agentes criminais e que têm, por vezes, resultados irremediáveis. A emergente relação entre as tecnologias de comunicação e as transações financeiras ilícitas é uma área que obriga a reflexão, especialmente no que diz respeito ao cibercrime e à forma como as forças policiais o combatem. O presente trabalho de investigação tem como objetivo último perceber e analisar o panorama português em termos da utilização das criptomoedas em atividades criminais assim como as respetivas medidas preventivas e de combate. Desta forma, a sociedade em rede inserida nesta economia digital deve ser consciente do impacto da criptomoeda para o seu desenvolvimento sustentável, o que implicará mudanças possivelmente estruturais nos vários atores económicos e sociais.

Palavras-chave

Cibercrime; Criptomoeda; Bitcoin; Segurança de informação; Segurança; Criminalização;

ABSTRACT

Although improved technology has greatly improved the quality and ease of daily life in recent years, it is not without its problems. One downside to technological advances is that terrorists and criminals are users, just like law-abiding citizens. With this new technology comes innovative means to move, store, and liquidate funds, often in ways that are not transparent or detectable, as the case of the emerging cryptocurrencies, which start to play a significant role on crimes executed on, or through the cyberspace. Unfortunately, the rhythm that the cyberspace is fixing itself on the user's daily life, so as on the corporation's processes, made forget certain questions related with safety and security, which would be crucial on the vulnerabilities exploitation prevention from the criminal agents, and which has sometimes irreparable results. The emerging nexus between communications technology and illicit financial transactions is one such area of concern, especially considering cybercriminal activities, and the way that criminal investigation forces combat it. The investigation work presented here has as a final objective to understand and analyse the Portuguese panorama in terms of cryptocurrencies uses on criminal activities and its preventive and combat measures to avoid this kind of practices.

Keywords

Cybercrime; Cryptocurrency; Bitcoin; Information Security; Security; Criminalization;

Índice Geral

Índice de Figuras

Índice de Tabelas

Índice de Apêndices

Acrónimos e abreviaturas

AI	*Artificial Intelligence*
APT	*Advanced Persistent Threat*
AV	*Anti-virus*
BTC	Bitcoin
C2C	*Criminal to criminal*
CaaS	*Crime-as-a-Service*
CEO	*Chief Executive Officer*
CERT	*Computer emergency response team*
CIO	*Chief Information Officer*
CISM	*Certified Information Security Manager*
CISO	*Chief Information Security Officer*
CNCS	Centro Nacional de Cibersegurança
CNP	*Card-not-present*
CNY	*China Yuan Renminbi currency code*[1]
CSE	*Child Sexual Exploitation*
CSEM	*Child Sexual Exploitation Material*
CSIRT	*Computer Security Incident Response Team*
CTI	*Cyber Threat Intelligence*
DDoS	*Distributed Denial of Service*
EUR	*Euro currency code*[1]
EUROPOL	*European Police Office*
FATF	*The Financial Action Task Force*
FinTech	*Financial Tecnhology*
FMI	Fundo Monetário Internacional
GDPR	*General Data Protection Regulation*
I2P	*Invisible Internet Project*
IOCTA	*Internet, Organised Crime Threat Assessment*
IoT	*Internet of Things*
IP	*Internet Protocol*

[1] Em concordância com a ISO 4217 (International Organization for Standardization, 2015);

ISO	*International Organization for Standardization*
KSN	*Kasperky Security Network*
ONU	Organização das Nações Unidas
opc	Órgãos de Polícia Criminal
OPSEC	*Operations Security*
OSINT	*Open-source intelligence*
P2P	*Peer-to-Peer*
PJ	Polícia Judiciária
RATs	*Remote Administration Tools*
SEPA	*Single Euro Payments Area*
SGSI	Sistema de Gestão de Segurança de Informação
SIEM	*Security Information and Event Management*
SO	Sistema Operativo
SOC	*Security Operations Center*
TAILS	*The Amnesic Incognito Live System*
TI	Tecnologias de Informação
TIC	Tecnologias de Informação e Comunicação
Tor	*The Onion Router*
URL	*Uniform Resource Locator*
USD	*United States Dollars*[1]
VC	*Virtual Currencies*
www	*World Wide Web*
XBT	*Bitcoin currency code*[1]

1.Introdução e identificação do tema

"Technology is making tremendous advances against hunger, disease and wasteful uses of energy. But it also empowers organized crime and raises the spectre of crippling cyber-attacks"

Eliasson, 2015

A forma como os indivíduos comunicam entre si é também o reflexo do desenvolvimento da comunidade onde estão inseridos. Neste sentido o advento da *Internet* como rede global de comunicações – leia-se conceito, infraestrutura e tecnologia - pode ser considerado o ponto alto da comunicação entre os seres humanos tendo em conta a proximidade, disponibilidade e acessibilidade que trouxe a quem de si se serve, explorando soluções criativas para as quais o limite está ainda longe de se dar a conhecer. Na última década tem sido observável um crescimento exponencial na evolução das Tecnologias de Informação (TI) que, aliadas ao fenómeno da Internet, fizeram surgir inovações tecnológicas disruptivas assim como novas ferramentas aplicacionais e plataformas que interligaram a população dos 4 cantos do planeta numa autêntica sociedade em ligada através do ciberespaço, um espaço virtual onde as noções espaciais e/ou temporais, podem desvirtuar os utilizadores da realidade através de uma apenas aparente sensação de segurança.

A transformação abrupta mencionada é uma mudança para a qual se considera que a sociedade não estava, nem está ainda, uniformemente preparada. Este facto é fruto da velocidade com que a mesma penetrou na sociedade, hoje caracterizada como sociedade de informação (Castells, 2003), dado o novo contexto social e de sociabilização e dada a transformação das mais básicas atividades quotidianas, muitas delas operacionalizadas, hoje, através do ciberespaço e que geraram uma autêntica relação de dependência subordinada às TI. No entanto, apesar de assim designada, esta sociedade tem dado provas de não conseguir acompanhar de forma unânime todo este processo, essencialmente no que toca à segurança da sua utilização. Um dos argumentos que dá força a esta problemática parte do pressuposto de que as particularidades das soluções disponíveis através do ciberespaço que de uma forma tão significativa se tornaram indispensáveis ao dia-a-dia dos indivíduos, são as mesmas que, na mesma medida, podem ser exploradas por quem, de forma perversa e/ou nociva, procura praticar atividades

criminais. Por acontecerem no ciberespaço, estas atividades denominadas por cibercrimes, independentemente da forma como são levadas a cabo, estão, nos dias que correm, omnipresentes no quotidiano dos cibernautas um pouco por todo o mundo.

Contribui também para a insegurança dos utilizadores do ciberespaço, uma das características intrínsecas ao processo de transformação para a atual sociedade de informação, segundo a qual está implícita a ideia de uma mudança nas formas de viver na sociedade contemporânea que a alavancam para uma verdadeira Era da Informação. Estas alterações têm aumentado sucessivamente o nível de exposição dos utilizadores, através não só da utilização progressiva das multiplataformas digitais, mas também através do fornecimento de dados *online.* Este fornecimento quase indiscriminado afigura-se, também ele, como uma ameaça, não fosse o facto de o tratamento dos dados, por parte das entidades que os recebem, nem sempre ser o mais adequado, podendo os mesmos ser extraviados e utilizados com intenções pejorativas. Esta exposição tornou-se constante e incontornável para os utilizadores da rede, seja na utilização dos serviços, ferramentas e aplicações que nela assentam, seja na partilha e distribuição de conteúdos digitais sob a forma de informação. Todavia são vistas com bons olhos as mudanças estruturais que a norma regulatória da União Europeia: *General Data Protection Regulation* (GDPR); vai impor aos Estados-membro e que tem como objetivo último o colmatar desta exposição dos utilizadores e tratamento descuidado dos seus dados pessoais (European Union, 2017).

Em paralelo, o processo de inclusão digital nunca foi tão acelerado como o é hoje, existindo mundialmente 3,5 milhares de milhões de pessoas com acesso à *Internet*, o que representa cerca de 40% da população mundial (Internet Live Stats, 2016). A velocidade a que este processo de transformação da sociedade decorre é exponencialmente mais acelerada do que qualquer outro processo revolucionário já observado, obrigando a um processo de habituação e preparação demasiado repentino para a utilização das novas TIC (Tecnologias de Informação e Comunicação). A celeridade do fenómeno em causa fez de alguns utilizadores vítimas. Vítimas por se encontrarem numa posição de particular vulnerabilidade e desproteção, no que ao cibercrime diz respeito. Uma tipologia de crime recente, pouco valorizada e compreendida pela sociedade e cujos efeitos são irremediavelmente subestimados no que concerne à sua definição e aplicação de medidas de combate por parte das entidades competentes.

Desde o ano de 2009, aquando do lançamento da primeira criptomoeda colocada em circulação, denominada *Bitcoin (*BTC ou XBT*)* (Nakamoto, 2009), que uma nova solução no campo das *Virtual Currencies* (VC's) se afigurou, sob o formato de um protocolo sustentado num algoritmo através de uma solução de rede *Peer-to-Peer* (P2P)[2], como uma inovação tecnológica possivelmente disruptiva face ao funcionamento tradicional do sistema financeiro, assim como das soluções de pagamentos e transações até à data existentes. Esta solução afirmou-se simultaneamente como resposta às necessidades e interesses da sociedade e dos mercados, em linha com as possibilidades mais eficazes que as novas soluções computacionais e de redes hoje permitem. Assim, surgiu neste formato uma nova solução tecnológica pragmática no que à transação de fundos diz respeito, mais eficaz e célere do que os mecanismos existentes até então e que, ao mesmo tempo, tem potencial disruptivo para transformar o *status quo* no que concerne à privacidade financeira da sociedade.

Esta hipotética transformação futura do paradigma financeiro está em linha com a já precedente tendência que sugere a transformação do sistema financeiro para um sistema financeiro maioritariamente digital, através de um fenómeno designado por *Financial Tenchology* (*FinTech).* Este passa pelo inevitável crescimento da digitalização da economia mundial que é, hoje, um fenómeno inigualável, onde se espera que o impacto das soluções de negócio por via eletrónica (*e-business)* e comércio eletrónico (*e-commerce)* no crescimento económico mundial alavanque mais de 27 biliões[3] de *United States Dollars* (USD) até 2020, um crescimento significativo face aos 23 biliões[4] de USD atuais (eMarketeer, 2016). Note-se no entanto que este fenómeno não é representativo da utilização da criptomoeda como moeda de compra em mercados *online*. No entanto, e face a este cenário, é plausível que a utilização desta solução venha a ganhar força e conquiste um importante papel neste processo, por ser a que melhor se ajusta ao mesmo, fruto da sua tipologia de aplicação, da sua arquitetura e das próprias características intrínsecas ao seu funcionamento como será explicado adiante.

O novo conceito de criptomoeda, inicialmente conhecido única e exclusivamente sob o formato do sistema *Bitcoin*, embora tenha posteriormente encontrado diferentes

[2] P2P - é uma arquitetura de rede onde cada um dos pontos da rede funciona tanto como cliente quanto como servidor, permitindo assim a partilha de serviços e dados sem a necessidade de um servidor central;
[3] O correspondente a 27.000.000.000.000 USD;
[4] O correspondente a 23.000.000.000.000 USD;

configurações noutros sistemas de criptomoedas, trouxe indiscutíveis benefícios para os seus utilizadores desde logo aos níveis da supressão de custos de emissão de moeda e da segurança dos seus utilizadores uma vez que não equaciona a existência de representação física de dinheiro, assim como aos níveis da confidencialidade e das intrínsecas barreiras à monitorização por parte de instâncias governativas ou reguladoras, liberdade na condução das suas transações e ainda da total propriedade sobre os seus fundos tendo em conta que o algoritmo BTC assenta num sistema parcialmente anónimo (Grinberg, 2011), descentralizado do poder corporativo e governativo e distribuído por todos os pontos da rede que correm o algoritmo *Bitcoin*. Outro dos benefícios para utilizadores do sistema de pagamentos BTC passa pelo pragmatismo e simplicidade associado às transações de capitais, para as quais contribuem as baixas taxas associadas a cada transação, quando comparadas com as taxas cobradas pelos sistemas de transações de pagamentos mais frequentemente utilizados, para os efeitos do presente estudo, denominados de meios de pagamento tradicionais[5] (Folkinshteyn, Lennon, & Reilly, 2015), assim como, o facto de estas transações terem o potencial de ser processadas significativamente mais rápido[6] que nos sistemas tradicionais, o que pode ser deduzido da Figura 1, e sem obstáculos que advenham de diferentes geografias entre as partes envolvidas na transação, independentemente de os fundos estarem sedeados em diferentes plataformas de *exchange*[7]. Outras comodidades podem ser elencadas, sendo que é de destacar o facto de dias não úteis não influenciarem o processamento das transferências de fundos tendo em conta que o sistema é autónomo e não requere mão-de-obra humana.

[5] As taxas cobradas pelas plataformas de troca de criptomoedas representam frações de cêntimo (≈0,0001 BTC por cada 1000 *bytes* de informação de uma transação) enquanto as taxas associadas à utilização do mecanismo BTC como sistema de pagamentos são, para os operadores de referência neste tipo de serviço, de apenas 1% depois do 1º milhão de BTC transacionadas, sendo até lá, gratuitas. Em termos comparativos, a taxa de uma transação internacional, à data de SET2017, para um montante de $100 foi de: $3,30 para a *PayPal Holding Inc.* (The Fee Calculator, 2017), $8 para *Western Union* (Western Union, 2017), e de $12 para *MoneyGram* (MoneyGram, 2017). Para uma transação equivalente a $100 em BTC a taxa cobrada dificilmente ultrapassará os 0.0001 BTC ou seja $0,3609 (BTC Exchange Rate, 2017);

[6] O tempo de uma transação em BTC varia mediante o volume de informação que cada transação comporta. No entanto e tal como mostra a Figura 1, o tempo médio de uma transação em BTC, quando compreendidas as transações efetuadas nos últimos dois anos, não chega aos 10 minutos (BlockChain, 2016), podendo até, em alguns casos, demorar poucos segundos a ser processada. Note-se ainda que não é expectável que transferências de montantes avultados demorem mais tempo a ser processadas. Apesar de conterem mais *bytes* de informação não é por isso que o processamento será mais demorado. Isto acontece porque os *miners* dão preferência ao processamento de grandes transações uma vez que são também as que lhes trazem maior retorno por terem de lhes aplicar mais esforço, ou por outras palavras, capacidade processamento.

[7] Entendam-se por plataformas de *exchange* os *players* que disponibilizam carteiras eletrónicas de *Bitcoin*, tais como *CoinBase*, *LocalBitcoin*, *Bitfinex*, *Kraken*, *BTCChina*, entre outros;

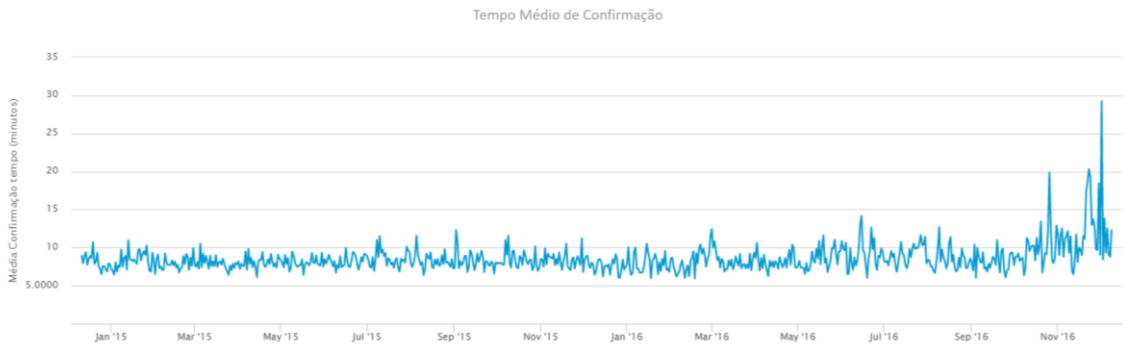


Figura 1 – Tempo médio, em minutos, para confirmação de transações, nos últimos 2 anos (BlockChain, 2016)

De igual forma, o facto de a BTC e neste aspeto específico, também as restantes criptomoedas, serem moedas de troca global que circulam exclusivamente *online*, confere-lhes a possibilidade de serem usadas em qualquer parte do mundo, não sendo aplicáveis as habituais burocracias e custos associados às conversões cambiais, resultando em menos custos para os utilizadores.

Todas estas características são vantajosas para os utilizadores que usufruem de um sistema autossustentável, isto é, um sistema que não está suportado por nenhuma instituição central e, por isso, não comporta custos resultantes do serviço oferecido, tal como acontece com os sistemas tradicionais. Este fator diferenciador deve-se ao próprio funcionamento da grande maioria dos algoritmos em que assentam as criptomoedas que, por serem partilhados e distribuídos, suportam automaticamente todo o processo das transações, através da aplicação de capacidade de processamento computacional de alguns nós da rede, denominados *miners*, na resolução de problemas criptográficos, gerados a cada nova transação e que desconstruídos, desbloqueiam essas mesmas transações.

Elencadas algumas das vantagens de utilização do sistema de criptomoedas, cedo se percebe que as mesmas seriam meritórias de um estudo exclusivo aos benefícios da sua utilização e ao potencial da sua crescente utilização como uma ameaça transformadora dos sistemas monetário e financeiro mundiais.

No entanto, o enfoque deste estudo passará pelo reverso da medalha, isto é, pelos desafios negativos que esta inovação trouxe para indivíduos, governos, organismos reguladores e mesmo ao mundo empresarial. Se por um lado a forma como o ecossistema BTC e das restantes criptomoedas foi pensado e criado traz uma série de benefícios para os seus utilizadores que o usam com fins lícitos, por outro lado, alguns encontraram em alguns formatos de moedas criptográficas, ferramentas que permitem alavancar novos métodos, estratégias e atividades criminais em ambiente digital, que dela se utilizam para ultrapassar controlos já existentes no sistema financeiro tradicional, encontrando na criptomoeda uma moderna forma de atuar ilicitamente no ciberespaço.

A criptografia que torna o ambiente das criptomoedas e as suas transações anónimas e dificilmente rastreadas ou monitorizadas, assim como o seu funcionamento através de uma arquitetura de rede P2P são um conjunto de fatores bastante apetecíveis para indivíduos, organizações criminais e até organizações terroristas que vêm no ciberespaço e na criptomoeda um novo ambiente operacional para atuarem. Estes agentes, dotados de um engenho audaz na procura de novas soluções para desempenharem as suas atividades com o mínimo de exposição possível, encontram neste algoritmo uma ferramenta eficaz com características que podem vir a alavancar um crescimento exponencial de fuga e evasão fiscal, agilizar processos de lavagem de dinheiro e facilitar transações de bens ilegais, por exemplo, através de mercados negros *online*. Funciona inclusivamente como um mecanismo facilitador de transações clandestinas de fundos entre criminosos, assumindo já cerca de 40% de todos os pagamentos entre criminosos, identificados através de entidades legais de países pertencentes à União Europeia e também como uma alternativa às sociedades bancárias em paraísos fiscais, mais conhecidas como *off-shores* (EUROPOL, 2015). É ainda uma solução perfeita para extorsões, pedidos de sequestro de qualquer tipo, ou até para ciberataques que envolvam transações de fundos. Por isto, a tecnologia inerente às criptomoedas tem vindo a ser considerada como um dos mecanismos que no futuro maior perigo pode trazer, direta ou indiretamente, à sociedade tendo também em conta que a sua utilização traz eficácia e solidez aos movimentos de capitais entre cartéis e aos financiamentos a organizações terroristas, fortalecendo-os (EUROPOL, 2015).

Posto isto, o presente estudo vai incidir sobre a esfera do cibercrime e as novas formas de atuação criminosa em meio eletrónico e/ou com recursos a ferramentas digitais, com especial enfoque na utilização das criptomoedas como ferramenta, veículo ou meio para a consumação desses mesmos crimes, enquanto analisa paralelamente quem e quais

são os alvos, as suas vulnerabilidades e de que forma se protegem ou são protegidos por outrem.

1.1. Justificação e Pertinência do trabalho

A Era da Informação, tal como Castells (2003) a descreve é caracterizada por ser um mundo livre no que toca ao acesso à informação e conhecimento num contexto onde o fluxo de informações é intenso e cresce a um ritmo exponencial. Note-se que, com este novo paradigma, no qual a forma como a informação é partilhada tanto se modificou, num cenário onde barreiras geográficas ou temporais deixaram de ser entraves à eficaz comunicação entre os Homens, a sociedade em rede acabou por torna-los mais próximos. Uma proximidade que lhes trouxe um conceito de liberdade mais abrangente e inclusivo, sendo que, no entanto, lhes trouxe, na mesma proporção, um espaço de interação menos seguro (Castells, 2003). Por ser uma plataforma onde os utilizadores estão crescentemente conectados e em multiplataformas e por se estimar que no ano de 2020 existam já seis dispositivos, ligados à rede *web*, por pessoa, espera-se que, cada vez mais, que a criminalidade se "servirá" da Internet (APAV - Associação Portuguesa de Apoio à Vítima, 2015). Este contexto torna-se compreensível se for tido em conta o facto de esta nova vertente ser apenas a digitalização de crimes tradicionais anteriormente existentes, num cenário cada vez mais convidativo para criminosos, não fosse o desconhecimento e consequente insegurança a que os utilizadores estão sujeitos no ciberespaço. No panorama atual relativo ao contexto nacional, os crimes informáticos, nas suas variadas formas[8], registaram um aumento de 190 casos, representando um acréscimo percentual de 41%, entre 2014 e 2015 (Sistema de Segurança Interna, 2015).

Este paradigma que sugere uma maior insegurança no ciberespaço pode traduzir-se em novos perigos para os quais os indivíduos desta sociedade de informação, sejam eles singulares ou coletivos, não estão convenientemente preparados[9]. Neste fenómeno, a tendência é de que a sociedade não consiga acompanhar a evolução das TIC em plena segurança e com consciência das consequências que advém da sua utilização, fruto da celeridade com que as novas ameaças se adaptam aos controlos que lhes são colocados,

[8] Foram considerados para esta análise os crimes acesso indevido ou ilegítimo/interceção ilegítima, falsidade informática, outros crimes informáticos, reprodução ilegítima de programa protegido, sabotagem informática, viciação ou destruição de dados/dano relativo a dados/programas, consubstanciados na Lei nº 109/2009, de 15 de Setembro – Lei do Cibercrime;

[9] 78% dos cibernautas portugueses estão mal informados sobre como se protegerem contra ameaças de cibercrimes (APAV, 2016);

quer através da sua capacidade de readaptação a um novo contexto, quer através de novas técnicas que contornem os controlos de segurança existentes. Neste aspeto é necessário ter em consideração que o ataque à vítima pode ser executado através de uma infinidade de diferentes configurações e estratégias, com tendência para que os procedimentos se multipliquem através diferentes configurações tendo como fim "despistar" ora os mecanismos de deteção de intrusão ou infeção dos sistemas dos utilizadores, ora as próprias autoridades competentes como os órgãos de polícia criminal (opc's).

Neste sentido e pese embora o facto de esta ser uma Era que oferece múltiplas possibilidades de aprendizagem, onde qualquer dispositivo ligado em rede tem potencial para se tornar um veículo para a obtenção de conhecimento e consequentemente um veículo para a criação consciente de opinião, livre-arbítrio e preparação do cidadão para a vida ativa, contribuindo para uma sociedade global mais equitativa no acesso ao conhecimento e munida de ferramentas que a fortalecem, existe ainda uma outra face da moeda, onde esta é simultaneamente uma Era na qual as mesmas ferramentas estão arbitrariamente disponíveis a todo os cidadãos que delas queiram usufruir, inclusivamente agentes que delas tirem partido com fins ilícitos e com intenção criminosa, levando assim à consumação de crimes em ambiente digital.

O expectável progresso desta realidade, se equacionado com a generalização potencial da utilização quotidiana da *world wide web* (*www)* por parte da população, vai conduzir a luta contra a criminalidade para uma nova esfera de complexidade, tal como é prova o facto de se estimar que, no ano de 2015, cerca de 689 milhões de pessoas terem sido vítimas de cibercrime, numa média de quase 22 novos casos a cada segundo, um aumento percentual de 10% face ao ano anterior e com um custo associado de 126 milhares de milhões de dólares despendidos em perda direta ou na sua resolução (Norton, 2016). A sofisticação dos crimes praticados no ciberespaço, ou através de ferramentas informáticas, coloca assim as vítimas numa posição de particular fragilidade e desproteção tendo em conta que se trata de um fenómeno recente, pouco valorizado e compreendido pela sociedade em geral e cujas consequências são ainda subestimadas, desvalorizando os perigos inerentes.

A interligação global implícita à utilização das novas TIC constitui uma plataforma operacional apetecível para quem procura explorar as suas vulnerabilidades e com isso encontrar oportunidades para obtenção de lucros, atacar concorrentes ou alvos frágeis, ou até obter para si, ou para outrem, vantagens patrimoniais, ou extrapatrimoniais. Este contexto torna evidente a ameaça que a presença *online* de organismos públicos,

instituições, corporações ou até dos indivíduos coloca através dos novos meios digitais para a consumação de crimes em novos formatos, que podem ser consumados por um agente singular, ou por organizações criminosas, tendo como destino um único alvo ou múltiplos alvos, individuais ou coletividades de cariz empresarial ou até organismos estatais, ora num contexto nacional, ora num contexto internacional.

A pertinência deste estudo está assim estritamente ligada ao paralelismo entre o incessante aparecimento de novas soluções tecnológicas alicerçadas nas novas TIC e a crescente dificuldade em combater a utilização das mesmas inovações tecnológicas num contexto criminal. Esta relação abriu espaço de atuação a quem procura novos métodos e técnicas de atuar no mundo do cibercrime, da mesma forma que aumentou a insegurança dos utilizadores do ciberespaço, agora expostos a novas vulnerabilidades. Note-se, neste âmbito, que soluções como certas criptomoedas, fruto das suas particularidades, têm sido crescentemente utilizadas como veículo facilitador de uma série de crimes anteriormente existentes, tal como mostra a Tabela 1, que viram nesta tipologia e arquitetura de dinheiro virtual, a solução perfeita para a consumação desses mesmos crimes agora em ambiente digital (EUROPOL, 2015).

Tabela* 1 – *Agentes, motivos, meio e exemplos associados às práticas criminosas em meio eletrónico, adaptado e traduzido de (EUROPOL, 2015)

Propósito do pagamento	**Pagamento por**	**Mecanismos de pagamento mais frequentes**	**Exemplos**
Vítima a agente do crime	Extorsão	BTC, Transferência Bancária, *paysafecard*	Pagamento resultante de extorsão devido a ramsonware[10] ou DDoS[11] (Distributed Denial of Service)
	Fraude	BTC, Transferência Bancária, *Western Union*	Fraudes ou esquemas online
Agente do crime a agente do crime	Mecanismos Counter-Anti-Vírus[12]	Paypal	Testes de *malware*[13] contra *Anti-virus* (AV) comerciais
	Dados	BTC, *Western Union*, *WebMoney*	Aquisição de dados financeiros comprometidos como dados de cartões de crédito
	DDoS	BTC	Contratação de serviço de DDoS
	Hosting[14]	BTC	Aquisição de *hosting* (including bulletproof)
	Malware	*Visa*, *Mastercard*, *WebMoney*, *Paypal*[15]	Aquisição de *malware* como RATs[16] (*Remote administration Tools*) ou *banking trojans*[17]
	Transações em mercados negros	BTC, *paysafecard*	Aquisição de bens ilícitos (drogas, armas, outros)
	Lavagem de Dinheiro	BTC, *Moneymules*, outros esquemas	Branqueamento de Capitais obtidos de forma ilícita
	Financiamento Terrorista	BTC, *Western Union*, Dinheiro Vivo	Transações ilícitas com o objetivo de financiar grupos com fins terroristas

[10] *Ransomware* é um tipo de *malware* que limita o acesso do utilizador ao sistema infetado cobrando um resgate (*ransom*) para que o acesso possa ser reestabelecido. Os *ransomwares* não permitem acesso externo ao computador infetado;
[11] *DDoS* – Ataque informático que tem como alvo servidores *web* e que tem como objetivo tornar os recursos de um sistema indisponíveis para os seus utilizadores;
[12] *Counter-Anti-Vírus* – é uma ferramenta desenhada para evitar a deteção por parte de *softwares anti-vírus* ou *anti-malware*, através de técnicas que disfarçam o seu conteúdo, normalmente mal-intencionado;
[13] *Malware* - é um termo geral utilizado para se referir a uma variedade de formas de *software* hostil ou intruso destinado a infiltrar-se num computador alheio de forma ilícita, com o intuito de causar alguns danos, alterações ou roubo de informações;
[14] *Hosting* - serviço que possibilita que pessoas ou empresas com sistemas *online* possam guardar informações, imagens, vídeo, ou qualquer conteúdo acessível por Web;
[15] Mais sobre *paysafecard* - https://www.paysafecard.com/pt-pt/produtos/paysafecard ; *Western Union* - https://www.westernunion.com; *WebMoney* - https://www.wmtransfer.com/eng/legal/codex.shtml ; e *Paypal* - *https://www.paypal.com/pt/home;*
[16] RATs - abreviatura de uma categoria de vírus que permitem que outros utilizadores controlem remotamente o computador infetado;
[17] *Banking trojans* – é um programa malicioso usado para obter informação confidencial sobre clientes de sistemas bancários *online* e de sistemas de pagamentos *online*;

Este dilema tem sido alvo de preocupação dos mais variados organismos internacionais e governos nacionais, tal como a *European Banking Authority* o fez notar em 2014:

> *"Os riscos (afetos aos sistemas de criptomoedas) são variados. Mais de 70 riscos diferentes foram identificados em variadas categorias, inclusive: riscos para utilizadores; riscos para os mercados; riscos à integridade dos sistemas financeiros, (lavagem de dinheiro e outras configurações de crimes financeiros); riscos aos sistemas de pagamentos; riscos para as autoridades reguladoras; entre outros. Simultaneamente as causas desses riscos foram também identificadas, assim como as medidas necessárias para a mitigação desses riscos. Os perigos inerentes passam pelo facto de os sistemas de criptomoedas serem potenciadores de esquemas fraudulentos; assim como pelo facto de alguns modelos de funcionamento descentralizado de alguns modelos de criptomoedas poderem ser alterados por algum nó de rede com maior poder computacional; ao mesmo tempo, outro perigo identificado é referente às questões de anonimização das partes envolvidas; ainda é preciso notar que o facto de não existir legislação regulatória aplicável consubstancia por si só, uma ameaça às partes envolvidas",* traduzido de European Banking Authority, 2014

1.1.1. Financiamento Terrorista e Lavagem de Dinheiro

As preocupações demonstradas quer por organismos reguladores, quer pelos mais variados opc's são justificadas pelas evidências existentes da utilização de criptomoedas num leque bastante vasto de atividades criminais previstas em grande parte das jurisdições mundiais e concretamente na jurisdição portuguesa. Note-se o facto de a utilização de criptomoedas como meio de troca ou de pagamentos não consubstancia por si só uma prática ilícita. Por outro lado, a sua utilização quando associada a tipificações de práticas criminais pode inserir-se no âmbito do cibercrime, quer através de práticas relativas à criminalidade informática, que através de práticas criminais com recurso a ferramentas informáticas.

No âmbito tratado neste subcapítulo, as atividades criminais com recurso a criptomoedas podem ser consumadas nomeadamente através das práticas de atividades de lavagem de dinheiro, designação pelo qual o crime de branqueamento de vantagens de proveniência ilícita é comummente conhecido e também pelas práticas de financiamento

terrorista, crimes previstos respetivamente pela Lei nº 25/2008, de 5 de junho e ainda pelo artigo do Código Penal Art. 368.º-A – Branqueamento – do Decreto de Lei nº 110/2015, de 26 de agosto e pelo Art. 5.º-A – Financiamento do Terrorismo da Lei nº52/2003, de 22 de agosto – Lei de Combate ao Terrorismo, respetivamente. Sobre este último, note-se a posição recente de organismos como a *European Police Office (*EUROPOL)[18] e a *The Financial Action Task Force* (FATF)[19] que, em sincronia, indicam que não existem evidências registas pelos aparelhos judiciais e de investigação criminal, da utilização de criptomoedas como método para financiar organizações terroristas. Referem também que a obtenção de financiamento destes grupos não tem sofrido alterações recentemente, continuando ainda a ser proveniente de atividades ligadas à exploração ilegal de petróleo, de crimes de sequestro e rapto com recurso a pedidos de resgate monetários, da venda de antiguidades furtadas (Moreira, 2015) e por parte de donativos privados pelos métodos tradicionais (EUROPOL, 2016). No entanto, o relatório *Emerging Terrorist Financing Risks* da FATF sugere que novos métodos de pagamento baseados em ferramentas tecnológicas podem surgir e figurar como uma vulnerabilidade emergente que pode crescer num futuro próximo (FATF, 2015).

Apesar do acima enunciado, alguns registos e documentos podem sugerir a utilização ou até mesmo o incentivo à utilização de criptomoedas como a BTC, como ferramenta para financiar organizações terroristas, como é o caso do *paper* publicado por *Amreeki Witness*, tido como um declarado apoiante da organização terrorista *ISIS*[20], denominado *Bitcoin and the Charity of Violent Physical Struggle*, onde declaradamente o autor apela a que os apoiantes da *Jihad*[21] utilizem soluções ligadas à tecnologia BTC com este fim (al-Munthir, 2014).

[18] Mais sobre EUROPOL - *https://www.europol.europa.eu/* ;
[19] Mais sobre *FATF* - *http://www.fatf-gafi.org/ ;*
[20] ISIS – *Islamic State of Iraq and Syria;*
[21] Termo árabe que significa "guerra santa";

"Para criar um Sistema de donativos completamente anónimo, capaz de enviar instantaneamente milhões de dólares em Bitcoins desde os Estados Unidos da América, Reino Unido, África do Sul, Gana, Malásia, Sri Lanka, ou qualquer outra geografia, diretamente para os bolsos da mujahideen[22] (...) O sistema (de bitcoins) (…) é simples, fácil e nós pedimos a Allah que acelere a sua utilização em nosso benefício.", traduzido de al-Munthir, 2014

De igual forma existem relatos de uma agência de transações financeiras da Indonésia - *Indonesian Financial Transactions Report and Analysis Cente* – que alertam para a utilização de *Bitcoins* no financiamento de organismos terroristas que operam através do Estado com maior percentagem de muçulmanos[23]. Esta situação já é inclusivamente alvo de preocupação por parte do governo indonésio, que registou um aumento para o dobro no que toca aos casos de financiamento a organizações terroristas no último ano (Jornal Económico, 2017).

Outras atividades criminais relacionadas com terrorismo podem também tirar recurso das redes digitais, ficando por isso consagradas pelo termo ciberterrorismo[24].

Na mesma medida estas preocupações ganham força quando equacionado o facilitismo que o protocolo *Bitcoin* e algoritmos semelhantes de outras criptomoedas vieram trazer à prática de crimes relacionados com a lavagem de dinheiro. Considerando a propagação da utilização das novas TIC na sociedade nos últimos anos, não é surpreendente que organizações criminais procurem explorar vazios legais ou técnicas que não os exponham, para alcançar os seus objetivos, cometendo assim velhos crimes, desta feita através de métodos modernos e com recurso a ferramentas informáticas.

Não é fácil precisar qual a dimensão dos montantes colocados em circulação que provêm de fontes ilegais, no entanto o Fundo Monetário Internacional (FMI) estima que pelo menos 600 milhares de milhões sejam "lavados" todos os anos, o equivalente a cerca de 1% do Produto Mundial Bruto (The World Factbook, 2016), sendo que a tendência de crescimento da utilização de técnicas sustentadas nos meios digitais é cada vez maior.

[22] Termo árabe cuja tradução remete para "guerreiro" ou "combatente", sendo comummente usado para fazer referência a alguém que se empenha na *jihad*, ou seja um guerreiro santo islâmico;
[23] Cerca de 88% da população da Indonésia declarou-se islâmica em 2010 (The World Factbook, 2016);
[24] Ciberterrorismo é o termo usado para descrever ataques terroristas executados com recurso à *Internet* e com o objetivo de causar danos a sistemas, redes ou equipamentos informáticos, geralmente através da sua intrusão e infeção com código malicioso.

Note-se, neste contexto, que o processo pelo qual as transações de criptomoedas se concretizam, circulando entre vários pontos da rede, com identidades protegidas criptograficamente, torna-as substancialmente mais difíceis de rastrear pelos organismos de investigação criminal. Estas características auxiliam os perpetradores desta prática específica na dissimulação necessária para colocar anonimamente dinheiro proveniente de fontes ilícitas em circulação, para qualquer lugar do mundo e em segundos, atuando de forma eficaz e sem deixar rasto (Böhme, Christin, Edelman, & Moore, 2015). Esta modalidade, também designada por *cyberlaundering*[25], é a forma mais segura para indivíduos ou organizações criminais, "lavarem" os seus fundos sem que instituições de governo, organismos de polícia, ou instituições bancárias percebam a origem do mesmo.

1.1.2. *Ramsomware* e *Sextortion*

De igual forma a pertinência do tema em estudo está ainda diretamente ligada à galopante ocorrência de ataques informáticos que se apoderam ilicitamente de informação crítica e/ou pessoal dos utilizadores e que, sob ameaça de a comprometerem ou até divulgarem, obrigam a que seja pago um resgate. Este é comumente solicitado em criptomoedas uma vez que os atacantes pretendem manter-se incógnitos.

Estes esquemas podem assumir diferentes formas, sendo que a maioria passa por atos de extorsão, onde alguém é coagido, por meio de ameaça ou violência, a agir de determinada forma com o objetivo de obter, para si ou para terceiros, vantagem, recompensa ou lucro, criminalizados em Portugal pelo Código Penal no Art. 223.º do Código Penal – Extorsão – do Decreto de Lei nº 110/2015. Os mais frequentes são conhecidos na gíria, por ataques de *ramsonware* e por *sextortion*[26].

No que concerne aos ataques denominados *ranmsonwares*, ou *crypto-ransomwares*, esta é uma realidade que afeta sistemas um pouco por todo o mundo e que tem como alvos ora máquinas de utilizadores individuais, ora máquinas corporativas ou de serviços de administração pública. As duas últimas são as mais procuradas por serem, normalmente mais rentáveis que os ataques a utilizadores individuais. São-no tendo em conta a criticidade da informação nestes contextos que por ser, muitas vezes, vital ao seu

[25] *Cyberlaundering* é o processo que se recursa de métodos de transferência eletrónica de fundos através da *Internet* como meio para disfarçar a fonte de fundos obtidos ilicitamente;

[26] *Sextortion* – refere-se à exposição e partilha de conteúdos (fotográficos ou vídeo) íntimos e do foro sexual, sem o consentimento da vítima, com o intuito de obter vantagens dessa partilha. Este tipo de crime acontece por norma nas redes sociais e tem um efeito psicológico altamente devastador sobre as vítimas (Polícia Judiciária, 2015);

pleno funcionamento, ou por se tratarem de dados pessoais sigilosos, fazem aumentar a probabilidade de pagamento do resgate. São-no também pelo facto de este tipo de código malicioso ter a capacidade de se difundir pela rede infetada e assim afetar um maior número de unidades, através da encriptação da informação que lá conste. Por isto o impacto causado na organização atacada tende a ser significativamente mais danoso, aumentando de igual forma a probabilidade de pagamento do resgate (Kaspersky Lab, 2016). Neste âmbito, Rogério Bravo, Inspetor-chefe da brigada de cibercriminalidade informática da Polícia Judiciária (PJ)[27], indicou estatísticas que referiam que cerca de 80% das vítimas passam por Técnicos Oficiais de Contas e Revisores Oficiais de Contas, assim como gabinetes de advogados, agrupamentos escolares e organismos que processem vencimentos (Bravo, 2015).

Em 2015 a incidência destes ataques aumentou 48,3% face ao ano anterior, tendo sido atacados nestes moldes mais 180 mil utilizadores. Há indícios que indicam ainda para uma tendência crescente na sofisticação dos ataques, alargando-se não só o espectro dos alvos como a robustez dos mesmos (Kaspersky Lab, 2015). Já no ano de 2016, os *softwares* de segurança *Kaspersky*[28], detetaram cerca de 1,5 milhões de infeções de *cryptoware* nos computadores onde corriam (Kaspersky Lab, 2016) . Esta combinação de fatores torna o combate a estas práticas criminosas mais difíceis, limitando a capacidade das autoridades, que se deparam desde início com a dificuldade de apurar a origem do ataque. A difusão geográfica do ciberespaço obriga, na maior parte dos casos a pedidos de cooperação internacional, tipicamente morosos e de resultado incerto.

Face a esta ameaça, novos desafios surgem no ambiente empresarial da era digital, obrigando a que seja repensado o próprio domínio da segurança de informação num contexto onde as mutações constantes dos ataques tornam sucessivamente obsoletos os protocolos, controlos e mecanismos de segurança existentes. Esta realidade obriga a que, por forma a salvaguardar a informação crítica e necessária ao normal funcionamento dos processos de negócio que tão importante é para a confidencialidade do segredo comercial e da consequente competitividade nos mercados, sejam sistematicamente repensados e reformulados os procedimentos e boas práticas relativas à utilização das TIC.

Outra das operações que tem vindo a envolver um substancial esforço operacional por parte dos opc's nacionais a quem esta matéria compete está relacionada com extorsões

[27] Mais sobre *PJ* - https://www.policiajudiciaria.pt/ ;
[28] Mais sobre *Kaspersky* - *https://www.kaspersky.pt/* ;

sexuais para as quais têm vindo a ser desenvolvidas estratégias preventivas e de alerta (Polícia Judiciária, 2015) (GNR | Protocolo internacional na área da cibersegurança, 2016). O fenómeno é comummente designado por *Sextortion* e passa essencialmente pela extorsão e coerção sexual de menores através de plataformas digitais. Este tipo de práticas, incorre na exploração sexual da vítima, ou na procura de práticas sexuais pedófilas, desde a transferência de imagens e/ou vídeos de cariz sexual do menor – *Child Sexual Exploitation Material* (CSEM) -, chegando até a atividades sexuais concretas. Muitas das vezes, o atacante procura obter ganhos financeiros através de técnicas de chantagem e/ou extorsão. Este processo habitualmente passa não só por um esquema de estratégias manipulativas com recurso a técnicas coercivas, ameaças e intimidação da vítima, mas também por técnicas de *deception* tais como engenharia social, *hacking*[29], e utilização de identidades falsas (EUROPOL, 2016).

O desconhecimento e ingenuidade de certos utilizadores que, conduzidos pela aliciação dos agentes criminosos, acabam por partilhar conteúdos íntimos é cada vez mais uma constante. Nesta matéria foi registado um aumento exponencial de casos em Portugal em 2015 face ao ano anterior (Polícia Judiciária, 2015).

O embaraço associado a estas situações tende a silenciar as vítimas, que nem sempre denunciam o crime. No entanto a utilização generalizada da utilização das redes sociais, onde nem todos os utilizadores têm o nível de educação mínimo para uma utilização segura, tornou-as uma plataforma tentadora para a prática deste tipo de crimes. A postura pouco prudente dos utilizadores alavancou este tipo de práticas que têm como consequência a sua exposição involuntária e resultante devassa grave da vida pessoal e profissional, assim como a vitimização em termos de extorsão e humilhação paralelamente ao efeito erosivo na confiança das vítimas.

1.1.3. Mercados negros

Outro dos aspetos que mais força dá à posição dos opc's e dos organismos reguladores tem que ver com utilização das criptomoedas em mercados ilegais *online* também conhecidos como mercados negros, que operam numa *Internet* paralela conhecida por *deepweb* ou *darknet*. Existentes fisicamente desde há muito, mercados com

[29] *Hacking* – atividade desenvolvida por indivíduos com fortes capacidades informáticas, com o objetivo de explorar configurações internas de dispositivos, programas e redes de computadores, que supostamente estariam seguros por mecanismos de segurança;

estas características caracterizam-se por estabelecerem uma plataforma de compra e venda de bens ilícitos. Com o advento da *Internet* e muito recentemente com o aparecimento das criptomoedas, estes mercados de comércio eletrónico ganharam força criando autênticas plataformas onde podem ser comercializados bens como armamento e drogas ilegais, conteúdos pedo pornográficos, mercadorias e objetos roubados ou contrafeitos dos mais variados tipos, conteúdos protegidos por direitos de autor, informação relativa a cartões de crédito, serviços de *hacking*, prescrições médicas, cópias de conteúdos protegidos por direitos de autor, entre outros.

Este fenómeno recente contribui para uma crescente economia paralela que tem no ciberespaço a sua origem, tirando recurso de certas características computacionais como a arquitetura de rede distribuída ponto-a-ponto, assim como das particularidades de *web browsers*[30] ou sistemas operativos[31] específicos, pautados pela possibilidade de navegar na rede anonimamente e sem que o endereço de *Internet Protocol* (IP) seja conhecido. Tiram ainda recurso das funcionalidades que as soluções de criptomoeda permitem, tais como as suas particularidades no que à total, ou parcial, anonimização diz respeito. Neste contexto, note-se que grande parte dos mercados existentes na *Darknet* têm já incorporado algum tipo de sistema de pagamento em criptomoeda na própria infraestrutura do *site* onde o mercado esteja alojado.

Esta combinação dificulta a investigação de um vasto leque de crimes que decorrem neste contexto singular, uma vez que a interceção de dados de tráfego, consubstanciada na legislação nacional através da Lei n.º 109/2009 de 15 de setembro - Lei do Cibercrime, que indiciem a prática de um crime é difícil de obter e raramente dá pistas claras, dificultando assim a identificação das partes envolvidas, assim como o bem transacionado e o valor alocada à transação para aquisição do bem.

