INSTITUTO SUPERIOR DE CIÊNCIAS POLICIAIS E SEGURANÇA INTERNA

“Cibercriminalidade e Cibersegurança”

Trabalho de Investigação Final

3.º Curso de Comando e Direção Policial

Autor: Fernando Moreira (Comissário)

Bamako, 28 de junho de 2019

Resumo

A cibersegurança e a cibercriminalidade são uma realidade em todos os espaços soberanos, transpondo fronteiras fácil e rapidamente. A UE e Portugal estão alinhadas numa estratégia de cibersegurança que procura fazer face a novos desafios nos quais organizações criminosas procuram lucros na área do crime tradicional associado às novas tecnologias. As forças e serviços de segurança a nível mundial encontram novos desafios na área do digital. Novas técnicas de investigação e colheita de prova, bem como legislações têm que ser desenvolvidas para tornar eficiente este novo combate ao crime. Palavras como *malware, ransomware, darknet* ou *internet* profunda, *internet* de superficie, IoT, TOR, I2P, criptomoedas, criptografia são alguns termos que compõem a temática tecnológica. Na dimensão jurídica, criminal palavras como transnacionalidade, cibercrime, extorsão criptoviral, crime organizado, ciberataques, ciberdiplomacia e conceitos como actuação poli-criminal e crime enquanto serviço disponível, serão apenas alguns dos vocábulos que se irão aflorar no presente trabalho.

Palavras chave: Darnek, IoT, PSP, Ransomware, TOR

Abstract

Cyber criminality and cyber security are a reality in all sovereign countries, crossing borders easily and quickly. The EU and Portugal are aligned in a cyber security strategy that seeks to address new challenges in which criminal organisations seek profits in the area of traditional crime associated with new technologies. Security forces and services world wide face new challenges in the area of digital. New investigative and evidence-gathering techniques and legislation must be developed to make this new fight against crime effective. Words such as malware, ransomware, Darknet, Deep Internet, Surface internet, IoT, TOR, I2P, Encryption are some terms that make up the technological theme. In the legal, criminal dimension, words like transnational, cyber-crime, crypto-extortion, organized crime, cyber-attacks, cybercrime and concepts like poly-crime and crime as menu available service, are just some of the words that will emerge in the present work.

Key words: Darnek, IoT, PSP, Ransomware, TOR

1. Introdução

Entender o presente é melhor preparar o futuro, com recurso ao método exploratório é procurado estudar e caracterizar a cibersegurança e cibercriminalidade, quais os seus agentes e qual o seu espaço e dimensão, bem como responder à questão: Qual o papel que um orgão de polícia criminal(OPC) como a Polícia de Segurança Pública(PSP) pode ter neste novo mundo digital? O presente artigo procura explorar publicações, relatórios, legislações nacionais e internacionais com implicações diretas sobre a temática em estudo. Numa abordagem de aproximação à realidade nacional, vai-se analisar o ciberespaço na sua dimensão, as "*internets*"e os seus diferentes níveis de acesso. Será dada uma visão do cibercrime e cibersegurança na América, as relações entre a criminalidade e cibercriminalidade na Europa e repercussões da forma e estrutura do crime organizado nesta, bem como o conceito de crime como serviço menu. Finalmente no plano nacional a estratégia de cibersegurança, estrutura, enquadramento e definições será revelada, culminando nos resultados operacionais estatísticos atuais.

"O princípio da responsabilidade, em geral, constitui o ponto de partida da ética" (Catarino, 2015, 23).

2. O espaço digital e a cibercriminalidade

2.1. Qual o tamanho da *internet*?

Desde o surgimento da *internet*, que a mesma não tem parado de crescer, quer em inovações, tamanho, complexidade, utilizadores e interações. Mas como se quantifica a *internet*?

Não existem respostas conclusivas, nem apenas uma forma de quantificação da *internet*, no entanto o sitio https://www.worldwidewebsize.com/ procura responder a essa questão considerando estimativas por defeito, do número de registos de páginas de todos os motores de busca ou gestores de domínios, sendo que em 15 de junho de 2019 estavam registadas pelo menos 5.78 biliões de páginas(*The size of the world wide web*, 2019).

Em 2014, estimava-se que iriam existir 1,7 aparelhos por pessoa ligados à *internet*, para 2020, a expectativa é de uma média de 4,3 aparelhos por pessoa (Strategy Analytics, 2014) e um aumento da capacidade de armazenamento do espaço cibernético de 33 ZB em 2018 - (um zettabyte (ZB) é o equivalente a um trilião de gigabytes), sendo ainda estimado um aumento para 175 ZB em 2025, que se fossem materializados em DVD´s empilhados, chegariam à lua 23 vezes ou contornariam a circunferência da terra 222 vezes(Reinsel, Gantz, Rydning, 2018). Tendo por base estudos publicados pela *Data Age 2025 White Paper by seagate Cheat Sheet* são enfatizadas as seguintes previsões para 2025: No ciberespaço 20% de todos os dados disponíveis terão o potencial de serem críticos; A média por pessoa de interações com a *internet* através de qualquer tipo de aparelho digital, será de 4800 por dia, 1 interação a cada 18 segundos; Mais de 25% da informação gerada no ciberespaço será em tempo real e a informação produzida por sistemas IoT (*internet ofthings* - sistemas digitais de utilidade pessoal ligados à *internet* através de *smartphones*, sensores, computadores) serão superiores a 95% desta produção; Apenas 20% da informação criada no ciberespaço terá utilidade para analistas, no entanto, apenas 15% desta informação será catalogada e analisada; 90% de todos os dados gerados no ciberespaço exigirão algum tipo de segurança, mas apenas cerca de 50% destes serão protegidos; De toda a produção informacional, 20%

terá o potencial de ser critica para as nossas vidas; A expectativa da taxa de crescimento de armazenamento de dados (CAGR - *compound aggregate growth rate*), entre 2015 e 2025, irá aumentar 30%, a potencialidade de aumento de dados críticos aumentará 37%, dados críticos aumentarão 39%, e o aumento de dados hipercríticos será de 54%. A média diária *percapita* de interações com o ciberespaço irá aumentar 20 vezes nos próximos 10 anos. Até 2025 as conexões à *internet* serão de 75% da população mundial, e a produção de informação em tempo real aumentará 150%, e apenas 20% de toda a informação produzida será útil se for catalogada, no entanto apenas 15% será efectivamente catalogada e analisada. Em 2015 menos de 30% do total de informação produzida no espaço cibernético foi realizado por empresas e em 2025 esse valor ascenderá a 60%. O esforço de gestão da informação no espaço cibernético recairá nas empresas privadas num valor superior a 97% e a percentagem de informação que requererá segurança atingirá quase 90% em 2025 (Khanduja, 2017).

2.2. As "*internets"* por detrás da cibercriminalidade

A cibercriminalidade atua em todos os diferentes níveis de *internet* existentes, sendo estas a *internet* de superfície, a *internet* profunda e a "*darkweb*". A denominada *internet* de superfície é onde a maioria dos utilizadores comuns navega, através de motores de busca comerciais "normais", entre outros e como por exemplo o Google e o Yahoo onde se pode encontrar todo o tipo de plataformas e serviços públicos e privados. É estimado que a maioria dos utilizadores, que fazem recurso a serviços "normais" na *internet* de superfície, representem apenas 1% do que é na realidade a *internet* no seu todo(Altvater, 2016).

Uma porção muito maior de espaço cibernético é composto pela *internet* profunda que inclui redes privadas de organizações, onde estão sediadas grandes bases de dados operadas por organizações privadas e públicas, estimando alguns especialistas que esta seja 400 a 500 vezes maior que a *internet* de superfície. A "*darkweb*", é um nível do ciberespaço que apenas está acessível através de softwares especiais que ocultam a identidade dos utilizadores, neste caso o número de identificação do aparelho electrónico (IP - *internet protocol*) e tem uma dimensão muito inferior à *internet* profunda (Thompson, 2015).

"A "*darkweb*" tem ligação com a *internet* de superfície, mas esta com recurso ao "*The Onion router*" - TOR, cria diversas camadas de encriptação, camuflando e

ocultando de forma eficaz identidades e registos de navegação, dificultando ou impossibilitando de forma séria as acções das forças e serviços de segurança" (Penn, 2018, 24).

2.3. A prova digital e a *internet* IoT

O artigo "*The new crime environment presents a new investigatory challenges por police*", transmite a ideia que a manipulação da prova digital e o domínio de conhecimento na área da encriptação é algo que deve ser considerado um desafio e uma realidade na investigação criminal atual, uma vez que "...toda a forma criminal atual tem relacionada uma componente digital. A perícia a *smartphones* do suspeito, ou da vítima do crime pode fornecer mensagens de texto, emails, fotografias, vídeos, publicações nas redes sociais, nomes de pessoas recentemente contactadas, pesquisas realizadas na *internet* realizadas pelo suspeito ou vítima, bem como pesquisas de endereços e localizações na aplicação do Google *maps*..." (Perez, 2018, 33), o mesmo descreve a prova digital sendo como o ADN e as impressões digitais, nos cenários de crime, uma vez que estas permanecem nestes de forma latente ou "escondidas", podendo atravessar fronteiras jurisdicionais rápida e facilmente, podendo ser alteradas, comprometidas ou destruídas com pouco esforço, sendo sensíveis ao tempo de recolha. A informação recolhida destas provas tem um alcance mais vasto e é mais difícil de obter, do que as provas tradicionais, representando desta forma um desafio maior.

Novas formas de recolha de prova, têm que ser criadas e desenvolvidas, como por exemplo nos sistemas de *bluetooh* incluídos nas viaturas que permitem a recolha dos registos de chamadas de telefones que com eles foram emparelhados, mesmo que os telefones estejam bloqueados ou inacessíveis, os rasto *Wi-Fi*, permitem recriar percursos (físicos e temporais) de aparelhos pessoais ou de viaturas que automaticamente se tentam ligar a redes *Wi-Fi* livres (não carecem de palavra passe). Os recursos caninos podem ser treinados para detetar dispositivos electrónicos, pois estes têm na sua concepção produtos químicos específicos (Policeforum, 2018).

A Cibercriminalidade nos Estados

3.1. América

Em 2015, o relatório anual do *Federal Bureau of Investigation*(FBI) do seu centro de queixas de crimes informáticos (www.ic3.gov), estimava que "...apenas 15%

das vitimas de crimes no ciberespaço comunicavam os factos às autoridades..." (FBI, 2015, 5). No relatório de 2018, este centro registou 351937 denúncias, e anunciou que entre 2014 até 2018, foi apresentada uma média anual de crescimento de denúncias de 5,46%, num total 1509679 queixas nestes 5 anos. Do ponto de vista dos prejuízos das vítimas, os registos em dólares de 2014 a 2018 ascenderam a $7,45 biliões de prejuízos com um crescimento médio anual de 25,59%. Deve ser tido em conta que o FBI em Fevereiro de 2018, especializou equipas para a recuperação de valores no seio do centro de queixas de crime informáticos (*Internet Crime Complaint Center*), denominadas RAT (*Recovery Asset Teams*). Estas equipas, apenas entre 02 de fevereiro de 2018 e 31 de dezembro de 2018 lidaram com 1061 queixas, conseguindo uma taxa de recuperação de valores na ordem dos 75%, devolvendo às vítimas $192,699,195.72 dos $257,096,991.65 que foram indevidamente afastados das suas esferas jurídicas, sendo que contudo na globalidade do cibercrime em 2018 os prejuízos foram de $2,706.4M. O centro de queixas electrónicas enunciado categoriza os incidentes criminais informáticos registados na sua plataforma, considerando vitimas, métodos e recursos tecnológicos envolvidos ou estratégias de investigação, da seguinte forma:

- Falta de pagamento / Falha na entrega - de bens ou serviços;

- Extorsão - obtenção de dinheiro ou bens pela intimidação ou ameaça de mal maior, abuso de autoridade;

- Furto de dados pessoais - obtenção de dados pessoais (sensíveis, confidenciais) de lugar protegido ou assegurado para sítio ou lugar não autorizado ou não assegurado, de forma a serem visualizados ou acedidos por pessoal não autorizado;

- Queixas incompletas (queixas feitas de forma incompleta não permitindo identificar qual o incidente criminal ocorrido);

- *Phishing/Vishing/Smishing/Pharming* - correio electrónico, mensagens de texto e chamadas telefónicas não solicitadas, realizadas por uma empresa legitima solicitando dados pessoais, financeiros e/ou *password´*s de acesso;

- BEC/EAC (*Business Email Compromise/Email Account Compromise*) - Esquema que visa empresas e privados que regularmente fazem pagamentos/transferências electrónicas de valores a fornecedores estrangeiros;

- Abuso de confiança - o criminoso ilude a vítima através de um esquema romântico, confiança ou amizade a transferir-lhe dinheiro, dados pessoais ou *password´*s;

- Assédio/ameaça de violência - O assédio ocorre quando o criminoso cria falsas acusações/factos relativamente à vitima de forma a intimidar. A ameaça é a intenção através de uma expressão, de infringir dor, ferimentos ou punição, se não for paga uma quantia;

- Taxas adiantadas - esquema em que à vítima é comunicado que foi selecionada para um empréstimo ou ganhou um grande prémio financeiro, mas que para o processo se concretizar terá que ser transferida uma quantia adiantada para pagamento de taxas administrativas;