Para que se perceba a dimensão do contexto em análise, um estudo de caso desenvolvido, em 2012, pelo *Information Networking Institute* da *Carnegie Mellon University*, relativo à plataforma ilegal de comércio eletrónico, *Silk Road*, a mais popular à data e que se tornou também na mais mediatizada aquando do seu encerramento resultante de uma

[30] TOR (*The Onion Router*) é uma solução de rede, gratuita e de código aberto, que pode ser utilizada através de um *web browser* e tem como particularidade o facto de garantir o anonimato dos utilizadores eu a utilizam para navegar na Internet, garantindo assim a privacidade da sua utilização;

[31] TAILS (*The Amnesic Incognito Live System*) é um sistema operativo criado com o objetivo de garantir a privacidade e segurança dos seus utilizadores. É frequentemente utilizado por utilizadores que querem contornar a censura de que podem ser vítimas em certos países. O sistema foi criado com uma série de soluções criptográficas que trazem segurança a quem o usa. No mesmo sentido tem a opção de utilizar redes que garantam o anonimato na navegação, como é o caso da rede TOR;

investigação encabeçada pelo *Federal Bureau Investigation* (FBI) em 2013, indica que as transações movimentadas no mercado *Silk Road* correspondiam entre 4,5% a 9% do total de transações na moeda *Bitcoin*. Tendo em conta a capitalização de mercado da BTC no período compreendido pelo estudo, esta percentagem corresponde a cerca de 15 milhões de USD movimentados através da plataforma, ou seja, transacionados internacionalmente no comércio de bens ilegais. Note-se que estes dados são referentes unicamente ao mercado *Silk Road* e apenas um ano depois da plataforma começar a utilizar esta criptomoeda como moeda de troca (Christin, 2012), sendo, por isto, uma pequena alusão ao cenário real do fluxo de capitais atual. Os últimos dados apontam para um aumento de cerca do triplo do número de traficantes dedicados a este negócio *online*, passando de 1031 em 2013 para 2744 em janeiro de 2016 (Kruithof, et al., 2016). As figuras 2 e 3 demonstram o estado da situação em termos de nº de vendedores e nº de transações registadas em janeiro de 2016, mediante país de origem.

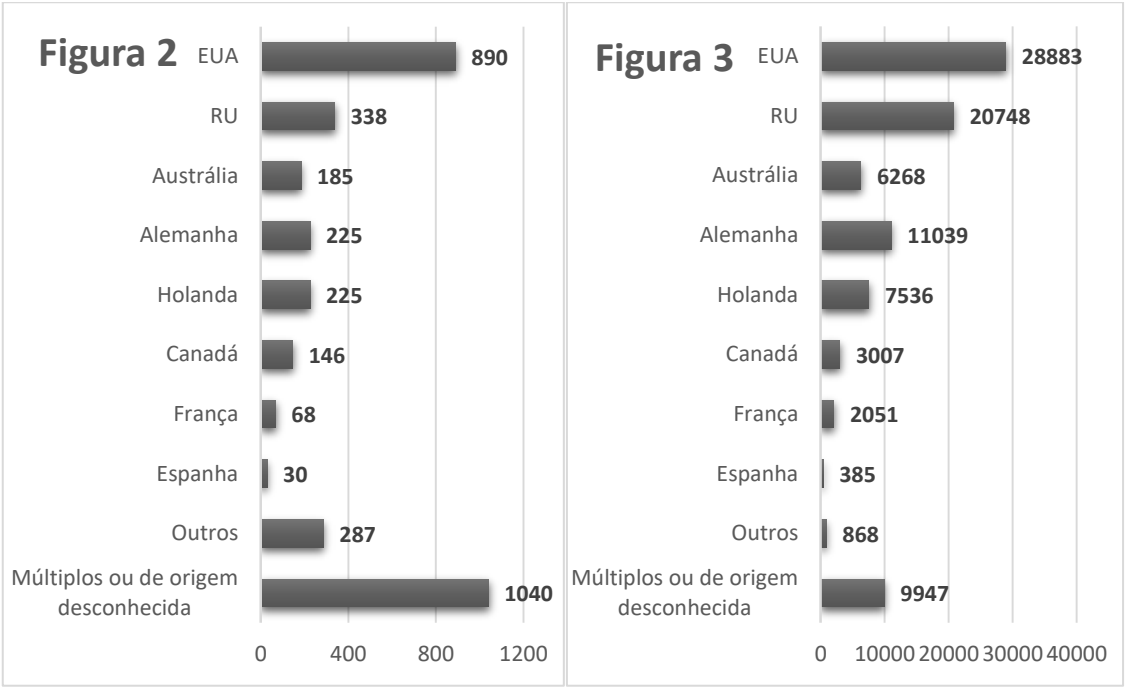


Figura 2 - Nº de vendedores registados em janeiro de 2016[32] (Kruithof, et al., 2016)
Figura 3 - Nº de transações registadas em janeiro de 2016[32] (Kruithof, et al., 2016)

[32] Os dados apresentados na Figura 2 e 3 consideram os seguintes mercados *AlphaBay, Cryptomarket, Dark Net Heroes League, French Dark Net, Dreammarket, Hansa, Nucleus, Python;*

É expectável que com o relativamente recente desenvolvimento de *interfaces friendly-user*, no que às redes anonimizadas diz respeito, o acesso às mesmas tenha crescido, uma vez a capacidade técnica dos utilizadores é cada vez menos um entrave à sua utilização. Contribuiu de igual forma para a generalização do conhecimento desta realidade e para o despertar da curiosidade da população, o mediatismo que envolveu o caso do julgamento e prisão de *Ross Ulbricht*, fundador e administrador da plataforma *Silk Road.* Acresce a isto o facto de os mercados anónimos *online* terem emergido substancialmente após o encerramento desta plataforma que, até ao término das suas operações figurava sozinha, disseminando cerca de 30 novos mercados com a mesma tipologia, no ano seguinte (Böhme, Christin, Edelman, & Moore, 2015), fazendo com o que o número e volume das transações triplicasse de 2013 para 2016 (Kruithof, et al., 2016). Este fenómeno tornou a luta judicial, contra esta renovada forma de crime, mais difícil tendo em conta que compradores e vendedores se dispersaram em diferentes pontos da rede, tornando a identificação dos mesmos ainda mais remota, tal como prova a Tabela 2 que, fazendo jus à ineficácia referida no combate a este tipo de criminalidade, indica o número de condenações registadas neste âmbito. Posto isto, novas questões surgem quanto à forma de combater esta criminalidade, sendo pouco claro se o encerramento das plataformas de venda com maior dimensão reduz realmente o comércio ilegal nestes moldes.

Tabela 2 - Número de condenações, motivo e país por crimes relacionados com mercados negros online (Gwern, 2016)

	Comprador	*Administrador ou fundador*	*Vendedor*	*Programador ou moderador*	*Desconhecido*	***Total***
EUA	99	2	44	4	6	155
Nova Zelândia	25	-	-	-	11	36
Alemanha	9	-	7	1	12	29
RU	12	-	13	-	2	27
Austrália	18	-	5	1	-	24
Suécia	-	-	19	-	-	19
Holanda	-	2	14	1	-	17
Áustria	6	-	2	-	-	8
Irlanda	-	-	7	1	-	8
Canadá	-	-	6	-	-	6
Índia	5	-	-	-	-	5
Noruega	1	-	4	-	-	5
Outros	10	2	6	2	-	20
Total	**185**	**6**	**127**	**10**	**31**	**359**

No contexto nacional é do conhecimento geral que a PJ tem investigações em curso neste âmbito, no entanto não se conhece ainda a dimensão nacional que os mercados que operam na *darknet* têm em termos de consumidores e traficantes (Coelho, 2016).

1.1.4. Ponto da situação

Todos os desafios acima elencados tornam a análise proposta pertinente tendo em conta o contributo significativo das criptomoedas para um crescente número de diferentes configurações na forma como se dão os crimes modernos no ciberespaço, desta feita num espaço operacional pouco regulado legalmente e onde os organismos de polícia criminal e as autoridades judiciais têm ainda dificuldade em operar quer em termos de prevenção, de investigação quer de punição.

No contexto nacional a criação da Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica (UNC3T) vem dar força a esta ideia, tal como é comprovado pelo decreto de lei transcrito abaixo, que demonstra a preocupação nesta

matéria, que por si só, é reveladora da dimensão do desafio em mãos e da necessidade em alocar esforços e meios para uma luta que se crê que acontecerá cada vez com maior incidência no ciberespaço.

> *"O desenvolvimento de uma estratégia adequada de combate ao cibercrime pressupõe que as entidades responsáveis pela respetiva prevenção e repressão detenham informação (cyber-intelligence) em tempo útil que possibilite, não só a deteção precoce de ataques digitais, mas também a compreensão da intenção criminosa associada ao uso, à comercialização e à disseminação de programas maliciosos. O estabelecimento de uma política criminal coerente para o cibercrime deve possibilitar uma atuação imediata (...) daí que se torne necessário a Polícia Judiciária reforçar o ajustamento com as estruturas europeias e internacionais de informação e contrainformação criminal (...) tendo em vista a luta eficaz contra o cibercrime assente na recolha e partilha de informações criminais (...) a unidade operacional especializada na Polícia Judiciária, típica de uma Polícia Científica, que permita alcançar a necessária resposta estrutural, preventiva e repressiva ao fenómeno do cibercrime e do ciberterrorismo, e que é inspirada no modelo adotado pelo EC3 (European Cybercrime Center) da EUROPOL, cujos pontos focais são o abuso sexual de crianças através da Internet, a fraude com os cartões e outros meios de pagamento eletrónico e virtuais, a criminalidade informática pura e a criminalidade praticada com recurso a meios informáticos."* (Decreto Lei nº 81/2016 de 28 de novembro, 2016)

Também a existência de uma estratégia nacional de segurança no ciberespaço, legalmente tipificada em Diário da República, através da Resolução do Conselho de Ministros n.º 36/2015 (Diário da República, 2015) é, por si só, reveladora da importância dada à questão, tendo sido fundada no compromisso de aprofundar a segurança das redes e da informação, como forma de garantir a proteção e defesa das infraestruturas críticas e dos serviços vitais de informação, e potenciar uma utilização livre, segura e eficiente do ciberespaço por parte de todos os cidadãos, das empresas e das entidades públicas e privadas.

Em tom de fecho, é compreensível que o intervalo deixado aberto entre as inovações tecnológicas já mencionadas e a dificuldade em combater quem delas tira partido, deu aso à exploração crescente de crimes como os enunciados acima. Dá força a

esta tendência crescente a complexidade em tipificar o conteúdo das atividades ilícitas consumadas no ciberespaço, não só devido à sua complexidade intrínseca como também devido à sua mutação constante e ao ambiente difuso onde as mesmas ocorrem. Esta conjuntura tornou ainda mais árdua a tarefa de prevenir as ameaças e de as combater, tanto por parte das entidades responsáveis operacionais como os opc's, como por parte dos indivíduos, das entidades gestoras no caso das empresas e até ao nível dos aparelhos de administração pública e de governo, tornando este tipo de crimes apetecíveis a quem ilegitimamente procura tirar partido para si, ou para interposta pessoa, ou até prejudicar ou causar dano ao seu alvo, através de técnicas informáticas sofisticadas.

Posto isto, é então pertinente refletir sobre esta temática por forma a compreender a dimensão do dilema em mãos, pesando o impacto e dano causados e assim perceber quais as consequências para vítimas e criminosos, no sentido de tentar prever qual a tendência futura e consequentes resultados deste tipo de práticas na sociedade.

2.Enquadramento conceptual e Modelo de Análise

2.1. Enquadramento conceptual

Figura 4 – Principais dimensões de análise

2.1.1. Criminalidade Informática

Na não existência de uma universalização conceptual consensual para criminalidade informática, fenómeno também designado por cibercrime, este acaba por ser um termo que é normalmente enquadrado mediante a enumeração das práticas que engloba. Assim o contextualiza a Organização das Nações Unidas (ONU) através de 14 comportamentos passíveis de constituírem cibercrimes, tal como esquematizado através da Tabela 3. Estes estão subdivididos em três categorias, são elas: Atos contra a confidencialidade, integridade e disponibilidade de dados e sistemas informáticos; Atos praticados através de computador para obtenção de benefícios pessoais ou financeiros; e Atos praticados através de computador cujo conteúdo incite a ódio, apoio terrorista ou explore pornografia infantil; (ONU, 2013).

Tabela 3 – Esquema conceptual para definição de práticas de cibercrime, adaptado e traduzido de (ONU, 2013)

Atos contra a confidencialidade, integridade e disponibilidade de dados e sistemas informáticos	• Acesso ilegal a Sistema informático; • Acesso ilegal, interceção ou aquisição de dados informáticos; • Interferência ilegal com sistema ou dados informáticos; • Produção, distribuição ou posse de ferramentas para uso indevido de computador; • Violação de meios de proteção de dados ou privacidade;
Atos praticados através de computador para obtenção de benefícios pessoais ou financeiros	• Fraude ou falsidade informática; • Ofensas relacionadas com a identidade praticadas através de computador; • Ofensas relacionadas com direitos de autor e marcas registadas praticadas através de computador; • Envio ou controlo do envio de *spam*; • Atos praticados através de computador que causem danos pessoais; • Solicitação e aliciamento de crianças através de computador;
Atos praticados através de computador cujo conteúdo incite a ódio, apoio terrorista ou explore pornografia infantil	• Incitamento ao ódio através de computador; • Produção, distribuição ou posse de pornografia infantil praticada através de computador; • Atos de apoio ao terrorismo praticados através de computador;

Já a Comissão Europeia define cibercrime como todos "*os atos criminosos praticados com recurso a redes de comunicação eletrónicas e sistemas de informação ou contra este tipo de redes e sistemas*". Acrescenta ainda que este termo se aplica a três categorias de atividades criminosas: a primeira abrange as formas tradicionais de criminalidade tais como a fraude ou a falsificação, mas num contexto específico de crimes cometidos em redes de comunicações eletrónicas e sistemas de informação; a segunda faz referência à publicação de conteúdos ilícitos em meios de comunicação eletrónicos tais como pornografia infantil, incitamento ao ódio racial, entre outros; por fim a terceira categoria é respeitante aos crimes exclusivos das redes eletrónicas, isto é, ataques contra sistemas de informação, bloqueio de serviços e pirataria (Comissão Europeia, 2007).

Posto isto, a divisão do conceito de cibercrime ganha duas dimensões: uma mais ampla e uma outra onde assume um conceito mais restrito. No sentido mais alargado enquadram-se as práticas criminais que acontecem através de meios informáticos, mesmo

que estes se afigurem apenas como um meio instrumental para a sua prática. Por outro lado, a conceptualização mais restrita diz respeito apenas aos crimes em que os meios digitais podem ser enquadrados como objeto do tipo legal de crime, sendo por isso indispensáveis à consumação do mesmo.

No entanto, é importante frisar que a conceptualização da cibercriminalidade implica a equação de um leque alargado de variáveis e variantes que dificultam a sua definição. Em termos ordinários pode considerar-se a versão digital de crimes que já aconteciam, isto é, não fosse a sua execução no ciberespaço, seriam crimes ditos tradicionais.

No contexto nacional, a criminalidade em meio informático pode consubstanciar-se, segundo a legislação portuguesa através da Lei nº 109/2009, de 15 de Setembro – Lei do Cibercrime, nos seguintes crimes: Falsidade informática, Dano relativo a programas ou outros dados informáticos, Sabotagem informática, Acesso ilegítimo, Interceção ilegítima, Devassa da vida privada, Devassa por meio informático, Violação de correspondência ou telecomunicações, Gravações e fotografias ilícitas, Furto e Burla Informática (APAV, 2016). Considere-se ainda, neste âmbito, a importância dos dados informáticos[33] e dos dados de tráfego[34] como meios de obtenção de prova em ambiente digital, dos quais a responsabilização criminal e a aplicação penal muito depende.

Note-se no entanto e face ao contexto de abordagem às criptomoedas deste estudo, tal como já foi referido no subcapítulo 1.1.1., que a utilização de criptomoedas como meio de troca ou de pagamentos não consubstancia por si só uma prática ilícita. Por outro lado, a sua utilização quando associada a tipificações de práticas criminais pode inserir-se no âmbito do cibercrime, quer através de práticas relativas à criminalidade informática, quer através de práticas criminais com recurso a ferramentas informáticas.

[33] Dados informáticos são qualquer representação de factos, informações ou conceitos sob uma forma suscetível de processamento num sistema informático, incluindo os programas aptos a fazerem um sistema informático executar uma função;

[34] Dados de tráfego» são os dados informáticos relacionados com uma comunicação efetuada por meio de um sistema informático, gerados por este sistema como elemento de uma cadeia de comunicação, indicando a origem da comunicação, o destino, o trajeto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente;

2.1.2. Criptomoeda

A criptomoeda, designação dada ao dinheiro existente exclusivamente sob a forma de informação criptografada, teve destaque em 2009 com o aparecimento de uma moeda única e exclusivamente digital, autossustentável e descentralizada de uma organização reguladora e fiscalizadora, que ganhou forma sob o lançamento *online* do algoritmo *Bitcoin*, que deu nome à criptomoeda que se encontra mais estabelecida atualmente, *Bitcoin*. Até há relativamente pouco tempo a autoria desta invenção era atribuída ao pseudónimo *Satoshi Nakamoto*, por ser esse o nome com o qual estava assinado o documento (Nakamoto, 2009) que descreve o algoritmo e que foi avançado *online* aquando do lançamento desta nova tecnologia. No entanto, o mistério no qual estava envolta a autoria do sistema BTC foi desvendado no início de MAI2016, quando após cinco meses de investigações levadas a cabo pelas autoridades australianas, o empresário *Craig Steven Wright*, assumiu numa entrevista à BBC, ser o criador da moeda virtual *Bitcoin* (BBC, 2016).

A tecnologia BTC está assente numa infraestrutura semelhante às restantes criptomoedas, sendo que os processos de funcionamento podem divergir do sistema BTC em algumas particularidades, no entanto os princípios base de arquitetura onde o sistema assenta, se regem, na sua grande maioria, pelas mesmas regras. Em termos genéricos e considerando o sistema BTC como exemplo, considerando sempre as semelhanças dos restantes sistemas de criptomoedas, a tecnologia tira recurso de uma arquitetura de rede distribuída, ou P2P, na qual os nós da rede que através do software *Bitcoin*, fazem correr o algoritmo, competem entre si, com a sua capacidade de processamento, para validar soluções criptográficas efetivando assim as transações. Este mecanismo, também conhecido por prova de esforço, ou *proof-of-work*, envolve esforço das partes que tentam decifrar os problemas criptográficos. Em caso de sucesso, esse esforço é recompensado com atribuição do montante de criptomoeda gerado através da solução da transação, ao nó de rede que conseguiu resolver o problema primeiro. A este processo dá-se o nome de *mining*. Note-se que a recompensa é tanto maior quanto maior for o nível de dificuldade – *hashrate* - em desconstruir a transação, isto é, uma transação de um montante elevado, tem como consequência um maior nível de informação associada, medido em *bytes*, e obrigará por isso a um maior esforço para a sua resolução. Esta mecânica torna desnecessária a intermediação das operações por parte de terceiros (Grinberg, 2011). Esta distribuição de esforço pelos nós de rede funciona de igual forma

como sistema de segurança, sendo que qualquer alteração ao algoritmo tenha de ser do acordo de todos, não podendo nenhuma ponto de rede discordar para que se dê tal alteração.

Outra das características deste sistema passa pelo total, ou parcial anonimato dos utilizadores, dependendo da criptomoeda em questão e dos processos inerentes ao seu funcionamento. Note-se que apesar de existir um registo público, denominado *Public Ledger*, onde estão elencadas todas as transações existentes desde o primeiro montante de BTC transacionado, está total, ou parcialmente garantido o anonimato de identidade e da localização de cada uma das partes envolvidas através de mecanismos criptográficos e de soluções de rede. A plataforma pública onde se encontram todos os registos de transações *Bitcoin* denomina-se *BlockChain.*

Um exemplo do funcionamento detalhado de uma transação é enunciado no subcapítulo 4.1.2.2..

2.1.3. Segurança de Informação

O domínio de segurança de informação está intrinsecamente relacionado à proteção de dados, informação ou de um conjunto de informações, assim como às esferas da segurança informática, de computadores e de sistemas. Em alguns casos e num contexto empresarial, a informação fora de suportes computacionais ou eletrónicos, pode entrar numa política de segurança de informação a par da segurança física e da segurança da infraestrutura tecnológica (ISO/IEC, 2005).

Este conceito ganhou ênfase com a generalização da utilização de ferramentas computacionais e soluções tecnológicas por parte dos indivíduos, empresas, administração pública e aparelhos governativos. Esta transformação tornou valiosos e por vezes sensíveis os conteúdos de um indivíduo ou de uma organização, cujo propósito seja útil fazendo, por isso, com que as suas propriedades de informação devam ser asseguradas. Note-se que pode estar em causa informação dos mais diferentes tipos, graus de sigilo e das mais variadas dimensões. Esta pode tanto ser relativa a clientes que exigem, com sustentação legal, que seja dado o devido tratamento aos seus dados, como pode também ser informação relativa a dados fiscais de toda a população de um Estado, bases de dados de palavras-chave, correspondência trocada através de correio eletrónico ou contatos telefónicos, faturação e dados bancários ou pode até estar por exemplo, em causa

informação de documentos confidenciais, ou mesmo segredos comerciais, entre outros tipos de informação (ISO/IEC, 2005).

O paradigma atual indicia os dados digitais e a informação gerada através desses dados, como os principais produtos da Era da informação, reforçando a ideia da urgência da sua conveniente proteção que pode ser ameaçada por fatores comportamentais dos seus utilizadores, pelo ambiente e infraestruturas em que está alojada, por intrusão indevida dos sistemas e possível acesso, danificação ou até roubo.

Face a este contexto onde novos riscos potenciais ameaçam o mundo empresarial, começa a surgir uma consciencialização dos gestores de empresas para esta necessidade urgente. Para enfrentar este desafio devem ser implementados controlos de segurança com o intuito de minimizar o nível de exposição ao qual as empresas estão expostas e assim garantir a segurança daquele que, muitas vezes, é o seu principal património e o garante da sua competitividade no mercado, a informação. Neste sentido algumas estratégias tecnológicas, organizacionais e humanas devem ser estudadas e implementadas transversalmente. Fazem parte deste leque de soluções a definição de políticas, normas e procedimentos, a formação e consciencialização dos utilizadores de sistemas para esta problemática, controlo de acessos físicos e lógicos, auditorias periódicas àquilo que envolve os processos considerados mais críticos, implementação de soluções criptográficas se necessário, gestão de incidentes, políticas de segurança das redes, entre outras medidas que permitam contribuir para a salvaguarda das propriedades de informação, listas de seguida (ISO/IEC, 2005):

- Disponibilidade – garantir que a informação esteja sempre disponível para ser utilizada quando os utilizadores necessitarem;
- Integridade – garantir a exatidão da informação face àquilo que são as suas características originais ou prévias alterações autorizadas;
- Confidencialidade – garantir que o acesso à informação é exclusivo a quem de direito, ou seja, apenas para entidades autorizadas;
- Autenticidade – garantir que a informação é autêntica;
- Não-repúdio – garantir que qualquer acesso, visualização ou modificação, seja identificado e por isso não possa ser negado;

É crucial que qualquer organização reconheça a importância da sua informação e a hierarquize mediante o seu nível de importância para que seja possível identificar que recursos devem ser alocados à gestão da sua proteção.

Este dilema de segurança não é exclusivo do contexto empresarial, embora possa ser nele que o impacto é maior. Ao nível dos indivíduos a realidade obriga a que sejam tomadas algumas precauções aquando da utilização das novas TIC, como foi já referido. Nem sempre as soluções habituais de utilização de um *anti-vírus* atualizado e de uma *firewall* ativa são suficientes para proteger a informação fornecida voluntária ou involuntariamente pelos utilizadores singulares. É necessário por isto que exista um *awareness* para estas questões para que a utilização seja prudente e os dados fornecidos o sejam somente quando do outro lado estiver um indivíduo ou entidade em quem se confie.

2.2. Modelo de Análise

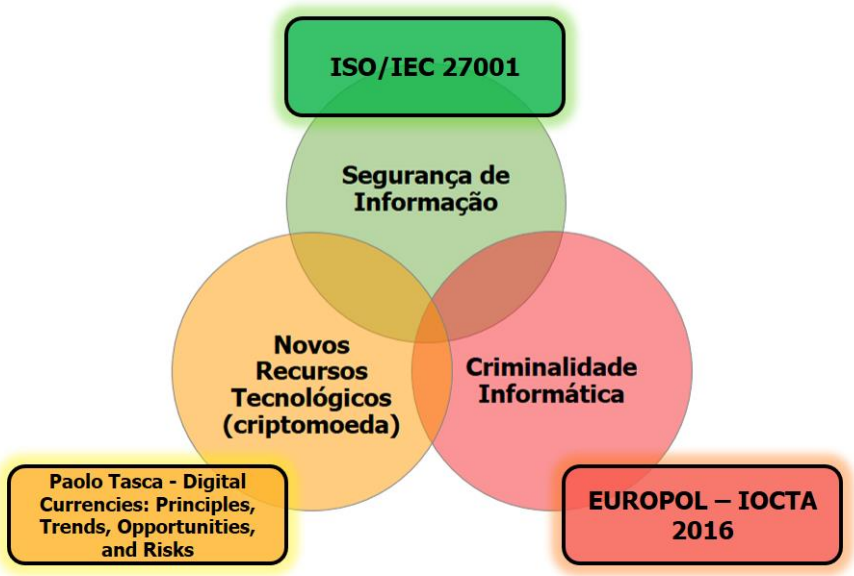


Figura 5 - Principais dimensões de análise e respetivos modelos de análise

Em termos esquemáticos, a Figura 5 apresenta a relação entre os principais conceitos ou dimensões de análise, nos quais o estudo vai incidir e os modelos de análise que servirão como referencias para sua sustentação.

Definiu-se ter como base para a dimensão de segurança de informação o referencial *International Organization for Standardization* (ISO) 27001 – Manual de procedimentos para a Gestão da Segurança de Informação - tendo em conta ser a referência, em meio corporativo, no que toca ao controlo eficaz da segurança da informação, com base nos princípios da confidencialidade, integridade, autenticidade e disponibilidade. (ISO/IEC, 2005). Por ser um *standard* internacional de referência, consideram-se as empresas certificadas e respetivos processos, seguidores das normas e procedimentos mais eficientes, trazendo confiança e reconhecimento a colaboradores, parceiros e clientes.

Dentro da mesma lógica, o relatório da EUROPOL – *Internet, Organised Crime Threat Assessment* (IOCTA), de 2016, será o modelo base de referência para análise da dimensão: Criminalidade Informática; considerou-se a competência e o reconhecimento da organização autora do relatório como uma das forças de polícia criminal de referência, que contou com contribuições das polícias competentes das temáticas em questão, dos 28 estados membro da União Europeia, analisadas pelo *staff* especializado da EUROPOL em colaboração com parcerias cooperativas no mundo empresarial, financeiro e até académico. O estudo em questão aborda questões chave aos níveis da criminalidade informática moderna, respetivas evoluções e tendências registadas no último ano e as principais ameaças resultantes (EUROPOL, 2016).

Por fim, definiu-se como referência para a dimensão dos novos recursos tecnológicos (criptomoeda) um relatório técnico rigoroso e detalhado que resulta numa análise quantitativa profunda e estruturada, transversal às várias áreas do conhecimento influenciadas pelo fenómeno das criptomoedas. Produzido pelo economista e académico *Paolo Tasca em 2015*, "*Digital Currencies: Principles, Trends, Opportunities, and Risks*", com o apoio para a investigação do *Deutsche Bundesbank* e da *Fintech* suíça ECUREX, o relatório descreve as inovações recentes no setor financeiro, com especial enfoque na tecnologia *Blockchain* e na *criptomoeda Bitcoin* numa análise multinível: sistémica, técnica, legal e aplicativa. Em paralelo, perspetiva tendências futuras com o intuito de dar a compreender oportunidades potenciais e riscos decorrentes da adoção de criptomoedas, à escala global (Tasca, 2015). Pela profundidade do estudo, por analisar e relacionar diferentes dimensões num mesmo contexto, pelo reconhecimento atribuído às instituições que promoveram o estudo e principalmente pelo autor que o concebeu, uma personalidade com provas dadas neste campo, definiu-se também este ensaio como referência de base à investigação.

3.Objetivos, Problema e Metodologia de Investigação

3.1. Objetivos da Investigação

Os objetivos deste trabalho de investigação passam por avaliar a crescente utilização de criptomoedas, no sentido de analisar as ocorrências da sua utilização em esquemas tipicamente ilícitos em meio eletrónico, ou através dele. Note-se neste âmbito que, apesar de ser referido, no decorrer do trabalho, o potencial das criptomoedas como uma ameaça para diferentes grupos, o objetivo último passará sempre por estudar a sua utilização em esquemas ilícitos. Neste sentido, compreenda-se que o fenómeno nunca aqui será considerando como uma ameaça *per si*. Ao invés disso, aquilo que aqui é enunciado como tal, são as atividades ilícitas que aliadas ao potencial das criptomoedas aquando da sua consumação, se tornam uma ameaça para a sociedade, assim como os desafios que paralelamente decorrem deste fenómeno. Ao mesmo tempo objetiva-se ainda perceber o consequente impacto causado na sociedade portuguesa, quer sejam atividades criminais dirigidas a indivíduos singulares ou mesmo a empresas, ou aparelhos de administração pública. Este enquadramento geral, assim como as respostas às questões de investigação levantadas permitirão perceber a proporção do problema em mãos. Ao mesmo tempo será importante perceber como lidam os órgãos de polícia criminal nacionais com este novo desafio.

Numa conjuntura que obriga a repensar o próprio domínio de segurança de informação, na medida em que novas ameaças podem obrigar a novos desafios para os quais devem ser equacionadas medidas preventivas e possivelmente até alterações nos antigos procedimentos por forma a salvaguardar informação crítica, pretende-se ainda conhecer qual o nível de *awareness* para esta realidade, assim como qual o impacto nas medidas e protocolos de segurança na gestão deste dilema de segurança no contexto empresarial.

Assim e de forma abreviada, definiram-se os seguintes objetivos:

- Enquadrar as ameaças em ambiente digital e analisar especificamente os crimes informáticos ou com recurso a ferramentas informáticas como é o caso da utilização das criptomoedas em ilícitos;
- Perceber genericamente qual o grau de sensibilização dos cidadãos portugueses, organismos do Estado e empresas nesta matéria;

- Analisar o impacto da consumação deste tipo de atividades nas empresas e nos órgãos administrativos;
- Compreender e analisar a posição das forças e serviços de segurança interna nesta matéria, nas esferas da investigação, deteção e intervenção em contexto nacional, ou em cooperação internacional;
- Perspetivar tendências futuras em termos de prevenção e capacidade de resposta para as ameaças identificadas por parte dos organismos reguladores e de polícia;

3.2. Formulação do Problema

A problemática apresentada encerra, a montante, uma questão central (QC):

QC ——> Qual a dimensão e impacto da utilização de criptomoedas na consumação de atividades criminais?

Desta QC foram deduzidas quatro questões derivadas (QD) cujas respostas deverão fundamentar esta investigação:

QD1 ——> De que forma estão organizações e indivíduos sensibilizados e preparados para ameaças em ambiente digital?

QD2 ——> Que crimes informáticos se recursam das criptomoedas para a sua consumação, ou que têm nelas um veículo para tal?

QD3 ——> Como é que as criptomoedas ameaçam empresas e indivíduos?

QD4 ——> Quais as perspetivas futuras quer em termos de incidência quer em termos de segurança?

No sentido de tratar tanto a QC como as QD's acima apresentadas, foram estabelecidas as seguintes hipóteses de resposta, que se esperam ver fundamentadamente validadas no decorrer da investigação:

H1 ——> O nível de sensibilização para estas questões é, na sua grande maioria, baixo, não estando as organizações e os indivíduos preparados para utilizar as TI de forma consciente e segura, face à exposição ao risco a que estão sujeitas;

H2 ⟶ Os crimes são consumados em algum momento através do ciberespaço, sendo que os mais frequentes passam pelo financiamento terrorista, lavagem de dinheiro obtido de forma ilícita, comércio e consumo de bens ilegais e até crimes de extorsão comummente conhecidos por *ramsonware* e *sextorsion*;

H3 ⟶ Fruto da tipologia das ferramentas utilizadas para a consumação dos crimes em ambiente digital, assim como da, cada vez maior, presença de informação crítica, a empresas e indivíduos, no ciberespaço, a ameaça é crescente, decorrendo da exposição a que está sujeita e do valor dessa mesma informação. Note-se ainda que a ameaça contempla um impacto substancial tendo em conta as consequências que delas advém, tais como o prejuízo na reputação do alvo atacado;

H4 ⟶ Estima-se que a incidência seja crescente no futuro, o que obrigará a uma abordagem mais eficiente dos opc's paralelamente a uma necessária consciencialização da população para estas ameaças, por forma a atenuar o seu impacto e assim aumentar a segurança da sociedade e ramo empresarial, em Portugal;

Posto isto e por forma a esquematizar o acima exposto, a Tabela 4 apresenta a matriz conceptual do trabalho de investigação.

Tabela 4 – Matriz conceptual do Trabalho

Questão Central	**Questões Derivadas**	**Hipóteses**
Qual a dimensão e impacto da utilização de criptomoedas na consumação de atividades criminais?	De que forma estão organizações e indivíduos sensibilizados e preparadas para ameaças em ambiente digital?	O nível de sensibilização é, na sua grande maioria, baixo, não estando as organizações e os indivíduos preparados para utilizar as TI de forma consciente e segura, face à exposição ao risco a que estão sujeitas;
	Que crimes informáticos se recursam de criptomoedas para a sua consumação, ou que têm nelas um veículo para tal?	Crimes consumados em algum momento através do ciberespaço, sendo os mais frequentes o financiamento terrorista, lavagem de dinheiro, comércio de bens ilegais e até crimes de extorsão;
	Como é que as criptomoedas ameaçam empresas e indivíduos?	A ameaça é crescente e crítica, decorrendo da exposição a que está sujeita a informação no ciberespaço e do respetivo valor, contemplando um impacto substancial tendo em conta as consequências que delas advém, tais como o prejuízo na reputação do alvo atacado;
	Quais as perspetivas futuras quer em termos de incidência quer em termos de segurança, no contexto nacional?	Estima-se que a incidência será crescente e obrigará a uma abordagem mais eficiente dos opc's paralelamente à consciencialização da população para estas ameaças, por forma a atenuar o seu impacto e assim aumentar a segurança da sociedade e ramo empresarial, em Portugal;

3.3. Abordagem

A abordagem de cariz qualitativo será a mais comummente utilizada no decorrer desta investigação exploratória, considerando que, apesar de serem usadas métricas no decorrer da mesma, serão essencialmente estudados fenómenos de natureza social de elevada novidade, para os quais a complexidade de comportamentos, perspetivas e fenómenos sociais, assim o exigem.

Tendo em conta a complexidade e inovação das temáticas abordadas e por forma a obter uma perspetiva transversal às diferentes dimensões de análise será consultado um painel de individualidades especializadas e com conhecimento vasto em alguma das dimensões de análise do estudo, constituído por personalidades cujas qualificações e/ou experiências profissionais lhes confiram perícia nas matérias que compõem ora a problemática geral do tema, ora uma das variáveis em estudo. A natureza do modelo de investigação definido, através das referidas entrevistas semi-estruturadas, advém da novidade do tema e consequente escassez de outras fontes dos domínios de conhecimento de fronteira em causa, tendo acabado por se revelar o método de investigação exploratório mais adequado. É apresentado de seguida e através da Tabela 5, um esquema de planificação do painel de especialistas a consultar, relativamente a cada uma das dimensões.

Neste sentido, definiu-se um painel de reconhecido mérito para cada uma das dimensões de análise, considerando, para a dimensão da criminalidade informática, algumas personalidades das forças de segurança nacionais e dos organismos de polícia, assim como das estruturas da política nacional para a cibersegurança. Relativamente à dimensão da segurança de informação, equacionaram-se indivíduos representantes das infraestruturas críticas nacionais, assim como outros especialistas ligados ao mundo empresarial e concretamente ao ramo da segurança informática. Por fim, para a dimensão dos novos recursos tecnológicos (criptomoedas) selecionou-se um painel de personalidades que possam contribuir com perspetivas variadas de quem esteve e/ou está, direta ou indiretamente relacionado e envolvido no mundo das criptomoedas, seja na vertente técnica, de negócio ou de utilizador.

Tabela 5 - Planificação do painel de especialistas a consultar

Dimensões de Análise	Personalidades a entrevistar
Criminalidade Informática	▪ **CAlm Gameiro Marques** – Diretor do Gabinete Nacional de Segurança[35]; ▪ **Rogério Bravo** – Inspetor-chefe da PJ para a área do cibercrime; ▪ **Carlos Cabreiro**- Diretor da UNC3T da PJ;
Segurança de Informação	▪ **Paulo Moniz –** Diretor de Segurança de Informação e Risco nas TIC da EDP[36]; ▪ **José Pereira -** Coordenador do Núcleo de Segurança, Comunicações e Centro de Dados da ESPaP[37]**;**
Novos recursos tecnológicos (criptomoedas)	▪ **M. Valente –** R&D Lead da *FullIT*[38]**;** ▪ ***"Riclas"*** - *Pro Trader* na plataforma de *Exchange LocalBTC*[39];

3.4. Metodologia de recolha e análise de informação

Para a materialização deste trabalho de investigação e no sentido de preservar o rigor científico a que se propõe, será aplicado o método Hipotético-dedutivo[40], segundo o qual se procurará uma reposta válida à questão central já identificada e assim contribuir para o conhecimento científico ao enquadrar o panorama da utilização de criptomoedas na criminalidade digital nacional.

Para tal serão utilizadas fontes documentais e bibliográficas, assim como estudos empíricos de interesse, tais como relatórios, artigos, livros, publicações em revistas relacionadas com o tema e conteúdos publicados *online* que se tenham revelado

[35] Mais sobre *Gabinete Nacional de Segurança* - *https://www.gns.gov.pt/ ;*
[36] Mais sobre *EDP* - *https://www.edp.com/ ;*
[37] Mais sobre *ESPaP* - *https://www.espap.pt/ ;*
[38] Mais sobre *FullIT* - *https://fullit.pt/ ;*
[39] Mais sobre *LocalBTC -; https://localbitcoins.com/ ;*
[40] O método hipotético-dedutivo é uma metodologia de investigação científica cuja construção parte de postulados identificados como modelo de interpretação do fenómeno estudado. O modelo gera, através de um trabalho lógico, hipóteses, conceitos e indicadores para os quais se terão de procurar correspondentes no real, conduzindo à questão central formulada *à priori*;

fidedignos e pertinentes para o objeto de estudo. Serão ainda consideradas como fontes de informação os contatos diretos feitos pelo autor, sob a forma de entrevistas a personalidades e organismos de interesse, representativos dos *stakeholders*. As mesmas serão semiestruturadas e adaptadas ao contexto profissional do entrevistado e à dimensão de análise segundo o qual cada entrevista decorre, tal como esquematizado no Apêndice 1.

Será tido em conta o rigor científico e a qualidade dos conteúdos que servem de base bibliográfica a este trabalho. Para mais, a abordagem qualitativa segundo a qual serão extraídos os contributos recolhidos em contexto das entrevistas seguirá uma abordagem denominada análise temática, concebida por Braun & Clarke, 2006, segundo a qual os dados recolhidos serão identificados, analisados e agrupados em categorias e padrões, ou temas, seguindo um método estruturado com vista à resolução do fenómeno em investigação. A análise temática processa-se através de seis fases que objetivam criar e estabelecer padrões concretos: Familiarização com os dados; Geração de códigos iniciais; Pesquisa de temas comuns entre os códigos; Revisão dos temas; Definição e denominação dos temas; e Produção do relatório final; (Braun & Clarke, 2006). Note-se ainda que este método de análise tem em conta a interpretação própria do autor o estudo.

Os conteúdos mencionados e referenciados e que servem de suporte à sustentação das ideias apresentadas são selecionados com base numa pesquisa exploratória que objetiva procurar e estabelecer hipóteses que serão testadas no decorrer da investigação. Essa análise dá lugar a uma descrição que identifica e classifica os elementos em observação, para mais tarde levar a cabo uma averiguação analítica dos resultados provenientes da fase exploratória, procurando localizar, identificar e relacionar as variáveis e causas em análise. Desta forma, a recolha de dados provenientes das fontes acima enunciadas e a sua interpretação deverá permitir validar as hipóteses e assim estabelecer de forma sustentada a explicação do problema.

Por fim, a investigação passará por uma análise preditiva e exploratória traçando, com base num racional, tendências futuras, tendo em perspetiva tanto a análise de dados como as evidências disponíveis e referenciadas na bibliografia.

Em todas as fases a investigação promete ser interrogativa, precisa e objetiva assim como garante ainda ser fruto de uma profunda revisão de literatura, consciente conhecimento do estado da arte e relacionamento das várias dimensões em presença.

3.5. Delimitações e dificuldades

Espera-se que a maior dificuldade possa ser sentida ainda na fase de recolha de informação e análise bibliográfica, tendo em conta o fenómeno recente em causa, onde os estudos já efetuados sobre as criptomoedas se prendem mais com a sua vertente tecnológica e arquitetura do que com a sua utilização criminal. Para mais, tendo em conta a especificidade do âmbito da investigação proposta, uma das limitações será a inexistência de estudos semelhantes com os quais se possam confrontar os resultados obtidos. Ainda que seja procurada informação num âmbito mais genérico, por exemplo relativo ao cibercrime, a limitação mantém-se tendo em conta a dificuldade em tipificar de forma unânime o tipo de criminalidade. Este fator oferece sérios obstáculos à existência de uma métrica rigorosa que permita avaliar a verdadeira dimensão e intensidade da problemática do cibercrime.

De igual forma, pode considerar-se uma outra dificuldade na recolha de informação e que está relacionada com a dimensão da amostra de personalidades entrevistadas. Considerando ser um tema emergente, para o qual algumas personalidades podem não estar confortáveis em prestar declarações sobre, fruto do contexto profissional onde se inserem, pode ter influência no número de entrevistas conseguidas.

Note-se ainda uma outra limitação deste estudo relacionada com a dificuldade de combater a cibercriminalidade com o quadro legal nacional existente, tendo em conta a constante mutação dos crimes praticados que são frequentemente e premeditadamente alterados por forma a não preencherem características do tipo criminal e assim evitar que possam ser penalmente responsabilizados pelos atos cometidos. Esta dificuldade afastou o autor de uma análise transversal a todo o processo criminal, isto é, uma análise que fosse desde a execução até à condenação do criminoso, por motivos de complexidade da questão e da incerteza associada em adquirir resultados concretos. Neste sentido, note-se ainda que, não obstante o contexto nacional, este tipo de práticas, criam dificuldades nunca enfrentadas anteriormente pelas autoridades, nomeadamente no que à recolha de provas digitais diz respeito. Esta complexidade provém de uma série de características típicas entre as quais a transnacionalidade da prática, onde as restrições territoriais são irrelevantes no ciberespaço, assim como das ferramentas de anonimização já abordadas e as complexas tecnologias utlizadas. Esta sequência acontece frequentemente em processos criminais decorridos no ciberespaço, comprovando-se que a lei está muitas vezes desajustada temporalmente da realidade praticada (Natário, 2013).

Uma análise de cariz legal e mais concretamente uma análise aos resultados efetivos da investigação criminal e respetiva condenações dos infratores poderá servir no futuro como um complemento à investigação em apreço. No entanto, neste momento e em contexto nacional especificamente, é clara a dificuldade em combater este fenómeno recente, tendo em conta que existem mais variantes de cibercrimes do que direito penal aplicado ao ciberespaço que cubra este tipo de crimes, fruto do que foi acima explanado. Assim é preciso ter em conta que apesar de o cibercrime ser, para a legislação nacional um conceito sedimentado e penalmente punível, as respostas legais existentes são ainda, muito incipientes. Outras complicações surgem no momento da investigação criminal começando na dificuldade legal de definir etimologicamente aquilo que se tenta regular através da legislação, uma vez que nem sempre é possível definir com exatidão "onde" ocorrem os crimes, nem através de que "meio" são cometidos. Por estes motivos e com intuito de restringir o âmbito de investigação, optou-se por deixar, para já, de parte as questões relacionadas com conteúdos legais.

4.Revisão da Literatura

A revisão literária efetuada equacionou estudos empíricos de interesse, tais como relatórios, artigos, livros, publicações em revistas relacionadas com o tema e conteúdos publicados *online* que se tenham revelado fidedignos e pertinentes para o objeto de estudo. Assim a exploração teórica serviu o propósito, na medida em que contribuiu, no entender do autor, para um maior domínio das temáticas em análise assim como para um conhecimento profundo do saber atual da comunidade científica, da imprensa, dos órgãos criminais e das organizações internacionais relativamente às dimensões de análise da investigação.

Neste sentido, optou-se por subdividir a observação detalhada do estado da arte do problema em estudo, nas diferentes dimensões de análise: Criminalidade Informática; Criptomoeda; e Segurança de Informação; equacionando duas obras para cada uma, sendo que as obras a que é feita referência neste capítulo são aquelas que foram consideradas, pelo autor do estudo, as mais válidas por contemplarem um maior rigor científico e por serem ao mesmo tempo atuais e consensualmente aceites pela comunidade científica, servindo de fonte para os estudos subsequentes, e em simultâneo por se ter verificado serem as mais adequadas no contexto desta investigação.

Note-se ainda que não foram encontrados estudos que equacionassem conjuntamente as mesmas dimensões de análise do presente, pelo que as obras apresentadas de seguida podem parecer desconectas, no entanto, servem o propósito de dar a conhecer o estado da arte de cada dimensão em análise *per si.* Para além disto deve ainda ser feita uma ressalva para o facto de não existirem, até à data, estudos públicos que relacionem esta realidade criminal específica no contexto nacional, pelo que não há sustento bibliográfico que sirva de suporte e/ou de confrontação para a questão da limitação geográfica definida para análise deste ensaio.

4.1. Estado da Arte

4.1.1. Criminalidade Informática

4.1.1.1. - Relatório da EUROPOL – *Internet, Organised Crime Threat Assessment* (IOCTA), de 2016;

Este que é também o documento que, neste estudo, serve de referencial para a análise da dimensão "Criminalidade Informática" aborda questões aos níveis da criminalidade informática moderna, respetivas evoluções, mudanças chave e tendências registadas no último ano e as correspondentes principais ameaças resultantes no ciberespaço.

Considerando que as recentes evoluções nas soluções computacionais aliadas aos recursos de rede têm vindo a facilitar o crescimento do cibercrime, este relatório dedica especial enfoque a três áreas específicas: os ciberataques, a exploração sexual infantil *online*; e fraudes nos pagamentos; começando por enfatizar a temática referindo que o incremento no volume, âmbito e configurações das práticas, aliadas ao risco assimétrico da realidade do cibercrime, atingiu um nível tal em certos países da União Europeia, que o registo de incidentes ocorridos no ciberespaço ultrapassou o registo de incidentes ditos tradicionais. Neste âmbito muito contribuiu a maturação do crime como um serviço – *Crime-as-a-Service* (CaaS). Um modelo transversal ao espectro da cibercriminalidade no que toca ao fornecimento de ferramentas e prestação de serviços, frequentemente procurados por grupos organizados extremistas, *hackers*[41] e/ou *hacktivistas*[42] na procura de meios que facilitem as suas operações. Note-se neste âmbito que as transações monetárias entre criminosos – Criminal to criminal (C2C) - têm, intransigentemente e por interesse de ambas as partes, de ser levadas a cabo com o maior nível de segurança e anonimato possíveis, sendo por isso as trocas em criptomoedas escolhidas preferencialmente.