- Furto de identidade - tomada de contas e cometimento de fraudes usando os dados pessoais de outrem;

- *Spoofing* - Número de telefone, email ou sitio ilícito simulando parecer legítimo, pretendendo fazer chamadas *robot* massivas ou envio massivo de email´s *spam*, recolher dados pessoais. Normalmente está relacionado com outros tipos de cibercriminalidade;

- Pagamento excessivo - à vítima é remetida um pagamento/comissão sendo instruída a ficar com uma parte e remeter o remanescente para outro sujeito ou empresa;

- Fraude de cartão de crédito - Termo lato envolvendo um cartão de crédito ou outros mecanismos similares de pagamento, tendo por base valores fraudulentos de pagamento;

- Emprego/contratação - um individuo crê estar a concorrer ou a trabalhar numa firma legitima e no percurso perde dinheiro ou vê-se envolvida em branqueamento de capitais ou mercadorias;

- Assistência técnica - Tentativa de obter remotamente acesso a equipamento electrónico, alegando ser de uma empresa técnica legitima, com a desculpa de limpar vírus ou *malwares*;

- Burla de venda, *timeshare* ou aluguer de imóveis;

- Falso funcionário público - uso da figura pública para tentativa de cobrança de verbas;

- Outros;

- Lotarias/sorteios/heranças - um individuo é contactado para receber um prémio de um sorteio ou lotaria que nunca participou, ou para receber uma herança de um familiar desconhecido, sendo-lhe solicitado o pagamento de uma taxa ou valor para poder receber os valores aludidos;

- Engano - Os serviços ou produtos apresentados online, e que foram fornecidos são manifestamente em número e qualidade inferior;

- Investimentos - Práticas de engano, que levam investidores a realizar trocas financeiras tendo por base falsas informações, prometendo grandes retornos em troca de pequenos investimentos;

- *Malware/scareware*/virus - programas informáticos que infectam e danificam computadores e sistemas informáticos. Por vezes são utilizadas táticas de intimidação/amedrontamento para exigir dinheiro;

- Furto de dados a empresas - furto de dados confidenciais, sensíveis de local seguro e protegido, para serem usados de forma indevida e por pessoal não autorizado;

- Direitos de autor e contrafacção - O furto e uso ilegal de ideias de outrem, invenções, expressões originais, incluindo segredos comerciais e produtos do tipo filmes, músicas e softwares;

- Negação de serviço - ataque informático a sitio ou sistema informático, atrasando ou impossibilitando o acesso aos seus serviços pelos seus usuários/clientes;

- *Ransomware* - Software malicioso que bloqueia o sistema informático, exigindo um pagamento pela reposição dos acessos;

- Crimes contra crianças - toda a forma de exploração/vitimização ou abuso que envolva crianças;

- Reenvios - sujeitos recebem encomendas/produtos ilegais ou comercializados de forma fraudulenta e subsequentemente reencaminham a mercadoria normalmente para o estrangeiro;

- Processos cíveis - questões não criminais que devem ser encaminhadas para tribunais cíveis;

- Caridade - Uso de falsas caridades, normalmente após desastres naturais, para angariar donativos legítimos;

- Assistência social e cuidados médicos - Esquemas para defraudar o estado social e sector privado de saúde, através de documentos falsos, informação individual furtada, para obtenção de medicamentos, serviços e vantagens financeiras. Esquema habitualmente iniciado por *email´s spam*, publicidade na *internet* e ligações a redes sociais, sítios ou fóruns fraudulentos;

- Jogo - Jogos *online*;

- Terrorismo;

- *Hacktivismo* - computador de um pirata informático cuja actividade visa a promoção uma causa politica ou social; (FBI, 2018).

3.2. União Europeia

A cibercriminalidade é uma ameaça real e um desafio essencial às novas formas de economia digital, assentes em códigos e palavras passe que fluem no espaço cibernético, vulneráveis a programas criminosos, que as capturam e utilizam fraudulentamente. O comércio de droga continua a ser o maior setor criminal a operar na União Europeia(UE), comparável a este está o emergente tráfico de migrantes. Estas organizações criminais têm demonstrado grande capacidade de movimento entre fronteiras UE, sendo que a tecnologia está presente nesta estratégia criminal organizada. Os recursos tecnológicos envolvidos nestas estratégias criminais vão muito além da *internet*, pois incluem todo o tipo de inovações, tais como *drones*, logística automatizada e tecnologias avançadas de impressão (Europol, 2017). Existindo também os crimes com ligação ao ciberespaço que "...são ações que apenas podem ocorrer com recurso a um computador, redes informáticas ou outras formas de tecnologias de comunicação. O cibercrime é um fenómeno global atingindo todos os estados membros

da UE e as suas fronteiras situam-se no espaço ilimitado da *internet*. O espaço de ataque continua a crescer na medida em que a sociedade se torna mais digital, comercial, com mais cidadãos, equipamentos e serviços públicos ligados à *internet*."(Europol, 2017, 28).

Quando se aborda o tema da cibercriminalidade terá necessariamente que se ter sempre em mente a necessidade do desenvolvimento de uma cultura de cibersegurança (UN, 2010), nesta perspectiva o relatório, SOCTA-2017 produzido na e para a comunidade de segurança europeia pela Europol, dirigido ao crime grave e altamente organizado, evidencia as conexões da criminalidade "tradicional" ao cibercrime. Os "velhos" crimes associados à produção, distribuição e tráfico de drogas, refinaram técnicas e aperfeiçoaram mecanismos logísticos, de propaganda e distribuição ao cliente. Encomendar, pagar, receber um produto ou serviço criminoso atualmente envolve apenas um conjunto de cliques, sequências de algoritmos, apenas deixando um rasto cibernético indelével, abstracto e indecifrável...

3.2.1.Caracterização do universo criminal europeu e ciber relações

As tendências criminais europeias estão a incluir além do tráfico de droga associado ao recrudescimento da cocaína e heroína (neste caso ainda que em valores relativamente baixos) (EMCDDA, 2018), migração ilegal e o crime organizado contra a propriedade. A Europol recomenda especial atenção em três áreas de interesse transversal para a atividade criminal a considerar: fraude documental, lavagem de dinheiro e a comercialização de produtos e serviços ilegais *online*. Rob Wainwright, diretor da Europol, refere na sua nota introdutória do referido relatório, que em 2013 existiriam 3600 organizações internacionais de crime organizado a operar na Europa, sendo que em 2017 já se identificavam cerca de 5000, indicando a emergência de pequenos grupos, que se mostraram particularmente empreendedores, no recurso a novas tecnologias *online,* tais como canais de comunicação encriptados e perspectivando-se num futuro o recurso a *drones*. Nesse mesmo relatório é definido que as nacionalidades envolvidas nos crimes são mais de 180, sendo que 60% destes criminosos eram cidadãos da UE, e que 30% a 40% das redes têm estruturas a nível internacional, e aproximadamente 20% destas eram de curta duração e apenas para suporte de uma actividade criminal específica. A composição destas organizações é variável, sendo que 76% eram compostas por 6 ou mais membros e 24% até 5 membros. Mais de um terço

da atividade criminal organizada está envolvida na produção, tráfico e distribuição de droga, destas 7 em 10 estão activas em mais do que três países, e com uma actuação poli-criminal uma vez que 45% actuam em mais do que uma área criminal, numa lógica de mercado de forma a controlar os riscos, reduzir custos e aumentar margens de lucro.A actividade destas organizações está presente em 3 ou mais países em 70% dos casos e 10% destas estão presentes em mais de 7 países. O recurso a trocas financeiras em criptomoedas e métodos de pagamento anónimo, existentes em plataformas *online*, através de canais encriptados, dificultam ou impossibilitam a identificação dos intervenientes no processo.