[41] *Hackers* - indivíduos que se dedicam, a conhecer, explorar e modificar aspetos internos de dispositivos, programas e redes de computadores, que supostamente estariam seguros por mecanismos de segurança;

[42] *Hacktivistas* – termo proveniente da junção entre *hacker* e ativismo, faz referência a quem desenvolve atividades de *hacking* com o fim de promover ideologias políticas, democracia, anti corrupção, anti opressão, liberdade de expressão, direitos humanos, ou outro ideal humanista;

Em termos de técnicas específicas de ataque o relatório faz referência a novas configurações de ataques de *phishing*[43] e de *DDoS*, mais complexos e de difícil resolução, dando, no entanto, especial destaque a ameaças mais frequentes atualmente, tais como *ramsonwares* e *banking trojans*, considerando que esta será uma tendência que não se alterará num futuro próximo.

Assim, o *ramsonware* foi considerado, pela EUROPOL, como sendo a ameaça-chave para os utilizadores do ciberespaço em 2016 e possivelmente nos anos consequentes, sendo por esse motivo uma das inquietações predominantes dos aparelhos legais da União Europeia, em matéria do digital. Os motivos desta preocupação prendem-se com um maior número de incidências que resultam de um vasto leque de novas configurações de ataque, denominadas *cryptoware,* sendo que cada uma tem características e propriedades únicas dificultando o seu combate. Para além do emprego de novas estratégias de comunicação anónimas, tais como utilização das redes Tor ou *Invisible Internet Project* (I2P)[44], os ataques atingiram níveis de sofisticação técnica profissional, oferecendo inclusivamente demonstrações gratuitas de desencriptação de ficheiros existentes na máquina infetada, como forma de provar a funcionalidade do sistema. Para além disto, e enquanto o início deste ciberataque se pautava por ataques a vulnerabilidades existentes em versões desatualizadas do sistema operativo (SO) *Windows,* atualmente algumas configurações dos ataques de *ramsonware* têm potencial para infetar um vasto leque de dispositivos móveis, assim como redes complexas típicas do setor industrial ou de aparelhos de governo. Independentemente da variante do ataque o método de pagamento do resgate é quase sempre pedido exclusivamente em criptomoedas, com grande preferência pela criptomoeda *Bitcoin* pela proteção em termos de anonimato que este tipo de sistemas oferece.

Outro dos pontos abordados pelo estudo passa pela extorsão e coerção sexual de menores através de plataformas digitais. Este tipo de práticas, tal como já foi explicitado anteriormente, incorre na exploração sexual da vítima menor de idade, ora com propósito

[43] *Phishing* – designa uma técnica de ataque informático que tem como objetivo a obtenção de informação pessoalmente identificável através de uma suplantação de identidade por parte de criminosos em contextos informáticos;

[44] I2P - é um *software* livre que disponibiliza o acesso a uma rede paralela à rede web e que permite que as aplicações de software enviem e recebam mensagens para outros na rede e de forma segura, sob pseudônimos, anonimizando os *users*;

sexual propriamente dito, ora na procura de obter ganhos financeiros através de técnicas de chantagem e/ou extorsão.

Apesar de os espaços operacionais mais comuns para este tipo de práticas serem plataformas onde os registos podem ser consultados, tais como redes sociais, jogos virtuais *online*, fóruns e outras aplicações frequentemente utilizadas pelos mais novos, a EUROPOL indica que mais de 45% dos agressores dão continuidade às ameaças em caso do não cumprimento das suas exigências por parte da vítima.

Outro fenómeno preocupante é ainda descrito pelo relatório como uma ameaça crescente e que passa pelo abuso sexual de crianças em direto e à distância, através de partilha de vídeo em *streaming*[45]. Esta disseminação de conteúdos abusivos, que tem depois continuidade sendo esses mesmos registos partilhados em redes P2P e em *sites* alojados em *internets* paralelas, contribui para o incremento da divulgação de CSEM, sendo em simultâneo uma fonte de receita para quem possui e partilha este tipo de conteúdos.

Mais uma vez a criptomoeda e especificamente a *Bitcoin*, assume um papel importante neste tipo de atividades, sendo normalmente a moeda de troca tanto no momento da extorsão entre agressor e vítima como no momento da partilha de conteúdos pedo pornográficos.

Relativamente à alusão que é feita às fraudes nos sistemas de pagamentos, o grande destaque é dado a fraudes resultantes de transações onde o cartão de pagamento não está presente – *Card-not-present* (CNP) – das quais advêm cerca de 66% do valor total das fraudes cometidas, um aumento considerável face ao ano anterior. Este fenómeno afetou variados setores e diferentes empresas que comercializam os seus produtos e serviços através de plataformas *e-commerce* e que são vítimas de pagamentos efetuados com cartões de crédito comprometidos. Geralmente os atacantes encontram uma vulnerabilidade no sistema de pagamentos da plataforma onde vão adquirir o bem ou serviço e exploram-no antes que seja identificado.

Em tom conclusivo, o *Internet Organized Crime Threat Assessment 2016* faz referência à utilização crescente dos recursos de anonimização e encriptação assentes em serviços e ferramentas utilizados com fins ilegais e que se afiguram como um sério

[45] *Streaming* – é uma transmissão contínua digital, que acontece numa rede através de pacotes, é frequentemente utilizada para distribuir conteúdo multimédia através da *Internet*;

impedimento à deteção, investigação e condenação dos criminosos em matéria de cibercrime. Neste sentido, a EUROPOL sugere um maior enfoque no desenvolvimento de *awareness* entre utilizadores e prevenção transversal, no que diz respeito a procedimentos e processos que podem aumentar o nível de cibersegurança de uma organização, num esforço combinado e cooperativo ao nível comunitário europeu e em linha com as parcerias público-privadas e o setor empresarial (EUROPOL, 2016).

4.1.1.2. - Relatório de *Maria Garnaeva, Fedor Sinitsyn, Yury Namestnikov, Denis Makrushin, Alexander Liskin, "Kaspersky Security Bulletin – Overall Statistics for 2016",* com o apoio da *Kaspersky Lab,* de 2016;

O relatório em análise é elaborado por uma organização que desenvolve e comercializa soluções de segurança dirigidas às TIC, sendo por isso todas as estatísticas apresentadas pelo mesmo, obtidas através da *Kaspersky Security Network* (KSN), uma rede distribuída de antivírus que aplica vários componentes de proteção *anti-malware*[46]. Os dados foram concedidos por utilizadores do antivírus, sendo provenientes de 213 países de todos os continentes, que assim participaram na troca global de informação com vista à análise de atividades maliciosas na *Internet.* Note-se que apesar da veracidade e do rigor do apresentado, este estudo tem por base apenas os dados recolhidos pela KSN, e que são afetos aos clientes que usam soluções de segurança *Kaspersky.* Por isto, os dados apresentados, não refletem a totalidade dos dados de interesse nesta matéria, representando apenas uma amostra.

Kaspersky Security Bulletin começa por apresentar alguns números por forma a dar uma ideia do cenário geral, do ano de 2016, no que toca à criminalidade informática, onde destaca que 31,9% dos computadores analisados foram alvo de *malware*, tendo sido infetados via *online.* Aponta ainda aos 261 774 932 URLs (*Uniform Resource Locator*) descobertos com algum tipo de código malicioso e aos 69 227 289 objetos de *software* maliciosos. No mesmo sentido 1 445 434 computadores foram alvos de ferramentas de encriptação, na sua grande maioria com recurso a criptomoedas para pagamento do resgate e consequente desencriptação de ficheiros.

Após esta apresentação sumária com alguns apontamentos de destaque do cenário criminal no ciberespaço, o *report* subdivide-se em quatro partes de relevo, tendo em conta aquilo que foi o panorama do cibercrime no ano de 2016, são elas: Aplicações vulneráveis

[46] *Anti-malware* - aplicações de *software* que que detetam e eliminam *malware;*

à exploração para ciberataques; Ameaças *online* (*web-based attacks*[47]); Ataques de *Crypto-ramsonware*; finalizando com uma secção onde mostra quais os países onde os utilizadores enfrentam maior risco de infeção *online;*

Assim e começando pela análise das aplicações vulneráveis à exploração para ciberataques verificou-se, em 2016, que a tendência verificada nos anos anteriores se mantém. Confirma-se assim que aplicações como *Adobe Flash Player*[48] (8% do total), *Microsoft Office* (13% do total) e *Internet Explorer* (50% do total) continuam a ser as preferidas dos cibercriminosos, tal como mostra a Figura 6, onde é evidente o predomínio da exploração dos *browsers* (cerca de 50% do total), através do alojamento de *exploits*[49], nas páginas *web,* para serem distribuídos a quem lhes aceder. Também aplicações baseadas em *Java*[50], assentes em sistema operativo *Android, Adobe Reader*, se encontram entre as mais exploradas.

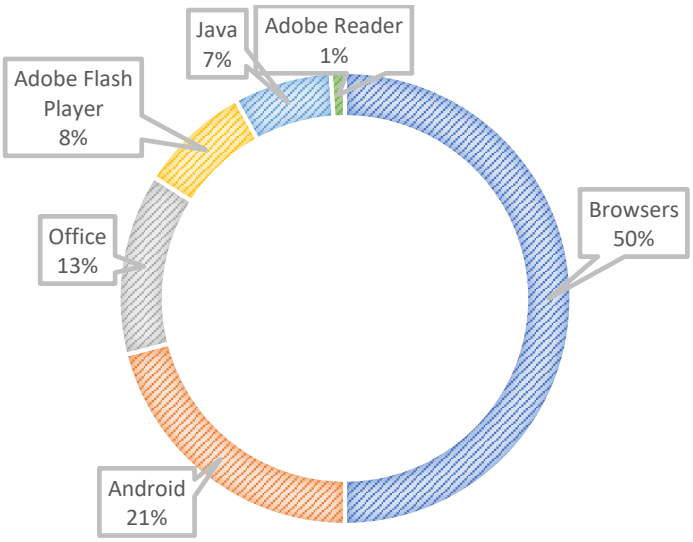


Figura 6 - Gráfico com distribuição em % dos exploits usados nos ciberataques, por aplicação atacada, em 2016, adaptado de (Kaspersky Lab, 2016)

[47] *Web based attacks* – Também denominados *web threats* é qualquer ataque informático que utilize a *world wide web* com o fim de cometer um crime informático;
[48] Mais sobre *Adobe Flash Player* em: http://get.adobe.com/flashplayer/about/ ; sobre *Microsoft Office* em*:* *http://get.adobe.com/flashplayer/about/ ;* e sobre *Internet Explorer* em: https://www.microsoft.com/en-us/download/internet-explorer.aspx ;
[49] *Exploits* – Um *exploit* é uma técnica de ataque informático que toma vantagem de um defeito, falha ou vulnerabilidade a fim de causar um comportamento acidental ou imprevisto a ocorrer no *software* ou *hardware* de um computador ou noutro dispositivo;
[50] Mais sobre *Java* em*:* *https://www.java.com/en/ ;* sobre Sistema Operativo *Android* em*:* *https://www.android.com/ ;* e sobre *Adobe Reader* em: https://get.adobe.com/reader/?loc=br;

Relativamente às ameaças *online,* ou *web-based attacks,* os antivírus *web* da *Kaspersky Lab* detetaram 69 277 289 objetos maliciosos, tais como *scripts*[51]*, exploits,* ficheiros executáveis, entre outros. Face a isto as soluções da *Kaspersky* detetaram e bloquearam mais de 758 milhões de ataques, alavancados por recursos *online,* localizados em 212 países espalhados pelo mundo. Neste âmbito foram identificados os 20 programas maliciosos, tal como demonstrado na Figura 7, mais frequentemente utilizados em ataques *online,* em 2016, sendo estes responsáveis por 96,6% dos ataques dados neste contexto. É percetível que a grande fatia dos ataques analisados nesta dimensão se devem a URLs maliciosos[52], seguidos de *Trojans*[53] de diferentes tipos. Os restantes tipos de ataques têm uma expressão diminuta, inferior a 1%.

	Nome	% do total de ataques
1	Malicious Url	77,26
2	Trojan-Clicker.HTML.Iframe.dg	8,15
3	Trojan.Script.Generic	6,74
4	Trojan.Script.Iframer	3,14
5	Trojan-Downloader.Script.Generic	0,35
6	Exploit.Script.Generic	0,20
7	Packed.Multi.MultiPacked.gen	0,15
8	Trojan.JS.Fbook.bh	0,13
9	Exploit.Script.Blocker	0,11
10	Trojan-Downloader.JS.Iframe.div	0,11
11	Trojan.JS.Redirector.ns	0,09
12	Trojan-Dropper.VBS.Agent.bp	0,08
13	Trojan-Downloader.JS.Agent.hjc	0,08
14	Trojan.JS.Iframe.ako	0,07
15	Trojan.Win32.Generic	0,06
16	Trojan.Win32.Generic	0,06
17	Trojan.JS.Agent.ckf	0,05
18	Trojan-Spy.HTML.Fraud.gen	0,05
19	Trojan.Win32.Invader	0,04
20	Exploit.SWF.Agent.gen	0,04

Figura 7 – Lista com os 20 programas maliciosos mais utilizados em 2016 (Kaspersky Lab, 2016)

[51] *Scripts* – é uma linguagem de programação que suporta scripts ou programas escritos para um sistema de tempo de execução especial que automatiza a execução de tarefas que poderiam alternativamente ser executadas uma por vez por um operador humano;
[52] URLs maliciosos - Um URL malicioso refere-se ao endereço de rede no qual se encontra algum recurso informático malicioso;
[53] *Trojans* - é um malware que entra no computador e cria uma porta para uma possível invasão;

No que concerne a ataques de *crypto-ransomware*, este que é um dos tópicos do relatório da *Kaspersky* que mais diretamente está relacionado com esta dissertação, é indicado que esta é uma ameaça crescente devido às novas variantes e diferentes modificações nos *malwares* desta categoria já existentes, por forma a conseguir contornar as soluções e controlos de segurança existentes. Nesta conjuntura, foram detetados durante o ano, mais de 54 mil modificações de *ramsonwares*, de 62 "famílias"[54] diferentes.

Assim, em 2016, quase 1,5 milhões de utilizadores das soluções assentes na *Kaspersky Security Network* foram atacados por algum tipo de ataque deste tipo. É importante considerar que o número real de incidentes é superior ao apresentado pelo estudo. Para além de nem todas as vítimas utilizarem soluções da *Kaspersky* e os números aqui apresentados são respeitantes ao grupo de utilizadores que as utilizam, dá-se ainda o caso de nem todos os ataques desta categoria serem considerados como tal. Isto pode dever-se à tipologia ou morfologia do ataque que, por se desviar do ataque de *ramsonware* típico ou conhecido pelas soluções *Kaspersky*, ou até por ser demasiado recente e por isso desconhecido das soluções *Kaspersky*, não sendo assim considerado como tal. Nota para o facto de, independentemente da sua morfologia, o resgate ser, na grande maioria das vezes, solicitado em criptomoedas.

O estudo elenca ainda as famílias de *ramsonwares* mais utilizadas pelos atacantes e as quais detêm um maior número de registos, como está representado na Figura 8. Assim o *cryptoware CTB-Locker* continua a ser o que detém maior número de registos (25,32%), seguido do *Locky* (com 7,07%) e do *TeslaCrypt* (6,54%). Uma breve ressalva para o facto de o *cryptoware – CTB Locker* - mais utilizado estar alojado na rede TOR, podendo ser disseminado a partir da mesma, tornando mais resiliente e atribuindo-lhe características de anonimidade, tornando remota a atribuição do ataque.

[54] Entenda-se por diferentes famílias, as diferentes arquiteturas de *software* sobre as quais podem assentar os *malwares* da categoria dos *crypto-ramsonwares,* embora se enquadrem dentro da mesma categoria de vírus;

	Nome	Fonte	% de vítimas atacadas
1	CTB-Locker	Trojan-Ransom.Win32.Onion / Trojan-Ransom.NSIS.Onion	25,32
2	Locky	Trojan-Ransom.Win32.Locky / Trojan-Dropper.JS.Locky	7,07
3	TeslaCrypt	Trojan-Ransom.Win32.Bitman	6,54
4	Scatter	Trojan-Ransom.Win32.Scatter / Trojan-Ransom.BAT.Scatter / Trojan-Downloader.JS.Scatter / Trojan.Dropper.JS.Scatter	2,85
5	Cryalk	Trojan-Ransom.Win32.Cryalk	2,79
6	CryptoWall	Trojan-Ransom.Win32.Cryptodef	2,36
7	Shade	Trojan-Ransom.Win32.Shade	1,73
8	(generis verdict)	Trojan-Ransom.Win32.Snocry	1,26
9	Crysis	Trojan-Ransom.Win32.Crusis	1,15
10	Cryrar/ACCDFISA	Trojan-Ransom.Win32.Cryrar	0,90

Figura 8 - Top 10 das famílias de ramsonware mais utilizadas (Kaspersky Lab, 2016)

O *report* faz ainda referência ao facto de a grande fatia das vítimas deste tipo de ataques (22,6%) pertencer ao setor corporativo. Tal como já foi referido no subcapítulo 1.1.2. esta tendência deve-se à criticidade da informação em ambiente empresarial, assim como ao número de máquinas ligadas à mesma rede e pelas quais o *malware* se pode espalhar, o que tem como resultado uma maior probabilidade de pagamento do resgate. As famílias de *cryptowares* utilizados para atacar o ambiente empresarial não variam significativamente, à exceção de um, denominado *Trojan-Ransom.Win32.Rakhni.* Esta arquitetura de *crypto-ramsonware* foi muito utilizada neste contexto e assume uma tipologia diferente, através da qual é disseminado por um ficheiro *downloader*, denominado *Trojan-downloader.Win32.Rakhni*. Este *downloader* é um ficheiro executável, embutido num documento .docx, e direcionado ao alvo, anexado via *e-mail*. Este ataque específico combina técnicas de *social engineering* uma vez que é normalmente dirigido aos departamentos de recursos humanos, dissimulando ser uma candidatura a uma oferta de emprego, onde um ficheiro enviado em anexo e que aparenta ser um *Curriculum Vitae* perfeitamente normal, quando, no entanto, contém um *cryptoware* que é desencadeado e começa a correr sem que a vítima se perceba. Segundo o relatório este ataque específico revelou-se extremamente eficaz e com uma tendência crescente de utilização nos ataques ao setor empresarial.

Por fim, o *report* faz ainda alusão aos países nos quais os utilizadores estão mais expostos ao risco de serem vítimas de *cryptoware*, com base nos registos levantados pela KSN. Os resultados servem como indicador da "agressividade" do ambiente no

ciberespaço, em diferentes partes do globo e podem ser consultados na Figura 9. Assim e de acordo com a categorização feita pelos autores do estudo, existem dois países no grupo de alto risco: Rússia (42,15%) e Cazaquistão (41,22%), cada um com mais de 40% de incidência na totalidade de máquinas com soluções de segurança *Kaspersky*; assim como existem 105 países no grupo de médio risco: entre os quais se registou uma incidência entre 20% a 39,99% na totalidade de máquinas com soluções de segurança *Kaspersky* e dos quais se destacam países como a Ucrânia (39%), o Brasil (38,83%), Espanha (38,23%), a China (36,53%), Portugal (35,86%), França (34,74%), a Turquia (29.3%), Canadá (29.5%), a Polónia (28.7%), a Austrália (26.2%), a Alemanha (26.2%), a Bélgica (25.3%), a Áustria (24.8%), os Estados Unidos da América (24%), a Suíça (23.6%), o Reino Unido (22.13%), entre outros.

	Estado	% de potenciais vítimas
1	Rússia	42,2
2	Cazaquistão	41,2
3	Itália	39,9
4	Ucrânia	39,0
5	Brasil	38,8
6	Azerbaijão	38,8
7	Espanha	38,2
8	Bielorrússia	38,0
9	Algéria	37,1
10	Vietnam	36,8
11	China	36,6
12	Portugal	35,9
13	França	34,7
14	Arménia	33,0
15	Grécia	32,9
16	Chile	32,8
17	Índia	32,6
18	Qatar	32,5
19	Indonésia	32,3
20	Moldávia	31,4

Figura 9 – Top 20 dos países onde os utilizadores estão mais sujeitos a cryptowares (Kaspersky Lab, 2016)

4.1.2. Criptomoeda

4.1.2.1. - Relatório de *Paolo Tasca, "Digital Currencies: Principles, Trends, Opportunities, and Risks"*, com o apoio para a investigação do *Deutsche Bundesbank* e da *Fintech* suíça *ECUREX*, de 2015;

Este que é também o referencial, neste estudo, para a análise da dimensão "Novos Recursos Tecnológicos (Criptomoeda)" é um relatório exaustivo e minucioso que contou com o apoio do *Deutsche Bundesbank*[55] assim como da *ECUREX Research and University of Zurich, Department of Banking and Finance*[56] que descreve as inovações trazidas para o setor financeiro pelas criptomoedas, através de uma análise às tendências, riscos e oportunidades desta transformação. Note-se que o estudo compreende um período específico de 4 anos, entre 2011 e 2015, sendo que é, dentro da bibliografia existente, o mais recente com este nível de rigor científico.

O autor começa por abordar o propósito da investigação referindo que o mote para o desenvolver passou essencialmente pela não existência de um estudo abrangente às criptomoedas que providenciasse uma profunda e conjunta análise quantitativa e qualitativa dos seus aspetos técnicos, aplicativos, económicos e legais. A seu ver as peças informativas existentes não passam de um manancial de informação disperso por artigos pouco rigorosos e pautados pela falta de investigação de suporte e de conhecimento técnico na área. Apesar de a obra começar com alguns capítulos introdutórios explicativos da mecânica e funcionamento do sistema BTC em si, esta obra merece destaque pelas conclusões de investigação alcançadas, que se revelam de maior interesse neste âmbito e que trazem novidades, até então não conhecidas no ecossistema das criptomoedas. Por este motivo, deixarei para já de parte a questão da mecânica e funcionamento do sistema BTC, a qual será, detalhadamente explicada, na análise do artigo Böhme, Chrsitin, Edelman, & Moore, 2015 sobre o qual me debruçarei de seguida no subcapítulo 4.1.2.2., ainda na dimensão de análise – Criptomoeda.

Em termos sumários o autor chegou a conclusões interessantes tal como é o facto de o montante médio transferido em USD, por cada transação através da rede de pagamentos *Bitcoin* ser, desde o segundo trimestre de 2013, superior ao homólogo em qualquer outra rede de pagamentos, tais como *VISA, Mastercard, Discover ou Western*

[55] Mais sobre *Deutsche Bundesbank* - *https://www.bundesbank.de;*
[56] Mais sobre *ECUREX Research and University of Zurich, Department of Banking and Finance* - *http://www.bf.uzh.ch/cms/en/department/department-of-banking-and-finance.html;*

Union[57], como é notório na Figura 10. No entanto, é preciso notar que isto se verifica mesmo sendo o número bruto de transações registadas, bastante inferior aos restantes métodos de pagamento. O que significa que este método de pagamento, apesar de não registar um número de transações tão significativo como os restantes métodos de pagamentos, regista, no entanto, regra geral transações que equacionam valores mais elevados.

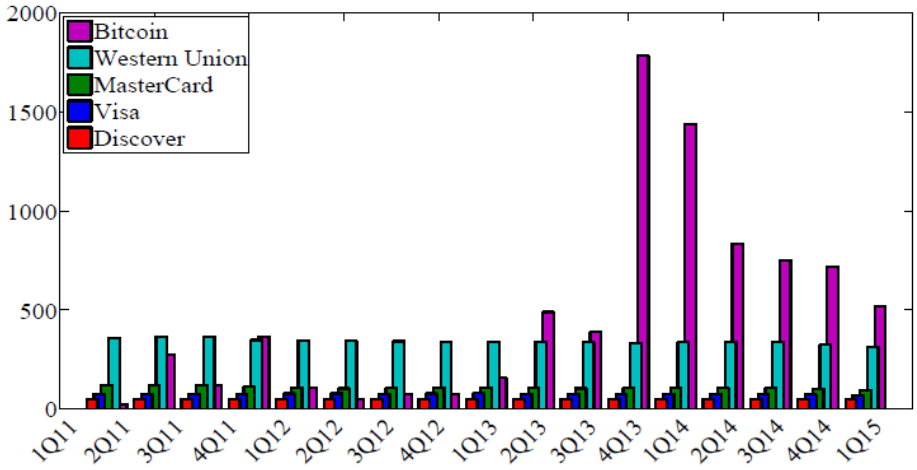


Figura 10 - Montante médio (em USD) transacionado (Tasca, 2015)

Note-se ainda que o volume total transacionado no sistema *Bitcoin* é ainda inferior aos restantes sistemas comparados, no entanto a tendência verificada é a de um crescimento constante e de uma aproximação célere ao segundo sistema menos utilizado – *Western Union* – representando no início de 2015, cerca de um quarto do volume transacionado pela *Western Union*, tal como mostra a Tabela 6.

[57] Mais sobre os sistemas de pagamentos enunciados: *VISA* - http://www.visa.com/; *Mastercard* - http://www.mastercard.com; *Discover* - https://www.discover.com/;

Tabela 6 - Volume em milhões de USD (Vol.) e nº de transações em milhões (Tx.), pelas maiores redes de pagamentos internacionais (Tasca, 2015)

Year	VISA		MasterCard		Discover		Western Union		Bitcoin	
	(Vol.)	(Tx.)	(Vol.)	(Tx.)	(Vol.)	(Tx.)	(Vol.)	(Tx.)	(Vol.)	(Tx.)
1Q11	15,153.8	198.3	8,011.0	65.6	746.5	14.7	208.8	0.6	0.04	0.002
2Q11	16,604.4	213.2	8,934.1	72.5	787.0	15.7	226.4	0.62	1.6	0.006
3Q11	17,033.0	217.7	9,285.7	77.1	787.0	15.4	231.9	0.63	0.92	0.008
4Q11	17,450.5	223.6	9,505.5	84.4	761.3	15.1	226.4	0.65	2.1	0.006
1Q12	16,934.1	215.7	9,329.7	84.8	804.3	15.8	214.3	0.62	0.7	0.007
2Q12	17,252.7	218.7	9,780.2	93.8	861.1	17.5	220.9	0.64	1.04	0.021
3Q12	17,582.4	225.3	10,087.9	95.4	860.9	17.6	216.5	0.63	2.47	0.032
4Q12	18,648.4	236.8	10,835.2	101.3	840.1	16.8	219.8	0.64	2.45	0.033
1Q13	18,120.9	227.9	10,406.6	95.1	819.2	16.1	207.7	0.61	8.12	0.052
2Q13	19,109.9	245.6	11,087.9	104.1	856.1	17.0	225.3	0.66	26.2	0.053
3Q13	19,175.8	252.1	11,494.5	109.9	850.5	17.1	231.9	0.69	19.3	0.050
4Q13	20,197.8	259.9	12,142.9	114.0	883.8	17.2	236.3	0.71	108.65	0.061
1Q14	19,011.0	249.9	11,483.5	108.2	850.4	16.5	223.1	0.66	91.01	0.063
2Q14	20,274.7	269.6	12,351.6	116.6	892.2	17.6	239.6	0.70	52.35	0.063
3Q14	20,703.3	275.9	12,714.3	120.5	881.0	17.5	242.9	0.72	51.07	0.068
4Q14	20,879.1	285.4	12,879.1	127.1	912.0	17.7	233.0	0.72	60.1	0.084
1Q15	19,263.74	275.6	11,681.32	121.3	852.32	16.3	214.29	0.68	48.80	0.094

Outra curiosidade no mercado das criptomoedas passa pela capitalização consolidada da *Bitcoin*, a qual domina predominantemente a distribuição da utilização das criptomoedas, sendo que a meio de 2014, cerca de 95% do valor bruto existente em criptomoedas era representado pela criptomoeda BTC, estando os restantes 5% distribuídos por mais de mil outras criptomoedas de representação significativamente inferior. No entanto, e apesar de se manter como criptomoeda hegemónica, outra criptomoeda – *Ripple*[58] – veio, em 2015, destacar-se pela primeira vez das restantes, chegando inclusivamente a conquistar alguns antigos utilizadores do sistema BTC, sem nunca ameaçar o seu posicionamento. Note-se ainda que algumas alterações aconteceram após o período compreendido pelo estudo. A capitalização do mercado acabou por se distribuir, perdendo a BTC o seu estatuto de dominância destacada, sendo hoje seguida pela criptomoeda *Ethereum*[59] e *Ripple*. Assim, ao dia 21AGO2017, a capitalização de mercado assentava nas seguintes percentagens: BTC – 46,4%, *Ethereum* – 20,91%, *Ripple* – 4,14%, restantes criptomoedas 28,55%, tal como está representado na Figura 11. A mesma figura prova ainda o que é apresentado por *Paolo Tasca*, no que concerne à predominância da criptomoeda BTC. Outras criptomoedas de menor relevância acabaram recentemente, por conquistar também a sua posição no mercado.

[58] Mais sobre a criptomoeda *Ripple* - https://ripple.com/ ;
[59] Mais sobre a criptomoeda *Ethereum* - https://www.ethereum.org/ ;

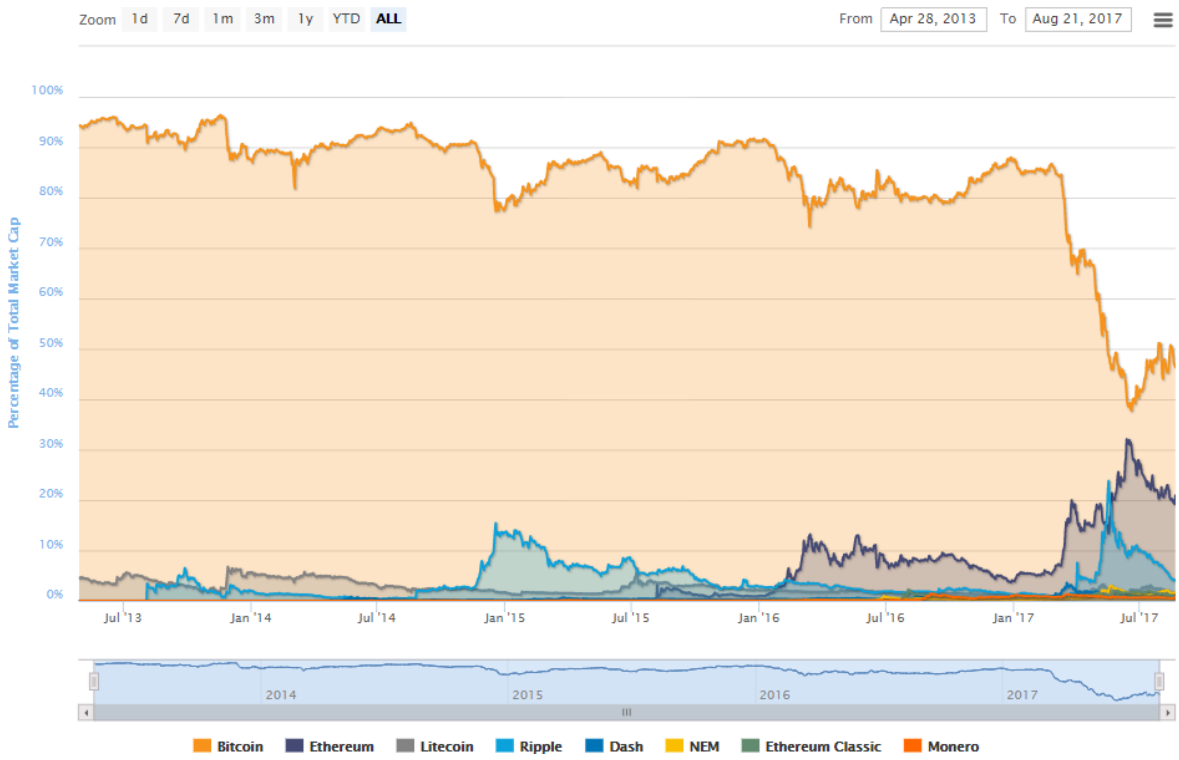


Figura 11 - Capitalização de mercado das criptomoedas em percentagem do total, entre ABR2013 e AGO2017 (Coin Market Cap, 2017)

Relativamente à distribuição geográfica das criptomoedas, o estudo de *Tasca* dá destaque à China em variados campos, detendo esta a primeira posição no que concerne ao número ativo de clientes *Bitcoin*, assim como na capacidade de *mining*, na qual desde o final de 2014 detém mais de 50% do mercado de *mining* e também no que toca ao nº de *Bitcoins* transacionadas por plataformas de troca, em CNY (*Chinese Yuan Renminbi)*, registando desde 2014, um valor três vezes superior às trocas de BTC por USD, assumindo também uma tendência crescente.

Neste contexto o autor afirma ainda que a indústria de *mining* está cada vez mais consolidada como um oligopólio, sobre o controlo maioritário de 5 ou 7 *mining pools*[60] dominantes. No período do estudo compreendido pelo autor, a fatia de mercado das 10

[60] M*ining pool* - é uma plataforma destinada à validação de transações entre endereços *Bitcoin.* Estas dedicam capacidade de processamento com o intuito de decifrar problemas criptográficos associados à validação das chaves geradas em cada transação. A cada transação resolvida, um novo bloco é fechado e novas *Bitcoins* ou frações de *Bitcoins* são geradas e atribuídas como recompensa às *mining pools*.

maiores *mining pools*[61] existentes representava cerca de 75% do total. Fazendo o paralelo para os dias que correm, esta é uma realidade que não se alterou, ganhando ainda maior ênfase a predominância de *mining pools* sedeadas na China.

Outra conclusão do autor, passa por questões relacionadas com a área de negócio, na qual o mesmo verificou que se registou, no período compreendido pelo estudo, um investimento superior a um milhar de milhão de USD em *startups* relacionadas com ambiente das criptomoedas, assumindo-se como um dos setores com um crescimento mais rápido no que toca ao investimento de capital, com cerca de 150% de taxa de crescimento entre o meio de 2012 e o meio de 2015, como se vê na Figura 12. Um fenómeno que segundo o autor revela a confiança depositada pelos investidores ora no mercado das criptomoedas, ora nas tecnologias subjacentes.

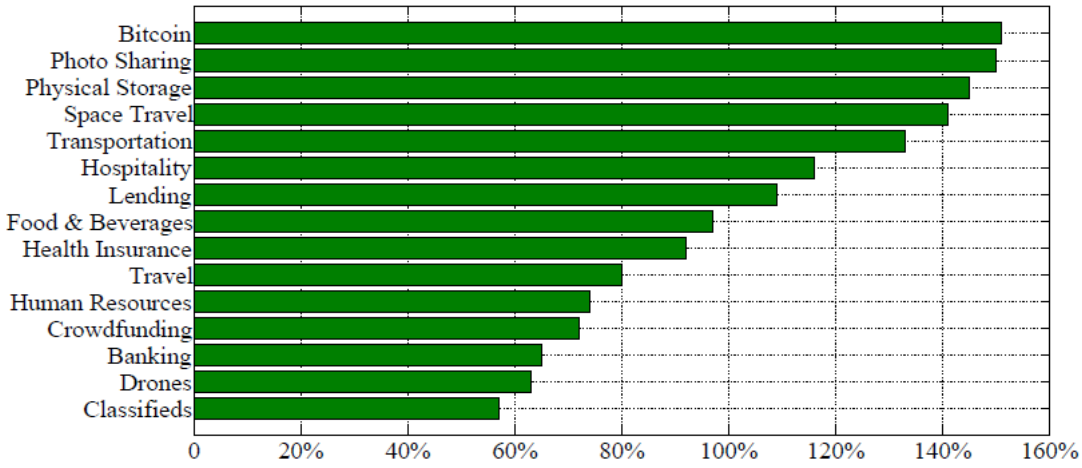


Figura 12 - Taxa de crescimento do investimento em startups por setor (Tasca, 2015)

Outra conclusão tem que ver com a distribuição da riqueza no ecossistema *Bitcoin*, pautado por uma crescente desigualdade na distribuição da posse da criptomoeda entre diferentes endereços. Este facto é comprovado por uma análise feita através do coeficiente de *Gini*[62], através do qual quão mais próximo do valor 1 se aproximar o coeficiente

[61] Para o efeito foram consideradas as *mining pools* com maior expressão, no período compreendido pelo estudo, entre as quais: *BTCChina Pool, P2Pool.org, DeepBit, Ozcoin, CloudHashing, KNCMiner, Bitfury, AntPool, EclipseMC, ASICMiner;*

[62] Coeficiente de *Gini* – é uma medida de desigualdade que pode ser usada para análise de qualquer distribuição. O resultado do coeficiente consiste num número entre 0 e 1, onde 0 corresponde à completa

chegado através da análise, mais desigual é a distribuição. Este facto é assim comprovado pelo cálculo feito por *Tasca*, evoluindo de um valor de cerca de 0,09 em 2010, para um valor de 0,99 em 2015, o que representa uma transformação da distribuição da riqueza de um momento em que a igualdade na distribuição era quase perfeita, para um momento oposto, em que a desigualdade na distribuição atinge também um nível quase perfeito. Conclui-se também que o crescimento desta desigualdade é o resultado de um fenómeno socioeconómico relacionado com a popularidade crescente da criptomoeda e da sua utilização, assim como da fragmentação dos endereços utilizados, os quais, na sua grande maioria são criados para utilizações únicas como medida de segurança e prevenção contra eventuais fraudes.

Por fim, *Tasca* conclui ainda que esta solução acaba por ser a mais barata em termos de custos para os intervenientes, no que diz respeito às transações de fundos. Assim como que, independentemente do montante transferido, as transações efetuadas em soluções que tenham por base uma plataforma como a *Blockchain*, vão sempre ser validadas em segundos, ou no máximo em poucos minutos, tal como sustenta a Figura 1. A grande vantagem passa pelo facto de estas transações não estarem sujeitas a intermediação humana, taxas cambiais, taxas específicas de transações internacionais, ou outro tipo de taxas aplicáveis, tornando o processo mais ágil.

Explanados os principais pontos alcançados por *Tasca* na sua investigação, resta fazer uma breve ressalva à confiança depositada na tecnologia *Blockchain* como uma inovação disruptiva, que poderá vir a ter usos variados em estruturas que se possam desintermediar e descentralizar, tirando ainda recurso da exponencial inovação tecnológica, capacidade de computação e solução de redes P2P, que poderão, no futuro, contribuir para um espaço digital colaborativo onde prestadores de serviços e clientes poderão trocar bens e serviços com custos marginais próximos do zero, tal como já acontece com as trocas em *Bitcoin*, um sistema e rede de pagamentos considerado por si como seguro, rápido, eficiente e barato.

igualdade e 1 corresponde à completa desigualdade. O índice de Gini é o coeficiente expresso em pontos percentuais (é igual ao coeficiente multiplicado por 100).

4.1.2.2. – Artigo *de Rainer Böhme, Nicolas Christin, Benjamin Edelman, e Tyler Moore, "Bitcoin: Economics, Technology, and Governance*", publicado em 2015, no *Journal of Economic Perspectives* — Volume 29, Nº 2;

Este artigo é motivo de análise pela explicação bem conseguida da forma como se processam as transações de *Bitcoins* entre os utilizadores. Ao mesmo tempo, o artigo poderia ser também enquadrado na revisão literária da dimensão de análise: Criminalidade Informática; pelo enfoque que dá aos crimes que se recursam da criptomoeda para a sua execução. No entanto, considerou-se que face à existência de outros estudos de qualidade para o efeito e em função da qualidade percebida no que concerne ao funcionamento da criptomoeda, este artigo se adequa melhor nesta dimensão.

Assim e para que se compreenda o funcionamento das transações no ecossistema *Bitcoin*, os autores deste artigo exemplificaram o processo através de um exemplo semelhante ao seguinte e que está ilustrado na Figura 13: imagine-se que *Alpha* (A) quer transacionar para *Bravo* (B), um montante equivalente a 1 BTC. Tendo em conta que as moedas virtuais são dinheiro sob o formato de informação, esta transação será equivalente a valor x de *bytes* de informação, onde A escreve a seguinte mensagem para B: "Eu, A, estou a dar a B, 1 BTC, numa transação onde o número de série da BTC transacionada é 123456"; A esta mensagem, A vai juntar um código que vai funcionar como assinatura da transação, ou seja, A processa a mensagem e encripta-a com uma chave-privada (k), para o endereço de *Bitcoins* particular de B. O processamento desta intenção de transação vai gerar uma chave-pública (K), que será também ela, comunicada a B. A partir deste momento, B (depois da verificação e validação dos outros membros da rede *Bitcoin*, que têm obrigatoriamente de confirmar que A detém o montante de BTCs que pretende transacionar, no momento em que deu ordem de transação) pode aceitar a transação. Assim, B recebe a mensagem e com as chaves que detém (chave-pública (K), chave-privada de A (K) e a sua chave-privada (K)), desencripta a assinatura. Se ambas as chaves coincidirem, a assinatura torna-se válida e a autenticidade, a integridade e o não-repúdio da mensagem estão garantidos.

A esta altura torna-se necessário, antes de prosseguir com a explicação da forma como o restante processamento da transação se dá, fazer uma explicação em termos genéricos de como funciona a *public ledger*, uma arquitetura que torna possível a eliminação de terceiros, ou de uma organização institucional, para a consumação da transação. Todos os nós da rede *Bitcoin* compõe coletivamente um "banco descentralizado" onde estão registadas publicamente todas as transações existentes até à

data. A esse registo dá-se o nome de *BlockChain.* Uma vez que o acesso ao registo é público, cada nó detém o registo de todas as BTCs existentes, conhecendo assim que endereços detém quais BTCs. Cada nó detém também o importante papel de verificar a legitimidade das transações, como será explicado de seguida.

Continuando com a descrição da transação, segue-se o processo de verificação. B, que também detém a informação que consta na *public ledger*, verifica de igual forma se a BTC com o número de série 123456 pertence efetivamente a A. Se se confirmar, B vai transmitir a todos os pontos da rede BTC, os *bytes* de informação afetos a esta transação, repetindo-se o processo de validação pelos restantes nós da rede. Por fim, e dada a transação, todos os nós da rede atualizam o registo da *public ledger* onde já consta que a *Bitcoin* com o número de série 123456, pertence agora a B.

Para que se perceba o desfecho completo do processo e alguma da terminologia dada é importante fazer nova ressalva. Cada transação detém um certo montante de informação, tal como foi referido, e essa informação é agrupada em blocos. Cada bloco tem capacidade para um certo montante de informação e quando se atinge esse limite, o bloco é fechado, passando-se ao seguinte. O nome da *public ledger* da BTC – *BlockChain* – deve-se a este esquema em blocos. Note-se agora que a cada nova transação, todas as transações até a data são revistas, o que significa que todos os blocos são, também eles, revistos, por forma a evitar a repetição de blocos e esquemas fraudulentos de *double-spending*. A validação da transação tem, como foi dito, de ser confirmada por todos os nós da rede antes de se efetivar. Neste processo de validação, dá-se uma competição entre os nós da rede que se dedicam a desconstruir os problemas criptográficos enunciados acima, através da aplicação da capacidade de processamento – *network hashing rate* -, através de uma estratégia de tentativa-erro que objetiva decifrar a chave que resolve o problema. Com o aumentar do número de transações e o consequente incremento da informação existente na *Blockchain* é natural que cada vez mais seja necessário maior poder de processamento para resolver cada transação, uma vez que o fenómeno de *mining difficulty rate* é cada vez mais acentuado.

Posto isto, o nó da rede que for o mais rápido a conseguir decifrar o problema criptográfico, tenha-se Charlie (C), vai ser recompensado como forma de incentivo e recompensa pelo esforço dedicado.

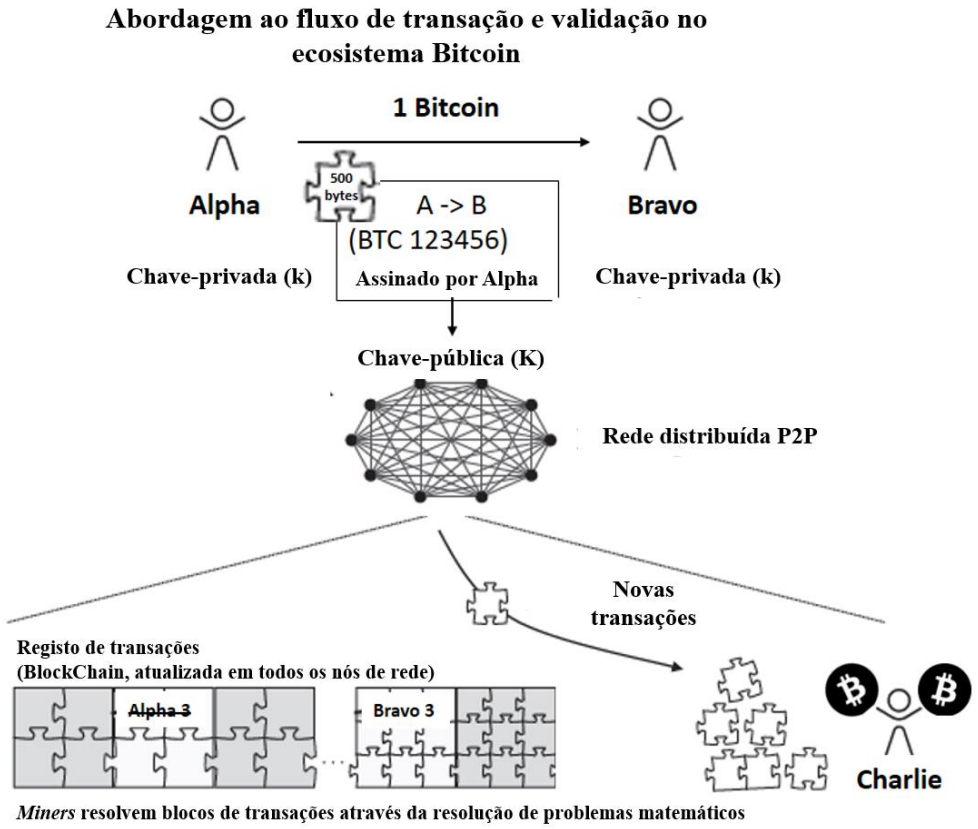


Figura 13 - Esquema representativo de uma transação Bitcoin, adaptado de (Böhme, Christin, Edelman, & Moore, 2015)

4.1.3. Segurança de Informação

4.1.3.1. - Referencial *International Organization for Standardization* (ISO) 27001 – Manual de procedimentos para a Gestão da Segurança de Informação;

Este que é também o referencial, neste estudo, para a análise da dimensão "Segurança de Informação", é a norma internacional para acreditação de empresas através da definição de um modelo através do qual se estabelece, implementa, opera, monitoriza, se analisa, se mantém e se melhora um Sistema de Gestão de Segurança de Informação (SGSI) de uma organização. Assim, a decisão estratégica da implementação da norma ISO 27001 tem como princípio geral a adoção de requisitos, processos e controlos com o intuito de uma mais eficiente gestão do risco.

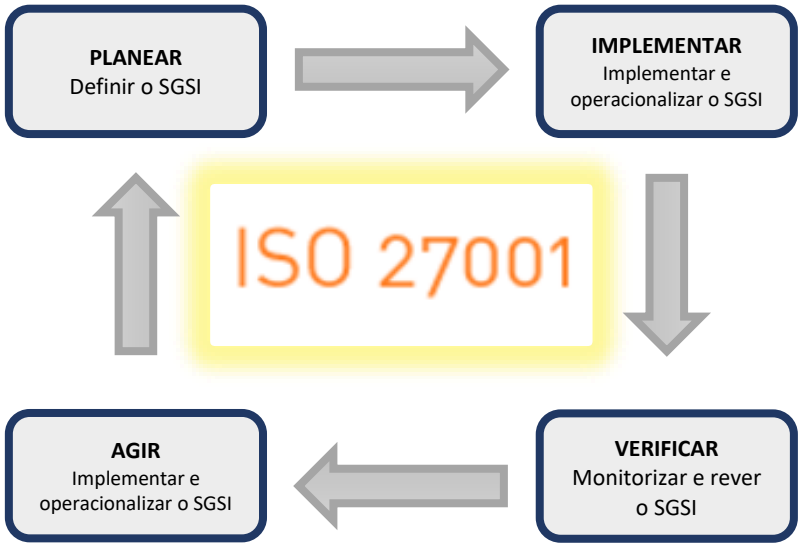


Figura 14 - Matriz com esquema operacional da norma ISO 27001, adaptado de (Integrity Consulting, 2017)

Em termos concretos a adoção e implementação da norma ISO 27001, esquematizada em termos de plano de ação pela Figura 14 proporciona às organizações a adoção de um modelo adequado no que toca à gestão de segurança da informação através de um modelo holístico de abordagem à Segurança e independente de marcas e fabricantes tecnológicos, visando temas e áreas transversais aos vários processos de negócios, tais como as telecomunicações, a proteção do meio físico, a continuidade de negócio, o licenciamento, os recursos humanos, a segurança aplicacional, entre outros.

Esta norma é composta por duas componentes diferenciadas: na primeira, são definidas regras e requisitos de cumprimento da norma, sendo feita referência aos aspetos que constam no esquema da Figura 15, entre os quais se destacam a definição do contexto específico da organização e a sua política de liderança, onde devem ser estipuladas e documentadas as funções e responsabilidades das chefias e colaboradores. Seguidamente e entrando na esfera da gestão da segurança de informação da organização, é requisito a definição de um plano de ação que enderece os riscos e possíveis oportunidades a que a informação está ou pode estar sujeita. Em paralelo deve proceder-se à definição de objetivos a alcançar. Devem ser ainda ponderados os recursos disponíveis face aos necessários para alcançar os objetivos propostos por forma a operacionalizar medidas com vista a uma melhor gestão da segurança de informação dentro da organização. Por fim é ainda definido como requisito para uma completa implementação da norma, um

mecanismo de avaliação de desempenho e, com base nisso, um plano de melhoria contínua e continuidade de negócio.

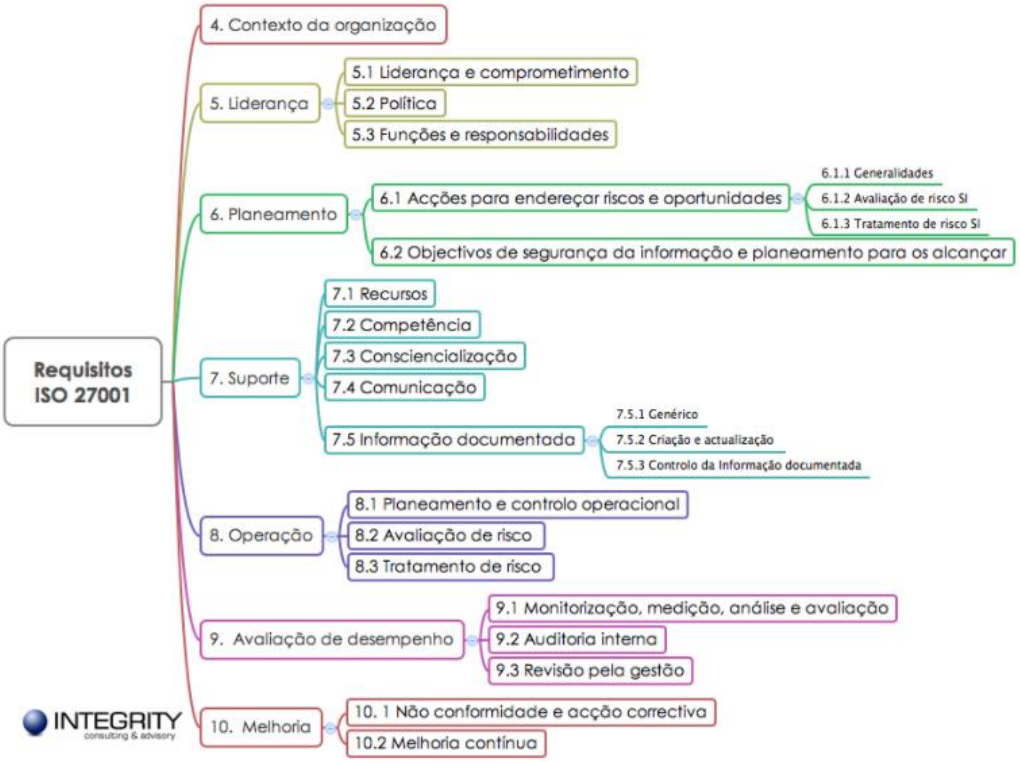


Figura 15 - Regras e requisitos de cumprimento da norma ISO 27001 (Integrity Consulting, 2017)

Na segunda, tal como mostra a Figura 16, são elencados um conjunto de controlos que as organizações devem adotar, segundo a norma. Note-se que os controlos devem ser ajustados ao contexto específico da organização, e da criticidade da informação que a empresa detém. Posto isto, os temas, ou grupo de controlos elencados no esquema da Figura 16, nada mais são, do que as principais áreas ou processos, para os quais as organizações devem olhar e perceber de que forma a sua informação está protegida em cada um destes pontos. O objetivo último desta análise passará por perceber onde é que a informação não está protegida, ou onde está mais vulnerável, por forma a implementar controlos de segurança que mitiguem ou eliminem as vulnerabilidades identificadas.

Figura 16 - Controlos a adotar pelas organizações segundo ISO 27001 (Integrity Consulting, 2017)

Para o setor organizacional a adoção de práticas de gestão documentadas na norma, estejam elas certificadas, ou não, representam um conjunto de benefícios para o seu meio envolvente. Em primeiro lugar consolida a reputação aparente da organização uma vez que demonstra preocupação na segurança da sua informação. Ao mesmo tempo, faz aumentar a fiabilidade dos processos face à garantia das propriedades da informação, assim como traz robustez aos investimentos orientados ao risco, na medida em que os mesmos deixam de se basear apenas em tendências. Na mesma medida a implementação da norma envolve o capital humano da organização no sentido podendo alcançar uma maior consciencialização para a importância da segurança de informação, ao mesmo tempo que fortalece a confiança e possivelmente a satisfação dos clientes e parceiros. Por fim, e em termos genéricos a implementação deste tipo de controlos traz fortes possibilidades de melhoria no desempenho operacional e eficiência da organização.

Por estes motivos este *standard* é a referência, em meio corporativo, no que toca ao controlo eficaz da segurança da informação fazendo inclusivamente com que determinadas organizações, deem preferência a organizações certificadas, como garante do cumprimento dos princípios estabelecidos pela mesma, providenciando assim aos seus clientes e parceiros um nível extra de conforto no que concerne à Segurança da Informação (ISO/IEC, 2005) (Integrity Consulting, 2017).

4.1.3.2. – Relatório da *European Union Agency for Network and Information Security, "ENISA Threat Landscape Report 2016 - 15 Top Cyber-Threats and Trends",* de 2016;

Considerando a estratégia da União Europeia para a cibersegurança que sublinha a importância da análise das ameaças no ciberespaço e respetivas tendências emergentes, este relatório afigura-se como uma peça de análise importante para a dimensão de segurança de informação. Neste sentido o relatório da ENISA contribui substancialmente para este objetivo estratégico, em particular na identificação das tendências recentes em termos de ciberameaças, assim como em compreender a evolução do cibercrime numa ótica transversal desde a motivação para a execução criminal, passando pela arquitetura do ataque em si, até às recomendações para prevenção, defesa e segurança de informação das potenciais vítimas.

A informação que consta neste *report* deve ser considerada principalmente aos níveis de decisão estratégica, sendo por isso dirigida a todos os *C-levels*[63], podendo ser considerada a longo-prazo, tendo sempre em conta que o ambiente sobre o qual reflete é pautado por constantes mutações, pelo que o planeamento de prevenção, segurança e reação deve ser revisto com frequência.

O relatório começa por destacar a crescente necessidade em coordenar a segurança operacional no ambiente empresarial como garante da plena atividade de negócio. Neste sentido ganha importância a ponte entre o CTI (*Cyber Threat Intelligence)* e a gestão do risco, considerando análises de risco periódicas para uma mais eficiente mitigação de risco e consequentes incidentes. Torna-se assim crucial a perceção, por parte dos perfis com poder decisório dentro das organizações, da importância do CTI na mitigação dos riscos inerentes às operações e à sobrevivência das suas empresas. Note-se, no entanto, que a relação entre o CTI e os quadros de topo, se encontra numa fase muito inicial de maturidade, não fosse uma habitual perceção errónea do risco e da exposição ao risco, por parte do poder decisório das organizações.

Semelhantemente é necessário conseguir compreender os processos críticos de negócio e perceber de que forma se refletem na segurança operacional, através de SOCs (*Security Operations Centers*) por exemplo. Resta ainda referir que esta é uma área de

[63] Entenda-se por *C-levels*, os cargos de chefias empresariais, tais como CEO (*Chief Executive Officer)*, CIO (*Chief Information Officer)*, CISO (*Chief Information Security Officer)*, CISM (*Certified Information Security Manager)*, etc.;

crescente investimento por parte dos Estados, através do *empowerment* dado às capacidades de ciberdefesa canalizadas às forças militares. Fruto desta nova realidade é expectável que o CTI se desenvolva rapidamente, podendo ser aplicado no contexto empresarial e no setor público, aquando da sua maturação.

Paralelamente, a ENISA faz referência à necessidade crescente na adoção de boas práticas na utilização das TIC. Políticas e ferramentas como o ISO27001 (ISO/IEC, 2005) dão suporte ao CTI, apoiando a deteção de padrões de ataque, assim como na correlação entre a informação obtida através dos instrumentos de *intelligence* e um dado indício que indique um possível incidente.

O relatório deixa ainda, em nota conclusiva, algumas considerações a serem tidas, dividindo-as em três áreas: de políticas; de negócio; e de investigação;

Ao nível político a ENISA defende a importância de se estabelecerem fóruns de discussão e análise de performance com os vários *stakeholders* com envolvimento no CTI, estejam eles inseridos no setor público ou privado. Mediante o estado da arte disponível em matéria de CTI, devem-se consolidar e definir os requisitos mínimos de segurança para as várias áreas de infraestrutura, de acordo com o setor em que insere, assim como de acordo com o tipo de serviço prestado e/ou utilizador a que se destina. Deve de igual forma continuar o esforço na amplificação de capacidades e treino na esfera da segurança digital, incentivando o fomento da aplicação das boas práticas na utilização das TIC, assim como disseminar o *awareness* para as ameaças digitais entre utilizadores.

Ao nível macro o estudo considera ainda que se deve procurar fortalecer a posição dominante da Europa em termos de segurança e privacidade, tendo-as em conta como vantagens competitivas no mercado global. Note-se ainda que uma posição dominante estabelecida, vai impulsionar a Europa como referência na área e terá como consequência direta ora crescimento económico pela prestação de serviços, ora maior experiência e conhecimento na resolução de incidentes e gestão de vulnerabilidades, podendo esse conhecimento ser aplicado internamente ora no ambiente empresarial, ora em matéria de defesa.

Ao nível das conclusões direcionadas à área de negócio, é aconselhado às empresas que utilizem as soluções e ferramentas disponíveis para as boas práticas na utilização das TIC, assim como sugerem que utilizem o CTI como uma ferramenta ativa que pode ser usada na simulação de ciberincidentes e ciberataques, tendo como objetivo testar as medidas de reação existentes. Esta abordagem pode despistar falhas nas políticas

de segurança e com isso alertar para a necessidade de a repensar, assim como os controlos previamente definidos, no sentido de mitigar o risco da forma mais eficiente possível. Assim, o CTI deve ajudar as organizações a estabelecerem uma política de gestão da segurança de informação mais ágil e flexível e que tenha em conta a gestão do risco alinhada com a arquitetura de segurança.

O relatório aconselha ainda à união de esforços por setor empresarial, sugerindo a partilha do *modus operandi* entre *stakeholders* do mesmo ramo, tendo por base uma posição não competitiva, mas sim de entreajuda. No mesmo espírito de cooperação, é ainda dado enfoque à importância do desenvolvimento de modelos de defesa ativa, envolvendo *stakeholders* de diversas áreas, como da ciberdefesa, centros de segurança nacional, entidades legais e forças militares, que devem, num certo nível de maturidade e consistência, ser canalizados para o setor empresarial.

Por fim, é ainda feita uma ressalva para a importância da aquisição de *software* no qual a segurança esteja pensada *by design*, assim como é ainda feito um alerta para os desafios que o fenómeno da IoT (*Internet of Things*) vai trazer em alguns ramos comerciais, aconselhando a que as organizações pensem nas soluções que utilizam e oferecem de forma redobrada.

Para terminar as notas conclusivas, restam as conclusões para investigação futura, o relatório sugere a definição de *roadmaps* de investigação para a AI (*Artificial Intelligence)* relacionada com a CTI, aos níveis, por exemplo, do reconhecimento automático de padrões de ataque e posterior disparar do alerta e reação através dos *injects* estabelecidos. Um mecanismo que pode vir a revelar-se útil na redução do tempo de resposta a incidentes, aumentando a qualidade da performance e a eficiência dos controlos de segurança implementados.

Outra das sugestões passa pela investigação de inovadores controlos de segurança face aos novos dilemas de segurança e novas técnicas de ataque. É importante que estes sejam pensados no sentido de fomentar a confiança entre componentes e/ou infraestrutura, mas também entre utilizadores.

Não descurando as soluções apresentadas de seguida, as mesmas passam pelo contínuo estudo da dimensão das ciberameaças, algo que deve ser ininterrupto face à constante mutação do ecossistema e consequente desenvolvimento de novas técnicas de ataque que contornem os controlos de segurança existentes. Assim as sugestões finais passam pelo estudo de código malicioso por forma a compreender a sua evolução, nível

de impacto, complexidade e sofisticação, assim como disponibilidade e atribuição, entre outros.

5. Análise à informação recolhida em investigação

5.1. Componente empírica – Entrevistas

Por forma a validar empiricamente as questões e hipóteses de investigação levantas *à priori*, tal como referido no subcapítulo 3.3., definiu-se um método de investigação exploratório, baseado em entrevistas junto dos peritos listados na Figura 17, apresentada abaixo. Foi elencado um grupo de personalidades variado, com elementos representativos dos *stakeholders* afetos às temáticas investigadas, especialistas no tema tendo adquirido, na sua grande maioria, conhecimento pela via académica e/ou profissional, ou até noutros casos, por interesse próprio. Foram abordadas para cima de 25 personalidades que, na perceção do autor, de alguma forma poderiam contribuir para o estudo, no entanto alguns fatores não permitiram que a amostra de personalidades entrevistadas fosse tão vasta quanto aquilo que seria desejável. No entanto, as personalidades que se mostraram gentilmente disponíveis para contribuir com o seu conhecimento para esta investigação fazem parte daqueles que, em Portugal, detêm um mais vasto conhecimento nestas matérias, proporcionando uma análise transversal através das diferentes formas como lidam com a criptomoeda, oferecendo uma visão distinta e complementar sobre esta problemática e enriquecendo com isso a própria investigação. Assim, para a dimensão da criminalidade informática foram feitos contatos com algumas personalidades de chefia das forças de segurança nacionais e dos organismos de polícia competentes na gestão de cibercrimes e de crimes com recurso a ferramentas informáticas, tendo sido entrevistados: CAlm Gameiro Marques – Diretor do Gabinete Nacional de Segurança; Inspetor-chefe Rogério Bravo – Inspetor-chefe da PJ para a área do cibercrime; e ainda Carlos Cabreiro – Diretor do UNC3T da PJ. Para a dimensão de segurança de informação foram consultados representantes das infraestruturas críticas nacionais, assim como especialistas ligados ao mundo empresarial e da administração pública, ligados concretamente ao ramo da segurança: Paulo Moniz – Diretor de Segurança de Informação e Risco nas TIC da EDP; e José Pereira – Coordenador do Núcleo de Segurança, Comunicações e Centro de Dados da eSPap. Finalmente, para a dimensão dos novos recursos tecnológicos, entrevistaram-se dois entusiastas da tecnologia das criptomoeda que lidam diariamente com as mesmas embora com propósitos diferentes: Mário Valente – *R&D Lead* na *FullIT*, que por interesse académico e profissional se tornou um dos maiores conhecedores da tecnologia e arquitetura

adjacente; por outro lado entrevistou-se uma personalidade que prefere, por questões de confidencialidade, ser referida neste trabalho sob o pseudónimo de *Riclas* e que trabalha diariamente com criptomoeda *Bitcoin*, tendo no negócio das transações uma atividade de negócio através da plataforma *Local BTC*, onde é considerado *ProTrader*, tendo realizado mais de 10000 transações com 4000 utilizadores diferentes espalhados pelo mundo, em cerca de 3 anos de atividade, obtendo como resultado uma marca de 100% de *score* positivo, o que significa que completou todas as transações em que esteve envolvido.

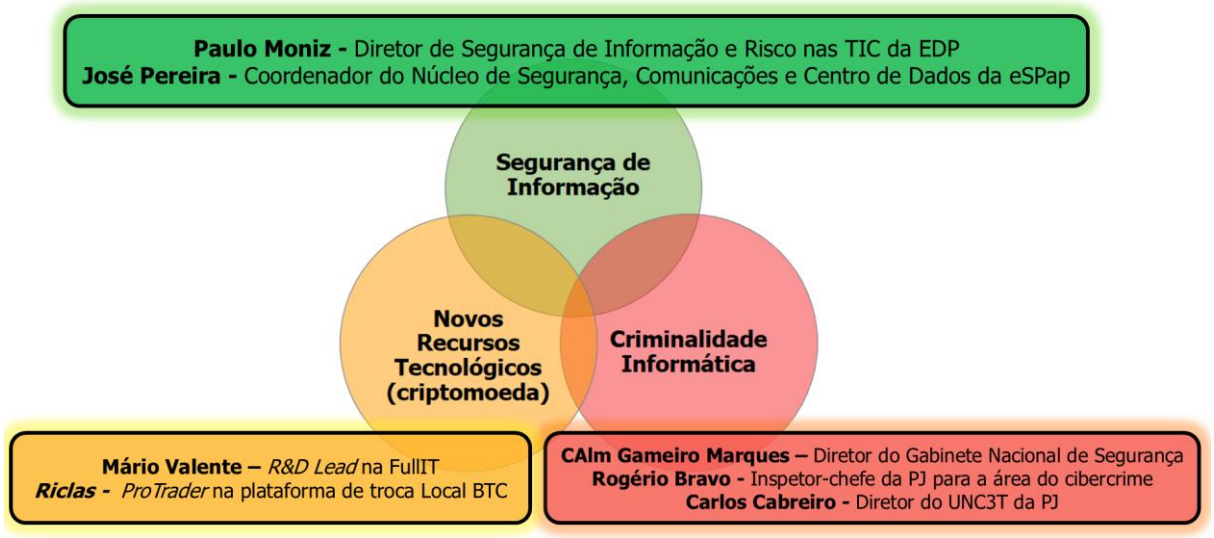


Figura 17 - Principais dimensões de análise e respetivas personalidades entrevistadas

As entrevistas efetuadas no âmbito do estudo, que podem ser encontradas através dos Apêndices 3 a 9, consubstanciaram o método de observação exploratória, tendo por isso obedecido a regras afetas ao rigor científico da investigação. Assim, todas as entrevistas foram semiestruturadas, isto é, foram preparadas através da construção de guiões de suporte. Para além disso as perguntas apresentadas, apesar de variarem em função da dimensão de análise na qual cada personalidade foi entrevistada e ainda da sua qualidade profissional enquanto entrevistado, foram pensadas para que o entrevistado pudesse dissertar sobre a questão, assumindo, por isso, características de resposta aberta. Os guiões das entrevistas, onde se encontram também as respostas dadas, assim como o

catálogo com todas as perguntas levantadas em situação de entrevista, podem ser encontrados na secção de Apêndices, no subcapítulo 7.2.

Tal como referido no subcapítulo 3.4. as entrevistas foram analisadas mediante um método Hipotético-dedutivo, segundo o qual se procurará uma reposta válida às questões de investigação através de uma abordagem de cariz qualitativo segundo a qual serão extraídos e analisados os depoimentos recolhidos em contexto das entrevistas. Serão assim avaliados seguindo uma abordagem denominada análise temática, concebida por Braun & Clarke, 2006, segundo a qual os dados recolhidos serão identificados, analisados e agrupados em categorias e padrões, ou temas, seguindo um método estruturado com vista à resolução do fenómeno em investigação.

Este método divide-se em 6 fases distintas, que serão explanadas em função do método de investigação definido no presente trabalho:

- Fase 1 – Ler atentamente os dados recolhidos em entrevista, prestando atenção a possíveis padrões que possam ser facilmente verificáveis;
- Fase 2 – Atribuir CODEs aos dados recolhidos em entrevista, nos quais seja aparentemente possível verificar um padrão face ao que foi perguntado ou até uma relação de interesse em função do contexto da investigação. Este é o primeiro momento de tratamento de dados, com vista à sua simplificação e normalização para facilitar a sua análise;
- Fase 3 – Relacionar os CODEs identificados com os THEMEs que haviam sido provisoriamente criados antes das entrevistas e que continuam sem ser definitivos, no entanto, é nesta fase que se começam a identificar redundâncias ou inconsistências nos THEMEs pré-definidos, quando confrontados com os CODE's obtidos;
- Fase 4 – Análise dos THEMEs. Nesta fase é necessário perceber de que forma os dados recolhidos e normalizados em CODEs sustentam os THEMEs em equação, olhando para o problema do ponto de vista teórico. Pode ser necessário, reformular os THEMEs;
- Fase 5 – Definição final dos THEMEs. Nesta fase já será possível identificar relações diretas e padrões coerentes entre os CODEs e os THEMEs;
- Fase 6 – Descrição dos resultados alcançados;

Posto isto, os THEMEs definidos previamente às entrevistas foram: *Awareness; CyberAttacks; Cryptocurrency Threats; Security; Victims; Infosec; BTC Technical Questions;* tendo sido com base nestes THEMEs, derivados das questões de interesse para a investigação, que foram pensadas as perguntas levantadas em situação de entrevista. Após esta provisória definição e realização das entrevistas, as declarações recolhidas nas entrevistas foram trabalhadas no sentido de as categorizar através de CODEs e com essa codificação, conseguir agrupá-las em cada um dos THEMEs acima elencados, por forma a encontrar possíveis ligações pergunta-resposta, assim como perceber o nível de consenso para cada pergunta e com isto aproximar-me das respostas às questões de investigação levantadas. Mais à frente no decorrer da investigação e já findadas e trabalhadas as entrevistas, os THEMEs foram repensados e definidos finalmente, tento sido definitivamente elencados os seguintes:

- *CyberAttacks* – Neste THEME foram elencados todos os CODEs relacionados com ataques e crimes informáticos ou com recurso a ferramentas informáticas, tendo sido principalmente consideradas as declarações relacionadas com ataques que de alguma forma são afetos às criptomoedas, mas não só. Assim consideraram-se como estando envolvidos neste THEME as afirmações envoltas na esfera dos seguintes conceitos, ou seus semelhantes: cibercrime, crime informático, crime com recurso a técnicas e/ou ferramentas informáticas, *Ramsonware*, *sextortion*, extorsão, resgates, financiamento terrorista, comércio em mercados negros, lavagem de dinheiro, evasão fiscal, branqueamento de capitais, exploração de vulnerabilidades, fragilidades, ameaças, entre outros;
- *Victims* – Neste contexto foram consideradas todas as respostas que estiveram diretamente relacionadas com o papel das vítimas de ciberataques com recurso a criptomoedas, tendo em conta as afirmações envoltas na esfera dos seguintes conceitos, ou seus semelhantes: Empresas, *corporate*, setor privado, administração pública, aparelhos de Estado, setor público, indivíduos singulares, indivíduos, exposição no ciberespaço, infraestruturas críticas, impacto, entre outros*;*
- *Awareness and InfoSec* – No que concerne a este THEME, foram tidas em conta as expressões relacionadas com a consciencialização das hipotéticas vítimas, assim como temas relacionadas com a segurança da informação, considerando-

se para o efeito, as respostas envoltas na esfera dos seguintes conceitos, ou seus semelhantes: Preparação, prevenção, alerta, exposição ao risco, sensibilização, precaução, órgãos de polícia criminal, forças de segurança, serviços de segurança, normas e boas práticas na utilização das TIC, ISO 27001, gestão da segurança de informação, criticidade da informação, segurança de informação, dados pessoais, entre outros*;*

- *BTC technical questions* – Por fim, foram consideradas para este THEME todas as afirmações que estavam relacionadas com o domínio mais técnico das criptomoedas, assim como fenómenos relativos às transações em criptomoedas. Para o efeito consideraram-se as afirmações envoltas na esfera dos seguintes conceitos, ou seus semelhantes: Criptografia, anonimização, rastreabilidade, dinheiro, moeda, redes ponto a ponto, P2P, sistema monetário, financeiro, económico, *status quo* financeiro, moeda física, taxas, custos, *BlockChain*, entre outros;

Após análise do conteúdo das entrevistas considerou-se que os THEMEs definidos inicialmente se deveriam manter, uma vez que se verificou que serviam o propósito de enquadrarem a substancial maioria das temáticas identificadas nos CODEs.

O processamento da informação recolhida, assim como os resultados brutos extraídos das entrevistas podem ser encontrados no capítulo seguinte.

5.2. Validação empírica: análise ao conteúdo das entrevistas

A análise seguidamente apresentada seguiu a estrutura apresentada no subcapítulo 5.1., com base nas perguntas elencadas no catálogo de perguntas, que pode ser consultado no Apêndice 2 e nas respetivas respostas dos entrevistados, cujas entrevistas podem ser consultadas na íntegra, nos Apêndices 3 até 9. No total foram catalogadas 29 perguntas diferentes, sendo que nem todas foram colocadas a todos os entrevistados, tendo sido colocadas apenas aquelas que se revelaram mais convenientes face ao perfil do entrevistado, ao contexto profissional e à dimensão de análise na qual foi inserido cada entrevistado. Das 29 questões catalogadas, foram colocadas 77 questões, distribuídas pelos entrevistados da seguinte forma: Paulo Moniz – 10; José Pereira – 9; Rogério Bravo – 11; Carlos Cabreiro - 12 ; Mário Valente – 11; *Riclas* – 13; e CAlm Gameiro Marques – 11; Foi feito o esforço para que as perguntas não indiciassem

qualquer tendência na resposta, no sentido de zelar pela imparcialidade da investigação. Assim, as declarações prestadas pelos entrevistados resultam única e exclusivamente do conhecimento próprio do tema abordado, assim como do entendimento que o entrevistado fez da pergunta e do que lhe pareceu ser o mais apropriado responder.

Note-se que a análise dos dados recolhidos nos casos em que uma dada pergunta foi colocada à maior parte do universo dos entrevistados, ou seja a pelo menos a 4, foi feita através do agrupamento dessa pergunta em *cluster*. Tendo depois sido analisadas todas as respostas dadas a essa pergunta, em bruto, por forma a facilitar a análise. Os CODEs resultantes foram enquadrados dentro dos THEMEs respetivos e das questões de investigação levantadas. Quando isto não foi possível, isto é, quando a pergunta foi feita apenas a 3, ou menos, entrevistados, a análise da reposta foi feita isoladamente, tendo depois sido enquadrada dentro da melhor forma dentro dos THEMEs e das questões de investigação levantadas.

Note-se ainda que nem todas as respostas obtidas se revelaram relevantes para a análise mediante este modelo, da mesma forma que nem todas se encaixam neste modelo dada a natureza das respostas, pelo que as respostas às perguntas com o ID-I, ID-J, ID-U e ID-X, apesar de apresentadas nos guiões das entrevistas e no catálogo de perguntas, presentes em apêndice, não estão aqui equacionadas. No entanto, não quer isto dizer que as mesmas tenham sido negligenciadas, tendo o seu conteúdo sido aproveitado para um melhor entendimento da realidade em estudo e para um resultado final de maior qualidade. Alguns desses apontamentos foram ainda abordados na descrição analítica das conclusões finais, podendo ser encontradas ora no subcapítulo 5.3., ora no subcapítulo 6.1..

Por fim, resta ainda uma ressalva para a codificação por cores dos THEMEs e dos respetivos CODEs identificados e afetos a cada tema. Esta estratégia serve o propósito de simplificar a leitura e interpretação dos dados nas tabelas que se seguem, tendo resultado na seguinte identificação: *CyberAttacks* [CYB]*; Victims* [VIC]; *Awareness and InfoSec* [AWA]*; BTC technical questions* [BTC-TQ]*;* Outro apontamento importante na leitura das tabelas abaixo face à codificação por cores, tem que ver com a categorização de CODEs que se possam inserir em mais do que um THEME, com a cor que mais se adeque dado o contexto da entrevista no momento em que a citação respeitante àquele CODE foi proferida.

Assim, para a questão ID-A[64]: *"Como vê o panorama nacional no que concerne aos crimes e ciberataques cujas criptomoedas contribuem para a sua consumação?"*, que foi colocada a todos os entrevistados e que pode ser enquadrada dentro dos THEMEs: *Awareness and InfoSec*; e *Cyberattacks*; foram verificados os CODEs apresentados na Tabela 7:

[64] A cada pergunta foi atribuído um ID único que a identifica. Esta codificação pode ser consultada no catálogo de perguntas, através do Apêndice 2;

Tabela 7 – Análise dos CODEs e THEMEs para a pergunta: Como vê o panorama nacional no que concerne aos crimes e ciberataques cujas criptomoedas contribuem para a sua consumação?

Segurança de Informação		Criptomoedas		Criminalidade Informática		
Paulo Moniz	José Pereira	Mário Valente	*Riclas*	CAlm Gameiro Marques	Rogério Bravo	Carlos Cabreiro
no panorama nacional associa-se muito a criptomoeda ao crime [CYB] cada vez mais esta ideia se está a desvanecer [CYB] valorização recente trouxe a palavra lucro para a discussão (…) vai, atrair pessoas, o que tem como consequência mais criminosos no "sistema" [CYB]	O que tenho testemunhado é preocupante (…) várias alternativas têm sido utilizadas para explorar as organizações mais vulneráveis [CYB] e-mail tem sido o meio privilegiado para ataques [CYB] este fenómeno tem vindo a crescer [CYB] também houve uma resposta cabal das entidades por forma a prevenirem-se contra futuras situações, através da sensibilização dos colaboradores [AWA]	ataques há muitos e são diários veem-se ataques a vir de muito lado, falamos de Criminalidade Informática, dentro do que a lei considera crimes informáticos [CYB] ataques vindo tanto dentro de Portugal como fora de Portugal, são muitos, mas críticos são poucos [CYB] Ataques concertados em Portugal são provenientes do estrangeiro e não de dentro [CYB] Em Portugal o crime informático, resume-se a ataques pontuais, simples, tratando-se do pequeno crime e não do crime organizado em escala persistente e avançado [CYB]	criptomoedas são usadas como substituto de dinheiro [BTC-TQ] tal como se fazem crimes com dinheiro físico, também se fazem com criptomoedas [CYB] tendência é um aumento do nº de carteiras e de new-incomers , portranto utilização vai crescer para o bem e também para o mal. [CYB]	os pedidos de resgates que decorrem de ataques de Ramsomware em Portugal ainda são, ou poucos ou desconhecidos [CYB] ainda não há obrigatoriedade das entidades (publicas ou privadas) de o reportarem e dizerem que foram comprometidas [VIC] Isto vai ser resolvido com a entrada em vigor no ano que vem com o GDPR) [AWA] vai permitir ter mais visibilidade sobre assuntos que envolvam a utilização das BTCs ou outras criptomoedas para propósitos menos legítimos [CYB] tendência crescent [CYB]	panorama nacional equaciona crimes como financiamento terrorista, lavagem de dinheiro, ramsomware, sextortion, comércio em mercados negros [CYB] as criptomoedas aparecem em todas essas vertentes, explorando as componentes do financiamento e da anonimização da fonte [CYB] Motivação monetária, com principal objetivo não do consumo da BTC dentro do mundo virtual, mas sim da transmutação da criptomoeda por dinheiro real [CYB] crimes relacionados com BTC são sempre relacionados com branqueamento de capitais [CYB] tendência de utilização é brutalmente crescente [CYB]	Criptomoedas trouxeram mais uma especificidade em termos do que pode ser um ato praticado com recurso a meios informáticos ou até de criminalidade informática [CYB] Trouxe especificidade na determinação da autoria do crime, pois passou a ser algo que não é controlado nem é passível de controlar imediatamente pelas autoridades associando ferramentas que proporcionam anonimização, com dinheiro quase anónimo, é ouro sobre azul para o mundo do crime [CYB] é uma tendência atual e em crescente e começa a ter uma credibilidade geral, uma vez que passou a constar nas rotinas das pessoas que compram online [CYB]

Para outra questão que foi colocada a 6 dos 7 entrevistados, concretamente a questão ID-B: *"Quais as consequências mais impactantes para as vítimas"*, que pode ser enquadrada dentro dos THEMEs: *Awareness e InfoSec;* e *Victims;* foram verificados os CODEs apresentados na Tabela 8:

Tabela 8 - Análise dos CODEs e THEMEs para a pergunta: "Quais as consequências mais impactantes para as vítimas?"

Segurança de Informação		Criptomoedas		Criminalidade Informática		
Paulo Moniz	José Pereira	Mário Valente	*Riclas*	CAlm Gameiro Marques	Rogério Bravo	Carlos Cabreiro
consequências no plano organizacional, afetando os serviços que são essenciais ao negócio [VIC] na vida pessoal dos *users* afeta em termos da perda financeira e da perda de dados sensíveis ou confidenciais [VIC]	Preocupação maior são as diversas variantes deste tipo de ataques [VIC] consequências passam pela inoperacionalidade e consequente perda de faturação pelo tempo inativo. [VIC]	É o tempo offline, ou seja, a perda de negócio durante o tempo em que estiveram em baixo [VIC]		consequência direta que está ligada ao pagamento do resgate [VIC] também, por causa própria natureza da BTC, o problema da atribuição [VIC]	consequências imediatas são as mais visíveis, perda monetária, de dados, etc., ou seja impacto operacional e financeiro [VIC] consequências mediatas são o estimular da imaginação criminal, para tirar partido dessas ferramentas, não para o ganho monetário, mas para o aproveitamento para sabotagem [CYB]	prática mais usual em que a vítima é impelida a pagar especificamente em criptomoedas são os ataques de Ramsonware [VIC] verifica-se que grande parte dos ataques informáticos se baseiam na obtenção de lucro e mais uma vez na tentativa de o criminoso encobrir o seu rastreio [VIC]

Para a questão ID-C: *"Para que grupo de vítimas (organismos públicos, corporate ou indivíduos) as consequências são mais danosas?"*, que foi colocada a 5 dos 7 entrevistados e que pode ser enquadrada dentro dos THEMEs: *Awareness e InfoSec;* e *Victims*; foram verificados os CODEs apresentados na Tabela 9:

Tabela 9 - Análise dos CODEs e THEMEs para a pergunta: "Para que grupo de vítimas (organismos públicos, corporate ou indivíduos) as consequências são mais danosas?"

Segurança de Informação		Criptomoedas		Criminalidade Informática		
Paulo Moniz	José Pereira	Mário Valente	*Riclas*	CAlm Gameiro Marques	Rogério Bravo	Carlos Cabreiro
Não há mais danoso que outro, cada uma à sua dimensão, existem sempre estragos [VIC] Para um indivíduo um incidente deste género pode quase ser uma catástrofe, mas obviamente que não tem a mesma dimensão que tem para empresas [VIC]	indivíduos são alvos mais fáceis por usarem redes públicas sem qualquer tipo de cuidado na sua utilização, partilhando até informação pessoal. [VIC]	os mais vulneráveis são as pessoas obviamente e são aquelas para quem um problema de segurança pode resultar num impacto relativo maior [VIC] Estado e empresas, estão menos vulneráveis e impactos podem ser maiores, mas se forem só financeiros tipicamente não significam algo de maior [VIC] (hospitais) estão, por norma, extremamente desprotegidos e repletos de dados críticos sendo muito apetecíveis pelo dinheiro que valem em mercados negros [VIC] estas falhas podem até ter um forte impacto financeiro, mas o problema é no dia em que tiverem impactos não tangíveis e deram o salto por exemplo para perdas humanas [VIC]		registos indicam-nos que as consequências mais danosas são para as entidades que têm compromissos com clientes, ou seja empresas [VIC]		Se olharmos à perda de informação, teremos em primeiro lugar os organismos estatais. Para um particular o mais importante pode ser o aspeto económico. [VIC]

Outra das questões que foi colocada a 6 dos 7 entrevistados, especificamente a questão ID-D: *"Considera que as potenciais vítimas estão sensibilizadas ou preparadas para lidar com a ameaça?"*, que pode ser enquadrada dentro dos THEMEs: *Awareness e InfoSec; Victims*; foram verificados os CODEs apresentados na Tabela 10:

Tabela 10 - Análise dos CODEs e THEMEs para a pergunta: "Considera que as potenciais vítimas estão sensibilizadas ou preparadas para lidar com a ameaça?"

Segurança de Informação		Criptomoedas		Criminalidade Informática		
Paulo Moniz	José Pereira	Mário Valente	*Riclas*	CAlm Gameiro Marques	Rogério Bravo	Carlos Cabreiro
EDP está sensibilizada [AWA] pessoas aqui são conhecedoras que existem ataques que pedem criptomoedas em troca [AWA] ao nível das operações e processos diários existem normas implementadas com vista à boa gestão do SGSI [AWA] com a implementação do ISO27k no nosso SOC temos perfeita integração de eventos com uma equipa de resposta a incidentes [AWA]	esforço no sentido de sensibilizar colaboradores da eSPap [AWA] temos o cuidado de divulgar através de ações de sensibilização no sentido criar o alerta para este problema de segurança e iniciativas dos atacantes mais recentes [AWA] já iniciámos a certificação ISO27001, e embora não a tenhamos concluído, todos os controlos aplicáveis, políticas e ações previstas, são executadas e uma realidade na eSPap [AWA]	Até há pouco tempo havia muito pouca perceção ao risco, aos impactos que pode ter e pouca sensibilização para o problema [AWA] só agora que se falou do GDPR é que subitamente as empresas se aperceberam do trabalho que tem que ser desenvolvido e das mudanças que têm que ser feitas [AWA] de há uns meses para cá tenho visto mais algum cuidado e interesse no assunto, uma vez que a coisa se tornou tangível em dinheiro [AWA] Na minha opinião isto vai-se refletir nas políticas internas de segurança e isso já se está a ver [AWA]		Promovemos muitas ações no sentido não da sensibilização específica para as questões relacionadas com as criptomoedas, mas para o tema da resiliência digital como um todo [AWA] GNS e CNCS (Centro Nacional de Cibersegurança) têm feito várias ações em escolas e universidades para os sensibilizar para estes temas e sobretudo para desmistificar a ideia de que este tema é apenas dos informáticos [AWA] Este é aliás um dos eixos da estratégia nacional de segurança no ciberespaço, a capacitação das pessoas [AWA] caminhamos no sentido de incrementar o nível de sensibilização e preparação para ciberincidentes [AWA]	Há sensibilização, muitas sabem [AWA]	empresas felizmente e considerando os últimos ataques de Ramsonware, revelaram que estavam com grande resiliência [AWA]

Relativamente à questão ID-E: *"As empresas vítimas de ciberataques que as comprometam têm por hábito reportar às autoridades competentes?"*, que foi colocada a 4 dos 7 entrevistados e que pode ser enquadrada dentro dos THEMEs: *Awareness e InfoSec; Victims*; foram verificados os CODEs apresentados na Tabela 11:

Tabela 11 - Análise dos CODEs e THEMEs para a pergunta: "As empresas vítimas de ciberataques que as comprometam têm por hábito reportar às autoridades competentes?"

Segurança de Informação		Criptomoedas		Criminalidade Informática		
Paulo Moniz	José Pereira	Mário Valente	*Riclas*	CAlm Gameiro Marques	Rogério Bravo	Carlos Cabreiro
		Em Portugal só não há mais consequências porque quem sofre ataques não comunica, nem às autoridades nem aos seus clientes. Se comunicassem obviamente que isso teria repercussões de negócio [VIC] portanto, não sofrem consequências pelo menos de reputação futura [VIC]		As organizações que não reportam acabam por ser descobertas, mais depressa se apanha um mentiroso que um coxo [VIC] existem mecanismos para se perceber se uma empresa foi ou não comprometida [VIC] Existem até entidades que ainda não sabem que foram comprometidas, mas, no entanto, já dão sinais no ciberespaço que foram comprometidas [VIC]	Números baixos… [VIC] Muitos pensam que têm soluções técnicas próprias e por isso não precisam de reportar [VIC] Outros reportam porque precisam de o fazer por questões burocráticas para abertura de processos-crime [VIC] grandes empresas reportam, uma vez que já têm políticas de segurança e normas de boas práticas implementadas [AWA] temos consciência que grande parte das empresas não reporta [VIC] questão da reputação nos mercados tem também muito peso no facto do não-report [VIC] vêm muitos custos associados e por vezes pouca eficácia dada a morosidade na resolução aquando do report às autoridades, preferindo por vezes pagar o resgate [VIC]	organizações do Estado têm obrigação de reportar uma vez que se trata de crime público [VIC] empresas deviam reportar [VIC] nível de report ainda não é o desejável, porque colocam a ênfase na quebra de segurança e uma vez ultrapassado o incidente não se vêm na obrigação de reportar [VIC]

Para outra das questões que foi colocada 5 dos 7 entrevistados, concretamente a questão ID-G: *"Qual o estado de maturidade na cultura de segurança das organizações nacionais?"*, que pode ser enquadrada dentro do THEME: *Awareness e InfoSec;* foram verificados os CODEs apresentados na Tabela 12:

Tabela 12 - Análise dos CODEs e THEMEs para a pergunta: "Qual o estado de maturidade na cultura de segurança das organizações nacionais?"

Segurança de Informação		Criptomoedas		Criminalidade Informática		
Paulo Moniz	José Pereira	Mário Valente	*Riclas*	CAlm Gameiro Marques	Rogério Bravo	Carlos Cabreiro
escala de 0 a 10 diria que ainda é 4 [AWA] algumas organizações de áreas específicas com um nível de maturidade de 8 [AWA] as pessoas não têm noção, regra geral mas dependendo da área ou do setor de atuação [AWA]	escala de 0 a 10 colocaria a eSPap entre o 7 e o 8 [AWA] existem ainda outras componentes que estamos a trabalhar mas que ainda não concluímos, como implementação de soluções de SIEM (*Security Information and Event Management)*, equipas de SOC [AWA]	existe algum desleixo ainda, mas já existem alguma consciencializaçã o para o impacto possível e portanto com o *boost* do GDPR, as organizações portuguesas e europeias vão fortalecer-se neste tópico [AWA]			O estado de maturidade pode ainda ser trabalhado nomeadamente o que deve ser feito é uma campanha de médio-longo prazo ativamente junto da academia, treinando os mais novos para este tipo de questões [AWA]	escalar é arriscado… trata-se de uma ambiente ambíguo porque depende do contexto subjacente, depende do ataque, da capacidade de resposta [AWA] Muito, ainda há muito que pode ser feito [AWA] grande parte do que há a ser feito tem que ver com a prevenção e educação. Isto só se atinge quando a população começa a ter uma perceção das consequências [AWA] não estamos nem melhor nem pior que outros países nesta matéria, até porque trabalhamos muito em cooperação. Mas temos os quadros e as competências adequadas à investigação do cibercrime. [AWA]

Concretamente para a questão ID-K: *"Considerando casos da mesma natureza e escala do "caso WannaCry 2.0", é expectável que novos cenários como este venham a acontecer?"*, que foi colocada a 6 dos 7 entrevistados e que pode ser enquadrada dentro do THEME: *Cyberattacks*; foram verificados os CODEs apresentados na Tabela 13:

Tabela 13 - Análise dos CODEs e THEMEs para a pergunta: "Considerando casos da mesma natureza e escala do "caso WannaCry 2.0", é expectável que novos cenários como este venham a acontecer?"

Segurança de Informação		Criptomoedas		Criminalidade Informática		
Paulo Moniz	José Pereira	Mário Valente	*Riclas*	CAlm Gameiro Marques	Rogério Bravo	Carlos Cabreiro
vão continuar a suceder [CYB] basta descobrir vulnerabilidades em superfícies de ataque muito vastas e é certo que vão ser exploradas [CYB] acho que estamos cada vez mais preparados e estes acontecimentos fazem com que as empresas cresçam em conjunto e melhorem os seus procedimentos, obrigando a que os ataques também tenham que ser mais sofisticados [AWA]	Certamente que pode [CYB] esse tipo de ataques têm vindo a ser cada vez mais problemáticos e mais intrusivos [CYB] a superfície de ataque explorável também é maior. Todas as organizações hoje, por mais pequenas que sejam, têm um Sistema de Informação, por isso o impacto também é maior e mais abrangente [VIC]	É naturalmente expectável [CYB] juntaram-se uma série de fatores que propiciaram o ataque , começando pelo parque muito grande de máquinas expostas a serem atacadas pelo *WannaCry* [VIC] tal como este, muitos outros buracos estão por aí à espera de serem explorados… E nem estou ainda a falar dos Zero-Days…[CYB]		Vai-nos acontecer. Pode ter a certeza que vai acontecer [CYB] melhor maneira de estarmos protegidos é estarmos preparados (…) não basta investir em tecnologia para nos proteger. Tem de se fomentar a maturidade digital das organizações. É necessário investir no capital humano e criar culturas de segurança internas [AWA]	o impacto, em Portugal, só não foi grande, objetivamente devido à tolerância de ponto dada pelo governo em consequência da visita do papa a Portugal [CYB] grande parte da função pública estivesse desligada [VIC] CNCS apercebeu-se que esse incidente se propagava através de uma vulnerabilidade para a qual não havia solução naquele momento e deu o alerta e quase como efeito Dominó, as empresas fizeram o shutdown [AWA] A confluência destes pontos mitigou os danos resultantes do malware [CYB] Consequência foi a indisponibilidade de serviços prestados [VIC] falamos aqui mais de sorte do acaso do que em planeamento de resposta para este incidente [VIC]	É expectável que continue a acontecer. Essa é a tendência que temos vindo a verificar no que toca aos ataques informáticos [CYB] Empresas foram muito resilientes do ponto de vista da resposta a este ataque [AWA]

Por fim e para outra das questões que foi colocada a todos os entrevistados, concretamente a questão ID-AC: *"Qual o potencial futuro das criptomoedas como ameaças em ambiente digital?"*, que pode ser enquadrada dentro dos THEMEs: *Awareness e InfoSec;* e *Cyberattacks*; foram verificados os CODEs apresentados na Tabela 14;

Tabela* 14 - *Análise dos CODEs e THEMEs para a pergunta: "Qual o potencial futuro das criptomoedas como ameaças em ambiente digital?"