O mercado da droga na UE gera lucros de 24 biliões de euros por ano, e das organizações criminosas activas no espaço comunitário, 35% destas estão envolvidas no tráfico de droga, 75% traficam mais do que um tipo de droga, bem como 65% estão envolvidas simultaneamente noutras actividades criminais. Apenas nos últimos 5 anos, foram identificadas na UE, 419 novas formas de drogas sintéticas, produzidas laboratorialmente(Europol,2017). O Observatório Europeu da Droga e da Toxicodependência (EMCDDA), afirma que no final de 2017 monitorizava mais de 670 novas substâncias psicoativas identificadas na Europa, não controladas internacionalmente, e que "em muitos casos estes produtos são produzidas a granel por empresas químicas e farmacêuticas da China. Daí, são expedidas para a Europa, onde são transformadas em produtos acabados, embaladas e vendidas." (EMCDDA, 2018, 32).O mesmo relatório estima que os traficantes/fornecedores de droga instalados na UE, seja responsáveis por cerca de 50% das vendas na *internet* "obscura" (*Darknet*) entre 2011 e 2015.

A comercialização e distribuição de todo o tipo de produtos ilícitos está em franco desenvolvimento não só na *Darknet*, mas também na *internet* de superfície. Nas plataformas digitais *online*, estão disponíveis todo o tipo de produtos à venda, pacotes de dados incluídos(Europol, 2017). Estas organizações apresentam a capacidade de operar por curtos períodos de tempo, ficarem letárgicas, podendo na nossa opinião indicar uma conexão à economia real e legitima, que as financia nesses períodos dormentes, o que nos leva à questão do crime organizado.

3.2.2. Crime Organizado

Porquê falar do crime organizado? Porque o seu conceito está intimamente relacionado com as características do cibercrime, na sua forma de atuação, organização, estrutura e objetivos.

As Nações Unidas definem o crime organizado como "*a structured group of three or more persons existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences in order to obtain, directly, a financial or other material benefit*" (UN, 2000, 4), definição semelhante foi aprovada pela UE na decisão quadro 2008/841/JAI, que considera uma organização criminosa como sendo, "...a associação estruturada de mais de duas pessoas, que se mantém ao longo do tempo e actua de forma concertada, tendo em vista a prática de infracções passíveis de pena privativa de liberdade ou medida de segurança privativa de liberdade cuja duração máxima seja, pelo menos, igual ou superior a 4 anos, ou de pena mais grave, com o objectivo de obter, directa ou indirectamente, benefícios financeiros ou outro benefício material.".

"Para quase todas as formas de crime organizado, os criminosos estão a desenvolver e adaptar a tecnologia de forma mais eficiente e eficaz. Este é talvez, o maior desafio das forças de segurança em todo o mundo, incluindo a UE." (Europol, 2017, 24). Estas inovações criminais associadas às novas tecnologias, elevaram o patamar da eficiência e eficácia criminal, desafiando Estados, forças e serviços de segurança a enfrentar o desafio do crime enquanto serviço.

3.2.3. O crime como serviço menu

"Os sítios de comercio da *Darknet* estão a tornar-se cada vez mais descentralizados. Não são apenas mercadorias comercializadas *online*, mas também serviços criminais.", sendo esta acedida "...por intermédio de softwares do tipo TOR "*The Onion Router*", I2P e *Freenet*."(Europol, 2017, 22).

Perspectiva-se que este comércio continue a crescer rapidamente num futuro próximo e que plataformas *online* sejam um factor chave na distribuição de todo o tipo de produtos ilícitos na UE. A *darknet* é um facilitador essencial para várias formas de actividade criminal incluindo tráfico de drogas, armas de fogo e *malwares*, de acordo com os especialistas Europol. As redes sociais também ocupam o seu espaço nesta

realidade, pois através do recurso a acrónimos ou "*hashtags*" os utilizadores de plataformas de partilha de fotografias podem organizar-se em comunidades de interesses, facilitando a partilha de informações e o tráfico de drogas com pagamento online e entrega por correio/estafetas.

Eis alguns produtos ilícitos específicos em matéria de cibercriminalidade que estão livremente disponíveis na *internet* a quem os quiser pagar como num restaurante:

- Softwares *malware* - é um termo genérico para toda a forma de ameaças que podem infectar/atingir um sistema informático, tais como *trojans, vírus, spywares, worms, rootkits*. Estes normalmente furtam dados pessoais tais como números de cartão de crédito, palavras passe de sistemas, e dados identificativos pessoais. Dá-se especial atenção aos *cryptowares*, que através de uma acção tipo cavalo de Tróia, lançam um ataque assente em algoritmos criptográficos a utilizadores individuais ou colectivos, públicos ou privados, ameaçando a publicação de dados privados, confidenciais ou comerciais, ou ameaçando bloquear indeterminadamente o acesso a publicações e sistemas, caso não seja pago um resgate, tratando-se de uma extorsão do tipo criptoviral.

- *Distributed Denial of Service* (DDos) - é uma ação concertada na qual múltiplos recursos informáticos comprometidos atacam computadores ou servidores, de forma a interromper um serviço de *internet*, um sítio, negando um serviço aos seus clientes ou proprietários.

- *Bullet proof hosting* - é um serviço que alguns domínios especializados disponibilizam, dando garantias "à prova de bala" de confidencialidade e integridade de acesso e disponibilização de dados.

- Serviços de anonimato - são serviços que permitem modificar o conteúdo ou a estrutura dos domínios, plataformas, de forma a dificultar ou impossibilitar a identificação dos seus detentores/proprietários.

- *Botnet wire* - É um recurso que auxilia a organizar ataques do tipo DDos, *spam*, furto de dados, permitindo ao seu detentor controlar a acção.

- Lavagem de dinheiro/branqueamento de capitais - serviços *online* que recebem dinheiro proveniente de acções ilícitas, e através de processos financeiros obscuros, o

conseguem injectar na economia real, gerando lucros lícitos, dissimulando a sua proveniência real.

3.3. Portugal

3.3.1. Estratégia de Cibersegurança, Estrutura, Enquadramento e Definições

A Convenção Europeia para o Cibercrime, pretendeu encaminhar os seus estados membros para uma estratégia concertada, estabelecendo definições técnicas e medidas a serem estabelecidas por estes em termos de: legislação, procedimentos judiciários, jurisdição, convencionando também os princípios e formas de cooperação internacional. Procurou estimular o desenvolvimento de acordos multi ou bilaterais entre estados membros nos domínios das convenções europeias da extradição e cooperação em matéria criminal (UE, 2001). Nesta sequência o Conselho da União Europeia, desenvolveu a decisão relativa a ataques contra sistemas de informação, obrigando os seus estados membros a criarem um ponto nacional operacional de contacto, para permitir a troca de informações relativamente a ataques informáticos 24 horas por dia e sete dias por semana (UE, 2005). Cumprindo a convenção e decisão quadro, Portugal a 15 Setembro de 2009, aprovou no seu ordenamento jurídico a lei nº109, vulgarmente denominada a lei do cibercrime, onde ficou definida a competência da Polícia Judiciária(PJ) como contacto permanente para a cooperação internacional, bem como para receber os pedidos internacionais de intercepção de transmissões de dados informáticos realizadas por via de um sistema informático localizado em Portugal. Ficou definido neste normativo o seguinte catálogo penal: falsidade informática, dano relativo a programas ou outros dados informáticos, sabotagem informática, acesso ilegítimo, intercepção ilegítima, reprodução ilegítima de programa protegido, a serem investigados pela PJ.

Em 2012 o Conselho de Ministros(CM) a 07 de fevereiro de 2012, aprovou a constituição de uma comissão instaladora do Centro Nacional de Cibersegurança(CNCS), que por razões orçamentais ficou integrado no Gabinete Nacional de Segurança(GNS), sem autonomia administrativa.

A 20 de maio de 2015 o CM aprovou a primeira Estratégia Nacional de Segurança do Ciberespaço(ENSC) e promoveu o CNCS a Autoridade Nacional com competência em matéria de cibersegurança, relativamente às entidades públicas e às

infra-estruturas críticas nacionais, bem como coordenador em matéria operacional no eixo do combate ao cibercrime.

O CM em 2017 constituiu o Conselho Superior de Segurança do Ciberespaço(CSSC), respondendo este directamente ao Primeiro Ministro, de forma a assegurar a coordenação político-estratégica da segurança do ciberespaço. Em 2018, procurando garantir um elevado nível de segurança comum nas redes e sistemas de informação em Portugal e na UE, é aprovada a 13 agosto a lei nº 46/2018. No seu artigo 7º é reforçada o CNCS como autoridade nacional e "ponto de contacto único nacional para efeitos de cooperação internacional, sem prejuízo das atribuições legais da Polícia Judiciária relativas a cooperação internacional em matéria penal.", devendo articular-se com as estruturas nacionais responsáveis pela ciberespionagem, ciberdefesa, cibercrime e ciberterrorismo.

Nova ENSC já em 2019 veio a ser aprovada pelo CM sendo na nossa opinião o documento mais completo em matéria de cibercriminalidade, publicado em Portugal e o que mais se aproxima da resolução nº 64/2011 de 21 de dezembro de 2009 das Nações Unidas em matéria do desenvolvimento de uma cultura de cibersegurança e esforço nacional na proteção de informação de estruturas criticas. Esta ENSC visa o período temporal 2019-2023, assentando em três objectivos: maximizar a resiliência, promover a inovação e gerar e garantir recursos, em matéria de cibersegurança. Desta destacam-se os seguintes conceitos:

Ciberespaço - consiste no ambiente complexo, de valores e interesses, materializado numa área de responsabilidade coletiva, que resulta da interação entre pessoas, redes e sistemas de informação.

Cibersegurança - consiste no conjunto de medidas e acções de prevenção, monitorização, deteção, reação, análise, e correção que visam manter o estado de segurança desejado e garantir a confidencialidade, integridade, disponibilidade e não repúdio da informação, das redes e sistemas de informação, das redes e sistemas de informação no ciberespaço, e das pessoas que nele interagem.

Cibercrime - entendem-se os factos correspondentes a crimes previstos na Lei do Cibercrime e ainda a outros ilícitos penais praticados com recurso a meios tecnológicos, nos quais estes sejam essenciais à prática do crime em causa.

A ENSC 2019-2023 reforçou a posição do CNCS como autoridade nacional para a Cibersegurança e "...como ponto único de contacto único nacional para efeitos de cooperação internacional em matéria de cibersegurança, sem prejuízo das atribuições legais cometidas a outras entidades, nomeadamente, ao Ministério Público e à Polícia Judiciária, relativas a cooperação internacional em matéria penal..."(CM, 2019, 2) bem como apelar à melhoria das "...capacidades da Polícia Judiciaria através do robustecimento das suas estruturas e das suas capacidades humanas e técnicas para a investigação e o combate ao cibercrime, fomentando os recursos humanos afetados a esta área e a sua capacidade de execução de medidas de obtenção de prova com recurso a meios técnicos, bem como a resposta às exigências de cooperação policial internacional;"(CM, 2019,3). Capacita o "CERT.PT" como equipa de resposta a incidentes de segurança informática nacional e procurar desenvolver no plano internacional a ciberdiplomacia. Define ainda que a cibersegurança é uma ação subsidiária integrando necessariamente infra-estruturas tecnológicas de entidades do sector privado e que complementarmente esta é uma responsabilidade partilhada por entidades públicas, privadas, colectivas ou individuais. No plano da prevenção, educação e sensibilização de uma cultura de cibersegurança é apelado aos princípios éticos, bem como ao reforço dos meios de recolha processamento de informação e capacidades de análise de forma a se conhecer os agentes de ameaça, intenções e capacidades.

No que concerne à proteção do ciberespaço a sua segurança é considerada parte integrante da segurança nacional e em caso de resposta pós-incidente, além das autoridades judiciárias, também as entidades do Sistema de Segurança Interna(SSI) e outras (que detenham informação relevante) fazem parte desta estratégia. Além das "grandes ameaças" a estruturas criticas, o ciberespaço abriu campo para novas formas criminais, originando condições para que se desenvolvam crimes antigos sob a capa de novos métodos(CM, 2019). Esta estratégia também prevê que as normas processuais penais se adaptem à realidade da prova digital, transfronteiriça e a agilização das ações investigatórias *online*, e em concreto às ações encobertas.

3.3.2. Estatística Nacional da Cibercriminalidade

Tendo por base o Relatório Anual de Segurança Interna(RASI) de toda a actividade do SSI do ano de 2018, são analisados de forma analítica todos os registos globais criminais participados em oito órgãos de policia criminal(OPC) nacionais.