Segurança de Informação		Criptomoedas		Criminalidade Informática		
Paulo Moniz	José Pereira	Mário Valente	*Riclas*	CAlm Gameiro Marques	Rogério Bravo	Carlos Cabreiro
Não vejo como ameaça [BTC-TQ] problema da BTC é que tal como os EUR e os USD também são usados para o mal… é como tudo. [CYB]	vejo com alguma dificuldade a evolução deste tipo de ataques [CYB] embora tenham vindo a ganhar adesão para fins ilícitos [CYB] o rastreio é cada vez maior por parte das autoridades [AWA]	Existe o mito do *untreaceable* e do "completamente anónimo", isto só não acontece se a *trade* for em *cash* [BTC-TQ] o objetivo último de um criminoso não é comprar BTC e depois ir fazer coisas más com a BTC (…) normalmente é ao contrário: eu faço algum crime e pagam-me em BTCs [CYB] o resumo é que as criptomoedas podem alavancar o crime informático no sentido de serem feitos um conjunto de crimes informáticos, ou com recurso à informática (venda de droga na *darkweb* por exemplo) que geram BTCs e têm por conseguinte os esquemas usados para as trocar por dinheiro [CYB] as BTCs podem ser trocadas ao vivo por dinheiro vivo, o que ainda é uma realidade muito diminuta em Portugal [CYB]	Não as vejo como ameaça, mas como alternativa [BTC-TQ] não surgiram crimes novos com as criptomoedas, o que surgiu foi uma reinvenção dos crimes antigos [CYB] a criptomoeda veio facilitar os crimes digitais [CYB] É mais uma ferramenta que permite agir criminalmente de forma diferente, não é para substituir mas é para reinventar e incrementar certas práticas [CYB]	Eu não as vejo como uma ameaça. O ser humano estranha a mudança e a novidade inicialmente [BTC-TQ] isto ameaça o status quo económico da nossa sociedade, nomeadamente a banca e o sistema monetário tal como o conhecemos [BTC-TQ] BTC é a abstração máxima da moeda física [BTC-TQ] Blockchain acaba por ser ainda mais fraturante no meio disto tudo [BTC-TQ] isto não é uma ameaça do meu ponto de vista, mas é acima de tudo um desafio [BTC-TQ] O dinheiro vivo também é usado para coisas más [BTC-TQ]	Uma coisa são as criptomoedas, outras coisas são as múltiplas utilizações que se podem dar à BlockChain. A principal ameaça pode vir daí [CYB] quando aparecerem os primeiros a tentarem promover o negócio nessas áreas, vai ser complicado [CYB]	Não sei se vai ser ameaça [BTC-TQ] criptomoedas só são uma ameaça se estiverem a suportar atividades criminais, em termos económicos, em termos de criminalidade organizada, até da própria autonomia dos países [CYB] no mundo do crime a questão da atribuição vai tornar isto ainda mais difícil. [CYB]

Após esquematização do conteúdo recolhido em entrevista e posterior observação do mesmo conteúdo é possível concluir que para as questões acima equacionadas se verificou o registo de CODEs presenta na Tabela 15.

Tabela 15 - Esquematização de registo de CODEs

ID da questão	CODEs registados
ID-A	*23x Cyberattacks; 2x A & Infosec; 1x Victims; 1x BTC TC;*
ID-B	*11x Victims; 1x CyberAttacks;*
ID-C	*9x Victims;*
ID-D	*17x A & Infosec*
ID-E	*14x Victms; 1x A & Infosec;*
ID-G	*11x A & Infosec;*
ID-K	*10x Cyberattacks; 4x A & Infosec; 5x Victims;*
ID-AC	*13x CyberAttacks; 1x A & Infosec; 10x BTC TC;*

É possível afirmar ainda que o CODE mais vezes detetado dentro das questões analisadas em *clusters* foi o de *Cyberattacks* com 47 registos, seguindo-se com 40 registos *Victims,* com 36 registos *Awareness & Infosec,* e por fim o CODE *BTC Technical Questions* foi registado 11 vezes. Uma vez que algumas questões levantadas estão diretamente relacionadas com uma dimensão de análise específica, foi possível estabelecer uma relação direta entre as dimensões de análise: Criminalidade Informática; e Segurança de Informação; e o registo de CODEs. Assim para as questões que incidiam na dimensão de Segurança de Informação: ID-A; ID-B; ID-C; ID-D, ID-E; e ID-G; registou-se uma predominância de CODEs afetos a *Victims,* seguida de *Awareness & Infosec* e *Cyberattacks.* Já para as questões analisadas diretamente relacionadas com a dimensão de Criminalidade Informática: ID-K; e ID-AC; verificou-se uma maior incidência de CODEs afetos a *Cyberattacks,* seguido de *BTC Technical Questions e Victims* e *Awareness & Infosec* com o mesmo número de registos.

5.3. Desenvolvimento

5.3.1. O nível de sensibilização das potenciais vítimas

No que concerne ao tópico relativo ao nível de sensibilização das hipotéticas vítimas de ciberataques, ou seja dos utilizadores do ciberespaço, sejam eles utilizadores singulares do ciberespaço, colaboradores empresariais passando por todos os níveis até às chefias e até aparelhos da administração pública, as respostas dos entrevistados foram consensuais relativamente ao nível consolidado de sensibilização e *awareness* das empresas e de uma fatia substancial de organismos públicos. Note-se que apesar da amostra de entrevistados consubstanciar apenas duas personalidades afetas a organismos públicos, o seu passado profissional e relações com os seus homólogos noutras organizações, proporciona-lhes um conhecimento do estado atual desta questão nos restantes organismos públicos, ou pelo menos, de uma grande maioria. Inclusivamente e face às respostas dadas à pergunta ID-D - *"Considera que as potenciais vítimas estão sensibilizadas ou preparadas para lidar com a ameaça?";* Paulo Moniz e José Pereira, entrevistados no âmbito da dimensão de análise de Segurança de Informação e responsáveis pela segurança de organizações que trabalham diretamente com o Estado, assim como Mário Valente, também conhecedor da questão para o setor empresarial, afirmaram existir um forte nível de sensibilização nas suas organizações para as questões dos ataques informáticos e até dos ataques informáticos que tiram partido dos sistemas de criptomoedas. Mário Valente indicou ainda que esta é uma tendência, que apesar de ainda estar descurada em algumas organizações, vai-se verificar cada vez mais, tendo em grande responsabilidade nesta variação, a transposição da regulação europeia GDPR. Neste sentido, os dois primeiros afirmaram ainda que as organizações onde cumprem funções têm sistemas de gestão da segurança de informação implementados e robustos, assim como os colaboradores são conhecedores das normas e boas práticas certificadas pela ISO 27001. Para além disto, Paulo Moniz referiu ainda que existe o cuidado de divulgar as ameaças através de ações de sensibilização no sentido de criar o alerta para os problemas de segurança no ciberespaço e iniciativas dos atacantes mais recentes. Esta ideia vai ao encontro do que foi avançado pelos entrevistados no domínio de criminalidade informática, tendo inclusivamente o CAlm Gameiro Marques enfatizado a importância das iniciativas de sensibilização para esta temática promovidas pelos organismos responsáveis (PJ, GNS, CNCS, Ministério da Defesa), tendo em vista a consolidação da resiliência digital nas organizações e a capacitação dos seus quadros para

os procedimentos a executar face às exigências recentes que os processos digitais obrigam.

Ainda neste âmbito, a pergunta ID-E - *"As empresas vítimas de ciberataques que as comprometam têm por hábito reportar às autoridades competentes?";* que está relacionada com as questões de sensibilização considerando que um *report* mais frequente por parte das vítimas pode contribuir para um fortalecimento geral das capacidades de resposta a incidentes, através de um trabalho colaborativo entre as várias organizações com um papel nesta matéria. Assim, os entrevistados para a dimensão de Criminalidade Informática consideraram que o hábito de *report* ainda não é um hábito das organizações do setor privado, tendo sido registados números baixos por parte dos mesmos. Os entrevistados pertencentes aos organismos de polícia nacionais afirmaram ainda que organismos públicos têm obrigação de reportar face à formulação legal de um crime público. No entanto, o mesmo não acontece relativamente a empresas privadas, uma vez que vêm muitos custos associados e relativa eficácia dada a morosidade na resolução aquando do *report* às autoridades, preferindo por vezes resolver o incidente internamente, o que chega a implicar pagar o resgate. Foi ainda feita referência por parte de Rogério Bravo e Mário Valente, ao facto de a questão da afetação da reputação das organizações comprometidas, motivar as mesmas a tentar silenciar o assunto fazendo com que não reportem.

Procurou-se ainda, junto dos entrevistados afetos a empresas, Paulo Moniz, José Pereira e Mário Valente, perceber qual o nível de perceção ao risco, por parte dos quadros de topo das organizações, através da pergunta ID-F: *"Ao nível do poder decisório, qual o nível de awareness e de perceção do risco p/ estes incidentes, por parte dos c-levels?";* tendo-se concluído que este é um assunto de interesse por parte dos *boards* das empresas nacionais e que existem níveis de sensibilização transversais a todas as camadas das organizações. Mário Valente indicou ainda que o nível de alerta despertou quando as questões do GDPR foram colocadas em cima da mesa, tendo gerado algum receio das consequências afetas ao não cumprimento da regulação e despertando assim alguma reação nas organizações mais descuidadas.

Por fim, abordou-se ainda a questão do estado de maturidade das organizações para lidarem com incidentes de segurança, através da pergunta ID-G: *"Qual o estado de maturidade na cultura de segurança das organizações nacionais?;* onde foi feita novamente referência, por Mário Valente, ao potencial positivo do GDPR nesta matéria. Quanto aos representantes dos opc's admitiram que existe ainda trabalho a ser feito no

sentido de trabalhar o estado de maturidade das organizações, nomeadamente estimulando para a prevenção através da educação e do trabalho cooperativo. Já Paulo Moniz afirmou que considerando todas as organizações nacionais de todos os tipos, setores e dimensão o nível de maturidade estará algures perto do 4, numa escala de 0 a 10, estando apesar disso algumas organizações de áreas específicas com um nível de maturidade de 8, referindo-se as áreas e empresas com atuação nos setores das TIC, ou organismos grandes e que lidam com informação crítica. De encontro ao que foi indicado por Paulo Moniz, também José Pereira indicou que na sua organização a nível de maturidade estará entre o 7 e 8, na mesma escala, considerando-o positivo mas admitindo que existem ainda outras componentes a serem trabalhadas, como a implementação de soluções de SIEM e equipas de SOC. Carlos Cabreiro destacou ainda a dificuldade em avaliar o nível de maturidade das organizações nesta matéria uma vez que esta avaliação está sujeita a um ambiente ambíguo uma vez que depende do contexto subjacente, depende do ataque, da capacidade de resposta, entre outras fatores.

Resumindo, a investigação empírica permitiu concluir relativamente ao nível de sensibilização das potenciais vítimas que existe um nível consistente aos níveis da sensibilização e conhecimento relativo a ciberataques e ciberincidentes dentro das organizações nacionais, sendo que é também consensual que esta tendência é crescente e portanto as mesmas vão fortalecer-se ainda mais, muitas por motivação própria, outras por via de obrigações legais. A perceção do risco leva inclusivamente algumas organizações de maior dimensão e estrutura a procurarem soluções de mitigação de risco assim como soluções de boas práticas na gestão da sua informação, o que indica que esta é também uma questão de interesse para os *C-levels*. Apesar disto o nível de *report* de incidentes está ainda aquém do desejado muito por culpa da morosidade do processo legal e da indefinição no que toca à eficiência da resolução e consequente mitigação do impacto seja ele uma perda financeira, operacional, de informação ou até de reputação. Quanto ao estado de maturidade, o universo dos entrevistados considerou-o positivo, fazendo no entanto referência à necessidade de trabalhar a constante aprendizagem nestas matérias, até face à constante mutação do ecossistema.

Resta ainda fazer referência a este tema face à metodologia de investigação e verificação dos dados recolhidos. Assim no concerne aos THEMEs verificados através da categorização dos CODEs, predominam as respostas que tiveram incidência nos

THEMEs: *Awareness & Infosec* para as perguntas ID-D, ID-F e ID-G e *Victims* para a pergunta ID-E.

5.3.2. Consequências para as vítimas

Interligada à questão da sensibilização das potenciais vítimas está o tópico das consequências para as efetivas vítimas de ciberataques, pelo que este foi também um assunto procurado junto dos entrevistados, através da pergunta ID-B: *"Quais as consequências mais impactantes para as vítimas";* para a qual as respostas foram de certa forma consensuais e todas elas equacionaram um leque variado de ciberataques, no entanto foi notória a referência direta aos ataques de *Ramsonware*. Os entrevistados para a dimensão de Segurança de Informação e também Mário Valente concordaram ao dizer que as principais consequências no plano organizacional estavam ligadas à inoperacionalidade e consequente perda de faturação pelo tempo inativo. Paulo Moniz indicou ainda que, para os utilizadores singulares, a perda dos dados e conteúdos pessoais e/ou confidenciais pode ser tão danosa como a própria perda financeira. Na mesma linha de pensamento, os representantes das forças de segurança indicaram que a consequência dos ataques está diretamente relacionada às motivações que levam os criminosos a levar a cabo este tipo de práticas e que passam pela obtenção de lucro e pela tentativa de encobrir o seu rastreio, que têm, por conseguinte, consequências imediatas como é o prejuízo financeiro da vítima e a possível perda de informação importante e também consequências mediatas que passam pela dificuldade na atribuição do crime e ainda pelo estímulo da imaginação criminal, para tirar partido destas ferramentas, não para o ganho monetário, mas para o aproveitamento para sabotagem.

Procurou-se ainda perceber, através da pergunta ID-C: *"Para que grupo de vítimas (organismos públicos, corporate ou indivíduos) as consequências são mais danosas?";* onde as respostas variaram substancialmente, não em função da dimensão de análise ou do contexto profissional de cada um dos entrevistados, mas sim em função do parecer pessoal. Assim Paulo Moniz, Mário Valente e Carlos Cabreiro referiram que é difícil colocar uma das opções como sendo a que mais é afetada por este tipo de práticas, considerando que aqui se coloca uma questão de escala e dimensão, isto é, o mesmo incidente pode ser quase catastrófico em termos financeiros para um indivíduo, no entanto nunca terá o mesmo impacto para organizações, sendo que para estas, o principal impacto será sempre a perda de informação crítica. Mário Valente indicou que apesar de os

indivíduos singulares estarem mais expostos, um problema de segurança resultará sempre num impacto relativo maior do que para Estado e empresas, que apesar de estarem menos expostos, podem sofrer impactos maiores, tendo por isso um impacto absoluto maior. Fez ainda referência à questão da insegurança da informação e das infraestruturas de rede e de sistemas afetos aos serviços de saúde, que estão, segundo ele, por norma, extremamente desprotegidos e repletos de dados críticos apetecíveis pelo dinheiro que valem, por exemplo em mercados negros. Já Rogério Bravo considerou que os registos existentes indicam que as consequências mais danosas são para as entidades que têm compromissos com clientes, ou seja empresas. Opinião contrária foi assumida por José Pereira que indicou que, no seu parecer, os indivíduos estão mais vulneráveis por não estarem tão alerta para este tipo de questões quanto as empresas e organismos públicos.

Assim a avaliação dos dados recolhidos depreende que no plano organizacional as consequências passam essencialmente pela perda de informação crítica e pelo tempo de inoperacionalidade a que a mesma possa estar sujeita e consequente perda de faturação pelo tempo inativo. Já para indivíduos as consequências passam também pela perda de informação crítica, mas principalmente pela perda financeira que podem estar sujeitas. Já relativamente ao grupo para o qual as consequências são mais impactantes, a pergunta gerou posições diferentes, considerando-se por isso que possivelmente seja difícil considerar um como o que mais é impactado, sendo por isso cada um afetado à sua proporção. Destaque assim para a questão da escala e dimensão do alvo atacado e dos *outputs* que o ataque vai ter como consequência.

Uma breve ressalva apenas para referência a este capítulo face à metodologia de investigação e verificação dos dados recolhidos. Assim no que concerne aos THEMEs verificados através da categorização dos CODEs, predominam as respostas que tiveram incidência no THEME: *Victims* para ambas as perguntas, sendo que na pergunta ID-B foi também gerado um CODE afeto aos *Cyberattacks*.

5.3.3. Cenário em Portugal

Um dos pressupostos de investigação passava por alcançar um conhecimento da realidade em estudo no contexto nacional, pelo que algumas perguntas foram levantadas com esse mesmo intuito. Assim a primeira questão levantada a todos os entrevistados ID-A: *Como vê o panorama nacional no que concerne aos crimes e ciberataques cujas criptomoedas contribuem para a sua consumação?";* sendo uma pergunta que abrange um grande leque de temáticas, suscitou diferentes reações. Os entrevistados afetos à Segurança de informação, assim como *Riclas,* consideram o fenómeno como estando em crescimento, o que se deve também à valorização recente da criptomoeda *Bitcoin* que, segundo estes, atraiu e vai continuar a atrair pessoas. Este *buzz* vai ter por conseguinte o aliciar de mais criminosos que se vão aproveitar do sistema das criptomoedas e de outros ciberataques através da exploração de vulnerabilidades e das variadas alternativas existentes, que apesar de estarem em constante mutação e transformação para se adaptarem aos controlos de segurança implementados e estabelecidos, têm, em grande parte dos casos, uma resposta sólida por parte das organizações. Neste âmbito Mário Valente indicou que os ciberataques são muitos, diários e provenientes dos mais variados pontos do globo, sendo que críticos são poucos e muito raramente são provenientes de Portugal. Dentro da dimensão de análise das criptomoedas *Riclas* afirmou que existe uma relação entre crimes com dinheiro físico e crimes praticados com criptomoedas, sendo que as segundas são comummente usadas como substituto do dinheiro, também no âmbito criminal. Quanto aos entrevistados afetos às forças de segurança, sendo aqueles que detêm uma visão genérica do panorama nacional no que concerne ao cibercrime, é consensual que se trata de uma tendência crescente e muito atual. Apesar de o panorama nacional equacionar vários crimes com recurso a criptomoedas como financiamento terrorista, lavagem de dinheiro, evasão fiscal, crimes de extorsão, ou até transações em mercados negros como tráfico de armas, drogas (Pinto, 2017) e outros produtos ilícitos, é nos ataques de *Ramsonware* que se verifica uma maior exploração por parte dos agentes criminais. Rogério Bravo indicou ainda que em todas as vertentes acima enunciadas, as criptomoedas aparecem como componentes de financiamento e anonimização da fonte, onde a principal motivação dos agentes do crime é a de obter lucro, sendo que, apesar desse lucro ser muitas vezes obtido em *Bitcoins,* o objetivo último não é o de as transacionar dentro do mundo digital, mas sim o de o transmutar de criptomoeda para dinheiro físico, após a consumação dos ilícitos que levaram à obtenção dessas mesmas

BTCs. Este facto leva a que os crimes relacionados com criptomoedas passem sempre também pelo crime de branqueamento de capitais obtidos a partir de atividades ilícitas. Carlos Cabreiro abordou ainda o tema na ótica da investigação criminal, onde considera que também no contexto nacional, crimes com estas características trouxeram novas especificidades na determinação da autoria do crime, onde a anonimização associada às ferramentas usadas aliciou novos agentes do crime.

Ainda no âmbito do cenário nacional, pode ser equacionada a pergunta ID-G: *"Qual o estado de maturidade na cultura de segurança das organizações nacionais?"*, já analisada no capítulo 5.3.1. e da qual se depreendeu que o estado de maturidade e a cultura de segurança nas organizações nacionais é crescente, existindo no entanto, ainda trabalho a ser feito no sentido de estimular para a prevenção através da educação e do trabalho cooperativo. Neste sentido, Carlos Cabreiro destacou ainda a dificuldade em avaliar esta matéria uma vez que está sujeita a um ambiente ambíguo uma vez que depende do contexto subjacente, dependendo do ataque e da capacidade de resposta, entre outros fatores. No entanto a conclusão chegada é a de que existe já um nível de maturidade positivo, mais forte nas organizações que estão muito expostas ao digital. Mário Valente contrapõe esta questão do ponto de visto do desenvolvimento aplicacional e dos posteriores processos operacionais, sendo que em resposta à pergunta ID-H: "*Como parte de empresa que desenvolve soluções, estas são desenvolvidas tendo em conta o conceito de Security by design?"* afirmou que pelas organizações por onde passou e com quem trabalhou, as aplicações desenvolvidas não eram criadas mediante este conceito e que muitas das soluções utilizadas, até por organismos públicos não são sequer auditadas em termos de código de desenvolvimento. Segundo o próprio este fenómeno deixa em aberto uma superfície explorável grande que aguarda o aparecimento de uma configuração de ataque que as explore.

Quanto aos entrevistados afetos a organizações, estes indicaram através das repostas dadas à pergunta ID-O: "*Quais os ataques informáticos mais dirigidos à EDP/ESPap e respetivo impacto?*"; que o CNCS e as forças de segurança têm um papel muito importante na prevenção e mitigação dos riscos inerentes e a que estão sujeitos as organizações nacionais, tendo os ciberincidentes como resultado um impacto pouco significativo. Face a isto, são registados maioritariamente ataques de *phishing* dirigidos a clientes mas também a colaboradores, tanto da EDP como da eSPap, sendo que foram já detetados ataques de DDoS aos sistemas da EDP.

Relativamente aos entrevistados afetos às forças de segurança e face à pergunta ID-Y: "*Há registo em Portugal, da utilização de criptomoedas para financiar organizações terroristas, para práticas de lavagem de dinheiro ou para comercialização de bens em mercados negros online?"; o*s membros da PJ responderam afirmativamente à existência deste tipo de práticas com recurso a criptomoedas em contexto nacional, sendo que Carlos Cabreiro deu destaque a crimes de partilha de conteúdos pedo pornográficos na Internet e de *sextortion*, os quais são muitas vezes pagos em criptomoedas, nomeadamente *Bitcoins*, tal como havia sido feita referência através do relatório da EUROPOL, IOCTA, 2016, no capítulo 4.1.1.. Em termos de eficácia da investigação, os mesmos declararam, face à pergunta ID-Z: *"Dadas as características das criptomoedas qual a eficiência da investigação no tracking das transações e na atribuição dos ataques?;"* que apesar de a investigação criminal não se poder suportar única e exclusivamente numa única fonte de prova é já possível através de certas ferramentas detetar o rasto de transações de criptomoedas, dependendo sempre da forma de atuar do agente criminal. Esta é uma situação que se complica apenas aquando da transação das criptomoedas por dinheiro vivo, ou até através de esquemas multi-distribuídos para lavagem de dinheiro, sendo estas tipificações os únicos cenários em que a investigação criminal perde muita eficiência.

Os mesmos agentes foram ainda questionados sobre o nível de preparação das forças de segurança nacionais, através da pergunta ID-AA: "*Qual o estado atual de preparação (prevenção/reação) das forças e serviços de segurança para lidarem com ciberincidentes deste tipo?";* sobre o qual destacaram a importância da cooperação europeia com a EUROPOL, assim como a capacitação de meios técnicos e do capital humano indispensável à boa condução da investigação criminal e importante também para eficiência da mesma. O entrevistado Rogério Bravo escalou ainda o nível de preparação das forças e serviços de segurança nacionais, atribuindo-lhe o nível 7 numa escala de 0 a 10. Associada à questão ID-AA está a questão ID-AB: "*O que pode ainda ser feito para que estas possam atingir um estado de maturidade que lhes permita estar preparadas para lidar com este tipo de ameaças e outras semelhantes?"*; para as quais o CAlm Gameiro Marques enfatizou a competência da resposta cooperativa dos organismos de governo afetos ao Ministério da Defesa que têm um papel importante em colaboração com as forças de segurança. Considera ainda fundamental o investimento paternalista a longo-prazo, no desenvolvimento de um forte e estruturado programa pelo qual fosse incutido nos jovens uma cultura que os torne mais resilientes do ponto de vista digital

desde o início da sua utilização tecnológica. Já a curto-médio prazo considera que algumas iniciativas estão já a ser alavancadas e começam já a contribuir para atingir um nível de maturidade superior, como é o caso da adequação da moldura legislativa para a realidade do cibercrime e ainda o fortalecimento cooperativo em termos dos controlos e procedimentos de reação a ciberincidentes.

Assim e fazendo o ponto da situação do cenário nacional no que diz respeito à utilização da criptomoeda, aos crimes consumados com recurso a esta e à capacidade de resposta das instâncias indigitadas para tal, aquilo que se percebeu com a análise ao conteúdo das entrevistas é que este é um fenómeno crescente, quer na utilização lícita como ilícita, o qual pode ser comparado à relação entre crimes com dinheiro físico e crimes praticados com criptomoedas, sendo as segundas comummente usadas como substituto do dinheiro em ambiente digital e também no âmbito criminal. Confirmou-se ainda que a prática criminal com recurso a criptomoedas consubstancia-se numa série de diferentes crimes, entre os quais: financiamento terrorista, relacionados com práticas de lavagem de dinheiro, evasão fiscal, para comercialização de bens em mercados negros *online*, para crimes relacionados com a partilha de conteúdos pedo pornográficos na Internet e ainda para extorsões, sejam práticas de *sextortion* ou de *Ramsonware.* Percebeu-se ainda que esta última tipificação de ataque é a que detém a maior percentagem de ataques reportados às autoridades, depreendendo-se que é aquela que ocorre com mais frequência. A motivação para a prática criminal nestes moldes, tanto em Portugal como no resto do mundo, passa pela obtenção de lucro que terá como fim a sua transmutação de criptomoeda para dinheiro físico, após a consumação dos ilícitos que levaram à obtenção dessas mesmas criptomoedas. Este facto leva a que os crimes relacionados com criptomoedas acabem sempre por estar também relacionados com branqueamento de capitais obtidos a partir de atividades ilícitas.

Tendo também em conta o que foi relatado em relação à eficiência e maturidade da investigação criminal e das forças de segurança nestes aspetos, percebeu-se que crimes com estas características trouxeram novas especificidades na determinação da autoria do crime. Apesar de ser já possível detetar o rasto de transações de criptomoedas quando estas são transacionadas através de plataformas e sistemas rastreáveis, existem ainda situações que deixam a investigação criminal pouco capacitada para a resolução do crime. No entanto conclui-se que as forças de segurança nacionais estão capacitadas de meios técnicos e do capital humano necessário à eficiência da investigação criminal, na qual a

cooperação com organismos de polícia estrangeiros e comunitários se revela também da máxima importância.

Por fim, verificou-se que o estado de maturidade e cultura de segurança das organizações acima mencionadas, assim como das organizações do setor privado nacional foi considerado consensualmente positivo e crescente. Sendo que existe ainda trabalho a ser feito no sentido de estimular para a prevenção através da educação e do trabalho cooperativo.

Resta ainda fazer referência a esta questão face à metodologia de investigação e verificação dos dados recolhidos. Assim no concerne aos THEMEs verificados através da categorização dos CODEs, predominam as respostas que tiveram incidência nos THEMEs: *Cyberattacks* para as perguntas ID-A e *Victims* para a pergunta ID-G. Relativamente às outras questões não comparadas em tabelas por terem sido colocadas a 3 ou menos entrevistados, como explicado no subcapítulo 5.2., a estatística foi feita diretamente através das entrevistas que constam nos apêndice 3 até 9 e do catálogo de perguntas, Apêndice 2, e verificou-se que para a pergunta ID-H o THEME predominante foi *Awareness & Infosec*, para a pergunta ID-O e ID-Y, *Cyberattacks*, para a pergunta ID-Z, *Cyberattacks* e *BTC Technical Questions* com tês registos cada e por fim, para as questões ID-AA e ID-AB o THEME predominante foi para ambas *Awareness & Infosec.*

5.3.4. Análise ao trading de Bitcoins

Para efeitos da análise ao *trading* de *Bitcoins*, foram consideradas única e exclusivamente questões colocadas ao entrevistado *Riclas*, uma vez que, do universo dos entrevistados, foi considerado como sendo aquele que tem conhecimentos mais robustos neste fenómeno. Estas questões foram criadas especificamente para este contexto de entrevista.

Assim procurou-se junto do mesmo, a realidade nacional em termos de *trading* de *Bitcoins* através da pergunta ID-P:" *Considerando os diferentes métodos de trocas de, como se divide em termos percentuais, o nº de transações em BTCs, tanto na compra como na venda de BTCs?*"; da qual se percebeu pelos números indicados pelo entrevistado que, em termos percentuais, em AGO2017, pelo método de transações *Single Euro Payments Area* (SEPA), foram realizadas 58% das transações, maioritariamente com países como a Espanha, França e Irlanda, sendo que as transações em *cash*, isto é,

em dinheiro vivo, figuraram em 32,27% do total, seguindo-se as transações nacionais com 6,47% e para outras formas de transação cerca de 3.26%. Os dados são avançados em percentagem, uma vez que o entrevistado solicitou para que não fossem revelados os montantes envolvidos. Note-se que estes dados são representantes da realidade do maior *trader* de BTC em Portugal, que revelou movimentar, através da plataforma *LocalBTC* uma média de 300 transações mensais através de instituições bancárias ou sistemas de pagamento rastreáveis e apenas cerca de 4 por mês em transações feitas em dinheiro vivo, percebendo-se por isso que o último acaba por ser claramente o método de transações que envolve montantes mais avultados, em congruência com o que indicia o estudo de Tasca, 2015, respondendo-se assim à questão ID-Q: "*Quais os métodos de transações que envolvem montantes mais avultados, tanto para compra como para venda de BTCs?*"; No que concerne à obtenção dos BTC que disponibiliza para troca e fazendo referência à pergunta ID-R: "*Os BTCs que tem para troca são provenientes de investimento próprio, ou de BTC adquiridas através de mining?*"; *Riclas* indicou que são provenientes de investimento próprio, apesar de no início ainda ter tentado gerar criptomoeda através de *mining*, atividade que acabou por desistir por não ter capacidade de processamento equiparada às grandes *pools* existentes na China, tendo-se por isso dedicado única e exclusivamente ao negócio das trocas.

Em resposta às perguntas ID-S e ID-T: "*Certamente quando tudo começou o preço unitário era significativamente mais baixo. A valorização da BTC alterou os padrões das trocas?*"; e "*A procura por Bitcoin é crescente?*"; o entrevistado assumiu não ter sentido alterações no padrão de troca diretamente associadas à recente valorização, no entanto destaca que apesar de sentir que a procura é crescente, o seu volume de trocas mantém-se regular desde o início de 2016, não conseguindo para isso apurar uma causa.

Quando levantada a temática do cibercrime e do papel das criptomoedas nesse fenómeno, *Riclas* admitiu, através da resposta à pergunta ID-V: "*Tendo em conta que os produtos ou serviços adquiríveis em BTC, em Portugal, ainda têm uma expressão muito reduzida, para que fins pensa que os indivíduos nacionais lhe compram BTC?*"; ter consciência do fim da utilização das *Bitcoins* obtidas através das transações que efetua numa alusão clara à instrumentalização da mesma em crimes informáticos, ou com recurso a ferramentas informáticas, indicando ainda, através da resposta à questão ID-W: "*Muitos dos pedidos de transações podem estar relacionados com o pagamento de resgates (ramsonwares/Sextortion). Neste contexto consegue dar um cenário em termos de frequência, montantes, feedback dos users que fazem estes pedidos*?"; que tem

conhecimento que muitas transações em todo o mundo servem propósitos de evasão fiscal e lavagem de dinheiro, no entanto não tem conhecimento do cenário real nacional, uma vez que a própria arquitetura do sistema de transações não o permite.

Posto isto, resta fazer referência a esta questão face à metodologia de investigação e verificação dos dados recolhidos. Assim no que concerne aos THEMEs verificados através da categorização dos CODEs. Considere-se que as questões analisadas que se enquadram neste capítulo não foram comparadas em tabelas, assim a estatística foi feita diretamente através da entrevista que consta no Apêndice 7 e do catálogo de perguntas, Apêndice 2, verificando-se que para as perguntas ID-P, ID-Q, ID-R, ID-S, ID-T, ID-U, ID-V, ID-W e ID-X os THEMEs predominantes foram na esmagadora maioria *BTC Technical Questions,* com 18 CODEs registados, tendo ainda sido gerados 4 CODEs afetos ao THEME *Cyberattacks.*

5.3.5. WannaCry 2.0

Outra observação foi levada a cabo desta feita relacionada com a análise do maior ataque de *Ramsonware* de que há registo e que ficou conhecido por *WannaCry 2.0*, o mesmo nome do *software* malicioso, da categoria de *crypto-ramsonwares* que infetou em MAI2017 mais de 200 mil sistemas informáticos (Shah, 2017) nos quais corria uma versão de SO *Windows XP*[65] para a qual já não existia suporte desde ABR2014. Ainda assim algumas empresas mais prudentes e cientes das boas práticas de gestão da segurança de informação haviam já instalado os *patches* de segurança para o SO, minorando por isso a superfície explorável de ataque, acabando por não ter sido afetadas.

O ataque de larga-escala foi disseminado através de técnicas de *phishing*, chegando a todos os setores incluindo serviços de telecomunicações, empresas de transportes, organizações governamentais, bancos, hospitais e universidades. Resultando num total de resgates pagos, até na ordem dos 50 mil USD, depositados em três endereços de carteira *Bitcoin*, descobertos por estarem incorporados no *software* malicioso, tendo sido, assim que identificados, monitorizados através de um *bot* (Kharpal, 2017).

Em Portugal, as empresas afetadas, entre as quais a Portugal Telecom[66] e a EDP, decidiram ativar os seus planos de segurança, restringindo o acesso ou desligando as suas

[65] Mais sobre *Windows XP* - https://support.microsoft.com/pt-pt/help/14223/windows-xp-end-of-support;
[66] Mais sobre a *Portugal Telecom* - https://www.telecom.pt/en-us;

redes internas (Perez, 2017), tal como referiu Paulo Moniz, Diretor Segurança e Risco nas TIC da EDP, que indicou, em resposta à pergunta ID-N: "*Como é que a EDP/eSPap experienciou o ataque Wannacry e qual respetivo impacto?*"; que a EDP havia experienciado o ciberincidente de uma forma positiva, uma vez que apesar de ter sido atacada, não teve focos de infeção, não tendo sido, apesar de tudo, dispensada a aplicação de medidas de contenção, tais como o *shutdown* completo da rede dos utilizadores. O entrevistado indicou ainda que a reposta ao incidente foi imediata e daí não ter tido consequências, para além das consequências operacionais inerentes ao *shutdown*. Apesar de tudo e segundo o próprio, no caso de ter existido infeção, as consequências poderiam não ter sido devastadoras, caso a mesma resposta fosse dada rapidamente, uma vez que existiam apenas cerca de 400 máquinas suscetíveis de serem atacadas, dentro de um universo de 18 mil. Assim, e ainda durante o *shutdown* as máquinas suscetíveis foram atualizadas através do mais recente *patch* de segurança, tendo sido depois restabelecida a conexão à rede progressivamente.

Também neste tópico os representantes dos opc's foram questionados relativamente às consequências do ataque através da pergunta ID-L: "*Qual considera ter sido a principal consequência deste ataque, para as vítimas nacionais?";* tendo Rogério Bravo indicado que a principal consequência foi a indisponibilidade dos serviços prestados pela companhia, inerentes ao *shutdown* das máquinas ligadas às redes corporativas. O entrevistado realçou o competente papel do CNCS que cedo se apercebeu que se tratava de um incidente que se propagava através da vulnerabilidade mencionada no início deste subcapítulo e para a qual não havia solução no momento. Assim o cibercentro lançou o alerta e recomendações de controlos aplicáveis de reação que acabaram por resultar eficientemente face ao contexto. Curiosamente, o Inspetor-chefe da PJ chama atenção para um fator externo que resultou numa tolerância de ponto dada pelo governo ao setor público, que minorou substancialmente a superfície de ataque ao nível da função pública. A confluência destes pontos foi, segundo Bravo, o grande *driver* que mitigou os danos resultantes de um ataque muito forte. Já Carlos Cabreiro indicou que a consequência financeira em todo o mundo foi reduzida face à abrangência "brutal" do ataque. Afirmou ainda que a mesma realidade se verificou em Portugal, onde se registaram consequências diminutas, comprovando que as empresas nacionais responderam bem, demonstrando capacidade de adaptação a cenários de ciberincidentes. As condições elencadas que relativizaram os impactos que o ataque teve em Portugal, confirmam-se com a resposta de *Riclas* à pergunta ID M: "*No dia do ataque WannaCry*

2.0 foram-lhe feitas muitas solicitações para compra de BTCs?"; onde o mesmo indicou que não notou grandes diferenças. Pese embora ter tido contactos do estrangeiro que suspeita que tenham sido efetuados com o intuito de pagar resgate relacionados com o *WannaCry 2.0*, não foram feitas solicitações de agentes nacionais, para o efeito.

Por fim no que toca a este caso de estudo, foi ainda procurado junto de 6 entrevistados, se estes esperam ataques semelhantes no futuro, através da questão ID-K: "*Considerando casos da mesma natureza e escala do "caso WannaCry 2.0", é expectável que novos cenários como este venham a acontecer?*"; tendo sido consensual a resposta de que vai voltar a acontecer e de que os agentes estão também cada vez melhor preparados para responder. No entanto é esperada uma maior sofisticação dos ataques informáticos que tendem a tornar-se mais problemáticos e intrusivos, mas também mais lucrativos e destrutivos, sendo estes os fatores que resultam numa motivação incessante na busca por vulnerabilidades que afetem uma grande parque de máquinas, uma vez que serão esses ataques que poderão gerar mais lucro. Destaque para a afirmação do CAlm Gameiro Marques que afirma que continua a ser necessário fomentar a maturidade digital das organizações, através do investimento no capital humano e na criação de culturas de segurança internas.

Resta ainda fazer referência a esta questão face à metodologia de investigação e verificação dos dados recolhidos. Assim no que concerne aos THEMEs verificados através da categorização dos CODEs, considere-se que apenas para a questão ID-K, foi considerada a análise das respostas em *cluster*, que consta da Tabela 15, sendo que para as restantes questões que se enquadram neste capítulo e que não foram comparadas em tabelas, a estatística foi feita diretamente através das entrevistas presentes nos Apêndices 3 até 9 e do catálogo de perguntas, Apêndice 2. Assim verificou-se que para a pergunta ID-K o THEME predominante foi *Cyberattacks* com 10 registos, enquanto para as perguntas de análise isolada se verificaram 5 CODEs para *Victims* na questão ID-L, para a pergunta ID-M o predomínio foi de C*yberattacks* com três registos e por fim, para a pergunta ID-N registaram-se 3 vezes CODEs relacionas com *Awareness & Infosec.*

5.3.6. O potencial das criptomoedas como ameaças em ambiente digital

Por fim e em tom de fecho tanto do desenvolvimento da investigação e respetiva análise através dos dados obtidos, como em tom de fecho também de todas as 7 entrevistas levadas a cabo, procurou-se perceber qual a perceção dos entrevistados face ao potencial futuro das criptomoedas, através da pergunta com o ID-AC: "*Qual o potencial futuro das criptomoedas como ameaças em ambiente digital?*"; tendo-se verificado que a grande maioria do universo dos entrevistados não as vê como ameaça direta, considerando que as criptomoedas são muito mais do que aquilo que representam para o mundo criminal, embora reconheçam que também aí, detêm um papel importante. Paulo Moniz e *Riclas* referiram que não surgiram crimes novos com o aparecimento das criptomoedas, mas sim uma reinvenção tipológica dos crimes antigos, podendo os crimes consumados com criptomoedas ser exatamente comparados aos mesmos crimes consumados com EUR, USD ou outra moeda. No entanto, reconhecem que as criptomoedas e particularmente a BTC veio facilitar os crimes digitais, sendo mais uma ferramenta que permite agir criminalmente com configurações de crime diferentes. Consideram que esta mutação não substitui as tipologias de crime anteriores ao aparecimento das criptomoedas, mas sim reinventa essas mesmas tipologias.

José Pereira, Mário Valente em resposta a esta pergunta e também os representantes dos opc's em resposta à pergunta ID-Z: "*Dadas as características das criptomoedas qual a eficiência da investigação na atribuição dos ataques e no tracking das transações?"*; tiveram uma abordagem semelhante indicando que o rastreio é cada vez mais musculado por parte das autoridades competentes, contribuindo para o desmistificar do mito do *untraceable*, fenómeno que só acontece em determinadas circunstâncias, como se deu a perceber no subcapítulo 5.3.3.. Neste sentido Carlos Cabreiro apesar de considerar que a investigação criminal está capacitada de quadros e ferramentas para enfrentar esta realidade, faz uma ressalva para o facto de considerar que as criptomoedas só consubstanciam uma ameaça pública se estiverem a suportar atividades criminais, podendo assumir-se então como ameaça não só para a própria investigação criminal em termos da atribuição, mas também em termos económicos ou até da própria autonomia dos Estados.

Mário Valente resume o futuro neste contexto como sendo uma realidade para a qual a sociedade se tem de preparar, uma vez que se trata de um fenómeno que vai alavancar, por certo, o cibercrime no sentido de serem feitos um conjunto de crimes

informáticos, ou com recurso à informática que geram BTCs e têm por conseguinte os esquemas usados para as trocar por dinheiro, ou seja para as lavar. Para o entrevistado, podem ser consideradas pelo menos duas variantes, nas quais as criptomoedas podem ser empregues em práticas criminosas: ora em crimes com recurso a ferramentas informáticas ou crimes informáticos propriamente ditos; ora em outros tipos de crimes específicos, não diretamente relacionados com ferramentas informáticas; dando o seguinte exemplo ilustrativo: "*as criptomoedas podem ser consideradas como alternativa moderna para crimes antigos, como é o caso da lavagem de dinheiro, onde em certos esquemas a criptomoeda é o fim de um crime que já existia antes do aparecimento das criptomoedas, tratando-se de uma forma moderna de praticar um crime antigo, no qual, em certas situações, é agora tirado proveito de recursos informáticos, não sendo neles que assenta a prática criminal. E podem também ser consideradas como instrumento para a consumação de um crime informático, onde através de um negócio ilícito online é gerado valor monetário, através por exemplo de algum tipo de sequestro ou da venda de substâncias ilícitas, e a forma de receber o valor conseguido, passa pela transação de criptomoedas. Assim as criptomoedas podem ter lugar na equação criminal em tipologias criminais diferentes, variando no fim da sua utilização, e no momento da consumação do crime em que são utilizadas.";* numa alusão clara ao desafio futuro que esta questão pode colocar à investigação criminal e à disrupção da tipologia criminal tradicional.

Resta ainda fazer referência a esta questão face à metodologia de investigação e verificação dos dados recolhidos. Assim no que concerne aos THEMEs verificados através da categorização dos CODEs respeitantes à pergunta ID-AC, predominam as respostas que tiveram incidência nos THEMEs: *Cyberattacks* com 13 registos, merecendo ainda destaque os CODEs gerados relativos a *BTC Technical Questions*, onde se verificaram 10 registos.

6.Conclusões

6.1. Considerações finais

Findada a exploração da investigação ao estudo da criptomoeda com enfoque nos desafios de substância criminal resta agora esquematizar as conclusões alcançadas.

Este projeto de dissertação propôs investigar o cenário criminal nacional, em ambiente digital e com recurso às criptomoedas analisando os desafios negativos que esta inovação tecnológico-financeira trouxe para indivíduos, governos, organismos reguladores e de polícia e mesmo ao mundo empresarial. O panorama onde o intervalo deixado em aberto entre as novas soluções tecnológicas e a dificuldade em combater quem delas tira partido, deu aso à exploração crescente de variados crimes com diferentes tipologias e com mais ou menos recurso a ferramentas informáticas. Este cenário tem vindo a tornar-se ainda mais alarmante face à tendência crescente da complexidade em tipificar o conteúdo das atividades ilícitas consumadas no ciberespaço, não só devido à sua sofisticação intrínseca como também devido à sua mutação constante e ao ambiente difuso onde as mesmas ocorrem, tendo como resultado uma mais árdua tarefa de prevenção e reação, tanto por parte das entidades responsáveis operacionais como os opc's, como por parte dos indivíduos, das entidades gestoras no caso das empresas e até ao nível dos aparelhos de administração pública e de governo. Note-se que se por um lado a forma como o ecossistema BTC e de outras criptomoedas foram pensados e criados trouxe uma série de benefícios para os seus utilizadores que o usam com fins lícitos, por outro lado, certos utilizadores encontraram nesta moeda criptográfica uma ferramenta que permite alavancar novos métodos, estratégias e atividades criminais em ambiente digital, que dela se utilizam como recurso para uma moderna forma de atuar ilicitamente no ciberespaço. Esta realidade aliada ao facto do crescente exponencial de utilizadores das TIC em contexto pessoal ou profissional, ao facto da crescente digitalização da economia e aliada ao aumento de casos de crime informático ou com recurso a ferramentas informáticas em Portugal, tornou este estudo pertinente no sentido de refletir sobre a temática por forma a compreender a dimensão e o impacto do dilema em mãos, pesando os dano causados e assim perceber quais as consequências para vítimas e criminosos, tentando ainda prever qual a tendência futura e consequentes resultados deste tipo de práticas na comunidade.

Em termos de enquadramento conceptual o estudo foi dividido em 3 dimensões de análise principais: Segurança de Informação; Novos recursos tecnológicos (criptomoedas); e Criminalidade Informática; para os quais foram definidos 3 modelos de análise, que foram considerados como referências e que passam pelas seguintes obras, respetivamente: *International Organization for Standardization* (ISO) 27001 – Manual de procedimentos para a Gestão da Segurança de Informação; *Paolo Tasca*, *Digital Currencies: Principles, Trends, Opportunities* (2015); EUROPOL – *Internet, Organised Crime Threat Assessment* (IOCTA), de 2016;

Neste âmbito a investigação propôs-se a perceber a conjuntura em termos de sensibilização e preparação da sociedade face à evolução deste processo, essencialmente no que toca à segurança da utilização das TIC, assim como a compreender e analisar a posição das forças e serviços de segurança interna nas esferas da investigação, deteção e intervenção em contexto nacional, ou em cooperação internacional, tendo ainda procurado perceber junto do setor empresarial, qual o nível de preparação das empresas para ameaças provenientes do ciberespaço. Outro dos motes para a investigação passou por perceber quais as configurações criminais que se recursam da utilização das criptomoedas, assim como a respetiva dimensão e impacto associado. Por fim procurou-se quais as perspetivas futuras quer em termos de incidência de ciberincidentes com configurações onde as criptomoedas fossem usadas, quer em termos de segurança. Para isto e considerando os pressupostos metodológicos que orientaram a investigação, definiram-se os seguintes objetivos a alcançar com o estudo: enquadrar as ameaças em ambiente digital e analisar especificamente os crimes e cibercrimes que se recursam de criptomoedas; perceber genericamente qual o grau de sensibilização dos cidadãos portugueses, organismos do Estado e empresas nesta matéria; analisar o impacto da consumação deste tipo de atividades nas empresas e nos órgãos administrativos; compreender e analisar a posição das forças e serviços de segurança interna nas esferas da investigação, deteção e intervenção em contexto nacional, ou em cooperação internacional; e ainda perspetivar tendências futuras em termos de prevenção e capacidade de resposta para as ameaças identificadas por parte dos organismos reguladores e de polícia; que culminaram com a definição de uma pergunta central orientadora de toda a investigação: QC - "Qual a dimensão e impacto da utilização da criptomoeda na consumação de atividades criminais?"; e ainda com a definição de 4 questões derivadas resultantes da desconstrução da questão central: QD1 - "De que forma

estão organizações e indivíduos sensibilizados e preparados para ameaças em ambiente digital?"; QD2 - "Que crimes informáticos se recursam das criptomoedas para a sua consumação, ou que têm nelas um veículo para tal?"; QD3 - "Como é que as criptomoedas ameaçam empresas e indivíduos?"; e QD4 - "Quais as perspetivas futuras quer em termos de incidência quer em termos de segurança?";

A investigação destas questões partiu de uma abordagem exploratória de cariz qualitativo para o qual, por ter sido tida em conta a complexidade e inovação das temáticas abordadas e com o intuito de obter uma perspetiva transversal às diferentes dimensões de análise, foi consultado um painel de individualidades especializadas que se podem considerar como *stakeholders* desta temática. Constituído por personalidades cujas qualificações e/ou experiências profissionais lhes conferem perícia nas matérias que compõem ora a problemática geral do tema, ora uma das variáveis específicas em estudo. Neste sentido estabeleceu-se o método Hipotético-dedutivo de recolha e análise de informação, segundo o qual se procurará uma reposta válida à questão central já identificada e assim contribuir para o conhecimento científico ao enquadrar o panorama da utilização das criptomoedas na criminalidade digital nacional. Para o efeito foram consideradas fontes documentais e bibliográficas de relevo assim como foram também consideradas como fontes de informação os contatos diretos feitos pelo autor, sob a forma de entrevistas a personalidades de interesse. As entrevistas consumadas seguiram um alinhamento semiestruturado e adaptado ao contexto profissional do entrevistado e à dimensão de análise segundo o qual cada entrevista decorre. No que concerne aos aspetos metodológicos resta ainda indicar que para cumprir o rigor científico e a qualidade dos conteúdos que serviram de base de investigação deste trabalho, a abordagem qualitativa segundo a qual foram extraídos os contributos recolhidos em contexto das entrevistas seguiu uma abordagem denominada análise temática Braun & Clarke, 2006, segundo a qual os dados recolhidos serão identificados, analisados e agrupados em categorias e padrões, ou temas, seguindo um método estruturado com vista à resolução do fenómeno em investigação.

Os resultados alcançados após análise da informação obtida pelas fontes acima enumeradas podem ser comparados com as hipóteses de investigação que haviam sido definidas previamente ao desenrolar da própria investigação propriamente dita, e que procuravam estabelecer *à priori* possíveis respostas a cada uma das questões de

investigação levantadas. Assim, para a primeira hipótese levantada na fase inicial da investigação: H1- ”O grau de sensibilização para estas questões é, na sua grande maioria, baixo, não estando as mesmas preparadas para utilizar as TI de forma consciente e segura, face à exposição ao risco a que estão sujeitas”; as conclusões do estudo contradizem esta afirmação, uma vez que mediante a informação recolhida em situação de entrevista existe já um nível consolidado de sensibilização e *awareness* das empresas e organismos públicos em Portugal, transversal a todas as posições da companhia, passando dos quadros de topo, aos colaboradores. Esta capacitação é mais consolidada em função da dimensão da organização e da respetiva alocação de recursos às áreas da segurança de informação. Verificou-se a existência de sistemas integrados de gestão da segurança de informação implementados e robustos, assim como o cuidado de formar e sensibilizar os colaboradores para que sejam conhecedores das normas e boas práticas certificadas pelo guia de boas práticas, ISO 27001. Considerando o enfoque do estudo nas criptomoedas, apurou-se que o setor corporativo trabalha também as ameaças provenientes deste tipo de ataques através de procedimentos com vista à sua prevenção e do desenvolvimento de capacidades de resposta. Percebeu-se também que a tendência de fortalecimento destas capacidades é crescente, sendo que a transposição da regulação europeia GDPR para a legislação nacional, contribuirá ainda mais para esta progressão.

No reverso da medalha, os indivíduos estão substancialmente mais expostos e menos preparados para lidar com este tipo de ameaças, face a uma posição de descura negligente afeta à não compreensão da probabilidade de ocorrência e respetivo impacto. Neste âmbito destaque para importância das iniciativas de sensibilização para esta temática promovidas pelos organismos responsáveis (PJ, GNS, CNCS, Ministério da Defesa), tendo em vista a consolidação da resiliência digital nos indivíduos e nas organizações, onde existe ainda o enfoque na capacitação dos seus quadros para os procedimentos a executar face às exigências recentes que os processos digitais obrigam.

Destaque ainda a ser dado à importância da cooperação entre todos os agentes, nacionais e internacionais, com um papel nestas questões, para um crescimento coletivo em termos de segurança no ciberespaço com vista ao bem comum. Neste tópico têm um papel relevante as forças de segurança, os serviços de inteligência, as instituições do Estado afetas à defesa, os organismos públicos e até as empresas privadas, no que toca à partilha de informação de interesse relativa a incidentes no ciberespaço. Note-se que, em Portugal, o cenário de *report* às autoridades de incidentes ocorridos no ciberespaço não é, ainda, um hábito das organizações do setor privado, tendo sido registados números

baixos em termos de *report*, não contribuindo assim para este fomento de conhecimento cooperativo. Assim, depreende-se que apesar de existir ainda trabalho a fazer em termos de maturidade para esta problemática, o estado de maturidade geral das organizações nacionais é positivo, ao contrário do que se previa antes da investigação.

Já para a segunda hipótese levantada na fase inicial da investigação: H2- ”Os crimes são consumados em algum momento através do ciberespaço, sendo que os mais frequentes passam pelo financiamento terrorista, lavagem de dinheiro obtido de forma ilícita, comércio e consumo de bens ilegais e até crimes de extorsão comummente conhecidos por *ramsonware* e *sextorsion”*; o estudo apurou que independentemente do crime específico de que se trate, todos os que tiram partido das criptomoedas estão em tendência crescente, não fossem características como a criptografia que torna o ambiente das criptomoedas e as suas transações anónimas, dificilmente rastreadas ou monitorizadas, assim como o seu funcionamento através de uma arquitetura de rede P2P. Este conjunto de fatores tornaram-se bastante apetecíveis para indivíduos, organizações criminais e até organizações terroristas que vêm no ciberespaço e na criptomoeda um novo espaço operacional para atuarem. Estes agentes, dotados de um engenho audaz na procura de novas soluções para desempenharem as suas atividades com o mínimo de exposição possível, têm assim, através dos algoritmos que sustentam as criptomoedas, ferramentas eficazes e com características que servem os seus propósitos trazendo eficácia e solidez aos movimentos de capitais subjacentes a práticas ilícitas. Posto isto, a hipótese estabelecida *à priori* acabou por se confirmar através das declarações prestadas pelos representantes das forças de segurança, aqueles que melhor visão genérica do panorama nacional no que concerne ao cibercrime têm. Assim existem registos em Portugal de crimes com recurso a criptomoedas como financiamento terrorista, lavagem de dinheiro, evasão fiscal, crimes de extorsão como o *sextortion*, crimes relacionados com a comercialização e partilha de conteúdos pedo pornográficos na Internet, ou até transações em mercados negros como tráfico de armas, drogas e outros produtos ilícitos, sendo que é nos ataques de *Ramsonware* que se verifica uma exploração mais frequente por parte dos agentes criminais, com uma procura de alvos maioritariamente focada no setor corporativo (Kaspersky Lab, 2016). Note-se no entanto que apesar da tipologia do crime a acusação tem sempre uma grande probabilidade de culminar no branqueamento de capitais uma vez que o objetivo último dos agentes criminais é o de transmutar criptomoeda para dinheiro físico, após a consumação dos ilícitos que levaram à obtenção

dessas mesmas criptomoedas. Sobre este fenómeno o relatado em 5.3.4. permitiu ainda estabelecer uma relação entre o branqueamento de capitais e as trocas de BTC*s* por dinheiro físico, as quais apesar de representarem quase 100 vezes menos a frequência mensal de transações face ao primeiro método de troca, as transferências bancárias SEPA, representam apenas menos 26% do volume total de trocas. Significando isto que apesar de o número de transações ser significativamente inferior, os montantes transacionados são expressivamente mais avultados.

No que diz respeito à terceira hipótese definida: H3 – "Fruto da tipologia das ferramentas utilizadas para a consumação dos crimes em ambiente digital, assim como da, cada vez maior, presença de informação crítica, a empresas e indivíduos, no ciberespaço, a ameaça é cada vez mais frequente, decorrendo da exposição a que está sujeita e do valor dessa mesma informação. Note-se ainda que a ameaça contempla um impacto substancial tendo em conta as consequências que delas advém, tais como o prejuízo na reputação do alvo atacado"; o estudo permitiu perceber que efetivamente a ameaça, em termos de perigos e riscos associados, é cada vez maior, apesar de os entrevistados considerarem que as criptomoedas são muito mais do que unicamente ameaças, sendo que aquilo que as pode eventualmente fazer figurar como ameaça, não é a própria criptomoeda em si, mas sim a sua utilização em esquemas tipicamente ilícitos. Tendo esta circunstância em conta, os perigos inerentes à sua utilização ilícita estão cada vez mais presentes, não só pelo facto de existir uma superfície de ataque progressivamente crescente, mas também pelo facto do número de consumação de crimes que em algum momento tiram partido dos sistemas de criptomoedas estar a crescer. Face a isto, urge ter em consideração que os impactos decorrentes desta cada vez mais presente ameaça passam por consequências no plano organizacional ligadas à inoperacionalidade e consequente perda de faturação pelo tempo inativo, à perda dos dados e conteúdos pessoais e/ ou confidenciais, à perda de reputação e à própria perda financeira afeta ao pagamento do resgate, se se der o caso. Do ponto de vista da investigação criminal a maior dificuldade passa pela atribuição do crime, que muitas vezes não permite que os autores sejam responsabilizados, e passa ainda pelo estímulo da imaginação criminal para tirar partido destas ferramentas. Por estes motivos, é possível afirmar que os opc's estão, de certa forma, limitados na resolução de incidentes deste tipo, não podendo muitas vezes ajudar as vítimas. Este facto tem ainda como consequência o estímulo da motivação dos

agentes criminais em prosseguirem com estas práticas por as considerarem seguras, tendo em consideração a relativa ineficácia dos opc's na resolução destas incidentes.

Percebeu-se ainda que é difícil definir para quem as consequências podem ser mais impactantes considerando que aqui se coloca uma questão de escala e dimensão, isto é, o impacto subjacente a dado ataque dependerá da dimensão do alvo afetado. Assim concluiu-se que para os organismos públicos as consequências de maior passam pelo tempo inoperacional e pela perda de informação crítica, tal como para o setor privado acrescendo-lhe ainda o abalo da reputação e as consequências financeiras que advenham do tempo inoperacional. Neste âmbito pode ter-se em conta o presente no subcapítulo 5.3.5., do qual se percebeu que a principal consequência que o ataque de *Ramsonware* de larga escala *WannaCry 2.0* passou pela indisponibilidade do serviço. Já para os indivíduos, aqueles que serão os alvos mais vulneráveis, as consequências mais impactantes passarão pela perda financeira direta afeta ao pagamento do resgate, ou até à perda de dados pessoais confidenciais.

Finalmente e no que concerne à última hipótese de investigação levantada: H4 – "Estima-se que a incidência seja crescente no futuro, o que obrigará a uma abordagem mais eficiente dos opc's paralelamente a uma necessária consciencialização da população para estas ameaças, por forma a atenuar o seu impacto e assim aumentar a segurança da sociedade e ramo empresarial, em Portugal"; é expectável que o futuro traga tanto uma disseminação crescente de ocorrências deste cariz como também uma crescente preocupação para as questões relacionadas com a cibersegurança e os ciberincidentes, por parte das potenciais vítimas, que resultará numa melhor preparação.

Assim, a investigação permitiu apurar que em termos de perspetivas futuras a incidência de ciberincidentes com recurso a criptomoedas vai continuar a crescer, uma vez que as criptomoedas e particularmente a BTC se tornaram numa ferramenta que efetivamente acabou por tornar os crimes digitais mais seguros para o agente criminal, facilitando a prática criminal moderna. Neste âmbito são esperados novos ataques de larga escala como o *WannaCry 2.0,* sendo que lhes é esperada também uma maior sofisticação que os poderá tornar problemáticos e intrusivos, assim como mais lucrativos e destrutivos. No entanto e apesar da mais consolidada configuração dos futuros ataques, espera-se que a resposta seja, na mesma medida, sólida o suficiente para minorar os impactos dos ataques. Confirma-se assim a posição levantada pela H4 no que diz respeito ao fortalecimento das capacidades e da capacitação de meios técnicos e do capital humano

indispensável à boa condução da investigação criminal por parte das forças de segurança nacionais, que devem continuar a cooperar por forma a alcançarem respostas sólidas em cooperação com os organismos de governo afetos ao Ministério da Defesa que detêm um papel importante em colaboração com as forças de segurança. Ainda, no sentido de aumentar o nível de segurança da sociedade e do ramo empresarial espera-se uma valorização do Estado para estas matérias, com enfoque na capacitação dos quadros por forma a torná-los mais resilientes do ponto de vista digital desde o início da sua utilização tecnológica e com enfoque na adequação da moldura legislativa para a realidade do cibercrime. Espera-se igualmente um investimento crescente em iniciativas e ações de sensibilização dirigidas tanto a indivíduos como funcionários do setor público e privado por forma a alcançar um nível de maturidade superior. No entanto percebeu-se também que este investimento, que procurará fazer face à consistência das ameaças e à sua progressiva proliferação, pode ser ainda insuficiente face a certas configurações de crimes que ainda deixam a investigação criminal pouco capacitada para a sua resolução.

Verificou-se além disso que o estado de maturidade e cultura de segurança das diferentes organizações nacionais caminha para uma solidificação coletiva das capacidades de resposta, tendo sempre em conta o seu já positivo estado de maturidade e cultura de segurança, comprovado pela resposta dada ao ciberincidentes *WannaCry 2.0.*

Analisadas e confrontadas as hipóteses de estudo com as conclusões alcançadas é evidente um alinhamento dos pressupostos de investigação com a realidade existente no contexto nacional, exceção feita à afirmação da H1 para a qual se percebeu que o nível de sensibilização e preparação das organizações nacionais era substancialmente mais consolidado do que o esperado.

Posto isto, confirma-se que o presente estudo cumpriu os pressupostos de investigação, no sentido em que obteve respostas concretas às questões que se propôs a tratar, contribuindo assim para uma posição consolidada e empiricamente verificada no que é respeitante aos desafios de substância criminal relativos às criptomoedas, em Portugal.

Em termos genéricos conclui-se que o cenário da criminalidade informática e dos crimes consumados com recurso a ferramentas informáticas, onde as configurações de crime se recursam, em algum momento, das criptomoedas, é, hoje, e será, no futuro, preocupante face à dimensão das ameaças decorrentes da utilização das criptomoedas em

atividades criminais e do consequente impacto, assim como face à crescente superfície de ataque explorável. Note-se que esta realidade não deve ser considerada tendo apenas em conta as práticas que decorrem com maior incidência e que têm como alvos prioritários as organizações e os indivíduos, como é o caso dos *Ramsonwares;* mas, ao invés disso, a ameaça decorrente da sua potencial utilização ilícita deve ser tida em conta numa perspetiva mais ampla face ao vasto leque de configurações criminais em que a criptomoeda pode desempenhar algum tipo de função. Dentro destas podem destacar-se os cibercrimes que ameaçam a segurança da sociedade como um todo, ou mesmo a segurança de um Estado: através por exemplo do financiamento terrorista com criptomoeda; também do ponto de vista da integridade do próprio sistema financeiro e fiscal: através de crimes relacionados com evasão fiscal e branqueamento de capitais; igualmente na esfera de incidência das ameaças aos indivíduos mais desprotegidos: através de crimes de extorsão sexual; podendo ser, por fim considerada outra classe ameaçada e que passa pela ineficiência do controlo e regulação do comércio de produtos e serviços ilícitos: através de crimes relacionados com recurso a plataformas de comércio de bens ilícitos como estupefacientes, armas, conteúdos pedo pornográficos assim como outros bens ou serviços ilícitos;

As potenciais ameaças consequentes das configurações acima elencadas variam em função do tipo de vítima atacada, sendo mais ou menos impactante dependendo da dimensão do alvo afetado. Nesta linha de raciocínio, ataques de *Ramsonware* dirigidos a organismos públicos têm consequências ao nível da operacionalidade e da perda de informação crítica, tal como acontece para o setor privado, afetado também financeiramente face ao tempo inoperacional e afetado em termos de reputação. O mesmo ataque para os indivíduos terá consequências mais impactantes aos níveis da perda financeira direta afeta ao pagamento do resgate, ou até à perda de dados pessoais confidenciais. Este último alvo ameaçado pode ser ainda vítima de outro tipo de crime com estas características que passa pela extorsão sexual, onde a vítima pode sofrer consequências do foro psicológico, assim como do foro financeiro, no caso de pagar a extorsão exigida. Outras ameaças decorrentes de crimes com recurso às criptomoeda assumem consequências ao nível estrutural de um Estado e da sua macroeconomia, assim como da sua segurança, como são casos os crimes de financiamento terrorista, evasão fiscal, branqueamento de capitais e comércio de produtos e serviços ilícitos, com recurso a criptomoedas.

No entanto, o cenário nacional é muito positivo no que diz respeito à sensibilização para as ameaças decorrentes de ataques informáticos com recurso a criptomoeda, à preparação em termos de capacidade de resposta e ao consequente nível de maturidade para estas questões, considerando organismos públicos, setor privado e forças de segurança.

Equacionando as grandes organizações do setor privado, o nível de *awareness* para as questões de segurança é transversal a todas as posições da companhia e a preocupação para estas questões é notória face à existência de sistemas integrados de gestão da segurança de informação implementados, assim como face ao cuidado demonstrado em formar e sensibilizar os colaboradores para que sejam conhecedores desta realidade. A tendência para a progressiva maturidade no setor empresarial é positiva face ao nível de consciencialização existente, assim como face à regulação europeia GDPR, que será transposta para as legislações nacionais em MAI2018.

No reverso da medalha e equacionando os indivíduos, estes estão efetivamente mais expostos e menos preparados para lidar com este tipo de ameaças face ao desconhecimento da realidade, ou pelo menos face ao desconhecimento de como proceder na utilização segura das TIC.

Assim e apesar de se concluir que o cenário geral é positivo, é importante considerar que este processo é dinâmico e está em constante mutação, pelo que as potenciais vítimas assim como os órgãos de investigação criminal e quem consigo trabalha em parceria, não se podem nunca considerar como conhecedores intemporais das ameaças existentes. Neste espectro e considerando a mutação constante do ecossistema envolvente, o trabalho cooperativo é fundamental para o acompanhamento contínuo da evolução do fenómeno com vista à respetiva maturidade e consolidação da resiliência digital dos utilizadores.

Em tom de fecho e considerando uma análise ao mesmo tempo retrospetiva e prospetiva, esta investigação permitiu perceber alguns dosusos decorrentes da evolução das TIC e das infraestruturas que lhes são afetas e que são a consequência de uma evolução galopante que nos conduziu a uma verdadeira Era da Informação. No entanto, e pese embora o facto de esta ser uma Era que oferece múltiplas possibilidades de aprendizagem, onde qualquer dispositivo ligado em rede poder ter capacidade para se tornar um veículo para a obtenção de conhecimento e consequentemente um veículo para a criação consciente de opinião, livre-arbítrio e preparação do cidadão para a vida ativa,

contribuindo para uma sociedade global mais equitativa no acesso ao conhecimento e munida de ferramentas que a fortalecem, existe ainda uma outra face da moeda, onde esta é simultaneamente uma Era na qual as mesmas ferramentas estão arbitrariamente disponíveis a todos os cidadãos que delas queiram usufruir, inclusivamente agentes que delas tirem partido com fins ilícitos e com intenção criminosa, levando assim à consumação de crimes em ambiente digital e com recurso a ferramentas informáticas. Esta dicotomia obriga e obrigará a uma aprendizagem contínua face às sucessivas ameaças emergentes, implicando um esforço sistémico na sensibilização e preparação dos utilizadores dos recursos digitais em rede.

Assim é válido afirmar que a evolução tecnológica chegou pela primeira vez a um ponto em que a regulação de um sistema, como o sistema *Bitcoin*,ou de outras criptomoedas, não está acessível a instituições, funcionando como um sistema anárquico, autónomo e autossuficiente. A própria infraestrutura e arquitetura sobre o qual o protocolo está assente, disperso por tantos pontos de rede distribuídos pelo globo, quantos aqueles que resultam na impossibilidade de manipulação e/ou intervenção humana. Este, que será o caminho futuro das soluções tecnológicas, comprova o poder infindável da computação distribuída ao invés da centralização e da intermediação da prestação de serviços por terceiros, assim como comprova, de igual forma que esta é também uma tendência progressivamente crescente no futuro. Tal como acontece hoje, esta tendência não será alheia a novos desafios que resultarão em ameaças para utilizadores dos mais variados níveis, que progressivamente deixarão de ter alternativas a esses mesmos sistemas e farão por isso parte da superfície explorável abrangida pelas referidas ameaças. Para estes, tornar-se-á mandatário a constante adaptação a estas ameaças através da procura incessante em conhecer a cena contemporânea no que lhes diz respeito e, face a isso, resta-lhes trabalhar na respetiva capacitação e maturidade das suas capacidades de resposta face ao contexto.

6.2. Linhas de investigação futuras

Note-se que pela contemporaneidade do tema das criptomoedas, várias são as áreas que ainda estão por explorar. Por ser uma área ainda pouco explorada relativamente à resolução criminal efetiva e às consequências legais aplicadas em crimes informáticos ou com recurso a ferramentas informáticas, concretamente quando a esses crimes está

implicada a utilização de criptomoedas, os trabalhos futuros a fazer podem passar por essa esfera de análise.

Um dos estudos de interesse e com uma possível ligação ao que esta tese aqui apresenta, passa pela dificuldade em combater a cibercriminalidade com o quadro legal nacional existente, tendo em conta a constante mutação dos crimes praticados, que são frequentemente e premeditadamente alterados pelos agentes criminais por forma a não preencherem características do tipo criminal e assim evitar que possam ser penalmente responsabilizados pelos atos cometidos. Assim seria de interesse para a comunidade científica o desenvolver de uma análise transversal a todo o processo criminal, isto é, uma análise que fosse desde a execução até à condenação do criminoso. Neste sentido, note-se ainda que, não obstante o contexto nacional, este tipo de práticas, criam dificuldades nunca enfrentadas anteriormente pelas autoridades, nomeadamente no que à recolha de provas digitais diz respeito. Esta complexidade é proveniente de uma série de características típicas entre as quais a transnacionalidade da prática, onde as restrições territoriais são irrelevantes no ciberespaço, assim como das ferramentas de anonimização já abordadas e as complexas tecnologias inerentes à sua utilização.

Uma análise de cariz legal e mais concretamente uma análise aos resultados efetivos da investigação criminal e respetivas condenações dos infratores poderá servir no futuro como um complemento ao estudo que apresento numa fase do fenómeno que se considera ser ainda inicial. No contexto nacional esta análise seria ainda de maior interesse, sendo que é preciso ter em conta que apesar de o cibercrime ser, para a legislação nacional um conceito sedimentado e penalmente punível, as respostas legais existentes são ainda, muito incipientes.

7.Referências bibliográficas

al-Munthir, T.-D. (julho de 2014). *Bitcoin wa Sadaqat al-Jihad - Bitcoin and the Charity of Violent Physical Struggle.* Obtido de alkhilafaharidat.files.wordpress.com: https://alkhilafaharidat.files.wordpress.com/2014/07/btcedit-21.pdf

APAV - Associação Portuguesa de Apoio à Vítima. (2015). *Manual Proteus - Prevenção, Informação e Apoio a Vítimas de Furto de Identidade Online.* Lisboa. Obtido em 03 de dezembro de 2016, de http://www.apav.pt/proteus/images/Proteus_PDF/ManualDeProcedimentosProteus-Portugal.pdf

APAV. (01 de dezembro de 2016). *www.apav.pt*. Obtido em 01 de dezembro de 2016, de http://www.apav.pt/cibercrime/: http://www.apav.pt/cibercrime/

BBC. (02 de maio de 2016). *Australian Craig Wright claims to be Bitcoin creator*. Obtido em 16 de maio de 2016, de http://www.bbc.com/news/technology-36168863

BlockChain. (10 de dezembro de 2016). *Median Transaction Confirmation Time.* Obtido em 10 de dezembro de 2016, de BlockChain: https://blockchain.info/charts/median-confirmation-time?timespan=all&showDataPoints=false&daysAverageString=1&show_header=true&scale=0&address=

Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, Technology, and Governance. *Journal of Economic Perspectives, 29 - Number 2—Spring*, 213–238. Obtido em 05 de dezembro de 2016, de http://pubs.aeaweb.org/doi/pdfplus/10.1257/jep.29.2.213

Braun, V., & Clarke, V. (2006). *Qualitative Research in Psychology* (Vol. 3).

Bravo, R. (2015). *Seminário de Cyber Risks, desafios e estratégias de gestão e mitigação.* Beja. Obtido em 30 de janeiro de 2017, de https://www.apseguradores.pt/APSBreve/APSBrevePost.aspx?APSBreveEditionId=8&APSBrevePostId=60

BTC Exchange Rate. (22 de setembro de 2017). *BTC Exchange Rate*. Obtido de http://bitcoinexchangerate.org/fees: http://bitcoinexchangerate.org/fees

Cabreiro, C. (10 de outubro de 2016). Especial CM - Crimes na Net. (J. Ferreira, Entrevistador) CMTV. CMTV, Lisboa.

Castells, M. (2003). *A Galáxia da Internet: Reflexões sobre a Internet, os negócios e a sociedade.* Rio de Janeiro: Jorge Zahar Editor.

Christin, N. (2012). *Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace.* Carnegie Mellon University, Information Networking Institute / Cylab. Pittsburgh, PA 15213: Carnegie Mellon University. Obtido em 05 de dezembro de 2016, de https://arxiv.org/pdf/1207.7139v2.pdf

Coelho, R. (15 de agosto de 2016). Tráfico de droga cresceu na darknet. Existem 50 mercados. *Diário de Notícias*, 17.

Coin Market Cap. (21 de agosto de 2017). *Coin Market Cap*. Obtido de https://coinmarketcap.com/charts/: Coin Market Cap

Comissão Europeia. (2007). *Rumo a uma política geral de luta contra o cibercrime.* Bruxelas: COMISSÃO DAS COMUNIDADES EUROPEIAS. Obtido em 10 de

dezembro de 2016, de http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52007DC0267&from=PT

Decreto Lei nº 81/2016 de 28 de novembro (2016). Obtido em 10 de dezembro de 2016, de http://www.policiajudiciaria.pt/PortalWeb/content?id=%7BC28E74D8-DAF7-4C74-824B-FBC964532E55%7D

Diário da República. (12 de junho de 2015). Diário da República. Lisboa, Portugal. Obtido em 22 de setembro de 2017, de https://www.cncs.gov.pt/content/files/rcm_36-2015.pdf

Eliasson, J. (2015). *13th United Nations Congress on Crime Prevention and Criminal Justice.* Doha. Obtido em 30 de janeiro de 2017, de http://www.unis.unvienna.org/unis/en/events/2015/crime_congress_cybercrime.html

eMarketeer. (2016). *Worldwide Retail Ecommerce Sales: The eMarketer Forecast for 2016.* New York: eMarketeer. Obtido em 22 de setembro de 2017, de https://totalaccess.emarketer.com/Login.aspx?ReturnUrl=%2fReports%2fViewer.aspx%3fR%3d2001849%26ecid%3dMX1371&R=2001849&ecid=MX1371

European Banking Authority. (2014). *EBA OPINION ON 'VIRTUAL CURRENCIES'.* Londres: European Banking Authority. Obtido em 03 de dezembro de 2016, de https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf

European Union. (25 de setembro de 2017). *http://www.eugdpr.org/*. Obtido de EU GDPR: http://www.eugdpr.org/

EUROPOL. (2015). *The Internet Organised Crime Threat Assessment.* The Hague, Netherlands: EUROPOL Corporate Publications. Obtido em 15 de abril de 2016, de https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta-2015

EUROPOL. (2016). *Changes in modus operandi of Islamic State terrorist attacks.* The Hague: EUROPOL Corporate Publications. Obtido em 05 de dezembro de 2016, de https://www.europol.europa.eu/sites/default/files/documents/changes_in_modus_operandi_of_is_in_terrorist_attacks.pdf

EUROPOL. (2016). *Internet Organised Crime Threat Assessment.* The Hague: European Police Office. Obtido em 30 de março de 2017, de https://www.europol.europa.eu/sites/default/files/documents/europol_iocta_web_2016.pdf

FATF. (2015). *Emerging Terrorist Financing Risks.* Paris: FATF Secretariat. Obtido em 05 de dezembro de 2016, de https://www.coe.int/t/dghl/monitoring/moneyval/Publications/Emerging-Terrorist-Financing-Risks.pdf

Fidelidade (Realizador). (2014). *Um dia calha a todos...* [Filme]. Obtido de https://www.youtube.com/watch?v=NGanV5ozLao

Folkinshteyn, D., Lennon, M., & Reilly, T. (2015). The Bitcoin Mirage: An Oasis of Financial Remittance. *Journal of Strategic and International Studies, Volume XX*, 118-124.

GNR | Protocolo internacional na área da cibersegurança (2016). [Filme]. Obtido em 07 de dezembro de 2016, de https://www.youtube.com/watch?v=O28gTvAqvow

Grinberg, R. (2011). Bitcoin: An Innovative Alternative Digital Currency. *HastingsScience & Tecnhology Law Journal*, 159-208.

Gwern. (2016). *TOR BLACK-MARKET-RELATED ARRESTS*. Obtido em 31 de janeiro de 2017, de gwern.net: https://www.gwern.net/Black-market%20arrests

Integrity Consulting. (05 de agosto de 2017). *ISO 27001 Sistema de Gestão de Segurança da Informação*. Obtido de ISO 27001 Sistema de Gestão de Segurança da Informação: https://www.27001.pt/

Internet Live Stats. (08 de dezembro de 2016). *Internet Live Stats*. Obtido de Internet Live Stats: http://www.internetlivestats.com/internet-users/

ISO/IEC. (2005). *International Standard - ISO/IEC 27001*. Geneva: ISO copyright office.

Jornal Económico. (10 de janeiro de 2017). Indonésia alerta para terrorismo financiado por Bitcoins e Paypal. *Jornal Económico*. Obtido em 30 de janeiro de 2017, de http://www.jornaleconomico.sapo.pt/noticias/indonesia-alerta-para-terrorismo-financiado-por-bitcoins-e-paypal-108903

Kaspersky Lab. (2015). *Kaspersky Security Bulleti - OVERALL STATISTICS FOR 2015.* Moscovo: GREAT. Obtido em 08 de dezembro de 2016, de https://securelist.com/files/2015/12/KSB_2015_Statistics_FINAL_EN.pdf

Kaspersky Lab. (2016). *Kaspersky Security Bulletin - Overall Statistics for 2016.* GREAT.

Kharpal, A. (15 de maio de 2017). *https://www.cnbc.com/2017/05/15/wannacry-ransomware-hackers-have-only-made-50000-worth-of-bitcoin.html*. Obtido de CNBC: https://www.cnbc.com/2017/05/15/wannacry-ransomware-hackers-have-only-made-50000-worth-of-bitcoin.html

Kruithof, K., Aldridge, J., Décary-Hétu, D., Sim, M., Dujso, E., & Hoorens, S. (2016). *Internet-facilitated drugs trade.* Rand Europe. Santa Monica, Calif., and Cambridge, UK: RAND Corporation. Obtido em 31 de janeiro de 2017, de www.rand.org/t/RR1607

MoneyGram. (22 de setembro de 2017). *MoneyGram*. Obtido de https://www.moneygram.com/wps/portal/moneygramonline/home/estimator: https://www.moneygram.com/wps/portal/moneygramonline/home/estimator

Moreira, I. (05 de agosto de 2015). Estado Islâmico vende o patrimônio cultural da Síria e do Iraque no mercado negro. *Revista Galileu*. Obtido em 05 de dezembro de 2016, de http://revistagalileu.globo.com/Sociedade/noticia/2015/08/o-estado-islamico-vende-o-patrimonio-cultural-da-siria-e-do-iraque-no-mercado-negro.html

Nakamoto, S. (janeiro de 2009). *Bitcoin: A Peer-to-Peer Electronic Cash System.* Obtido em 07 de abril de 2016, de www.bitcoin.org: https://bitcoin.org/bitcoin.pdf

Natário, T.-c. R. (outubro de 2013). O combate ao cibercrime: anarquia e ordem no ciberespaço. *Revista Militar*. Obtido em 01 de dezembro de 2016, de https://www.revistamilitar.pt/artigo/854

Norton. (2016). *Cyber Security Insights Report.* Nova Iorque: Edelman Intelligence. Obtido em 03 de dezembro de 2016, de https://www.symantec.com/content/dam/symantec/docs/reports/2016-norton-cyber-security-insights-report.pdf

ONU. (2013). *Comprehensive Study on Cibercrime.* Nova Iorque: UNODC - United Nations on Drugs and Crime. Obtido em 10 de dezembro de 2016, de https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

Perez, F. (12 de maio de 2017). *http://visao.sapo.pt/actualidade/portugal/2017-05-12-Portugal-Telecom-afetada-em-ataque-informatico-mundial*. Obtido de Visão: http://visao.sapo.pt/actualidade/portugal/2017-05-12-Portugal-Telecom-afetada-em-ataque-informatico-mundial

Pinto, P. (29 de março de 2017). *https://pplware.sapo.pt/informacao/portugal-casal-enviava-droga-todo-mundo/*. Obtido de PPLWare: https://pplware.sapo.pt/informacao/portugal-casal-enviava-droga-todo-mundo/

Polícia Judiciária. (11 de setembro de 2015). *http://www.policiajudiciaria.pt/PortalWeb/page/%7B29B4A2A6-0632-41AD-A920-3718CEA63BBF%7D*. (Diretoria de Lisboa e Vale do Tejo) Obtido em 08 de dezembro de 2016, de Polícia Judiciária: http://www.policiajudiciaria.pt/PortalWeb/page/%7B29B4A2A6-0632-41AD-A920-3718CEA63BBF%7D

Shah, S. (15 de maio de 2017). *https://www.v3.co.uk/v3-uk/news/3010138/number-of-wannacry-victims-now-over-200-000-says-kaspersky*. Obtido de V3: https://www.v3.co.uk/v3-uk/news/3010138/number-of-wannacry-victims-now-over-200-000-says-kaspersky

Sistema de Segurança Interna. (2015). *Relatório Anual de Segurança Interna.* Lisboa: Gabienete do Secretário Geral - Sistema de Segurança Interna.

Tasca, P. (2015). *Digital Currencies: Principles, Trends, Opportunities and Risks.* Zurique, Suíça: ECUREX. Obtido em 23 de abril de 2017, de https://ssrn.com/abstract=2657598

The Fee Calculator. (22 de setembro de 2017). *http://thefeecalculator.com/*. Obtido de The Fee Calculator: http://thefeecalculator.com/

The World Factbook. (10 de dezembro de 2016). *The World Factbook*. Obtido de The World Factbook: https://www.cia.gov/library/publications/the-world-factbook/geos/xx.html

Western Union. (22 de setembro de 2017). *Western Union*. Obtido de https://www.westernunion.com/us/en/price-estimator/continue.html: https://www.westernunion.com/us/en/price-estimator/continue.html

World Business Culture. (2017). *World Business Culture*. Obtido em 05 de March de 2017, de World Business Culture: http://www.worldbusinessculture.com/Mexican-Business-Communication-Style.html

8.Material de Suporte

8.1. Apêndices

Dimensões de Análise	Personalidades a entrevistar	Ponto de Contacto	Qualidade	links úteis	Data de envio de e-mail	Follow-Up	LIDO	Data REU
Criminalidade Informática	§ CAlm Gameiro Marques – Diretor do Gabinete Nacional de Segurança;	BM	Diretor-Geral do GNS	-	03/ago/17		x	7AGO 14H30
	§ Rogério Bravo – Inspetor-chefe da PJ para a área do cibercrime;	JG	Inspetor-Chefe da PJ para a área do Cibercrime	-	03/ago/17	25/ago/17	x	30AGO 15h30
	§ Carlos Cabreiro- Diretor da UNC3T da PJ;	JG	Diretor do UNC3T		03/ago/17		x	13SET 11h
	§ Gonçalo Ribeiro – Antigo especialista adjunto para a investigação de criminalidade informática e tecnológica da PJ;							
	§ Sara Bento – Investigadora da Unidade Nacional de Contraterrorismo da PJ;							
Segurança de Informação	§ Paulo Moniz – Diretor de Segurança de Informação e Risco nas TIC da EDP;	BM/PMS	Diretor de Segurança e Risco da EDP	https://www.computerworld.com.pt/2015/11/24/edp-desenvolve-projecto-piloto-de-aprendizagem-por-maquina/	03/ago/17	25/ago/17	x	01SET 11h
	§ Carlos Alexandre – Responsável por segurança da CGD;	BM	Responsável pela área da Segurança - CGD	https://www.linkedin.com/in/carlos-alexandre-1ab45943/?ppe=1	03/ago/17	25/ago/17	x	
	§ José Alegria – Chief Security Officer da PT;	BM	Chief Security Officer of Portugal Telecom	www.linkedin.com/in/joalegria/?ppe=1 http://www.cio.pt/tag/jose-alegria	03/08/2017 via mail + linkedin	25AGO2017 via Linkedin		
	§ José Pereira - ESPAP;	PMS	Coordenador do Núcleo de Segurança, Comunicações e Centro de Dados	https://www.espap.pt/newsletter/Paginas/Quem-e-quem-na-eSPap-jul2015.aspx	03/ago/17	25/ago/17	x	11SET 18h15
	§ Luís Filipe Tavares – Diretor-Geral da Globsernet;	BM	CEO da Globsernet	https://www.linkedin.com/in/luis-filipe-tavares-567503/?ppe=1	03/08/2017 via mail + linkedin	25/ago/17	x	REU não aconteceu

								por incompatibilidade de horários
	§ Pedro Veiga – Coordenador no CNCS;	JG	https://www.cncs.gov.pt/sobre-nos/contactos-cncs/	https://www.linkedin.com/in/pedro-veiga-8815192/	03/08/2017 via mail p CNCS	25AGO2017 via Linkedin	x	
	§ José Carlos Martins - Ex-responsável do GNS	BM	Professor da AM	-	03/ago/17	25/ago/17	x	REU não aconteceu por incompatibilidade de horários
	§ Lino e Santos – Head of Operations no CNCS;	JG	https://www.cncs.gov.pt/sobre-nos/contactos-cncs/	https://www.linkedin.com/in/lino-santos-6a150b7/?ppe=1	03/08/2017 via mail p CNCS		x	
				-				
Novos recursos tecnológicos (criptomoedas)	§ Rui Miguel Silva – Coordenador do Laboratório Ubinet do Instituto Politécnico de Beja;	JG	Membro do Laboratório UbiNET Beja - UbiNET - Segurança Informática e Cibercrime	http://ubinet.ipbeja.pt/membros/rui_miguel_silva.html	03/ago/17	25/ago/17	x	
	§ M. Valente – Palestrante da CIIWA - FullIT	BM	Full IT	https://pt.linkedin.com/in/mvalente e http://mvalente.eu/	17/ago/17		x	24AGO às 17h
	§ Jorge Silva Carvalho – Palestrante da CIIWA e Diretor-Geral da 2048 - Empresa de Segurança;	BM	Palestrante CIIWA	-	03/ago/17	25/ago/17		
	§ Nuno Mendes – Diretor-Geral da WhiteHat Portugal;	JG	CEO da WhiteHat	-	03/ago/2017 via linkedin	25AGO2017 via Linkedin	x	
	§ Ourivesaria online – Helena Botelho;	JG?			03/ago/2017 e-mail enviado			
	§ *Riclas* - Pro Trader LocalBTC	JG	Pro Trader LocalBTC - 100% score em cerca de 10000 transações com 4000 parceiros diferentes	https://localbitcoins.com/p/riclas/	28/ago/17		x	1SET2017 - 12h30 Tecnico (Alameda)

Apêndice 1 - Mapa Convocatória entrevistas

						Análise Qualitativa	
Check análise	Perguntas	ID	Frequência	Personalidade	QD od se insere	THEMEs	CODEs na resposta
	Qual o panorama nacional no que concerne aos crimes e ciberataques cujas criptomoedas contribuem para a sua consumação?	A	7	Gmarques; Mvalente; Pmoniz; Riclas; Rbravo; Jpereira; Ccabreiro;	[QC e QD2]	*Awareness & InfoSec; Cyberattacks;*	*23x Cyberattacks; 2x A & Infosec; 1x Victims; 1x BTC TC;*
	Quais as consequências mais impactantes para as vítimas?	B	6	Gmarques; Mvalente; Pmoniz; Rbravo; Jpereira; Ccabreiro;	[QC; QD3]	*Awareness & InfoSec; Victims;*	*11x Victims; 1x CyberAttacks;*
	Para que grupo de vítimas (organismos públicos, corporate ou indivíduos) as consequências são mais danosas?	C	5	Gmarques; Mvalente; Pmoniz; Jpereira; Ccabreiro;	[QC; QD3]	*Awareness & InfoSec; Victims;*	*9x Victims;*
	Considera que as potenciais vítimas (utilizadores do ciberespaço) estão sensibilizadas ou preparadas para lidar com a ameaça?	D	6	Gmarques; Mvalente; Pmoniz; Rbravo; Jpereira; Ccabreiro;	[QD1]	*Awareness & InfoSec; Victims;*	*17x A & Infosec*
	As empresas vítimas de ciberataques que as comprometam têm por hábito reportar às autoridades competentes?	E	4	Gmarques; Mvalente; Rbravo; Ccabreiro;	[QD1; 4]	*Awareness & InfoSec; Victims;*	*14x Victms; 1x A & Infosec;*
	Ao nível do poder decisório, qual o nível de awareness e de perceção do risco p/ estes incidentes, por parte dos c-levels?	F	3	Mvalente; Pmoniz; Jpereira;	[QD1]	*Awareness & InfoSec; Victims;*	*13x Infosec;*
	Qual o estado de maturidade na cultura de segurança das organizações nacionais?	G	5	Mvalente; Pmoniz; Rbravo; Jpereira; Ccabreiro;	[QD1; 4]	*Awareness & InfoSec;*	*11x A & Infosec;*
	Como parte de empresa que desenvolve soluções, estas são desenvolvidas tendo em conta o conceito de *Security by design?*	H	1	Mvalente	[QD1]	*Awareness & InfoSec;*	*4x A & Infosec;*
	A solução para uma mais eficiente segurança de informação passa por uma menor exposição e presença online, ou por políticas de gestão da segurança de informação?	I	2	Gmarques; Mvalente;	[QD1; 4]	*Awareness & InfoSec;*	*5x A & Infosec;*
	Quem é o principal responsável por tomar medidas (opc's, governo, ou iniciativa própria de empresas e indivíduos)?	J	1	Gmarques;	[QD1; 4]	*Awareness & InfoSec;*	*2x A & Infosec*
	Considerando casos da mesma natureza e escala do "caso WannaCry 2.0", é expectável que novos cenários como este venham a acontecer?	K	6	Gmarques; Mvalente; Pmoniz; Rbravo; Jpereira; Ccabreiro;	[QC e QD1;2;3]	*Cyberattacks*; + Subcapítulo 5.3.5.	*10x Cyberattacks; 4x A & Infosec; 5x Victims;*

	Qual considera ter sido a principal consequência deste ataque, para as vítimas nacionais?	L	2	Rbravo; Ccabreiro;	[QC e QD1;2;3]	*Cyberattacks; Victims* + Subcapítulo 5.3.5.	*5x Victims; 3x A& Infosec; 3x Cyberattacks;*
	No dia do ataque *WannaCry 2.0* foram-lhe feitas muitas solicitações para compra de BTCs?	M	1	Riclas;	[QC e QD1;2;3]	*Cyberattacks; Victims; BTC Technical Questions*; + Subcapítulo 5.3.5.	*3x Cyberattacks;*
	Como é que a EDP/eSPap experienciou o ataque Wannacry e qual respetivo impacto?	N	2	Pmoniz; Jpereira;	[QC e QD2;3]	*Cyberattacks; Awareness & InfoSec; Victms*; + Subcapítulo 5.3.5.	*3x A & Infosec; 2x Victims*
	Quais os ataques informáticos mais dirigidos à EDP/ESPap e respetivo impacto?	O	2	Pmoniz; Jpereira;	[QD2;3]	*Cyberattacks; Awareness & InfoSec; Victms*;	*2x CyberAttacks; 1x A & Infosec;*
	Considerando os diferentes métodos de trocas de BTCs, como se divide em termos percentuais, o nº de transações em BTCs, tanto na compra como na venda de BTCs?	P	1	Riclas;	[QC]	*BTC Technical Questions;*	*4x BTC TQ;*
	Quais os métodos de transações que envolvem montantes mais avultados, tanto para compra como para venda de BTCs?	Q	1	Riclas;	[QC]	*BTC Technical Questions;*	*4x BTC TQ;*
	Os BTCs que tem para troca são provenientes de investimento próprio, ou de BTC adquiridas através de *mining*?	R	1	Riclas;	[QC]	*BTC Technical Questions;*	*2x BTC TQ;*
	Certamente quando tudo começou o preço unitário era significativamente mais baixo. A valorização da BTC alterou os padrões das trocas?	S	1	Riclas;	[QC]	*BTC Technical Questions;*	*3x BTC TQ;*
	A procura por Bitcoin é crescente?	T	1	Riclas;	[QC]	*BTC Technical Questions;*	*3x BTC TQ;*
	O facto de as suas carteiras serem endereços com um nº grande de movimentações, o que é do conhecimento dos utilizadores, fez com que alguma vez tenha sido vítima de uma tentativa de ataque?	U	1	Riclas;	[QC; QD2;3;4]	*Cyberattacks; Awareness & InfoSec; Victims; BTC Technical Questions;*	*2x BTC TQ;*
	Tendo em conta que os produtos ou serviços adquiríveis em BTC, em Portugal, ainda têm uma expressão muito reduzida, para que fins pensa que os indivíduos nacionais lhe compram BTC?	V	1	Riclas;	[QC; QD2]	*Cyberattacks; BTC Technical Questions;*	*2x CyberAttacks;*
	Muitos dos pedidos de transações podem estar relacionados com o pagamento de resgates. Neste contexto consegue dar um cenário em termos de frequência, montantes, *feedback* dos *users* que fazem estes pedidos?	W	1	Riclas;	[QC; QD2;3]	*Cyberattacks; Victims; BTC Technical Questions;*	*2x CyberAttacks;*

	Certamente está alerta para o facto de muitos criminosos procurarem transações em pessoa e em dinheiro vivo, como forma de não deixar rasto na obtenção das BTC, alguma vez teve a sensação de estar perto do crime?	X	1	Riclas;	[QC; QD2;3]	*Cyberattacks; BTC Technical Questions;*	*2x CyberAttacks;*
	Há registo em Portugal, da utilização de criptomoedas para financiar organizações terroristas, para práticas de lavagem de dinheiro ou para comercialização de bens em mercados negros online?	Y	2	Rbravo; Ccabreiro;	[QC; QD2;]	*Cyberattacks;*	*4x CyberAttacks;*
	Dadas as características das criptomoedas qual a eficiência da investigação na atribuição dos ataques e no *tracking* das transações?	Z	2	Rbravo; Ccabreiro;	[QD3]	*Awareness & InfoSec; BTC Technical Questions;*	*3x Cyberattacks; 3x BTC TQ;*
	Qual o estado atual de preparação (prevenção/reação) das forças e serviços de segurança para lidarem com ciberincidentes deste tipo?	AA	3	Gmarques; Rbravo; Ccabreiro;	[QD4]	*Cyberattacks; Awareness & InfoSec;*	*1x Cyberattacks; 5x A & Infosec; 1x Victims;*
	O que pode ainda ser feito para que estas possam atingir um estado de maturidade que lhes permita estar preparadas para lidar com este tipo de ameaças e outras semelhantes?	AB	1	Gmarques;	[QD4]	*Awareness & InfoSec;*	*5x A & Infosec; 1x Victims;*
	Qual o potencial futuro das criptomoedas como ameaças em ambiente digital?	AC	7	Gmarques; Mvalente; Pmoniz; Riclas; RBravo; Jpereira; Ccabreiro;	[QD4;]	*Awareness & InfoSec; Cyberattacks;*	*13x CyberAttacks; 1x A & Infosec; 10x BTC TC;*

Apêndice 2 - Catálogo de perguntas levantadas em situação de entrevista

Entrevista - CAlm Gameiro Marques - Diretor Geral GNS

Data - 07AGO2017 14h30

Local – Gabinete Nacional de Segurança - Rua Da Junqueira 69, 1300 Lisboa

Estrutura entrevista:

a) Apresentação
b) Explicação do objeto de investigação;
c) Explicação do intuito da entrevista – "O que procuro e onde quero chegar?"
d) Perguntas diretamente relacionadas com o problema e temas da investigação:

Temas -» *Awareness & InfoSec; Cyberattacks;/*

1. **ID-A - Qual o panorama nacional no que concerne aos crimes e ciberataques cujas criptomoedas contribuem para a sua consumação?**

João Nuno Gaspar
Cyberattacks

João Nuno Gaspar
Victims

João Nuno Gaspar
Awareness and Infosec

João Nuno Gaspar
Awareness and Infosec

João Nuno Gaspar
Cyberattacks

João Nuno Gaspar
Cyberattacks

R: [As respostas q lhe vou dar, não vão tocar na área do crime informático] Nós o que sabemos é que a incidência de pedidos de resgates q decorrem de ataques de Ramsomware a organizações em Portugal ainda são, ou poucos ou desconhecidos. Porque ainda não há obrigatoriedade das entidades (publicas ou privadas) de o reportarem e dizerem que foram comprometidas. Isto vai ser resolvido com a entrada em vigor no ano que vem da lei de cibersegurança, que ainda é um projeto de lei mas que terá de ser publicada até maio de 2018 e que decorre da transposição de uma diretiva da EU. Isto conjugado com a regulamentação do regulamento geral da proteção de dados, vai permitir ter mais visibilidade sobre assuntos que envolvam a utilização das BTCs ou outras criptomoedas para esses propósitos menos legítimos. E, portanto, dado o contexto, a resposta objetiva à sua pergunta é: são poucos ainda. No entanto espera-se que esta seja uma tendência crescente, aliás a semana passada tivemos conhecimento a partir do CNCS que surgiu um novo modelo de BTC que tem como objetivo proporcionar transações mais rápidas e em maior quantidade, através de uma arquitetura de transação mais ágil e rápida.