O CNCS no âmbito das funções do GNS dispõe do CERT.PT, que em 2018, registou um aumento de 0,8% do número de incidentes que de forma direta ou indireta afetaram o Estado, num universo de 2456 incidentes reportados originando 629 processos resolvidos com sucesso(25,61%). Este universo é decomposto por incidentes de recolha de informação, tentativa de intrusão 60, *Malware* 204, Outros 138 (RASI, 2018).

O CERT.PT, no mesmo período temporal em modo automático, processou cerca de 333 milhões de registos, uma média mensal de cerca de 28 milhões de observáveis, significando isto uma alteração discreta de estado num sistema, dispositivo, serviço ou estado lógico, resultante de uma ação contra um determinado alvo. Destas alterações de sistema, apenas 17% se encontravam relacionadas com o ciberespaço nacional (RASI, 2018). Deduzindo-se desta forma que 83% das ameaças totalizadas, foram realizadas do exterior do espaço nacional.

Tabela 1

Registos da equipa de resposta a incidentes (CERT.PT)

Incidentes	**2018**
SPAM	119
C&C	21.626
Distribution	822
Malware	405.866
Phishing	58.142
Ids Alert	7.830
Blacklist	2.885.640
Compromissed	7.937
Brute-force	47.331
Botnet drone	1.030.717
Vulnerable service	51.071.703

Scaner	68.748
Observáveis Ciberespaço Nacional	55.606.362

Nota. Fonte RASI(2018, 136)

Na área da criminalidade informática é identificada uma diminuição criminal de 52 casos (-5,3%) face a 2017, num total de 924 casos, invertendo a tendência de subida desde 2004 (RASI, 2018).

Tabela 2

Registos de criminalidade informática

Tipologia	2018
Acesso / intercepção ilegítima	395
Sabotagem informática	226
Falsidade informática	220
Outros crimes informáticos	47
Viciação / destruição / dano dados, programa	32
Reprodução de programa protegido	4

Nota. Fonte RASI(2018, 47)

Quanto a investigações cibercriminais a PJ declarou ao RASI em 2018, que estas originaram 102 arguidos e 6 detidos e a burla informática e nas comunicações (crime previsto no código penal artº 221), terá originado 296 arguidos, 46 detidos e 14 prisões preventivas.

É esclarecido que "...no domínio do cibercrime poderá distinguir-se entre, crime ciberdependente; exploração sexual de menores online; fraude em meios de pagamento; crime ciberestrutural e branqueamento de capitais provenientes do cibercrime." (RASI, 2018, 48).

Analisando a burla informática e nas comunicações no contexto da criminalidade geral nacional, foram registados 9783 casos com um aumento de 20,1% (1634 casos) face a 2017, num universo de 18 crimes, que no seu todo representam 71% da criminalidade denunciada, a mesma tem um peso de 2,9%. Este aumento identificado representa o maior valor absoluto do universo criminal nacional (RASI, 2018).

4. Relações, contradições e inconsistências

É aceite que a *internet* na sua estrutura e fonte de novas realidades é evolutiva, dinâmica e dir-se-ia que sofre de um efeito Big-Bang, estando em expansão quanto à sua capacidade, dimensão, número de utilizadores, interações, ligações e formas criminais.

A *internet* do ponto de vista técnico designasse como de superfície, profunda e "Darknet", sendo esta muitas vezes confundida com a *internet* profunda. Uma nova dimensão da *internet* emerge, com a designação de IoT, relacionada com aparelhos digitais "personalizados" que num futuro próximo será responsável pela produção de 95% de toda a informação disponível na *internet*.

Quanto aos dados existentes no ciberespaço é entendido pelos analistas informáticos que numa sociedade digital e na perspectiva do perigo para a sua segurança, estes são classificados de: potencialidade crítica, crítica e hipercrítica. No entanto, nas recomendações, convenções, estratégias, leis nacionais e internacionais tais definições são inexistentes.

A nova realidade digital tem reflexo no crime "tradicional" uma vez que à cena do crime estarão potencialmente associados provas digitais, indeléveis e latentes (como o ADN e as impressões digitais), requerendo capacidades técnicas forenses acrescidas para a sua recolha, tratamento e validação judicial. Na área específica da cibercriminalidade conhecimentos avançados de criptografia são requeridos para descodificar dados nas cenas digitais criminais.

O FBI dispõe de um centro de queixas por crimes e incidentes informáticos (www.ic3.gov), estimando que apenas 15% das vítimas denunciaram os fatos, tendo a sua taxa de denúncias sofrido um aumento médio anual de 5,46% entre 2014 e 2018. Em igual período temporal este serviço registou um aumento médio anual de 25,59% no que concerne a prejuízos das vítimas. Considerando 34 tipologias de registos, para este centro é canalizada toda a forma de incidente ou crime que tenha a vertente informática (como por exemplo crimes contra crianças e terrorismo).

A UE tem uma criminalidade internacional organizada na qual o tráfico de droga e migrantes, representam os maiores lucros, sendo que na sua estratégia criminal está enquadrada a tecnologia, que não se limita à *internet*, incluindo drones, logística

automatizada, tecnologias avançadas de impressão. As plataformas digitais sediadas na *darknet* (com suporte criptográfico), publicitam, vendem e distribuem transnacionalmente todo o tipo de bens e serviços criminais de forma anónima, indetectável. É verificado que a criminalidade organizada internacional está em expansão, uma vez que entre 2013 e 2017 esta teve um aumento de 28%, num universo de cerca de 5000 organizações identificadas.

O crime organizado pela sua caracterização jurídica é muito ajustado à realidade de organização, estrutura, modo de atuação e objetivos do cibercrime.

No plano nacional em 2009 é aprovada a lei do cibercrime, originando um catálogo de 6 cibercrimes, a serem investigados pela PJ, bem como sendo nesta atribuída a competência de contacto permanente para a cooperação internacional. Em 2012 é constituída a CNCS, e em 2015 é aprovada a 1ª ENSC que promoveu o CNSC a Autoridade Nacional de Cibersegurança(ANCS) e a coordenador em matéria operacional no combate ao cibercrime. Em 2017 é constituído o CSSC, dependendo diretamente do Primeiro Ministro de forma a assegurar a coordenação político-estratégica da segurança do ciberespaço. O CNCS em 2018 vê reforçada as suas competências passando a ser o ponto único nacional para efeitos de cooperação internacional.