EU: Para além de ciberataques como os ramsonwares há registo em Portugal do recurso às BTC para outro tipo de crimes como financiamento terrorista, moeda de troca em mercados negros, etc?

R: Que eu tenha conhecimento não.

Temas -» *Awareness & InfoSec; Cyberattacks; Victims;*

2. **ID-B - Quais as consequências mais impactantes para as vítimas?**

João Nuno Gaspar
Victims

João Nuno Gaspar
Victims

R: Para já a consequência direta que está ligada ao pagamento do resgate, depois por causa própria natureza da BTC, o problema da atribuição. Porque a BTC até tem o Blockchain que estão interligados, a BC que até foi concebida com o propósito de retirar intermediários que não acrescentam valor à transação e que intrinsecamente acabam por, por um lado trazer segurança através da anonimização dos fluxos financeiros. Assim e como tudo tem o seu lado bom, mas também o seu lado mau, a principal consequência acaba por ser o pagamento e a atribuição do atacante.

EU: Se me permite, há pouco falava dos poucos reports ou denúncias registadas quanto a este tipo de ataques, surge a questão da reputação das empresas, que optam por pagar e não tornar público que foram atacadas.

João Nuno Gaspar
Victims

João Nuno Gaspar
Victims

João Nuno Gaspar
Victims

R: Sim, mas tudo se acaba por saber, mais depressa se apanha um mentiroso que um coxo. Por mais que as empresas digam que não são atacadas e que têm a reputação imaculada, mais tarde ou mais cedo isso acaba por se saber e existem mecanismos para se perceber se uma empresa foi ou não comprometida. Existem até entidades que ainda não sabem que foram comprometidas, mas, no entanto, já dão sinais no ciberespaço que foram comprometidas.

3. **ID-C - Para que grupo de vítimas (órgãos administrativos, corporate ou indivíduos) as consequências são mais danosas?**

João Nuno Gaspar
Victims

R: Penso que os registos nos indicam que as consequências mais danosas são para as entidades que têm compromissos com clientes, pelo que possivelmente para as empresas... Mas um ciberataque nunca é simpático para ninguém.

4. **ID-D - Considera que as potenciais vítimas (utilizadores do ciberespaço) estão sensibilizadas ou preparadas para lidar com a ameaça?**

João Nuno Gaspar
A & InfoSec

João Nuno Gaspar
A & InfoSec

João Nuno Gaspar
A & InfoSec

João Nuno Gaspar
A & InfoSec

R: Nós temos vindo a fazer com a PJ e com outras entidades muitas ações dirigidas a públicos distintos, no sentido não da sensibilização específica para as questões relacionadas com as criptomoedas, mas para o tema da resiliência digital como um todo. Temos desenvolvido formações – cursos de introdução à cibersegurança -, assim como os cibertemas (FEV foi dedicado ao ramsonware) e temos também, quer o GNS quer o CNCS, têm feito várias ações em escolas e universidades (onde se formam gestores) para os sensibilizar para estes temas e sobretudo para desconstruir a ideia de que há muito tem sido criada de que este tema é um tema apenas dos informáticos. Pelo contrário este é um tema de comandante ou da gestão de topo uma vez que as consequências se podem ramificar para todas as áreas operacionais como o recrutamento, do investimento, da produção, do capital humano, etc. Este é aliás um dos eixos da estratégia nacional de segurança no ciberespaço, a capacitação das pessoas. Portanto penso que caminhamos no sentido de incrementar o nível de sensibilização e preparação para ciberincidentes.

Temas -» *Cyberattacks;*

5. **ID-K - Considerando casos da mesma natureza e escala do "caso WannaCry 2.0", é expectável que novos cenários como este venham a acontecer?**

João Nuno Gaspar
CyberAttacks

João Nuno Gaspar
A & InfoSec

João Nuno Gaspar
A & InfoSec

R: Vai-nos acontecer. Pode ter a certeza que vai acontecer, tal como nós lhes costumamos chamar são os Known unknowns, isto é, vai acontecer, só não sabemos quando. No entanto a melhor maneira de estarmos protegidos é estarmos preparados, porque não basta investir só em tecnologia para supostamente nos proteger. É importante conseguir fomentar a maturidade digital das organizações. É necessário investir no capital humano, promovendo também as ações que há pouco falei. Mas também conhecermo-nos bem internamente, criando uma cultura de segurança que, no entanto, não deve ser obsessiva. Por isto, no nosso entendimento as culturas de segurança devem-se pautar por análises de gestão do risco e em função dessa análise devem-se desenvolver ações diversificadas em função desse mesmo risco. Analisando sempre a segurança transversalmente e em todas as suas componentes – física, das pessoas, eletrónica e da informação. Por exemplo na seg inf. as organizações devem assim refletir e caracterizar a sua informação em x clusters, hierarquizando-a por ordem de importância e em função dessa hierarquização, devem ter estratégias para a segurar. Devem pensar quais são as joias da coroa em termos de informação, tal como na época dos castelos a segurança era pensada essencialmente em termos físicos.

Temas -» *Cyberattacks; Awareness & InfoSec;;*

6. **ID-AA - Qual o estado atual de preparação (prevenção/reação) das forças e serviços de segurança para lidarem com ciberincidentes?**

[respondido abaixo]

7. **ID-AB - O que pode ainda ser feito para que estas possam atingir um estado de maturidade que lhes permita estar preparadas para lidar com este tipo de ameaças e outras semelhantes?**

João Nuno Gaspar
A & Infosec

João Nuno Gaspar
A & Infosec

João Nuno Gaspar
A & Infosec

João Nuno Gaspar
A & Infosec

João Nuno Gaspar
A & Infosec

R: Há várias coisas a fazer, aliás há muito por fazer. Uma das coisas e pessoalmente a que considero a mais importante, e que passa pelas áreas governamentais do ensino, isto é, pelo Ministério da Educação e pelo da Ciência e Tecnologia, ou seja a cobertura do ensino obrigatório até ao 12º e ensino universitário e politécnico respetivamente, tem que ver com o desenvolvimento de um forte e estruturado programa pelo qual desde pequenos fosse incutido nos jovens uma cultura que fizesse com que eles fossem muito mais resilientes do ponto de vista digital desde o início da sua utilização tecnológica. É preciso notar que o coeficiente de ingenuidade de um jovem aquando da sua utilização das TIC acarreta vários perigos, perigos esses que são exacerbados pela desvirtuação do próprio conceito de privacidade, sem prejuízo do que estão a expor a quem está do outro lado, que se pode aproveitar dessa ingenuidade e desvalorização inocente da privacidade, para fazer algo de perverso às suas vítimas. Para mim era aí que deveria ser feito o maior investimento, ainda que seja a médio-longo prazo, é urgente um investimento estruturante, um investimento que prepararia melhor os cidadãos de Portugal e os adultos do futuro para viverem numa economia e numa realidade cada vez mais digital. Para isto não é preciso inventar muito, basta ver o que outros Estados estão a fazer neste sentido e adaptar em conformidade ao nosso contexto. Em termos de curto-prazo há coisas que estão a ser feitas, tais como adequar a moldura legislativa para o efeito, o que está a ser feito em conjunto com outras entidades do estado, desenvolver e fortalecer também uma família de procedimentos que já existem (já foram testado e melhorados no Wannacry e no Petya), e que face a um incidente se desencadeiem através das entidades que os tem de resolver de forma célere e expedita. Assim o CNCS, no limite das suas competências enquanto coordenador destas matérias, definiu procedimentos que devem ser executados

em função do cenário. Por exemplo o Wannacry é cenário 3 isto desencadeia reações da PJ do SIS ou de outras forças de segurança. Os procedimentos foram desenvolvidos por todos e portanto assim que um incidente seja detetado, o primeiro a detetá-lo reporta-os através da rede de CSERT's, e o CNCS decide vamos por em prática os procedimentos para o cenário x e executam imediatamente, minimizando o tempo de resposta e mitigando a propagação.

João Nuno Gaspar
Victims

8. ID-I - A solução para uma mais eficiente segurança de informação passa por uma menor exposição e presença online, ou por políticas de gestão da segurança de informação?

João Nuno Gaspar
A & Infosec

R: Só pode ser pela 2.ª uma vez que a segunda é inevitável. Hoje as empresas que optam por não usar o digital não têm hipótese de sobreviver perante uma concorrência digitalizada. Mais importante ainda é o mindset dos board of directors (c-level) considerem o digital como aspeto de negócio. O negócio passa pelo digital e não é o digital que passa pelo negócio. O negocio só se faz se empresa existir digitalmente. Tem de haver um CSO, CISO ou um CIRO ou um q reporta diretamente ao CEO.

João Nuno Gaspar
A & Infosec

9. ID-J - Quem é o principal responsável por tomar medidas (opc's ou iniciativa própria de empresas e indivíduos)?

João Nuno Gaspar
A & Infosec

R: Eu não concordo muito com o Estado paternalista. Eu acho que o Estado tem de dar o exemplo. Pode dar orientações e/ou sugestões, mas tem sobretudo de dar o exemplo. Os estados mais desenvolvidos o que fazem é criar associações com entidades privadas fortes que em conjunto conseguem contribuem para que a sociedade seja mais madura do ponto de vista digital. Por exemplo pretendo que até ao fim do ano chegue a um protocolo bilateral com todas as universidades nacionais que tratem o tema da resiliência digital, com o objetivo de colaborar de forma eficaz e incrementando o conhecimento comum. O que o estado deve fazer é fomentar estas parcerias com os centros de saber e dar também o exemplo.

Temas -» *Awareness & InfoSec; Cyberattacks;*

João Nuno Gaspar
BTC TQ

10. ID-AC - E qual o potencial futuro das criptomoedas como ameaças em ambiente digital?

João Nuno Gaspar
BTC TQ

R: Eu não as vejo como uma ameaça. O ser humano estranha a mudança e a novidade inicialmente, então chama-lhe uma ameaça, mas há-de a entranhar. Mas veja que isto ameaça o status quo económico da nossa sociedade, nomeadamente a banca e o sistema monetário tal como o conhecemos. Este é um assunto que não interessa ao establishment já viu? Se a BTC ou outras criptomoedas se impuserem, para que vão servir os bancos? A BTC é a abstração máxima da moeda física... Mas muito mais do que a BTC, o Blockchain acaba por ser ainda mais fraturante no meio disto tudo. Portanto isto não é uma ameaça do meu ponto de vista, mas é acima de tudo um desafio. O dinheiro vivo também é usado para coisas más, não existem os paraísos fiscais? Não existem países na Europa que mesmo estando na EU também tiram partido disso em detrimento dos outros Estados? Portanto, em suma à sua ultima questão não a vejo como uma ameaça. É tanto uma ameaça como é o € ou o $ podem ser ameaças, ou outras moedas que usam o dinheiro com fins ilícitos. Agora existe mais uma, é escondida não se vê, mas primeiro tem de se perceber como funciona, penso que daqui a uns anos o mundo se vai adaptar a isto e ainda havemos de tirar partido das criptomoedas. É tudo uma questão de tempo e de adaptação, é uma inovação.

João Nuno Gaspar
BTC TQ

João Nuno Gaspar
BTC TQ

João Nuno Gaspar
BTC TQ

João Nuno Gaspar
BTC TQ

João Nuno Gaspar
BTC TQ

Apêndice 3 - Guião de entrevista e respetivas respostas – Calm Gameiro Marques

Entrevista – Mário Valente - R&D Lead at FullIT (Analyzing, choosing and implementing innovative technologies) - 91 454 15 78

Data - 24AGO2017 17h00

Local – Ruido Visual; Pc Alvalade, 6 - 2oF (Edifício por cima do CC, entrada do lado esquerdo do restaurante Mercantina)

Estrutura entrevista:

a) Apresentação
b) Explicação do objeto de investigação;
c) Explicação do intuito da entrevista – "O que procuro e onde quero chegar?"
d) Perguntas diretamente relacionadas com o problema e temas da investigação:

Temas -» *Awareness & InfoSec; Cyberattacks; Victims;*

1. **ID-A - Como vê o panorama nacional no que concerne aos crimes e ciberataques cujas criptomoedas contribuem para a sua consumação?**

R: A perceção que tenho no geral é que é preciso distinguir Crim Inf. em Portugal feita em Portugal vs Feita por portugueses. Ou seja, ataques há muitos, eu sei isso porque dirigi a informática do Ministério da Justiça por 3 anos, e os ataques eram diários. Isso acontece quase em todo o mundo. Vamos pôr desta maneira, em 3 anos, só 3 ou 4 vezes é que nós identificamos ameaças – APT's (Advanced Persistent Threats – que achámos por bem comunicar à PJ. E só uma vez é que houve uma intervenção dos serviços de informação (SIS). Portanto isto para dizer que se veem ataques a vir de muito lado, falamos de Criminalidade Informática, dentro do que a lei considera crimes informáticos. Agora para chegar a pontos extremos, são bastante menos. Assim, quando digo isto vindo tanto dentro de Portugal como fora de Portugal, são muitos, mas críticos são poucos. Agora pensando em crimes informáticos praticados por portugueses é residual e fundamentalmente tratam-se de scans a pc's e redes feitos por scriptkiddys que andam a pisar onde não devem. Ataques concertados em Portugal são provenientes do estrangeiro e não de dentro. Em Portugal o crime informático, olhando para ele como um todo, tratam-se de tentativas de acesos indevidos e fraudes em cartões de crédito, multibanco, códigos pin, falsificação de assinaturas, roubo de passwords. Trata-se do pequeno crime e não do crime organizado em escala persistente e avançado.

João Nuno Gaspar Cyberattacks
João Nuno Gaspar Cyberattacks
João Nuno Gaspar Cyberattacks
João Nuno Gaspar Cyberattacks
João Nuno Gaspar Cyberattacks

Temas -» *Awareness; Security; Victims; Infosec;*

2. **ID-B - Quais as consequências mais impactantes para as vítimas?**

R: É o tempo offline, ou seja, a perda de negócio durante o tempo em que estiveram em baixo. Para além desse há o caso dos bancos, onde existem casos identificados de pessoas que perderam dinheiro por transferências indevidas ou mal identificadas. Em termos individuais estamos a falar de abusos de credenciais nos bancos, em termos de empresas são os custos operacionais. Em Portugal só não há mais consequências porque quem sofre ataques não comunica, nem às autoridades nem aos seus clientes, estamos a falar em caso de um *data breach* ou caso de abusos de sistemas, qualquer que seja o ataque, não comunicam e, portanto, não se sabe[...] Se comunicassem obviamente que isso teria repercussões de negócio. Agora as empresas quando sofrem ataques, efetivamente não comunicam, mesmo que estejam em bolsa, sim há casos, e, portanto, não sofrem consequências pelo menos de reputação futura. Inclusivamente já fiz auditorias a empresas nacionais cotadas em bolsa e o cenário é negro... Se os investidores soubessem (risos). Enfim, para o bem de todos esperamos que com o GDPR comecem a comunicar.

João Nuno Gaspar Victims
João Nuno Gaspar Victims
João Nuno Gaspar Victims
João Nuno Gaspar Victims

3. **ID-C - Para que grupo de vítimas (órgãos administrativos, corporate ou indivíduos) as consequências são mais danosas?**

R: Há uns anos atrás, estava num conferência e perguntavam-me se eu quisesse estragar estragos por onde é que começava? Escolhia possivelmente um hospital, tendo em conta que infraestruturas críticas nacionais como a rede elétrica, distribuição agua, comunicações etc, que tipicamente até já têm algum nível de segurança. Facilmente, muito facilmente se consegue acesso a redes internas onde estão ligados equipamentos de suporte à vida, de BD's de saúde, análises médicas, exames médicos... Portanto, entre pessoas, empresas e Estado, os mais vulneráveis são as pessoas obviamente e são aquelas para quem um problema de segurança pode resultar num impacto maior em termos de significado para as suas vidas. Note-se que em dimensão absoluta pode parecer pequeno, mas para aquele individuo em especifico, tem um impacto muito grande. No Estado e nas empresas, estão menos vulneráveis e os impactos podem ser muito maiores, no entanto se esses impactos forem só os financeiros tipicamente não significam algo de maior[...] Eu se quiser mesmo causar estragos, não vou roubar a BD da segurança social nem nada parecido... Agora no dia em que alguém mandar abaixo uma rede critica de um Hospital, aí temos um problema grave... Portanto eu diria que pesando estes dois extremos, dos indivíduos vs empresas/estado e passando por esta questão do valor absoluto do prejuízo vs valor intangível do problema, existem alguns sítios que podem ter grandes repercussões, um deles são os Hospitais e aí tanto se aplica a Estado como aos privados. Seja de que tipo forem estão, por norma, extremamente desprotegidos e estão repletos de dados críticos sendo muito apetecíveis pelo dinheiro que esses dados valem, por exemplo em mercados negros. Assim, para estes as falhas podem até ter um forte impacto financeiro, mas o problema é no dia em que tiverem impactos não tangíveis ou mensurados em dinheiro, podendo ser até falhas que podem ter como consequência vidas humanas.

João Nuno Gaspar Victims
João Nuno Gaspar Victims

4. **ID-D - Considera que as potenciais vítimas (utilizadores do ciberespaço) estão sensibilizadas ou preparadas para lidar com a ameaças?**

R: Até há bem pouco tempo, muito pouca perceção ao risco, aos impactos que pode ter, pouca sensibilização para o problema, pouco conhecimento sobre o problema também... Digo até recentemente, mas refiro-me mais ou menos até Maio de 2017. Embora já se soubesse do GDPR há mais tempo, só agora é que subitamente as empresas se aperceberam do trabalho que tem que ser desenvolvido e das mudanças que têm que ser feitas e é interessante, porque eu penso que o alerta só despertou, porque as empresas leram aquela parte das multas, sabe? Portanto subitamente de há uns meses para cá tenho visto mais algum cuidado e interesse no assunto, uma vez que a coisa foi tangibilizada em lei e em dinheiro.

João Nuno Gaspar A & InfoSec
João Nuno Gaspar A & InfoSec
João Nuno Gaspar A & InfoSec

EU: E na sua opinião isso vai refletir-se na criação de políticas internas de segurança?

R: Sim, isso já se está a ver. Há inclusivamente organismos públicos que querem criar centros de respostas a incidentes de segurança, porque estão a aperceber-se que não têm outra alternativa.

João Nuno Gaspar A & InfoSec

5. **ID-E - As empresas vítimas de ciberataques que as comprometam, têm por hábito reportar às autoridades competentes?**

R: Respondido na 2;

Temas -» *Awareness & InfoSec; Victims;*

6. **ID-F - Ao nível do poder decisório, qual o nível de awareness e de perceção do risco p/ estes incidentes, por parte dos c-levels?**

R: Respondido na 4;

7. **ID-G - Qual o estado de maturação na cultura de segurança das organizações nacionais?**

R: Respondido na 4; + Existe algum desleixo ainda, mas já existem alguma consciencialização para o impacto possível e portanto com o boost do GDPR, as organizações portuguesas e europeias vão fortalecer-se neste tópico;

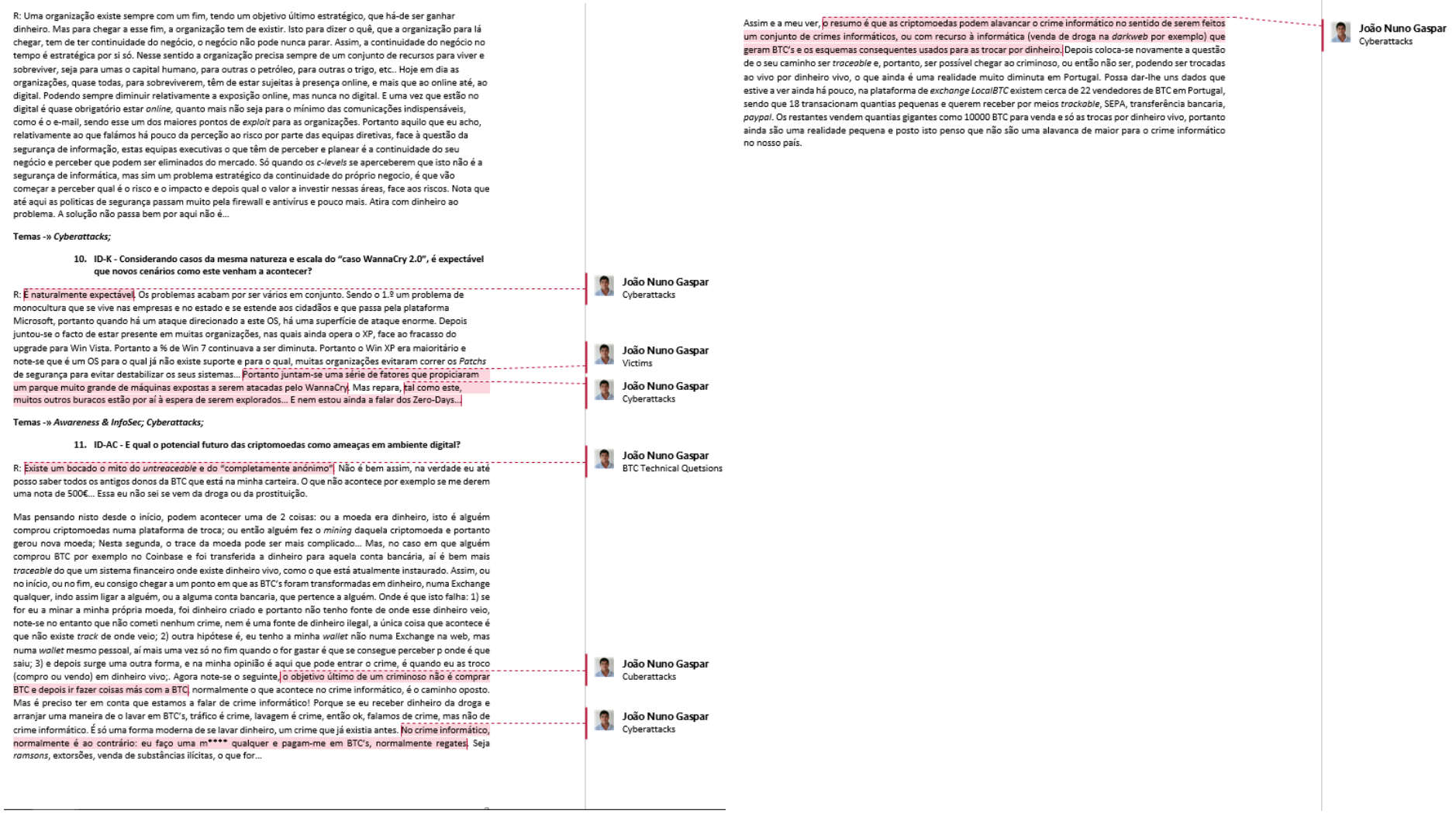
João Nuno Gaspar A & InfoSec

8. **ID-H - Como parte de empresa que desenvolve soluções, estas são desenvolvidas tendo em conta o conceito de *Security by design?***

R: Não são, a resposta é simples. Pode ser que comece a mudar num futuro próximo. Mais uma vez posso falar de organismos públicos, pedem auditorias para uma aplicação que esteja a ser desenvolvida (um portal ou um site)... no entanto esquecem-se de auditar o código. E é assim que funciona um bocadinho... Nestes casos, somos nós, ou a minha equipa que, quando nos são solicitados trabalhos de segurança, sugere que sejam auditados também os códigos. Portanto a solução é muito simples, há ferramentas open-source que correm o código de uma ponta à outra à procura de vulnerabilidades, no entanto a falta de sensibilidade para o tema é tanta que nem lhes passa pela cabeça essa hipótese. Já nem estou a falar do desenvolvimento *by design*, onde programadores desenvolvem e pensam a arquitetura do sistema por forma a garantir segurança e privacidade, já estou a falar um bocadinho à frente, ou seja, desenvolve-se esta aplicação, de repente apercebemo-nos que não tivemos muito este *mindset* da segurança, epá então o mínimo seria que pedissem a alguém que lhes faça correr esta ferramenta para ver se encontramos potenciais buracos. Nem isto acontece, nas maiores consultoras de IT que trabalham com organismos públicos.

João Nuno Gaspar A & Infosec;
João Nuno Gaspar A & Infosec;
João Nuno Gaspar A & Infosec;
João Nuno Gaspar A & Infosec;

9. **ID-I - A solução para uma mais eficiente segurança de informação passa por uma menor exposição e presença online, ou por políticas de gestão da segurança de informação?**



R: Uma organização existe sempre com um fim, tendo um objetivo último estratégico, que há-de ser ganhar dinheiro. Mas para chegar a esse fim, a organização tem de existir. Isto para dizer o quê, que a organização para lá chegar, tem de ter continuidade do negócio, o negócio não pode nunca parar. Assim, a continuidade do negócio no tempo é estratégica por si só. Nesse sentido a organização precisa sempre de um conjunto de recursos para viver e sobreviver, seja para umas o capital humano, para outras o petróleo, para outras o trigo, etc.. Hoje em dia as organizações, quase todas, para sobreviverem, têm de estar sujeitas à presença online, e mais que ao online até, ao digital. Podendo sempre diminuir relativamente a exposição online, mas nunca no digital. E uma vez que estão no digital é quase obrigatório estar *online*, quanto mais não seja para o mínimo das comunicações indispensáveis, como é o e-mail, sendo esse um dos maiores pontos de *exploit* para as organizações. Portanto aquilo que eu acho, relativamente ao que falámos há pouco da perceção ao risco por parte das equipas diretivas, face à questão da segurança de informação, estas equipas executivas o que têm de perceber e planear é a continuidade do seu negócio e perceber que podem ser eliminados do mercado. Só quando os *c-levels* se aperceberem que isto não é a segurança de informática, mas sim um problema estratégico da continuidade do próprio negocio, é que vão começar a perceber qual é o risco e o impacto e depois qual o valor a investir nessas áreas, face aos riscos. Nota que até aqui as politicas de segurança passam muito pela firewall e antivírus e pouco mais. Atira com dinheiro ao problema. A solução não passa bem por aqui não é...

Temas -» *Cyberattacks;*

10. ID-K - Considerando casos da mesma natureza e escala do "caso WannaCry 2.0", é expectável que novos cenários como este venham a acontecer?

João Nuno Gaspar
Cyberattacks

R: É naturalmente expectável. Os problemas acabam por ser vários em conjunto. Sendo o 1.º um problema de monocultura que se vive nas empresas e no estado e se estende aos cidadãos e que passa pela plataforma Microsoft, portanto quando há um ataque direcionado a este OS, há uma superfície de ataque enorme. Depois juntou-se o facto de estar presente em muitas organizações, nas quais ainda opera o XP, face ao fracasso do upgrade para Win Vista. Portanto a % de Win 7 continuava a ser diminuta. Portanto o Win XP era maioritário e note-se que é um OS para o qual já não existe suporte e para o qual, muitas organizações evitaram correr os *Patchs* de segurança para evitar destabilizar os seus sistemas... Portanto juntam-se uma série de fatores que propiciaram um parque muito grande de máquinas expostas a serem atacadas pelo WannaCry. Mas repara, tal como este, muitos outros buracos estão por aí à espera de serem explorados... E nem estou ainda a falar dos Zero-Days...

João Nuno Gaspar
Victims

João Nuno Gaspar
Cyberattacks

Temas -» *Awareness & InfoSec; Cyberattacks;*

11. ID-AC - E qual o potencial futuro das criptomoedas como ameaças em ambiente digital?

João Nuno Gaspar
BTC Technical Quetsions

R: Existe um bocado o mito do *untreaceable* e do "completamente anónimo". Não é bem assim, na verdade eu até posso saber todos os antigos donos da BTC que está na minha carteira. O que não acontece por exemplo se me derem uma nota de 500€... Essa eu não sei se vem da droga ou da prostituição.

Mas pensando nisto desde o início, podem acontecer uma de 2 coisas: ou a moeda era dinheiro, isto é alguém comprou criptomoedas numa plataforma de troca; ou então alguém fez o *mining* daquela criptomoeda e portanto gerou nova moeda; Nesta segunda, o trace da moeda pode ser mais complicado... Mas, no caso em que alguém comprou BTC por exemplo no Coinbase e foi transferida a dinheiro para aquela conta bancária, aí é bem mais *traceable* do que um sistema financeiro onde existe dinheiro vivo, como o que está atualmente instaurado. Assim, ou no início, ou no fim, eu consigo chegar a um ponto em que as BTC's foram transformadas em dinheiro, numa Exchange qualquer, indo assim ligar a alguém, ou a alguma conta bancaria, que pertence a alguém. Onde é que isto falha: 1) se for eu a minar a minha própria moeda, foi dinheiro criado e portanto não tenho fonte de onde esse dinheiro veio, note-se no entanto que não cometi nenhum crime, nem é uma fonte de dinheiro ilegal, a única coisa que acontece é que não existe *track* de onde veio; 2) outra hipótese é, eu tenho a minha *wallet* não numa Exchange na web, mas numa *wallet* mesmo pessoal, aí mais uma vez só no fim quando o for gastar é que se consegue perceber p onde é que saiu; 3) e depois surge uma outra forma, e na minha opinião é aqui que pode entrar o crime, é quando eu as troco (compro ou vendo) em dinheiro vivo;. Agora note-se o seguinte, o objetivo último de um criminoso não é comprar BTC e depois ir fazer coisas más com a BTC, normalmente o que acontece no crime informático, é o caminho oposto. Mas é preciso ter em conta que estamos a falar de crime informático! Porque se eu receber dinheiro da droga e arranjar uma maneira de o lavar em BTC's, tráfico é crime, lavagem é crime, então ok, falamos de crime, mas não de crime informático. É só uma forma moderna de se lavar dinheiro, um crime que já existia antes. No crime informático, normalmente é ao contrário: eu faço uma m**** qualquer e pagam-me em BTC's, normalmente regates. Seja *ramsons*, extorsões, venda de substâncias ilícitas, o que for...

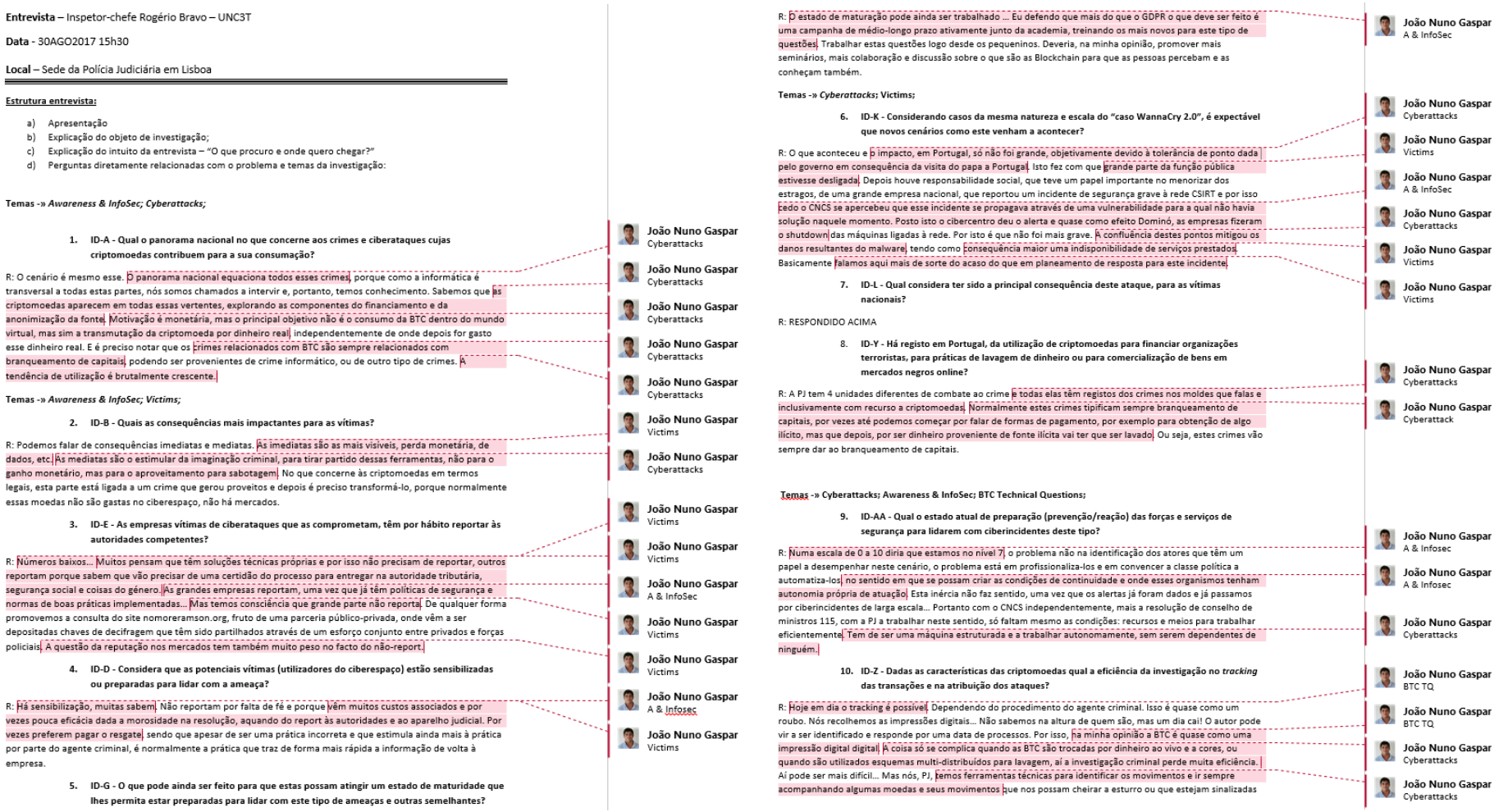
João Nuno Gaspar
Cuberattacks

João Nuno Gaspar
Cyberattacks

Assim e a meu ver, o resumo é que as criptomoedas podem alavancar o crime informático no sentido de serem feitos um conjunto de crimes informáticos, ou com recurso à informática (venda de droga na *darkweb* por exemplo) que geram BTC's e os esquemas consequentes usados para as trocar por dinheiro. Depois coloca-se novamente a questão de o seu caminho ser *traceable* e, portanto, ser possível chegar ao criminoso, ou então não ser, podendo ser trocadas ao vivo por dinheiro vivo, o que ainda é uma realidade muito diminuta em Portugal. Possa dar-lhe uns dados que estive a ver ainda há pouco, na plataforma de *exchange LocalBTC* existem cerca de 22 vendedores de BTC em Portugal, sendo que 18 transacionam quantias pequenas e querem receber por meios *trackable*, SEPA, transferência bancaria, *paypal*. Os restantes vendem quantias gigantes como 10000 BTC para venda e só as trocas por dinheiro vivo, portanto ainda são uma realidade pequena e posto isto penso que não são uma alavanca de maior para o crime informático no nosso país.

João Nuno Gaspar
Cyberattacks

Apêndice 4 - Guião de entrevista e respetivas respostas – Mário Valente



Entrevista – Inspetor-chefe Rogério Bravo – UNC3T

Data - 30AGO2017 15h30

Local – Sede da Polícia Judiciária em Lisboa

Estrutura entrevista:

a) Apresentação
b) Explicação do objeto de investigação;
c) Explicação do intuito da entrevista – "O que procuro e onde quero chegar?"
d) Perguntas diretamente relacionadas com o problema e temas da investigação:

Temas -» *Awareness & InfoSec; Cyberattacks;*

1. **ID-A - Qual o panorama nacional no que concerne aos crimes e ciberataques cujas criptomoedas contribuem para a sua consumação?**

R: O cenário é mesmo esse. O panorama nacional equaciona todos esses crimes, porque como a informática é transversal a todas estas partes, nós somos chamados a intervir e, portanto, temos conhecimento. Sabemos que as criptomoedas aparecem em todas essas vertentes, explorando as componentes do financiamento e da anonimização da fonte. Motivação é monetária, mas o principal objetivo não é o consumo da BTC dentro do mundo virtual, mas sim a transmutação da criptomoeda por dinheiro real, independentemente de onde depois for gasto esse dinheiro real. E é preciso notar que os crimes relacionados com BTC são sempre relacionados com branqueamento de capitais, podendo ser provenientes de crime informático, ou de outro tipo de crimes. A tendência de utilização é brutalmente crescente.

Temas -» *Awareness & InfoSec; Victims;*

2. **ID-B - Quais as consequências mais impactantes para as vítimas?**

R: Podemos falar de consequências imediatas e mediatas. As imediatas são as mais visíveis, perda monetária, de dados, etc. As mediatas são o estimular da imaginação criminal, para tirar partido dessas ferramentas, não para o ganho monetário, mas para o aproveitamento para sabotagem. No que concerne às criptomoedas em termos legais, esta parte está ligada a um crime que gerou proveitos e depois é preciso transformá-lo, porque normalmente essas moedas não são gastas no ciberespaço, não há mercados.

3. **ID-E - As empresas vítimas de ciberataques que as comprometam, têm por hábito reportar às autoridades competentes?**

R: Números baixos… Muitos pensam que têm soluções técnicas próprias e por isso não precisam de reportar, outros reportam porque sabem que vão precisar de uma certidão do processo para entregar na autoridade tributária, segurança social e coisas do género. As grandes empresas reportam, uma vez que já têm políticas de segurança e normas de boas práticas implementadas… Mas temos consciência que grande parte não reporta. De qualquer forma promovemos a consulta do site nomoreramson.org, fruto de uma parceria público-privada, onde vêm a ser depositadas chaves de decifragem que têm sido partilhados através de um esforço conjunto entre privados e forças policiais. A questão da reputação nos mercados tem também muito peso no facto do não-report.

4. **ID-D - Considera que as potenciais vítimas (utilizadores do ciberespaço) estão sensibilizadas ou preparadas para lidar com a ameaça?**

R: Há sensibilização, muitas sabem. Não reportam por falta de fé e porque vêm muitos custos associados e por vezes pouca eficácia dada a morosidade na resolução, aquando do report às autoridades e ao aparelho judicial. Por vezes preferem pagar o resgate, sendo que apesar de ser uma prática incorreta e que estimula ainda mais à prática por parte do agente criminal, é normalmente a prática que traz de forma mais rápida a informação de volta à empresa.

5. **ID-G - O que pode ainda ser feito para que estas possam atingir um estado de maturidade que lhes permita estar preparadas para lidar com este tipo de ameaças e outras semelhantes?**

R: O estado de maturação pode ainda ser trabalhado … Eu defendo que mais do que o GDPR o que deve ser feito é uma campanha de médio-longo prazo ativamente junto da academia, treinando os mais novos para este tipo de questões. Trabalhar estas questões logo desde os pequeninos. Deveria, na minha opinião, promover mais seminários, mais colaboração e discussão sobre o que são as Blockchain para que as pessoas percebam e as conheçam também.

Temas -» *Cyberattacks*; Victims;

6. **ID-K - Considerando casos da mesma natureza e escala do "caso WannaCry 2.0", é expectável que novos cenários como este venham a acontecer?**

R: O que aconteceu e o impacto, em Portugal, só não foi grande, objetivamente devido à tolerância de ponto dada pelo governo em consequência da visita do papa a Portugal. Isto fez com que grande parte da função pública estivesse desligada. Depois houve responsabilidade social, que teve um papel importante no menorizar dos estragos, de uma grande empresa nacional, que reportou um incidente de segurança grave à rede CSIRT e por isso cedo o CNCS se apercebeu que esse incidente se propagava através de uma vulnerabilidade para a qual não havia solução naquele momento. Posto isto o cibercentro deu o alerta e quase como efeito Dominó, as empresas fizeram o shutdown das máquinas ligadas à rede. Por isto é que não foi mais grave. A confluência destes pontos mitigou os danos resultantes do malware, tendo como consequência maior uma indisponibilidade de serviços prestados. Basicamente falamos aqui mais de sorte do acaso do que em planeamento de resposta para este incidente.

7. **ID-L - Qual considera ter sido a principal consequência deste ataque, para as vítimas nacionais?**

R: RESPONDIDO ACIMA

8. **ID-Y - Há registo em Portugal, da utilização de criptomoedas para financiar organizações terroristas, para práticas de lavagem de dinheiro ou para comercialização de bens em mercados negros online?**

R: A PJ tem 4 unidades diferentes de combate ao crime e todas elas têm registos dos crimes nos moldes que falas e inclusivamente com recurso a criptomoedas. Normalmente estes crimes tipificam sempre branqueamento de capitais, por vezes até podemos começar por falar de formas de pagamento, por exemplo para obtenção de algo ilícito, mas que depois, por ser dinheiro proveniente de fonte ilícita vai ter que ser lavado. Ou seja, estes crimes vão sempre dar ao branqueamento de capitais.

Temas -» Cyberattacks; Awareness & InfoSec; BTC Technical Questions;

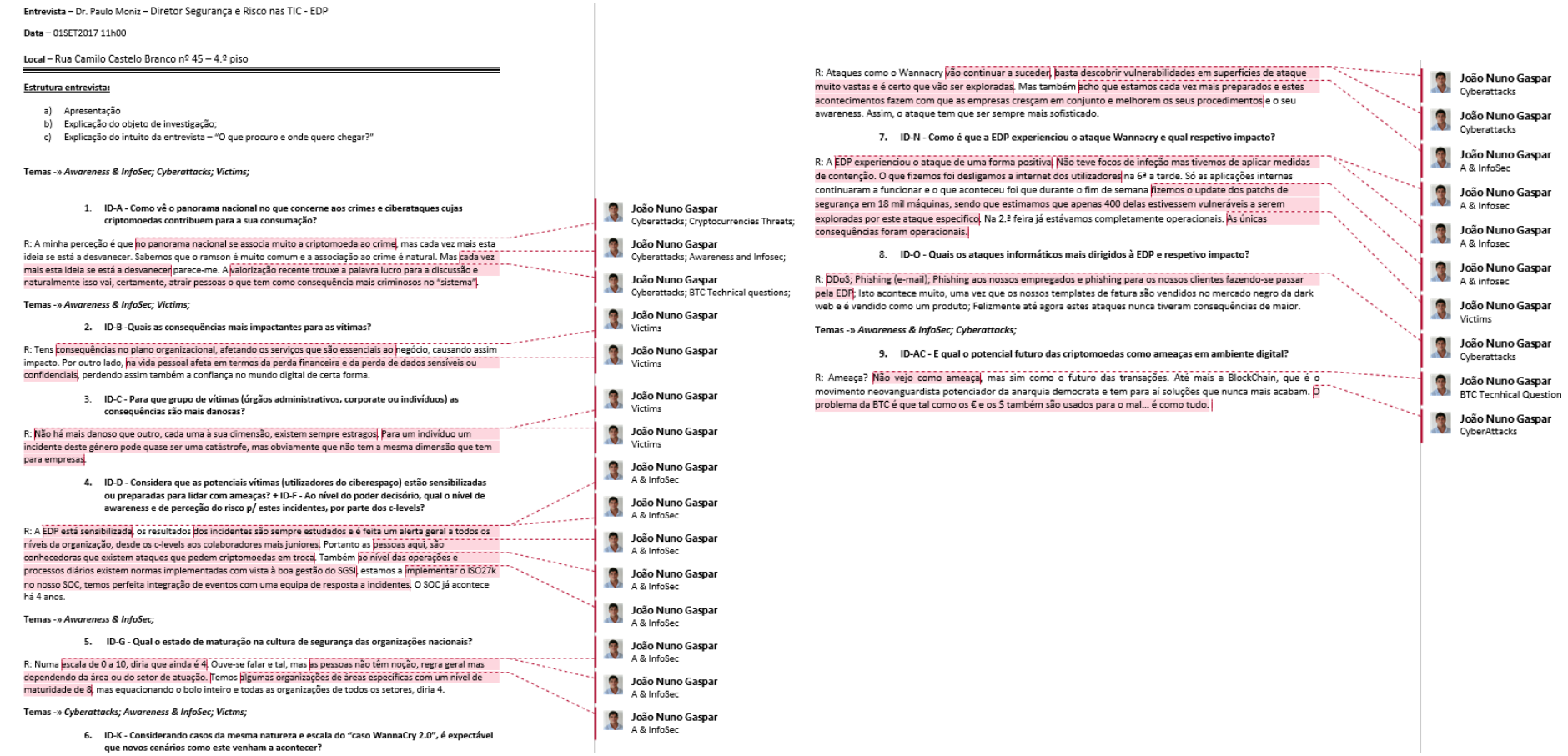
9. **ID-AA - Qual o estado atual de preparação (prevenção/reação) das forças e serviços de segurança para lidarem com ciberincidentes deste tipo?**

R: Numa escala de 0 a 10 diria que estamos no nível 7, o problema não na identificação dos atores que têm um papel a desempenhar neste cenário, o problema está em profissionaliza-los e em convencer a classe política a automatiza-los, no sentido em que se possam criar as condições de continuidade e onde esses organismos tenham autonomia própria de atuação. Esta inércia não faz sentido, uma vez que os alertas já foram dados e já passamos por ciberincidentes de larga escala… Portanto com o CNCS independentemente, mais a resolução de conselho de ministros 115, com a PJ a trabalhar neste sentido, só faltam mesmo as condições: recursos e meios para trabalhar eficientemente. Tem de ser uma máquina estruturada e a trabalhar autonomamente, sem serem dependentes de ninguém.

10. **ID-Z - Dadas as características das criptomoedas qual a eficiência da investigação no *tracking* das transações e na atribuição dos ataques?**

R: Hoje em dia o tracking é possível. Dependendo do procedimento do agente criminal. Isso é quase como um roubo. Nós recolhemos as impressões digitais… Não sabemos na altura de quem são, mas um dia cai! O autor pode vir a ser identificado e responde por uma data de processos. Por isso, na minha opinião a BTC é quase como uma impressão digital digital. A coisa só se complica quando as BTC são trocadas por dinheiro ao vivo e a cores, ou quando são utilizados esquemas multi-distribuídos para lavagem, aí a investigação criminal perde muita eficiência. Aí pode ser mais difícil… Mas nós, PJ, temos ferramentas técnicas para identificar os movimentos e ir sempre acompanhando algumas moedas e seus movimentos que nos possam cheirar a esturro ou que estejam sinalizadas

Apêndice 5 - Guião de entrevista e respetivas respostas – Inspetor-chefe Rogério Bravo



Entrevista – Dr. Paulo Moniz – Diretor Segurança e Risco nas TIC - EDP

Data – 01SET2017 11h00

Local – Rua Camilo Castelo Branco nº 45 – 4.º piso

Estrutura entrevista:

a) Apresentação
b) Explicação do objeto de investigação;
c) Explicação do intuito da entrevista – "O que procuro e onde quero chegar?"

Temas -» *Awareness & InfoSec; Cyberattacks; Victims;*

1. **ID-A - Como vê o panorama nacional no que concerne aos crimes e ciberataques cujas criptomoedas contribuem para a sua consumação?**

R: A minha perceção é que no panorama nacional se associa muito a criptomoeda ao crime, mas cada vez mais esta ideia se está a desvanecer. Sabemos que o ramson é muito comum e a associação ao crime é natural. Mas cada vez mais esta ideia se está a desvanecer parece-me. A valorização recente trouxe a palavra lucro para a discussão e naturalmente isso vai, certamente, atrair pessoas o que tem como consequência mais criminosos no "sistema".

Temas -» *Awareness & InfoSec; Victims;*

2. **ID-B -Quais as consequências mais impactantes para as vítimas?**

R: Tens consequências no plano organizacional, afetando os serviços que são essenciais ao negócio, causando assim impacto. Por outro lado, na vida pessoal afeta em termos da perda financeira e da perda de dados sensíveis ou confidenciais, perdendo assim também a confiança no mundo digital de certa forma.

3. **ID-C - Para que grupo de vítimas (órgãos administrativos, corporate ou indivíduos) as consequências são mais danosas?**

R: Não há mais danoso que outro, cada uma à sua dimensão, existem sempre estragos. Para um indivíduo um incidente deste género pode quase ser uma catástrofe, mas obviamente que não tem a mesma dimensão que tem para empresas.

4. **ID-D - Considera que as potenciais vítimas (utilizadores do ciberespaço) estão sensibilizadas ou preparadas para lidar com ameaças? + ID-F - Ao nível do poder decisório, qual o nível de awareness e de perceção do risco p/ estes incidentes, por parte dos c-levels?**

R: A EDP está sensibilizada, os resultados dos incidentes são sempre estudados e é feita um alerta geral a todos os níveis da organização, desde os c-levels aos colaboradores mais juniores. Portanto as pessoas aqui, são conhecedoras que existem ataques que pedem criptomoedas em troca. Também ao nível das operações e processos diários existem normas implementadas com vista à boa gestão do SGSI, estamos a implementar o ISO27k no nosso SOC, temos perfeita integração de eventos com uma equipa de resposta a incidentes. O SOC já acontece há 4 anos.

Temas -» *Awareness & InfoSec;*

5. **ID-G - Qual o estado de maturação na cultura de segurança das organizações nacionais?**

R: Numa escala de 0 a 10, diria que ainda é 4. Ouve-se falar e tal, mas as pessoas não têm noção, regra geral mas dependendo da área ou do setor de atuação. Temos algumas organizações de áreas específicas com um nível de maturidade de 8, mas equacionando o bolo inteiro e todas as organizações de todos os setores, diria 4.

Temas -» *Cyberattacks; Awareness & InfoSec; Victms;*

6. **ID-K - Considerando casos da mesma natureza e escala do "caso WannaCry 2.0", é expectável que novos cenários como este venham a acontecer?**

R: Ataques como o Wannacry vão continuar a suceder, basta descobrir vulnerabilidades em superfícies de ataque muito vastas e é certo que vão ser exploradas. Mas também acho que estamos cada vez mais preparados e estes acontecimentos fazem com que as empresas cresçam em conjunto e melhorem os seus procedimentos e o seu awareness. Assim, o ataque tem que ser sempre mais sofisticado.

7. **ID-N - Como é que a EDP experienciou o ataque Wannacry e qual respetivo impacto?**

R: A EDP experienciou o ataque de uma forma positiva. Não teve focos de infeção mas tivemos de aplicar medidas de contenção. O que fizemos foi desligamos a internet dos utilizadores na 6ª a tarde. Só as aplicações internas continuaram a funcionar e o que aconteceu foi que durante o fim de semana fizemos o update dos patchs de segurança em 18 mil máquinas, sendo que estimamos que apenas 400 delas estivessem vulneráveis a serem exploradas por este ataque específico. Na 2.ª feira já estávamos completamente operacionais. As únicas consequências foram operacionais.

8. **ID-O - Quais os ataques informáticos mais dirigidos à EDP e respetivo impacto?**

R: DDoS; Phishing (e-mail); Phishing aos nossos empregados e phishing para os nossos clientes fazendo-se passar pela EDP. Isto acontece muito, uma vez que os nossos templates de fatura são vendidos no mercado negro da dark web e é vendido como um produto; Felizmente até agora estes ataques nunca tiveram consequências de maior.

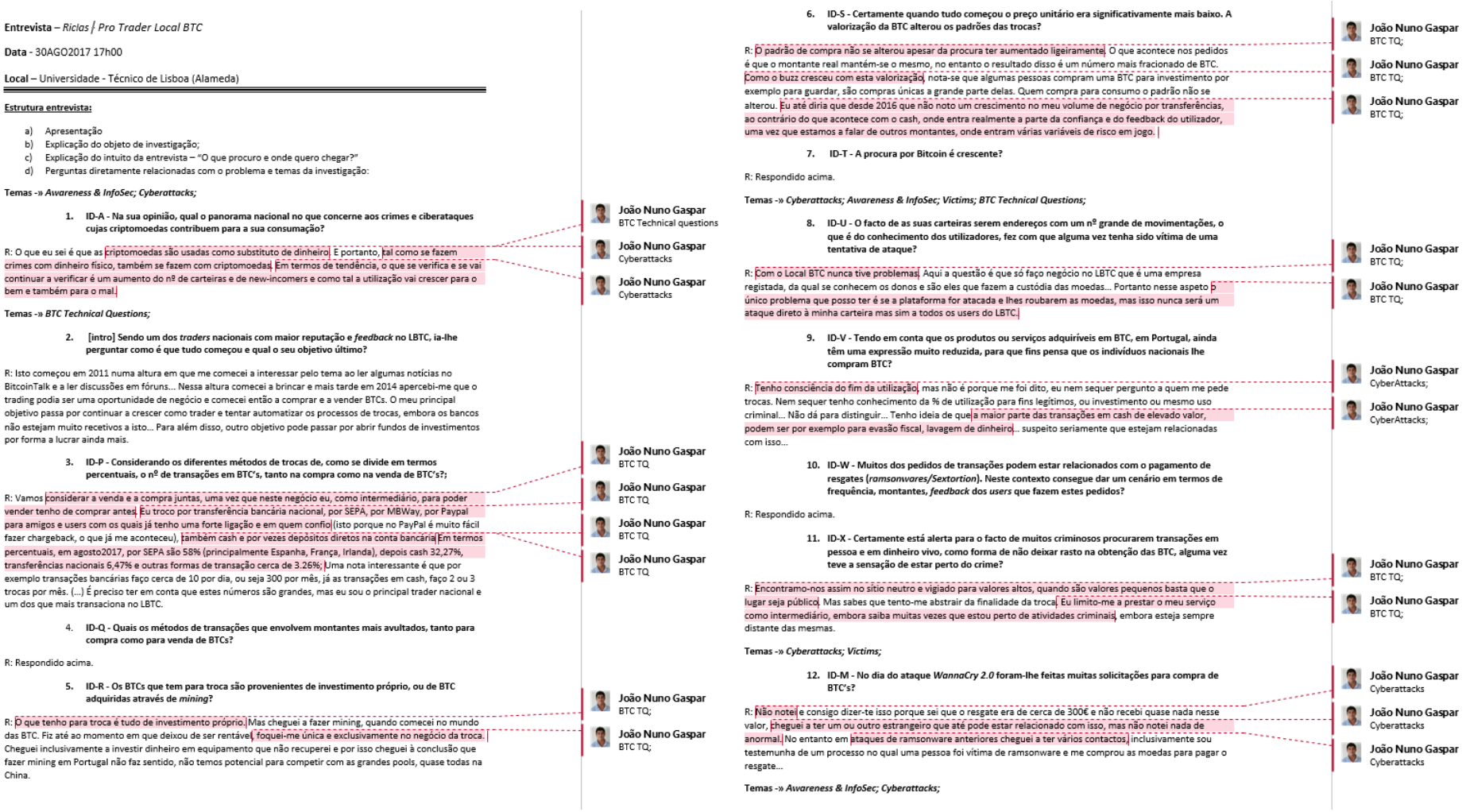
Temas -» *Awareness & InfoSec; Cyberattacks;*

9. **ID-AC - E qual o potencial futuro das criptomoedas como ameaças em ambiente digital?**

R: Ameaça? Não vejo como ameaça, mas sim como o futuro das transações. Até mais a BlockChain, que é o movimento neovanguardista potenciador da anarquia democrata e tem para aí soluções que nunca mais acabam. O problema da BTC é que tal como os € e os $ também são usados para o mal... é como tudo.

João Nuno Gaspar – Cyberattacks; Cryptocurrencies Threats;
João Nuno Gaspar – Cyberattacks; Awareness and Infosec;
João Nuno Gaspar – Cyberattacks; BTC Technical questions;
João Nuno Gaspar – Victims
João Nuno Gaspar – Victims
João Nuno Gaspar – Victims
João Nuno Gaspar – Victims
João Nuno Gaspar – A & InfoSec
João Nuno Gaspar – A & InfoSec
João Nuno Gaspar – A & InfoSec
João Nuno Gaspar – A & InfoSec
João Nuno Gaspar – A & InfoSec
João Nuno Gaspar – A & InfoSec
João Nuno Gaspar – A & InfoSec
João Nuno Gaspar – A & InfoSec
João Nuno Gaspar – Cyberattacks
João Nuno Gaspar – Cyberattacks
João Nuno Gaspar – A & InfoSec
João Nuno Gaspar – A & Infosec
João Nuno Gaspar – A & Infosec
João Nuno Gaspar – A & infosec
João Nuno Gaspar – Victims
João Nuno Gaspar – Cyberattacks
João Nuno Gaspar – BTC Tecnhical Question
João Nuno Gaspar – CyberAttacks

Apêndice 6 – Guião de entrevista e respetivas respostas – Paulo Moniz;



Entrevista – *Riclas | Pro Trader Local BTC*

Data - 30AGO2017 17h00

Local – Universidade - Técnico de Lisboa (Alameda)

Estrutura entrevista:

a) Apresentação
b) Explicação do objeto de investigação;
c) Explicação do intuito da entrevista – "O que procuro e onde quero chegar?"
d) Perguntas diretamente relacionadas com o problema e temas da investigação:

Temas -» *Awareness & InfoSec; Cyberattacks;*

1. **ID-A - Na sua opinião, qual o panorama nacional no que concerne aos crimes e ciberataques cujas criptomoedas contribuem para a sua consumação?**

R: O que eu sei é que as criptomoedas são usadas como substituto de dinheiro. E portanto, tal como se fazem crimes com dinheiro físico, também se fazem com criptomoedas. Em termos de tendência, o que se verifica e se vai continuar a verificar é um aumento do nº de carteiras e de new-incomers e como tal a utilização vai crescer para o bem e também para o mal.

Temas -» *BTC Technical Questions;*

2. **[intro] Sendo um dos *traders* nacionais com maior reputação e *feedback* no LBTC, ia-lhe perguntar como é que tudo começou e qual o seu objetivo último?**

R: Isto começou em 2011 numa altura em que me comecei a interessar pelo tema ao ler algumas notícias no BitcoinTalk e a ler discussões em fóruns... Nessa altura comecei a brincar e mais tarde em 2014 apercebi-me que o trading podia ser uma oportunidade de negócio e comecei então a comprar e a vender BTCs. O meu principal objetivo passa por continuar a crescer como trader e tentar automatizar os processos de trocas, embora os bancos não estejam muito recetivos a isto... Para além disso, outro objetivo pode passar por abrir fundos de investimentos por forma a lucrar ainda mais.

3. **ID-P - Considerando os diferentes métodos de trocas de, como se divide em termos percentuais, o nº de transações em BTC's, tanto na compra como na venda de BTC's?;**

R: Vamos considerar a venda e a compra juntas, uma vez que neste negócio eu, como intermediário, para poder vender tenho de comprar antes. Eu troco por transferência bancária nacional, por SEPA, por MBWay, por Paypal para amigos e users com os quais já tenho uma forte ligação e em quem confio (isto porque no PayPal é muito fácil fazer chargeback, o que já me aconteceu), também cash e por vezes depósitos diretos na conta bancária. Em termos percentuais, em agosto2017, por SEPA são 58% (principalmente Espanha, França, Irlanda), depois cash 32,27%, transferências nacionais 6,47% e outras formas de transação cerca de 3.26%; Uma nota interessante é que por exemplo transações bancárias faço cerca de 10 por dia, ou seja 300 por mês, já as transações em cash, faço 2 ou 3 trocas por mês. (...) É preciso ter em conta que estes números são grandes, mas eu sou o principal trader nacional e um dos que mais transaciona no LBTC.

4. **ID-Q - Quais os métodos de transações que envolvem montantes mais avultados, tanto para compra como para venda de BTCs?**

R: Respondido acima.

5. **ID-R - Os BTCs que tem para troca são provenientes de investimento próprio, ou de BTC adquiridas através de *mining*?**

R: O que tenho para troca é tudo de investimento próprio. Mas cheguei a fazer mining, quando comecei no mundo das BTC. Fiz até ao momento em que deixou de ser rentável. Foquei-me única e exclusivamente no negócio da troca. Cheguei inclusivamente a investir dinheiro em equipamento que não recuperei e por isso cheguei à conclusão que fazer mining em Portugal não faz sentido, não temos potencial para competir com as grandes pools, quase todas na China.

6. **ID-S - Certamente quando tudo começou o preço unitário era significativamente mais baixo. A valorização da BTC alterou os padrões das trocas?**

R: O padrão de compra não se alterou apesar da procura ter aumentado ligeiramente. O que acontece nos pedidos é que o montante real mantém-se o mesmo, no entanto o resultado disso é um número mais fracionado de BTC. Como o buzz cresceu com esta valorização, nota-se que algumas pessoas compram uma BTC para investimento por exemplo para guardar, são compras únicas a grande parte delas. Quem compra para consumo o padrão não se alterou. Eu até diria que desde 2016 que não noto um crescimento no meu volume de negócio por transferências, ao contrário do que acontece com o cash, onde entra realmente a parte da confiança e do feedback do utilizador, uma vez que estamos a falar de outros montantes, onde entram várias variáveis de risco em jogo.

7. **ID-T - A procura por Bitcoin é crescente?**

R: Respondido acima.

Temas -» *Cyberattacks; Awareness & InfoSec; Victims; BTC Technical Questions;*

8. **ID-U - O facto de as suas carteiras serem endereços com um nº grande de movimentações, o que é do conhecimento dos utilizadores, fez com que alguma vez tenha sido vítima de uma tentativa de ataque?**

R: Com o Local BTC nunca tive problemas. Aqui a questão é que só faço negócio no LBTC que é uma empresa registada, da qual se conhecem os donos e são eles que fazem a custódia das moedas... Portanto nesse aspeto o único problema que posso ter é se a plataforma for atacada e lhes roubarem as moedas, mas isso nunca será um ataque direto à minha carteira mas sim a todos os users do LBTC.

9. **ID-V - Tendo em conta que os produtos ou serviços adquiríveis em BTC, em Portugal, ainda têm uma expressão muito reduzida, para que fins pensa que os indivíduos nacionais lhe compram BTC?**

R: Tenho consciência do fim da utilização, mas não é porque me foi dito, eu nem sequer pergunto a quem me pede trocas. Nem sequer tenho conhecimento da % de utilização para fins legítimos, ou investimento ou mesmo uso criminal... Não dá para distinguir... Tenho ideia de que a maior parte das transações em cash de elevado valor, podem ser por exemplo para evasão fiscal, lavagem de dinheiro... suspeito seriamente que estejam relacionadas com isso...

10. **ID-W - Muitos dos pedidos de transações podem estar relacionados com o pagamento de resgates (*ramsomvares/Sextortion*). Neste contexto consegue dar um cenário em termos de frequência, montantes, *feedback* dos *users* que fazem estes pedidos?**

R: Respondido acima.

11. **ID-X - Certamente está alerta para o facto de muitos criminosos procurarem transações em pessoa e em dinheiro vivo, como forma de não deixar rasto na obtenção das BTC, alguma vez teve a sensação de estar perto do crime?**

R: Encontramo-nos assim no sítio neutro e vigiado para valores altos, quando são valores pequenos basta que o lugar seja público. Mas sabes que tento-me abstrair da finalidade da troca. Eu limito-me a prestar o meu serviço como intermediário, embora saiba muitas vezes que estou perto de atividades criminais, embora esteja sempre distante das mesmas.

Temas -» *Cyberattacks; Victims;*

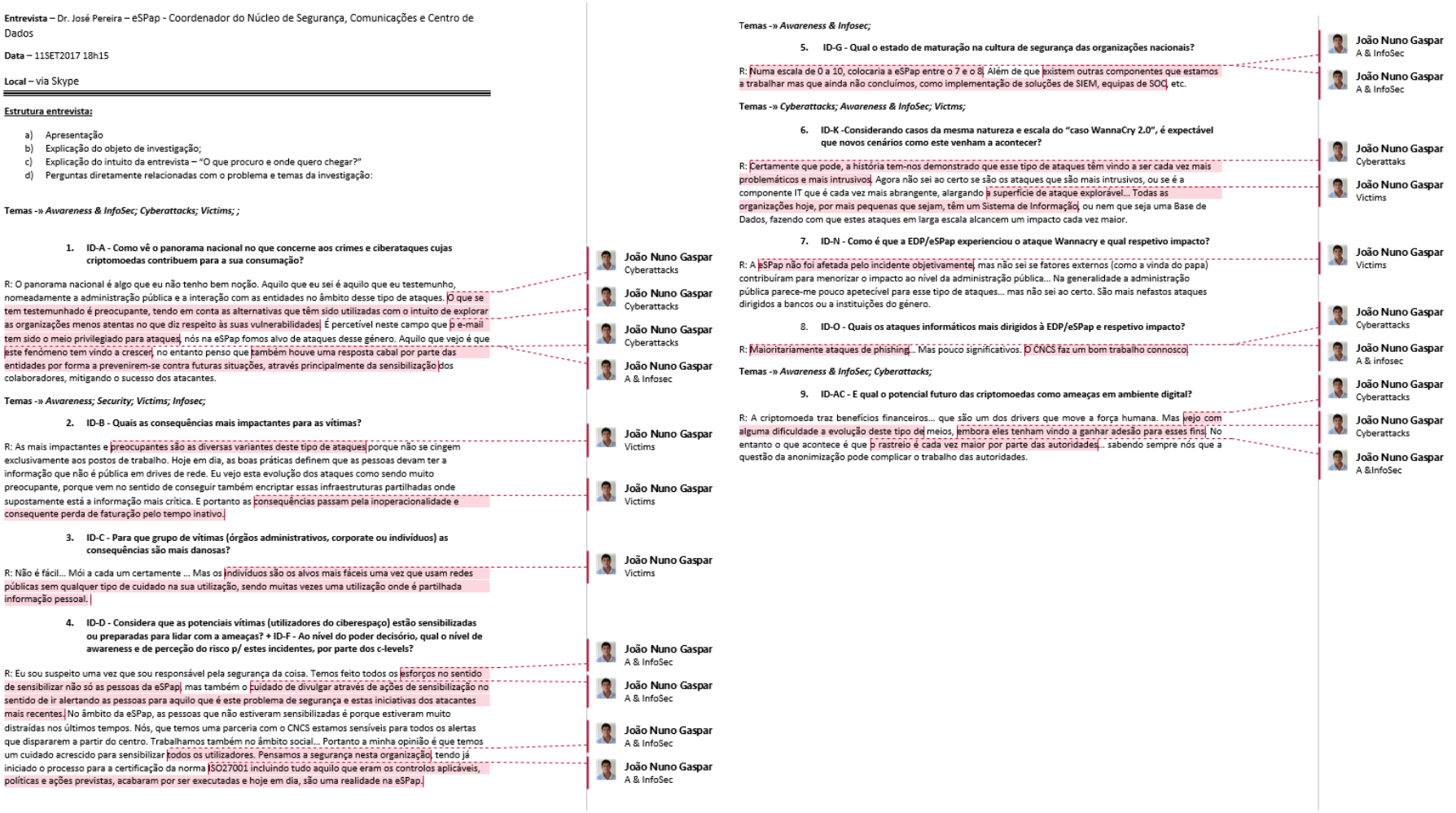
12. **ID-M - No dia do ataque *WannaCry 2.0* foram-lhe feitas muitas solicitações para compra de BTC's?**

R: Não notei e consigo dizer-te isso porque sei que o resgate era de cerca de 300€ e não recebi quase nada nesse valor, cheguei a ter um ou outro estrangeiro que até pode estar relacionado com isso, mas não notei nada de anormal. No entanto em ataques de ramsonware anteriores cheguei a ter vários contactos, inclusivamente sou testemunha de um processo no qual uma pessoa foi vítima de ramsonware e me comprou as moedas para pagar o resgate...

Temas -» *Awareness & InfoSec; Cyberattacks;*

João Nuno Gaspar — BTC Technical questions
João Nuno Gaspar — Cyberattacks
João Nuno Gaspar — Cyberattacks
João Nuno Gaspar — BTC TQ
João Nuno Gaspar — BTC TQ
João Nuno Gaspar — BTC TQ
João Nuno Gaspar — BTC TQ
João Nuno Gaspar — BTC TQ;
João Nuno Gaspar — BTC TQ;
João Nuno Gaspar — BTC TQ;
João Nuno Gaspar — BTC TQ;
João Nuno Gaspar — BTC TQ;
João Nuno Gaspar — BTC TQ;
João Nuno Gaspar — CyberAttacks;
João Nuno Gaspar — CyberAttacks;
João Nuno Gaspar — BTC TQ;
João Nuno Gaspar — BTC TQ;
João Nuno Gaspar — Cyberattacks
João Nuno Gaspar — Cyberattacks
João Nuno Gaspar — Cyberattacks

Apêndice 7 - Guião de entrevista e respetivas respostas – Riclas



Entrevista – Dr. José Pereira – eSPap - Coordenador do Núcleo de Segurança, Comunicações e Centro de Dados

Data – 11SET2017 18h15

Local – via Skype

Estrutura entrevista:

a) Apresentação
b) Explicação do objeto de investigação;
c) Explicação do intuito da entrevista – "O que procuro e onde quero chegar?"
d) Perguntas diretamente relacionadas com o problema e temas da investigação:

Temas -» *Awareness & InfoSec; Cyberattacks; Victims; ;*

1. **ID-A - Como vê o panorama nacional no que concerne aos crimes e ciberataques cujas criptomoedas contribuem para a sua consumação?**

R: O panorama nacional é algo que eu não tenho bem noção. Aquilo que eu sei é aquilo que eu testemunho, nomeadamente a administração pública e a interação com as entidades no âmbito desse tipo de ataques. O que se tem testemunhado é preocupante, tendo em conta as alternativas que têm sido utilizadas com o intuito de explorar as organizações menos atentas no que diz respeito às suas vulnerabilidades. É percetível neste campo que o e-mail tem sido o meio privilegiado para ataques, nós na eSPap fomos alvo de ataques desse género. Aquilo que vejo é que este fenómeno tem vindo a crescer, no entanto penso que também houve uma resposta cabal por parte das entidades por forma a prevenirem-se contra futuras situações, através principalmente da sensibilização dos colaboradores, mitigando o sucesso dos atacantes.

Temas -» *Awareness; Security; Victims; Infosec;*

2. **ID-B - Quais as consequências mais impactantes para as vítimas?**

R: As mais impactantes e preocupantes são as diversas variantes deste tipo de ataques porque não se cingem exclusivamente aos postos de trabalho. Hoje em dia, as boas práticas definem que as pessoas devam ter a informação que não é pública em drives de rede. Eu vejo esta evolução dos ataques como sendo muito preocupante, porque vem no sentido de conseguir também encriptar essas infraestruturas partilhadas onde supostamente está a informação mais crítica. E portanto as consequências passam pela inoperacionalidade e consequente perda de faturação pelo tempo inativo.

3. **ID-C - Para que grupo de vítimas (órgãos administrativos, corporate ou indivíduos) as consequências são mais danosas?**

R: Não é fácil... Mói a cada um certamente ... Mas os indivíduos são os alvos mais fáceis uma vez que usam redes públicas sem qualquer tipo de cuidado na sua utilização, sendo muitas vezes uma utilização onde é partilhada informação pessoal.

4. **ID-D - Considera que as potenciais vítimas (utilizadores do ciberespaço) estão sensibilizadas ou preparadas para lidar com a ameaças? + ID-F - Ao nível do poder decisório, qual o nível de awareness e de perceção do risco p/ estes incidentes, por parte dos c-levels?**

R: Eu sou suspeito uma vez que sou responsável pela segurança da coisa. Temos feito todos os esforços no sentido de sensibilizar não só as pessoas da eSPap, mas também o cuidado de divulgar através de ações de sensibilização no sentido de ir alertando as pessoas para aquilo que é este problema de segurança e estas iniciativas dos atacantes mais recentes. No âmbito da eSPap, as pessoas que não estiveram sensibilizadas é porque estiveram muito distraídas nos últimos tempos. Nós, que temos uma parceria com o CNCS estamos sensíveis para todos os alertas que dispararem a partir do centro. Trabalhamos também no âmbito social... Portanto a minha opinião é que temos um cuidado acrescido para sensibilizar todos os utilizadores. Pensamos a segurança nesta organização, tendo já iniciado o processo para a certificação da norma ISO27001 incluindo tudo aquilo que eram os controlos aplicáveis, políticas e ações previstas, acabaram por ser executadas e hoje em dia, são uma realidade na eSPap.

João Nuno Gaspar – Cyberattacks
João Nuno Gaspar – Cyberattacks
João Nuno Gaspar – Cyberattacks
João Nuno Gaspar – A & Infosec
João Nuno Gaspar – Victims
João Nuno Gaspar – Victims
João Nuno Gaspar – Victims
João Nuno Gaspar – A & InfoSec
João Nuno Gaspar – A & InfoSec
João Nuno Gaspar – A & InfoSec
João Nuno Gaspar – A & InfoSec

Temas -» *Awareness & Infosec;*

5. **ID-G - Qual o estado de maturação na cultura de segurança das organizações nacionais?**

R: Numa escala de 0 a 10, colocaria a eSPap entre o 7 e o 8. Além de que existem outras componentes que estamos a trabalhar mas que ainda não concluímos, como implementação de soluções de SIEM, equipas de SOC, etc.

Temas -» *Cyberattacks; Awareness & InfoSec; Victms;*

6. **ID-K -Considerando casos da mesma natureza e escala do "caso WannaCry 2.0", é expectável que novos cenários como este venham a acontecer?**

R: Certamente que pode, a história tem-nos demonstrado que esse tipo de ataques têm vindo a ser cada vez mais problemáticos e mais intrusivos. Agora não sei ao certo se são os ataques que são mais intrusivos, ou se é a componente IT que é cada vez mais abrangente, alargando a superfície de ataque explorável... Todas as organizações hoje, por mais pequenas que sejam, têm um Sistema de Informação, ou nem que seja uma Base de Dados, fazendo com que estes ataques em larga escala alcancem um impacto cada vez maior.

7. **ID-N - Como é que a EDP/eSPap experienciou o ataque Wannacry e qual respetivo impacto?**

R: A eSPap não foi afetada pelo incidente objetivamente, mas não sei se fatores externos (como a vinda do papa) contribuíram para menorizar o impacto ao nível da administração pública... Na generalidade a administração pública parece-me pouco apetecível para esse tipo de ataques... mas não sei ao certo. São mais nefastos ataques dirigidos a bancos ou a instituições do género.

8. **ID-O - Quais os ataques informáticos mais dirigidos à EDP/eSPap e respetivo impacto?**

R: Maioritariamente ataques de phishing... Mas pouco significativos. O CNCS faz um bom trabalho connosco.

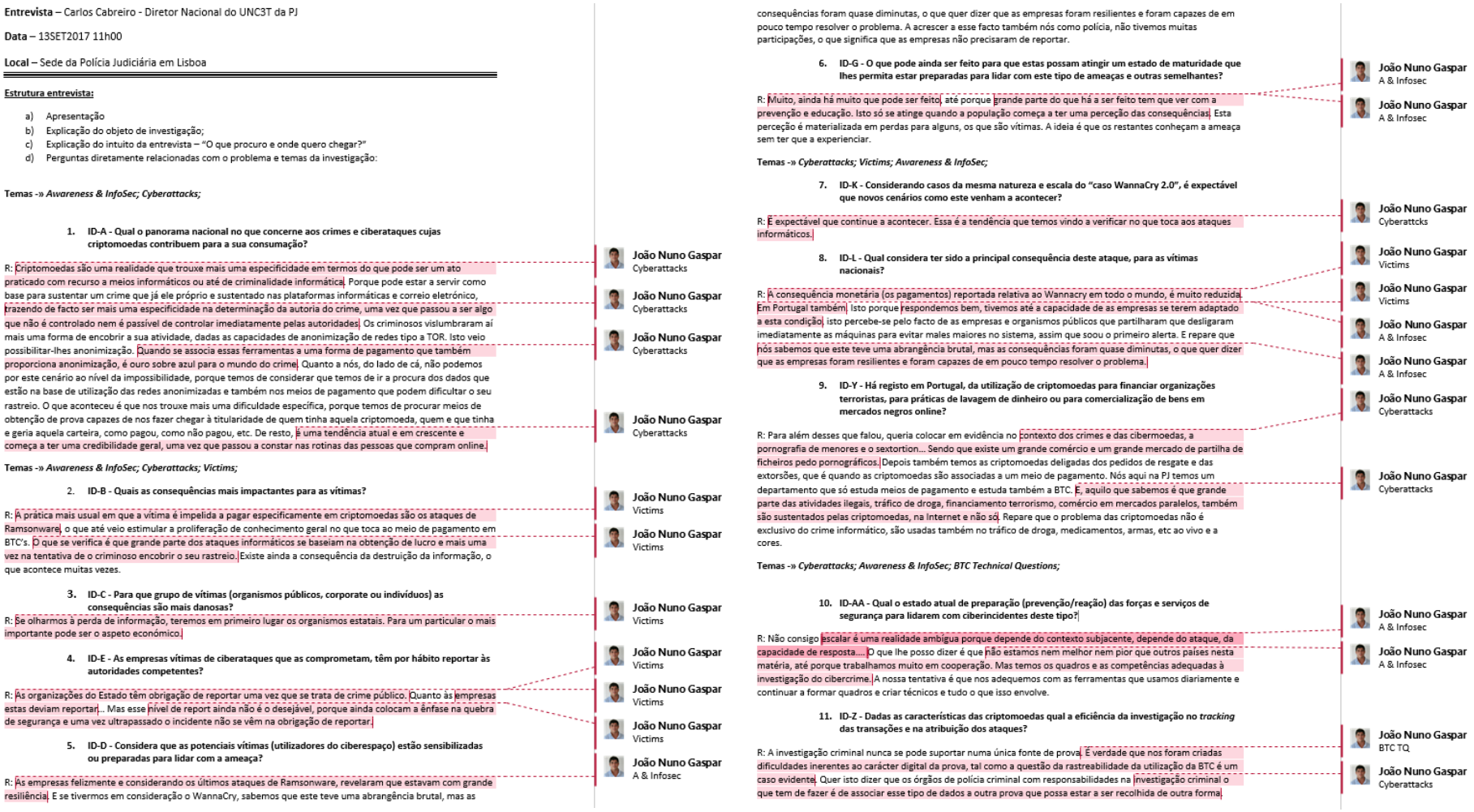
Temas -» *Awareness & InfoSec; Cyberattacks;*

9. **ID-AC - E qual o potencial futuro das criptomoedas como ameaças em ambiente digital?**

R: A criptomoeda traz benefícios financeiros... que são um dos drivers que move a força humana. Mas vejo com alguma dificuldade a evolução deste tipo de meios, embora eles tenham vindo a ganhar adesão para esses fins. No entanto o que acontece é que o rastreio é cada vez maior por parte das autoridades... sabendo sempre nós que a questão da anonimização pode complicar o trabalho das autoridades.

João Nuno Gaspar – A & InfoSec
João Nuno Gaspar – A & InfoSec
João Nuno Gaspar – Cyberattaks
João Nuno Gaspar – Victims
João Nuno Gaspar – Victims
João Nuno Gaspar – Cyberattacks
João Nuno Gaspar – A & infosec
João Nuno Gaspar – Cyberattacks
João Nuno Gaspar – Cyberattacks
João Nuno Gaspar – A &InfoSec

Apêndice 8 - Guião de entrevistas e respetivas respostas – José Pereira



Entrevista – Carlos Cabreiro - Diretor Nacional do UNC3T da PJ

Data – 13SET2017 11h00

Local – Sede da Polícia Judiciária em Lisboa

Estrutura entrevista:

a) Apresentação
b) Explicação do objeto de investigação;
c) Explicação do intuito da entrevista – "O que procuro e onde quero chegar?"
d) Perguntas diretamente relacionadas com o problema e temas da investigação:

Temas -» *Awareness & InfoSec; Cyberattacks;*

1. **ID-A - Qual o panorama nacional no que concerne aos crimes e ciberataques cujas criptomoedas contribuem para a sua consumação?**

R: Criptomoedas são uma realidade que trouxe mais uma especificidade em termos do que pode ser um ato praticado com recurso a meios informáticos ou até de criminalidade informática. Porque pode estar a servir como base para sustentar um crime que já ele próprio e sustentado nas plataformas informáticas e correio eletrónico, trazendo de facto ser mais uma especificidade na determinação da autoria do crime, uma vez que passou a ser algo que não é controlado nem é passível de controlar imediatamente pelas autoridades. Os criminosos vislumbraram aí mais uma forma de encobrir a sua atividade, dadas as capacidades de anonimização de redes tipo a TOR. Isto veio possibilitar-lhes anonimização. Quando se associa essas ferramentas a uma forma de pagamento que também proporciona anonimização, é ouro sobre azul para o mundo do crime. Quanto a nós, do lado de cá, não podemos por este cenário ao nível da impossibilidade, porque temos de considerar que temos de ir a procura dos dados que estão na base de utilização das redes anonimizadas e também nos meios de pagamento que podem dificultar o seu rastreio. O que aconteceu é que nos trouxe mais uma dificuldade específica, porque temos de procurar meios de obtenção de prova capazes de nos fazer chegar à titularidade de quem tinha aquela criptomoeda, quem e que tinha e geria aquela carteira, como pagou, como não pagou, etc. De resto, é uma tendência atual e em crescente e começa a ter uma credibilidade geral, uma vez que passou a constar nas rotinas das pessoas que compram online.

Temas -» *Awareness & InfoSec; Cyberattacks; Victims;*

2. **ID-B - Quais as consequências mais impactantes para as vítimas?**

R: A prática mais usual em que a vítima é impelida a pagar especificamente em criptomoedas são os ataques de Ramsonware, o que até veio estimular a proliferação de conhecimento geral no que toca ao meio de pagamento em BTC's. O que se verifica é que grande parte dos ataques informáticos se baseiam na obtenção de lucro e mais uma vez na tentativa de o criminoso encobrir o seu rastreio. Existe ainda a consequência da destruição da informação, o que acontece muitas vezes.

3. **ID-C - Para que grupo de vítimas (organismos públicos, corporate ou indivíduos) as consequências são mais danosas?**

R: Se olharmos à perda de informação, teremos em primeiro lugar os organismos estatais. Para um particular o mais importante pode ser o aspeto económico.

4. **ID-E - As empresas vítimas de ciberataques que as comprometam, têm por hábito reportar às autoridades competentes?**

R: As organizações do Estado têm obrigação de reportar uma vez que se trata de crime público. Quanto às empresas estas deviam reportar... Mas esse nível de report ainda não é o desejável, porque ainda colocam a ênfase na quebra de segurança e uma vez ultrapassado o incidente não se vêm na obrigação de reportar.

5. **ID-D - Considera que as potenciais vítimas (utilizadores do ciberespaço) estão sensibilizadas ou preparadas para lidar com a ameaça?**

R: As empresas felizmente e considerando os últimos ataques de Ramsonware, revelaram que estavam com grande resiliência. E se tivermos em consideração o WannaCry, sabemos que este teve uma abrangência brutal, mas as consequências foram quase diminutas, o que quer dizer que as empresas foram resilientes e foram capazes de em pouco tempo resolver o problema. A acrescer a esse facto também nós como polícia, não tivemos muitas participações, o que significa que as empresas não precisaram de reportar.

6. **ID-G - O que pode ainda ser feito para que estas possam atingir um estado de maturidade que lhes permita estar preparadas para lidar com este tipo de ameaças e outras semelhantes?**

R: Muito, ainda há muito que pode ser feito, até porque grande parte do que há a ser feito tem que ver com a prevenção e educação. Isto só se atinge quando a população começa a ter uma perceção das consequências. Esta perceção é materializada em perdas para alguns, os que são vítimas. A ideia é que os restantes conheçam a ameaça sem ter que a experienciar.

Temas -» *Cyberattacks; Victims; Awareness & InfoSec;*

7. **ID-K - Considerando casos da mesma natureza e escala do "caso WannaCry 2.0", é expectável que novos cenários como este venham a acontecer?**

R: É expectável que continue a acontecer. Essa é a tendência que temos vindo a verificar no que toca aos ataques informáticos.

8. **ID-L - Qual considera ter sido a principal consequência deste ataque, para as vítimas nacionais?**

R: A consequência monetária (os pagamentos) reportada relativa ao Wannacry em todo o mundo, é muito reduzida. Em Portugal também. Isto porque respondemos bem, tivemos até a capacidade de as empresas se terem adaptado a esta condição, isto percebe-se pelo facto de as empresas e organismos públicos que partilharam que desligaram imediatamente as máquinas para evitar males maiores no sistema, assim que soou o primeiro alerta. E repare que nós sabemos que este teve uma abrangência brutal, mas as consequências foram quase diminutas, o que quer dizer que as empresas foram resilientes e foram capazes de em pouco tempo resolver o problema.

9. **ID-Y - Há registo em Portugal, da utilização de criptomoedas para financiar organizações terroristas, para práticas de lavagem de dinheiro ou para comercialização de bens em mercados negros online?**

R: Para além desses que falou, queria colocar em evidência no contexto dos crimes e das cibermoedas, a pornografia de menores e o sextortion... Sendo que existe um grande comércio e um grande mercado de partilha de ficheiros pedo pornográficos. Depois também temos as criptomoedas deligadas dos pedidos de resgate e das extorsões, que é quando as criptomoedas são associadas a um meio de pagamento. Nós aqui na PJ temos um departamento que só estuda meios de pagamento e estuda também a BTC. E, aquilo que sabemos é que grande parte das atividades ilegais, tráfico de droga, financiamento terrorismo, comércio em mercados paralelos, também são sustentados pelas criptomoedas, na Internet e não só. Repare que o problema das criptomoedas não é exclusivo do crime informático, são usadas também no tráfico de droga, medicamentos, armas, etc ao vivo e a cores.

Temas -» *Cyberattacks; Awareness & InfoSec; BTC Technical Questions;*

10. **ID-AA - Qual o estado atual de preparação (prevenção/reação) das forças e serviços de segurança para lidarem com ciberincidentes deste tipo?**

R: Não consigo escalar é uma realidade ambígua porque depende do contexto subjacente, depende do ataque, da capacidade de resposta.... O que lhe posso dizer é que não estamos nem melhor nem pior que outros países nesta matéria, até porque trabalhamos muito em cooperação. Mas temos os quadros e as competências adequadas à investigação do cibercrime. A nossa tentativa é que nos adequemos com as ferramentas que usamos diariamente e continuar a formar quadros e criar técnicos e tudo o que isso envolve.

11. **ID-Z - Dadas as características das criptomoedas qual a eficiência da investigação no *tracking* das transações e na atribuição dos ataques?**

R: A investigação criminal nunca se pode suportar numa única fonte de prova. É verdade que nos foram criadas dificuldades inerentes ao carácter digital da prova, tal como a questão da rastreabilidade da utilização da BTC é um caso evidente. Quer isto dizer que os órgãos de polícia criminal com responsabilidades na investigação criminal o que tem de fazer é de associar esse tipo de dados a outra prova que possa estar a ser recolhida de outra forma.

João Nuno Gaspar Cyberattacks
João Nuno Gaspar Cyberattacks
João Nuno Gaspar Cyberattacks
João Nuno Gaspar Cyberattacks
João Nuno Gaspar Victims
João Nuno Gaspar Victims
João Nuno Gaspar Victims
João Nuno Gaspar Victims
João Nuno Gaspar Victims
João Nuno Gaspar Victims
João Nuno Gaspar A & Infosec
João Nuno Gaspar A & Infosec
João Nuno Gaspar A & Infosec
João Nuno Gaspar Cyberattcks
João Nuno Gaspar Victims
João Nuno Gaspar Victims
João Nuno Gaspar A & Infosec
João Nuno Gaspar A & Infosec
João Nuno Gaspar Cyberattacks
João Nuno Gaspar Cyberattacks
João Nuno Gaspar A & Infosec
João Nuno Gaspar A & Infosec
João Nuno Gaspar BTC TQ
João Nuno Gaspar Cyberattacks

Apêndice 9 - Guião de entrevista e respetivas respostas – Inspetor Cabreiro