Nova ENSC para o período temporal 2019-2023 foi aprovada pelo CM, enfatizando o reforço das competências do CNSC como ponto único nacional para efeitos de cooperação internacional, relegando a PJ nessa função definitivamente, mantendo no entanto nesta e no Ministério Público os contactos internacionais para efeitos de cooperação internacional penal. Estabelece ainda conceitos técnicos, tais como: ciberespaço, cibersegurança e cibercrime. Sendo no nosso entender a definição de cibercrime que maior impacto irá trazer no SSI, uma vez que abre o conceito de cibercrime a outros ilícitos penais praticados com recurso a meios tecnológicos, nos quais estes sejam essenciais à prática do crime em causa, originando que outros OPC´s do SSI possam no âmbito das suas competências legais, proceder necessariamente a investigações classificadas como cibercrime (sendo que até ao momento apenas a PJ trabalhava dentro desse conceito no âmbito da lei do cibercrime). Estranhamente as entidades do SSI apenas são envolvidas na ENSC, no sentido de aumentarem a sua resiliência a ataques informáticos e num cenário de resposta pós-incidente, nunca outros

OPC´s são incluídos na lógica da necessidade de reforço de meios e atualização de capacidades forenses.

É evidente a aposta na PJ como a polícia dos cibercrimes, através do reconhecimento da necessidade do reforço das suas capacidades de recursos humanos, técnicos, forenses(obtenção de prova), estruturas e cooperação internacional (entenda-se penal). Reconhece-se uma miríade de ameaças internacionais ao ciberespaço nacional (na senda dos planos internacionais), bem como um emergente mundo "novo" de IoT, sendo criado o CERT.PT, equipa de resposta a incidentes de segurança informática nacional, bem como a ciberdiplomacia, para dar resposta a estes novos fatores.

O CERT.PT registou um aumento de 0.8% do número de incidentes que afetaram o Estado, apresentando uma taxa de sucesso na suas respostas de 25,61%, processando em modo automático 333 milhões de observáveis(alteração discreta de estado de um sistema, alvo de uma ação externa), dos quais apenas 17% das ações se encontravam relacionadas com o ciberespaço nacional, implicando que 83% destas ações foram realizados do exterior do ciberespaço nacional.

Relativamente à Tabela 1 não existe qualquer nota explicativa(no RASI) da natureza dos dados técnicos nela indicados, nem quantos incidentes registados originaram comunicação a autoridades judiciais.

Os crimes informáticos (na realidade os cibercrimes) apresentaram uma redução de 52 casos (-5,3%), num total de 924 registos.

No RASI, o Crime ciberdependente; exploração sexual de menores online; fraude em meios de pagamento; crime ciberestrutural e branqueamento de capitais provenientes do cibercrime, não apresenta valores, apenas indicadores de tendência.

O crime de burla informática e nas comunicações (não incluído na lei do cibercrime, mas enquadrando-se na sua atual definição), terá originado 296 arguidos, 46 detidos e 14 prisões preventivas, de acordo com os dados fornecidos pela PJ ao RASI. Contudo analisada a criminalidade geral do pais, observa-se que este tipo de crime registou o maior aumento absoluto de registos no universo criminal nacional, com 1637 casos (20,1%) no total de 9783. O RASI não esclarece se os dados da PJ refletem a totalidade deste fenómeno criminal, nem esclarece quais os OPC´s que procederam às investigações deste crime de natureza informática. No RASI em matéria de

cibercriminalidade e criminalidade informática não inclui qualquer referência a valores financeiros atingidos por esta criminalidade.

5. Conclusão

A *darknet* encerra o núcleo das organizações criminais europeias em expansão, carecendo a policia de elevadas capacidades técnicas na área da computação e criptografia, para preservar, colher e validar provas digitais dos seus crimes no ciberespaço.

As associações criminosas aumentaram 28% na zona euro, impulsionadas pelas novas tecnologias, atuando em simultâneo em diversos países europeus, disponibilizando os seus produtos, serviços técnicos e logísticos criminais no ciberespaço como se fossem um serviço normal.

Da IoT, relacionada com os aparelhos digitais "personalizados" surge a prova digital latente nos cenários de crime "tradicional", empurrando os OPC´s "tradicionais" para o mundo do ciberespaço, implicando nestas organizações que os seus patrulheiros (normalmente os primeiros a chegar a um cenário de crime) passem a ter formação da gestão do cenário do crime na vertente digital. Também na área da formação de meios Cinotécnicos deverá ser incluída a busca por telemóveis e outros aparelhos digitais, tais como discos rígidos ou *pendrives*.

A definição do que são dados potencialmente críticos, críticos ou hipercríticos para a vida em sociedade digital, bem como quais os deveres de cuidado e proteção dos produtores e detentores destes, poderá ajudar as autoridades judiciárias a determinar a medida da pena dos ciberinfratores.

O FBI regista e disponibiliza diversos dados relativamente à cibercriminalidade nomeadamente taxas de denúncia, cifras negras estimadas e valores de prejuízo sofrido pelas vítimas, considerando-se esta uma boa prática, devendo o RASI refletir também essa realidade.

Tendo o CNCS a qualidade de Autoridade Nacional da Cibersegurança e coordenador em matéria operacional no combate ao cibercrime, implica que todos os OPC´s do SSI passem a incluir na sua atividade operacional as recomendações, pareceres e determinações por esta autoridade emanadas.

A nova definição de cibercriminalidade prevista na ENSC 2019-2023, leva a que crimes "tradicionais" praticados com recurso a meios tecnológicos, nos quais estes sejam essenciais à prática do crime em causa, passem a ter a conotação de cibercrime. Consequentemente toda a estatística, colheita de dados produzida por OPC´s, deve passar a prever esta opção nos crimes "tradicionais", de forma a se poder quantificar esta nova influência tecnológica na realidade criminal e identificar quais os OPC´s que investigam cibercrimes e em que medida e tipologia.

A análise de toda a cibercriminalidade deveria estar centrada num único ponto, de forma a fazer face a fenómenos do tipo "burla informática e nas comunicações", evitando taxas de crescimento criminal elevadas, que provavelmente têm pontos criminais e tecnológicos comuns na origem.

A ENSC 2019-2023 não deverá limitar-se a apostar na PJ como a policia do cibercrime mas deverá também incluir outros OPC´s no plano interno nacional, na medida em que estes terão que fazer prova na vertente digital e tecnológica de uma forma diária e constante.

O CERT.PT deverá passar a incluir no RASI um anexo de definições referentes a Tabela 1, bem como quantos dos incidentes por estes registados foram comunicados às autoridades judiciais.

Tal como os novos fenómenos cibercriminais não têm fronteiras, parece-nos que a estrutura legislativa de forças e serviços de segurança deve começar a incorporar ideias mais abertas e flexíveis para o seu combate. Equipas mistas de trabalho, "*task forces*" devem começar a ser recorrentemente utilizadas, permitindo à investigação criminal gerir talentos entre as diversas forças e serviços de segurança nacionais na senda da lógica da racionalidade de meios e recursos públicos.

A formação de especialistas com competências na área do digital permitirá que as investigações se foquem no essencial e que provas podem ser obtidas, permitindo guiar as investigações de forma mais eficiente e eficaz, sendo ainda necessário investimento na melhoria das ferramentas tecnológicas ao dispor das policias para colheita de dados, bem como leis ajustadas a estes conceitos.

Deste estudo se conclui que a PSP tem um papel a desempenhar no combate ao cibercrime, nomeadamente nos crimes "tradicionais" aos quais o recurso a meios

tecnológicos sejam essenciais à prática do crime em causa, como por exemplo no crime da burla informática e nas comunicações. Esta organização deverá providenciar formação de investigadores, patrulheiros, equipas lufoscópicas, e binómios cinotécnicos na área da gestão do cenário do crime na vertente digital. Deverá ainda reformular métodos de colheita de informação estatística de forma a se poder aferir o trabalho desempenhado nesta área, bem como subordinar a sua atividade operacional à Autoridade Nacional da Cibersegurança.

Referências

Altvater (2016), Prosecutors' Center for Excellence - Combatting Crime on the Dark Web: How Law Enforcement and Prosecutors are Using Cutting Edge Technology to Fight Cybercrime, Retrieved from: https://pceinc.org/wp-content/uploads/2016/01/20161219-Combatting-Crime-on-the-Dark-Web-How-Law-Enforcement-and-Prosecutors-are-Using-Cutting-Edge-Technology-to-Fight-Cyber-Crime-PCE-Altvater.pdf, (visitado a 20/06/2019)

Assembleia da República Portuguesa(2009), lei nº 109/2009 de 15 Setembro - Lei do Cibercrime

Assembleia da República Portuguesa(2018), Lei nº 46/2018 - Regime jurídico do Ciberespaço, DR nº 155 de 13/08/2018

Bousquet (2018), Data-Smart City Solutions.https://datasmart.ash.harvard.edu/news/article/mining-social-media-data-policing-ethical-way (visitado 14/03/2019)

Catarino, G. M. (2015). Redes sociais: Responsabilidade, reserva e comportamento. In A. P. B. Homem, & E. T. Lopes (Coords.), *Ética e redes sociais* (pp. 17-40). Lisboa: Centro de Estudos Judiciários. Retrievedf rom: http://www.cej.mj.pt/cej/recursos/ebooks/outros/eb_Etica_Redes_Sociais.pdf, (visitado 14/03/2019)

CM(2012), Resolução do Conselho de Ministros nº 42/2012, DR nº 74/2012, Cria a Comissão Instaladora do Centro Nacional de Cibersegurança(CNCS)

CM(2015), Resolução do Conselho de Ministros nº 36/2015, DR nº 113/2015, Estratégia Nacional de Segurança do Ciberespaço e atribuição de Autoridade Nacional ao CNCS

CM(2017), Resolução do Conselho de Ministros nº 115/2017, DR nº 163/2017, Cria o Conselho Superior de Segurança do Ciberespaço(CSSC)

CM(2019), Resolução do Conselho de Ministros nº 92/2019, DR nº 108/2019, Estratégia Nacional de Segurança do Ciberespaço (ENSC)

EMCDDA(2018), Relatório do Observatório Europeu da Droga e da Toxicodependência - Tendências e evoluções, Retrieved from: http://www.emcdda.europa.eu/system/files/publications/8585/20181816_TDAT18001PTN_PDF.pdf, ISBN 978-92-9497-325-2, ISSN 2314-9175 (visitado 24/06/2019)

EUROPOL(2017), SOCTA - Serious and organized crime threat assesment, ISBN 978-92-95200-77-7, Retrieved from: https://publications.europa.eu/en/publication-detail/-/publication/a0c983b4-1db0-11e7-aeb3-01aa75ed71a1/language-en (visitado 24/06/2019)

FBI(2015), Internet Crime Complaint Center, Internet crime report, Retrived from: https://pdf.ic3.gov/2015_IC3Report.pdf (visitado 12/06/2019)

FBI(2018), Internet Crime Complaint Center, Internet crime report. Retrived from: https://pdf.ic3.gov/media/annualreport/2018_IC3Report.pdf (visitado 12/06/2019)

Perez (2018), The new crime environment presents new investigatory challenges for police, In The changing nature of crime and criminal Investigations, ISBN 978-1-934485-42-2

Penn (2018), How crime is changing, In The changing nature of crime and criminal Investigations, ISBN 978-1-934485-42-2, Retrived from: https://www.policeforum.org/assets/ChangingNatureofCrime.pdf(visitado 24/06/2019)

Policeforum (2018), The changing nature of crime and criminal investigations : How criminal investigations are changing: What agencies are doing to address the changing nature of crime, retrieved from https://www.policeforum.org/assets/ChangingNatureofCrime.pdf (visitado 11/06/2019)

Khanduja (2017), Quality Assurance and Project Management - Data Age 2025 White Paper by Seagate Cheat Sheet, Retrieved from https://itknowledgeexchange.techtarget.com/quality-assurance/data-age-2025/ (visitado 11/06/2019)

RASI(2018), Gabinete do Secretário Geral - Sistema de Segurança Interna - Relatório Anual de Segurança Interna, Retrieved from: https://www.portugal.gov.pt/download-ficheiros/ficheiro.aspx?v=ad5cfe37-0d52-412e-83fb-7f098448dba7 (visitado 24/06/2019)

Reinsel, Gantz, Rydning (2018), Data Age 2025: The Digitization of the World - From Edge to Core, Retrieved from: https://www.seagate.com/files/ww-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf (visitado 11/06/2019)

Strategyanalytics(2014), Retrieved from https://www4.strategyanalytics.com/default.aspx?mod=pressreleaseviewer&a0=5609 (visitado 10/06/2019)

The size of the World Wide Web (The Internet)(2019), https://www.worldwidewebsize.com/, visitado (22/06/2019)

Thompson (2015), Bussiness Insider - Beyond Google: Everything You Need to Know About the Hidden Internet, Retrieved from https://www.businessinsider.com/difference-between-dark-web-and-deep-web-2015-11, visitado (20/06/2019)

UE(2001), Convenção do Conselho da Europa nº 185, Cibercriminalidade, 23/11/2001.

UE(2005), Decisão Quadro do Conselho da Europa nº 222, Ataques contra os sistemas de informação, Jornal Oficial da União Europeia de 16/03/2005

UE(2008), Decisão Quadro do Conselho nº 841/JAI de 24/10/2008, Jornal oficial da União Europeia de 11/11/2008

UN(2000), Resolução da Assembleia Geral das Nações Unidas nº55/25 de 15/11/2000, Transnational Organized Crime.

UN(2010), Resolução da Assembleia Geral das Nações Unidas nº64/422 de 21/12/2009, Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastrutures.