NOVA SCHOOL OF LAW
CEDIS
CENTRO DE I&D SOBRE DIREITO E SOCIEDADE

VARIA

A Vertente "Cyber" da Criminalidade Organizada

Diogo A. M. R Dias Azedo
Mestrando em Direito e Segurança
Jurista e Pós Graduado em Investigação Criminal

RESUMO

Este trabalho pretende debruçar-se sobre criminalidade organizada e a sua evolução tecnológica.

Devido a esta evolução (das TIC), a Cibersegurança assume uma importância cada vez mais especial no Ciberespaço e na Segurança dos Estados.

Com as novas tecnologias e com a inovação constante das próprias, as ameaças e os riscos provenientes do ciberespaço estão em permanente mutação.

Tecnologias estas, que são bastante vulneráveis, isto porque "...por um lado, trazem claros benefícios à sociedade, por outro lado, vêm aumentar, de forma significativa, os riscos decorrentes da sua dependência e da quantidade de informação armazenada e em circulação, expondo o Estado, as empresas e os cidadãos." [1].

[1] 4º parágrafo da Estratégia Nacional de Segurança do Ciberespaço;

NOVA SCHOOL OF LAW
CEDIS
CENTRO DE I&D SOBRE DIREITO E SOCIEDADE
VARIA
Nº 1
CEDIS WORKING PAPERS
MARÇO 2020

O desenvolvimento do mundo digital, foi um fenómeno que se interligou com o mundo da criminalidade organizada, como não podia deixar de ser.

Este tipo de criminalidade já era conhecida pela sua complexidade, mas devido à evolução tecnológica dos últimos dez anos, com ela evoluiu a complexidade dos crimes organizados.

Mostra-se relevante abordar este tema não só no âmbito das caraterìsticas do crime organizado e da cibercriminalidade, como também nas possíveis ações estratégicas no combate contra estes tipos de criminalidade.

Atualmente a União Europeia é um dos palcos de estreia destas ameaças e de diversas formas de criminalidade, que produzem consequências a nível internacional, a criminalidade organizada (e os seus cibercrimes) não é excepção.

PALAVRAS-CHAVE

Cibersegurança; Ciberespaço; Criminalidade Organizada; Cibercriminalidade; Ações Estratégicas.

ABSTRACT

This working paper intends to focus on organized crime and its technological evolution.

Due to this (ICT) evolution, Cybersecurity assumes an increasingly special importance in Cyberspace and State Security.

With new technologies and constant innovation of their own, threats and risks from cyberspace are constantly changing.

These technologies, which are quite vulnerable, because “... on one hand, they bring clear benefits to society, on the other hand, they significantly increase the risks arising from their dependence and the amount of information stored and in circulation, exposing the State, companies and citizens. ”.

NOVA SCHOOL OF LAW
CEDIS
CENTRO DE I&D SOBRE DIREITO E SOCIEDADE
VARIA
Nº 1
CEDIS WORKING PAPERS
MARÇO 2020

The development of the digital world, is a phenomenon that´s interconnected with the world of organized crime, as it could not be otherwise.
This type of crime was already known for its complexity, but due to the technological evolution of the last ten years, the complexity of organized crimes has evolved with it.
It is relevant to address this issue not only in the context of the characteristics of organized crime and cybercrime, but also in the possible strategic actions to combat these types of crime.
Currently, the European Union is one of the first stages of these threats and of various forms of crime, which have consequences at the international level, the organized crime (and its cybercrimes) is no exception.

KEYWORDS

Cybersecurity; Cyberspace; Organized Crime; Cybercrime; Strategic Actions.

Lista de Siglas

A.P.A.V - Apoio à Vítima;

C.E.D.N - Conceito Estratégico de Defesa Nacional;

E.N.S.C - Estratégia Nacional de Segurança do Ciberespaço;

L.C - Lei do Cibercrime;

L.C.C.O - Lei de Combate ao Crime Organizado;

O.N.U - Organização das Nações Unidas;

T.I.C - Tecnologias de Informação e Comunicação;

U.E - União Europeia.

1. Criminalidade Organizada

1.1. Complexidade Conceitual

O crime organizado é um fenômeno que atinge (de forma discreta) uma sociedade nos seus vários pontos críticos: como a política, a economia, o próprio Estado, ou seja, a sociedade como um todo. Está presente todos os dias nas nossas vidas, como um parasita. Desenvolve-se de forma a adaptar-se às novas realidades e necessidades de uma sociedade.

Antes de avançar para o cerne do tema de trabalho, mostra-se relevante (tentar) definir criminalidade organizada.

Após uma vasta pesquisa, facilmente chegamos à conclusão que definir criminalidade organizada é uma tarefa bastante complexa. Têm sido apresentadas inúmeras definições ou melhor, tentativas de definições, que tem impedido o consenso num conceito preciso e único de criminalidade organizada.

Para Paulo Borges, esta dificuldade deve-se "não só devido à ausência de um critério consensual, mas também das dificuldades da sua tipificação legal" [2].

O Dr. Francisco Proença Garcia também compartilha esta ideia, ao afirmar que " o crime organizado tira partido das diferenças, ainda acentuadas, entre as legislações nacionais dos países. São muitas vezes as diferenças entre as definições de determinado tipo de crime que permitem entrar com mais facilmente em certos mercados do que outros." [3].

Alguns autores baseiam-se na comparação entre a criminalidade comum e a organizada para alcançarem uma definição.

[2] Borges, P. (2002) - p.15;
[3] Garcia, F. (2019) - p.162;

Na opinião de José Braz, o crime comum "integra condutas ilícitas, praticadas geralmente de forma isolada e individual, suscetíveis de assumir formas de violência gratuita, destituídas de qualquer sentido estratégico", enquanto o crime organizado "compreende o conjunto de condutas ilícitas praticadas de forma coletiva, sistemática, integrada e continuada, visando alcançar objetivos estrategicamente definidos" [4].

John Conklin adiciona ao conceito, que a distinção entre o crime organizado dos outros tipos de crimes é a durabilidade e a complexidade da actividade criminosa em causa.

Tem características em comum com organizações formais como a divisão de tarefas, uma estrutura de autoridade hierárquica e um controlo entre os níveis da hierarquia

Como afirma o Dr. Francisco Garcia "a estrutura do crime organizado é muito desenvolvida, durável e a sua organização pode ser comparável à de uma empresa." [5].

Os autores Andre Bossard [6] e Howard Abadinsky [7] caracterizaram o crime organizado em 4 pontos:

- A 1ª característica é a permanência, estes grupos criminosos são criados com o objetivo de permanecerem com estabilidade, para que seja possível praticarem os seus tipos de crime.

- A 2ª característica, a estruturação. Os grupos criminosos estabelecem as suas estruturas em tradições locais antigas. Estabelecendo uma organização interna, dividida por membros.

[4] Braz, J. (2004) - p. 269;
[5] Garcia, F. (2019) - p.160;
[6] Bossard, A. (1990);
[7] Abadinsky, H. (2010);

- A 3ª característica é a presença de uma hierarquia bem definida, baseada em obediência, fidelidade e lealdade.

- Por último, temos como característica, o segredo. A "lei da organização", isto é, nunca revelar informações que possam prejudicar de qualquer forma o grupo criminoso.

Assim, verificamos que os grupos de criminalidade organizada vivem numa realidade completamente diferente, tendo as suas próprias normas, dentro de uma organização estabelecida por uma hierarquia e por uma disciplina forte. Utilizando todos os meios possíveis para alcançar o seu fim.

Na definição dada por Ortmeier, "Organized crime is defined as any relatively permanent group of individuals that systematically engage in illegal activities with economic gain as its primary goal. It involves the coordination of numerous persons in the planning and execution of illegal acts or the pursuit of legitimate goals through unlawful means. Organized crime's existence is maintained through the use of threats, intimidation, force, monopoly control, and corruption. Revenues from illegal activities are used to develop legitimate businesses to use as covers for more illegal activity." [8].

No meio destas definições, devemos dar primazia às definições da Organização das Nações Unidas e da União Europeia. Sendo estas instituições, umas das principais (se não as principais) combatentes ao crime organizado transnacional.

[8] Tradução livre do autor: o crime organizado é definido como qualquer grupo relativamente permanente de indivíduos que se envolvam sistematicamente em atividades ilegais com ganho económico como sua meta principal. Envolve a coordenação de numerosas pessoas no planejamento e execução de atos ilegais ou na busca de objetivos legítimos por meios ilegais. A existência do crime organizado é mantida através do uso de ameaças, intimidação, força, controle de monopólio e corrupção. As receitas de atividades ilegais são usadas para desenvolver negócios legítimos que por fim são utilizados para praticar mais atividades ilegais;

A O.N.U apresenta a sua definição no artigo 2º, al. a) da Convenção Contra a Criminalidade Organizada Transnacional de 2000 (entrou em vigor em 2003), onde considera a criminalidade organizada como "um grupo estruturado de três ou mais pessoas, existindo durante um período de tempo e actuando concertadamente com a finalidade de cometer um ou mais crimes graves ou infracções estabelecidas na presente Convenção, com a intenção de obter, directa ou indirectamente, um benefício económico ou outro benefício material" [9].

Oito anos depois, a U.E através da sua Decisão-Quadro 2008/841/JAI do Conselho, no seu artigo 1º, nº 1, define criminalidade organizada como uma "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...com o objectivo de obter, directa ou indirectamente, benefícios financeiros ou outro benefício material." [10].

1.2. Ameaça Transnacional e Multissectorial

Nas palavras de Abel Couto, uma ameaça é tradicionamente "...qualquer acontecimento ou ação, de variada natureza que contraria a consecução de um objetivo e que, normalmente, é causadora de danos, materiais ou morais. No âmbito da estratégia, consideram-se, principalmente, as ameaças provenientes de uma vontade consciente, analisando o produto das possibilidades pelas intenções" [11]. Isto é, "...determinada situação é geradora de uma ameaça se o seu agente

[9] Convenção da ONU contra a Criminalidade Organizada Transnacional;
[10] Decisão-Quadro 2008/841/JAI do Conselho da U.E;
[11] Couto, A. (1989) - p. 329;

tiver possibilidades ou capacidades para a sua concretização e se também tiver intenções de a provocar" [12], afirma Luís Escorrega.

No entanto, esta definição parece ser insuficiente, como afirma o Dr. Francisco Gracia "...este conceito, por não ser suficientemente abrangente, apresenta no momento difíceis problemas quando procuramos precisar o que compreende." [13].

Já para José Nogueira, considera ser um "...um ato ofensivo, uma antecâmara da agressão, portanto, uma realidade estratégica sem ser ainda guerra, que não desaparece quando a agressão é efectivada" [14].

O Relatório da O.N.U de 2004, apresenta um conceito de ameaça de nível transacional "Any event or process that leads to large-scale death or lessening of life chances and undermines States a the basic unit of the international system is a threat to international security. " [15]. O mesmo relatório identificou a criminalidade organizada como uma das seis principais ameaças à segurança internacional das próximas décadas.

No entanto, as ameaças que enfrentamos estão em constante mutação, evoluindo de forma a se inserirem na nossa sociedade, tendo em conta as nossas necessidades. Assim podemos constatar na Comunicação da Comissão da U.E em relação à Estratégia de Segurança Interna "as nossas sociedades defrontam graves ameaças cuja dimensão e grau de sofisticação têm vindo a aumentar. Actualmente, muitos desafios em matéria de segurança assumem uma natureza

[12] Escorrega, L (2009);
[13] Garcia, F. (2019) - p.153;
[14] Nogueira, J. (2005)- p.18;
[15] Relatório da O.N.U (2004) - p.12;
Tradução livre do autor: Qualquer evento ou processo que leve à morte em larga escala ou diminua as chances de vida e prejudique os Estados como unidade básica do sistema internacional é uma ameaça à segurança internacional;

transfronteiras e multissectorial" [16] e a criminalidade organizada certamente não é excepção. Assim afirmou o Secretário-Geral da O.N.U, "if crime crosses all borders, so must law enforcement." [17].

Segundo N. Lourenço "as ameaças circulam facilmente neste mundo global. As fronteiras são fáceis de transpor, não sendo novidade que na sociedade aberta atual o crime transnacional organizado aumentou rapidamente na última década. As organizações criminosas acabam por beneficiar do fraco controle dos Estados sobre as fronteiras e do fim das barreiras comerciais" [18]. Isto porque a ameaça proveniente do crime organizado está "...mais relacionada com a evolução da sua natureza do que com a sua dimensão…foi adaptando a sua estrutura, a sua forma de operar e as suas actividades à realidade que o rodeava, estando em mutação permanente e sempre em busca da maximização do lucro." [19]..."o resultado desta mutação traduziu-se numa maior dificuldade na deteção das actividades ilegais e no controlo dos movimentos dos grupos em questão." [20].

O C.E.D.N (de Portugal) reconhece a cibercriminalidade como uma das principais ameaças à segurança nacional e global da próxima década. Ameaça esta que tem como alvo as ***"...***redes indispensáveis ao funcionamento da economia e da sociedade da informação globalizada...são uma ameaça crescente a infraestruturas críticas, em que potenciais agressores (terroristas, criminalidade

[16] Comunicação da Comissão Europeia- Estratégia de Segurança Interna. p. 2;
[17] Discurso de abertura do Secretário-Geral para a convenção da O.N.U contra a criminalidade organizada transnacional. Tradução livre do autor: "Se o crime atravessa todas as fronteiras, também deve atravessar com ele a aplicação da lei.";
[18] Lourenço, N. (2009) - p. 85;
[19] Garcia, F. (2019) - p. 158;
[20] Garcia, F. (2019) - p. 161;

organizada, Estados ou indivíduos isolados) podem fazer colapsar a estrutura tecnológica de uma organização social moderna." [21].

2. Cibercriminalidade

2.1. A Segurança do Ciberespaço

Antes desenvolvermos a cibercriminalidade e o seu respectivo catálogo, é necessário definir dois conceitos que andam de mãos dadas com a cibercriminalidade, o Ciberespaço e a (sua) Cibersegurança.

O prefixo "Cyber" foi empregue pela 1ª vez em 1948, pelo Sr. Norbert Wiener no seu livro "Cybernetics", onde afirma que o ciberespaço é "o interface entre o Homem e a máquina produz um novo ambiente ou um ambiente alternativo" [22].

No ano 1984, o escritor William Gibson contribuiu para evolução do conceito, ao considerá-lo como "a consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphical representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the non-space of the mind, clusters and constellations of data…" [23], ou seja, "o ciberespaço é uma alucinação coletiva" [24].

[21] C.E.D.N. - pp. 21 e 22;
[22] Apontamentos da 2ª aula de Cibersegurança - Slides;
[23] Gibson, W. (1984). Tradução livre do autor: uma alucinação consensual sentida diariamente por bilhões de operadores legítimos, em todas as nações, por crianças aprendendo conceitos matemáticos ... Uma representação gráfica de dados abstraídos dos bancos de todos os computadores do sistema humano. Complexidade impensável. Linhas de luz variam no não espaço da mente, aglomerados e constelações de dados;
[24] Apontamentos da 2ª aula de Cibersegurança - Eng. Lino Santos;

A palavra espaço neste termo é entendida como uma metáfora, isto porque, quando não temos forma de definir algo, utilizamos outra palavra como bengala [25].

"A fronteira entre o espaço físico e o ciberespaço é o computador à frente do utilizador. O ciberespaço é uma realidade (virtual) criada pelo nossos sentidos." [26].

Assim o afirma a Estratégia Nacional de Segurança do Ciberespaço "o ciberespaço transpõe a vida real para um mundo virtual, com características únicas que impõem novas formas de interação e de relacionamento." [27].

Ao contrário da maior parte dos conceitos informáticos, o ciberespaço não tem uma definição consensual e padronizada. Geralmente é utilizado para descrever o mundo virtual de computadores, que se interligam através da Internet.

No entanto, o Eng. Lino Santos apresentou-nos uma definição bastante completa, que descreve o ciberespaço como um "conjunto de sistemas informáticos – dispositivos, redes de comunicação, programas de computador e aplicações –, a informação neles processada, armazenada e transmitida, bem como os seus utilizadores, formando um espaço virtual de:

- interacção social;
- expressão de liberdade e democracia;
- oportunidade" [28].

Com as novas tecnologias e com a inovação constante das próprias, as ameaças e os riscos provenientes do ciberespaço estão em permanente mutação. Tecnologias estas que são bastante vulneráveis, isto porque "...por um lado, trazem claros benefícios à

[25] Apontamentos da 2ª aula de Cibersegurança - Dr. Professor Armando Marques Guedes;
[26] Apontamentos da 2ª aula de Cibersegurança - Eng. Lino Santos;
[27] 5º parágrafo da Estratégia Nacional de Segurança do Ciberespaço;
[28] Apontamentos da 2ª aula de Cibersegurança - Slides;

sociedade, por outro lado, vêm aumentar, de forma significativa, os riscos decorrentes da sua dependência e da quantidade de informação armazenada e em circulação, expondo o Estado, as empresas e os cidadãos." [29]. Portugal não é excepção, "...não restam, hoje em dia dúvidas de que Portugal está tão vulnerável a ataques cibernéticos como qualquer outro país." [30].

O Eng. Lino Santos afirma ser "...incontestável que o ciberespaço introduziu profundas alterações na forma como os cidadãos, as organizações e os Estados se relacionam entre si." [31].

O que nos leva à necessidade da Cibersegurança, na proteção do ciberespaço e dos seus utilizadores. Temos "assistido a um desenvolvimento acelerado da sociedade da informação e a uma crescente dependência das TIC em funções vitais do funcionamento do País." [32].

Lino Santos considera que temos de diminuir o progresso tecnológico e aumentar a capacidade da sociedade de lidar com tal progresso. A diferença entre o progresso tecnológico e a capacidade da sociedade, representam riscos e uma grande vulnerabilidade para sofrer consequências [33].

De forma geral, a cibersegurança consiste na segurança efetiva e eficaz de sistemas informáticos [34], isto é, um conjunto de ações preventivas e repressivas com o objectivo de diminuir as ameaças e os riscos existentes no ciberespaço, como também chegar à autoria dos mesmos (que muitas vezes se concretizam).

[29] 4º parágrafo da Estratégia Nacional de Segurança do Ciberespaço;
[30] Entrevista do Eng Lino Santos à Renascença - 1º parágrafo;
[31] Eng. Lino Santos. E-Jornal, p.94;
[32] 2º parágrafo da Estratégia Nacional de Segurança do Ciberespaço;
[33] Apontamentos da 3ª aula de Cibersegurança - Eng. Lino Santos;
[34] Cordeiro, R. (2012) - p. 48;

Outra característica do ciberespaço é o anonimato, que traz elevadas dificuldades na identificação dos cibercriminosos, "...este espaço virtual garante algum grau de anonimato a quem o utiliza, o que levanta, novamente, dificuldades quanto à atribuição dos actos praticados ou à identificação dos seus autores." [35].

Tendo em conta, as suas características (transnacional, global e anónimo), torna-se muito complexo implementar medidas de segurança, o que por consequência facilita a consumação de crimes por utilizadores que (provavelmente) no mundo real não cometeriam [36].

Isto é, não é necessária a presença física do indivíduo para que possa praticar crimes, desta forma cria-se um ambiente mais que favorável para as actividades das organizações da criminalidade organizada [37].

No entanto, há que ter em conta que o "cibercrime é uma parcela da cibersegurança" [38].

2.2. Cibercrime

A diferença entre um crime "típico" (onde se insere o crime organizado) e o cibercrime, é o recurso a computadores e/ou à Internet [39].

O cibercrime é outro conceito que se mostra difícil de definir, isto porque envolve tecnologias em permanente evolução e não tem fronteiras, o que levanta dificuldades de competência legislativa territorial.

[35] Eng. Lino Santos. E-Jornal, p. 95;
[36] United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime (2013). p. 8;
[37] Santos, P; Bessa, R; Pimentel, C. (2008);
[38] Apontamentos da 1ª aula de Cibersegurança - Dr. Professor Armando Marques Guedes;
[39] APAV Cibercrime;

Majid Yar entende que "a major problem for the study of cybercrime is the absence of a consistent current definition..." [40].

A United Nations Office on Drugs and Crime, também não nos consegue proporcionar uma definição consensual, embora considere mais adequado inserir neste conceito, não os tipos de atos em si, mas um conjunto de condutas que podem ser agrupadas, tendo em conta o objecto do crime ou o seu "modus operandi" [41].

No ano 2003, Portugal não tinha "...nenhum texto legal que consagre a expressão cibercrime…nenhum dispositivo legal que use, refira ou defina esta expressão" [42].

Seis anos depois, entrou em vigor a Lei do Cibercrime (Lei nº 109/2009).

No entanto, o termo de cibercrime continua sem definição.

Lourenço Martins e Garcia Marques, interpretam o cibercrime como "... todo o acto em que o computador serve de meio para atingir um objectivo criminoso ou em que o computador é alvo simbólico desse acto ou em que o computador é objecto de crime" [43]. Importante relembrar que o computador por si só, não representa qualquer ameaça (real), é sempre necessário a vertente humana para que se pratique qualquer ilícito (ciber) criminal.

Definição esta, que veio corresponder na sua maioria, com a definição que foi apresentada através de um comunicação da Comissão da U.E em relação ao "Rumo a uma política geral de luta contra o cibercrime". Esta comunicação define cibercrime como "os actos criminosos praticados com recurso a redes de comunicações electrónicas e sistemas de informação ou contra este tipo de redes e sistemas." [44].

---

[40] Yar, M. (2006) - p. 9. Tradução livre do autor: "o maior problema no estudo do cibercrime, é a ausência de uma definição consistente e corrente…";
[41] United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime (2013) - p. 11;
[42] Verdelho, P. (2003) - p. 347;
[43] Garcia, M; Lourenço, M. (2011) - p. 16;
[44] Comunicação da Comissão da U.E (Rumo a uma política geral de luta contra o cibercrime) - p. 2;

A própria comunicação divide o cibercrime em três categorias de actividades criminosas [45]:

- Formas tradicionais de criminalidade (como a fraude ou falsificação);
- Publicação de conteúdos ilícitos em meios de comunicação eletrônicos (por exemplo a pornografia infantil ou incitamento ao ódio racial);
- Crimes exclusivos das redes eletrónicas, ou seja, crimes eletrónicos propriamente ditos (como ciberataques, bloqueio de serviços e pirataria).

No entanto, estas categorias têm uma característica (desastrosa) em comum "...o facto de poderem ser cometidos em grande escala e de ser muito grande a distância geográfica entre o acto criminoso e os seus efeitos." [46].

Tal característica, leva o autor do crime a sentir-se mais "...seguro e, não sendo investigado, descoberto e punido, não desiste de uma prática que lhe permiteusufruir de bens avultados..." [47], isto porque o "facto das comunicações se processarem a nível planetário entre uma rede infindável de computadores, em que se considera faltar o elemento territorialidade para se poder impor o direito nacional" [48].

Problemática que tem afetado profundamente a investigação criminal deste tipo de crimes, tornando-a muito difícil e por vezes até impossível.

Conferindo aos cibercriminosos "um constante o sentimento de impunidade" [49].

[45] Comunicação da Comissão da U.E (Rumo a uma política geral de luta contra o cibercrime) - p. 2;
[46] Comunicação da Comissão da U.E (Rumo a uma política geral de luta contra o cibercrime) - p. 2;
[47] Guedes, M. (2009) - p. 499;
[48] Santos, P; Bessa, R; Pimentel, C. (2008) - p. 5;
[49] Apontamentos da 3ª aula de Cibersegurança - Eng. Lino Santos;

A A.P.A.V realizou um estudo em 2013, a treze mil indivíduos entre os 18 e os 64 anos de 24 países, chegando à conclusão que existem 378 milhões de vítimas de cibercrime por ano, 1 milhão por dia e 12 por cada segundo. [50].

Desta forma, mostra-se necessário que haja investigadores criminais cada vez mais especializados nesta vertente criminal.

2.3. A Evolução Tecnológica do Crime Organizado

O desenvolvimento do mundo digital, foi um fenómeno que se interligou com o mundo da criminalidade organizada, como não podia deixar de ser.

Este tipo de criminalidade já era conhecida pela sua complexidade, mas devido à evolução tecnológica dos últimos dez anos, com ela evoluiu a complexidade dos crimes organizados.

Como podemos confirmar na Estratégia Nacional de Segurança do Ciberespaço, ".. o mundo em rede desenvolve novos modos de atuação com características únicas, de onde se destacam o cibercrime e, em particular, o cibercrime organizado, associado à fraude bancária e à usurpação de identidade com este mesmo propósito..." [51].

A A.P.A.V reafirma a posição da E.N.S.C, ao afirmar que os "...instigadores mais perigosos deste tipo de crimes são as organizações criminosas, que controlam todo o processo do furto de identidade, desde a obtenção dos dados até ao branqueamento do capital." [52]

[50] APAV Cibercrime;
[51] E.N.S.C - 7º parágrafo;
[52] APAV Cibercrime;

Já em 2007, através da comunicação da Comissão U.E (supramencionada), se reconhecia que o cibercrime tinha uma tendência para a criminalidade organizada, o "...número de cibercrimes está a aumentar e as actividades criminosas estão a tornar-se cada vez mais sofisticadas e internacionalizadas. Há indicações claras no sentido de um envolvimento crescente de organizações criminosas no cibercrime" [53].

Actualmente podemos constatar que a criminalidade organizada assume uma natureza nova, devido à sua transnacionalidade, às tecnologias inovadoras e os fluxos migratórios que permitem a estruturação [54].

Desde muito cedo, que estes grupos criminosos se aperceberam das vantagens tecnológicas que podiam ser utilizadas na consumação de crimes, como para a ocultar os seus lucros e membros da organização [55].

A Internet veio trazer um novo paradigma a estas organizações criminais, ao garantir uma rapidez na comunicação, como o seu anonimato devido às comunicações encriptadas [56].

Antes de mais, é relevante mencionar que a comunidade digital no seu geral tem acesso a 20% da internet, a tão conhecida Surface Web, isto é, a parte comum da internet que é acessível através de motores de busca como a Google e a Yahoo [57].

Os outros 80%, dizem respeito a uma parte da internet que poucos têm acesso, e muitos nem sequer tem conhecimento dela, a Dark Web [58].

O nosso Dr. Professor Armando Marques Guedes, comparou este acesso à internet com um "Iceberg", ou seja, a ponta do iceberg que é vista por toda gente é a Surface

[53] Comunicação da Comissão da U.E (Rumo a uma política geral de luta contra o cibercrime) - p. 3;
[54] Davin, J. (2007) - p. 3;
[55] Davin, J. (2007) - p. 60;
[56] Davin, J. (2007) - p. 42;
[57] Ramalho, D. (.2013) - p. 385;
[58] Ramalho, D. (.2013) - p. 393;

Web, e debaixo do mar onde não se vê a maior parte do iceberg é considerada a Dark Web [59].

É através da Dark Web, que estes grupos fazem o recrutamento de membros para a suas redes criminosas ou simplesmente para fazer um serviço exclusivo, que irá beneficiar a organização como um todo.

Nas palavras do Eng. Lino Santos, a criminalidade organizada olha para a internet como "uma montra de uma loja" [60], onde pode comprar e vender uma variedade de serviços e produtos ilícitos [61].

Em 2014, o Conselho Europeu realizou um projecto de conclusões sobre o desenvolvimento de uma Estratégia de Segurança Interna da U.E renovada, identificando este tipo de criminalidade como uma das principais ameaças e desafios para os próximos anos, e chama atenção para as ameaças provinientes de novas tecnologias.

Afirmando que as "ameaças novas e emergentes deverão ser identificadas e acompanhadas de perto com recurso a uma abordagem baseada na recolha de informações…ameaças e desafios resultantes do recurso às novas tecnologias: as avarias nas principais tecnologias da informação e de comunicação podem criar problemas de segurança. O maior número de instrumentos tecnológicos e de comunicação disponíveis proporciona igualmente aos grupos de criminalidade organizada a oportunidade de visar pessoas ou empresas..."[62].

[59] Apontamentos da 3ª aula de Cibersegurança;
[60] Apontamentos da 3ª aula de Cibersegurança - Eng. Lino Santos;
[61] Davin, J. (2007) - p. 42;
[62] Projecto de conclusões do Conselho sobre o desenvolvimento de uma Estratégia de Segurança Interna da U.E renovada.- p. 7 e 8;

Podemos tentar identificar alguns dos crimes organizados praticados diretamente através da internet através do Regulamento (UE) 2016/794.

A U.E cria a Europol e atribui-lhe como objetivo "...apoiar e reforçar a ação das autoridades competentes dos Estados-Membros e a sua cooperação mútua em matéria de prevenção e luta contra a criminalidade grave que afete dois ou mais Estados-Membros, o terrorismo e formas de criminalidade que afetem um interesse comum abrangido por uma política da União, constantes da lista do anexo I"[63].

Desta lista podemos identificar como cibercrimes (da família da criminalidade organizada):

- Branqueamento de capitais;
- Burla e fraude;
- Criminalidade informática;
- Crimes contra os interesses financeiros da União;
- Abuso de informação privilegiada e manipulação do mercado financeiro;
- Abuso e exploração sexual, incluindo material relacionado com o abuso sexual de crianças e aliciamento de crianças para fins sexuais;

Já o nosso ordenamento, publicou a Lei n.º 5/2002 de 11 de Janeiro - Medidas de Combate à Criminalidade Organizada (conhecida por L.C.C.O.).

Esta lei apresenta no seu artigo 1º um leque de tipos de ilícitos que constituem a criminalidade organizada. A maior parte dos crimes com uma vertente "cyber" já foram supramencionados na lista anterior, à excepção de :

[63] Art. 3º do Regulamento (UE) 2016/794;

- Dano relativo a programas ou outros dados informáticos;
- Sabotagem informática;
- Acesso ilegítimo a sistema informático.

Segundo Mariano Carrión (ex-diretor da Europol) esta agência " promove a gestão rápida e eficaz do fluxo de informações" [64], onde a cooperação policial é uma caraterística essencial para o funcionamento da Europol.

3. Estratégias de combate à Criminalidade Organizada

3.1. Ações Estratégicas da União Europeia

O 1º objetivo referido na Comunicação da Comissão Europeia em relação à Estratégia de Segurança Interna em Acção é o desmantelamento das redes criminosas. A própria comunicação apresenta-nos um conjunto de ações para que a U.E possa alcançar o seu objetivo:

- Compreender o modus operandi dos membros da organização, de forma a que consiga identificá-los e por fim desmantelar a rede criminosa;
- Proteger a economia contra a infiltração deste tipo de criminalidade, que (através da corrupção) compromete a confiança nas instituições públicas e no sistema económico;
- Confiscar os produtos do crime, "no intuito de combater o incentivo financeiro das redes de criminalidade, os Estados-Membros devem envidar todos os esforços

[64] Carrión, M. (2005). pp. 199;

possíveis para apreender, congelar, gerir e confiscar os produtos do crime e garantir a sua não recuperação pelos criminosos." [65].

Tem como 3º objectivo, reforçar os níveis de segurança para os cidadãos e as empresas no ciberespaço, através:

- Desenvolver as capacidades no domínio da aplicação da lei e judiciário, ao estabelecer "...no âmbito das estruturas existentes, um centro de cibercriminalidade, através do qual os Estados-Membros e as instituições da UE poderão desenvolver capacidades operacionais e analíticas para as investigações e a cooperação com parceiros internacionais...O centro de cibercriminalidade deve tornar-se o ponto nevrálgico do combate europeu à cibercriminalidade."[66]. Centro este que já existe desde 2013;

- Trabalhar com as empresas para capacitar e proteger os cidadãos, ou seja, todos "...os Estados-Membros devem assegurar a fácil comunicação pelos cidadãos de actos de cibercriminalidade."

- Melhorar a capacidade de resposta aos ciberataques, de forma a que todos os Estados-Membros tenham "uma equipa de emergência de resposta no domínio informático que funcione em boas condições" [67].

[65] Comunicação da Comissão Europeia- Estratégia de Segurança Interna. p. 5 e 6;
[66] Comunicação da Comissão Europeia- Estratégia de Segurança Interna. p. 10;
[67] Comunicação da Comissão Europeia- Estratégia de Segurança Interna. p. 11;

3.2. Estratégia de Defesa Nacional (Portuguesa)

O nosso ordenamento jurídico também reconhece o crime organizado transnacional e a cibercriminalidade como principais ameaças à segurança nacional (como global).

O C.E.D.N é um instrumento indispensável para a resposta às (novas) ameaças da segurança nacional. Define "...os aspetos fundamentais da estratégia global a adotar pelo Estado para a consecução dos objetivos da política de segurança e defesa nacional." [68]

Uma das principais ameaças levantadas pelo C.E.D.N é a Criminalidade Transnacional Organizada e a Cibercriminalidade, como podemos verificar no seu Cap.III, no ponto 3.2 - "Principais riscos e ameaças à segurança nacional".

A criminalidade organizada devido à sua "...posição geográfica de Portugal como fronteira exterior da UE e o vasto espaço aéreo e marítimo sob sua jurisdição lhe impõem particulares responsabilidades" [69].

A cibercriminalidade é considerada "...uma ameaça crescente a infraestruturas críticas, em que potenciais agressores (terroristas, criminalidade organizada, Estados ou indivíduos isolados) podem fazer colapsar a estrutura tecnológica de uma organização social moderna" [70].

[68] C.E.D.N - p. 9;
[69] C.E.D.N - p. 22;
[70] C.E.D.N - p. 22;

As ações estratégicas adoptadas pelo C.E.D.N, para o combate ao **Crime Organizado Transnacional** são as seguintes [71]:

- Reforçar a cooperação internacional;
- Melhorar a capacidade de prevenção e combate (ao crime organizado;
- Aperfeiçoar os mecanismos de coordenação (entre as entidades de organismos competentes).

Dando especial prioridade às Ações de [72]:

- Fiscalização, "...de medidas fiscais e fiscalizadoras rigorosas, procurando dificultar a lavagem de dinheiro...através de uma estratégia económica…" [73];
- Detecção e rastreio do tráfico de droga sob jurisdição nacional (aéreo e marítimo) "através do combate e destruição de áreas de produção de estupefacientes…" [74]; e
- Combate às redes de imigração clandestina e do tráfico de seres humanos, "...e o apoio adicional à polícia de fronteiras para impedir a entrada de imigrantes clandestinos." [75].

No caso da **Cibercriminalidade,** as linhas de ação prioritárias adoptadas pelo C.E.D.N, são as seguintes [76]:

[71] C.E.D.N - p. 46;
[72] C.E.D.N - p. 46;
[73] Garcia, F. (2019) - p.188;
[74] Garcia, F. (2019) - p.188;
[75] Garcia, F. (2019) - p.188;
[76] C.E.D.N - p. 46;

- "Garantir a proteção das infraestruturas de informação críticas, através da criação de um Sistema de Proteção da Infraestrutura de Informação Nacional (SPIIN);
- Definir uma Estratégia Nacional de Cibersegurança;
- Montar a estrutura responsável pela cibersegurança, através da criação dos órgãos técnicos necessários;
- Sensibilizar os operadores públicos e privados para a natureza crítica da segurança informática e levantar a capacidade de ciberdefesa nacional".

Tendo Portugal estas características, mais fundamental se mostra a necessidade da cooperação das forças de segurança a nível nacional como transnacional.
Uma das formas criadas pela União Europeia, mais eficazes de combate da criminalidade organizada e a cibercriminalidade é a cooperação entre a Europol e os órgãos policiais competentes de cada Estado-Membro.
Tal cooperação policial, tem de ser efetuada de forma a prevenir e a perceber o funcionamento deste tipo de crimes.
Através da confiança mútua e da partilha de responsabilidades entre os Estados-Membros e a Europol, a União Europeia alcança a tão desejada Segurança Interna.

Conclusão

Creio que o tema elaborado por este trabalho seja extremamente complexo de travar por completo, isto porque, as suas características estão se sempre a inovar e as suas problemáticas dispersam-se por diversos campos.

A Comunidade Internacional enfrenta constantemente novas formas de criminalidade organizada e por consequência sofre uma diminuição da sua segurança. Em relação a estas novas formas de criminalidade organizada, dá-se especial relevância à cibercriminalidade, que atinge (na maior parte das vezes, de uma forma discreta) uma sociedade em vários pontos críticos como a política, a economia, o próprio Estado, ou seja, a sociedade como um todo.

A história já nos mostrou a dimensão da ameaça e das possíveis consequências advindas deste tipo de criminalidade.

Apesar dos Estados-Membros serem os primeiros responsáveis pela sua segurança, estas ameaças originárias do crime organizado, exigem uma resposta eficaz e coordenada, que já não pode ser dada só pelo próprio Estado (atingido). Uma das formas criadas pelo Sistema Internacional, mais eficaz de combate à criminalidade organizada e os seus cibercrimes é a cooperação entre os órgãos policiais de cada Estado e as instituições e agências internacionais competentes. Como por exemplo o Centro Europeu da Cibercriminalidade. Tal cooperação policial, tem de ser efetuada de forma a prevenir e a perceber o funcionamento deste tipo de crimes.

Através da confiança mútua e da partilha de responsabilidades, alcança-se a tão desejada Segurança Internacional.

Referências Bibliográficas

- ABADINSKY, H. *Organized Crime,* 9th ed.. Belmont, CA: Wadsworth, 2010;
- APONTAMENTOS e Slides da 2ª e 3ª aula de Cibersegurança;
- BORGES, P. *O Crime Organizado.* São Paulo: Editora, 2002;
- BRAZ, J. *Cooperação Internacional na Luta contra o tráfico de droga.* In Revista Polícia e Justiça, Janeiro/Junho 2004 II série n.º 3. Lisboa: Instituto Superior de Polícia Judiciária e Ciências Criminais, 2004;
- BOSSARD, A. *Transnational Crime and Criminal Law*. Chicago: Office of International Criminal Justice, 1990;
- CARRIÓN, M. - *Cooperação Policial na União Europeia : protecção dos cidadão europeus contra o crime organizado internacional.* Europa: Novas Fronteiras Espaço de liberdade, segurança e justiça. 2005;
- CONKLIN, J. *Criminology, 10th* ed. Boston: Pearson, 2010;
- COUTO, A. *Elementos de Estratégia* – Apontamentos para um curso. Volume I. Lisboa: Instituto de Altos Estudos Militares, 1989;
- CORDEIRO, R. *"Ataques de DDOS, Medidas Preventivas"*, in Segurança e Defesa, Revista Trimestral, n.o21, Maio-Agosto 2012;

- DAVIN, J. A *Criminalidade Organizada Transnacional, A Cooperação Judiciária e Policial na UE*, 2ª edição revista e aumentada, Almedina, Novembro. 2007;
- LOURENÇO, N. Segurança, *Sentimento de Insegurança e Estado de Direito. O espectro axial da relação de direitos, liberdades e garantias e poderes de Estado.* Em: Liberdade e Segurança. Lisboa: Ministério da Administração Interna, 2009;
- GARCIA, F. *A Guerra e Estratégia Revisitadas*. Lisboa: Universidade Católica, 2019;
- GIBSON, W. *Neuromancer*, HarperCollins, 1984;
- GARCIA, M; LOURENÇO, M. *Direito da Informática, 2a Ed.* Coimbra. Almedina, 2011;
- NOGUEIRA, J. *Pensar a Segurança e Defesa*. Instituto da Defesa Nacional. Lisboa: Edições Cosmo, 2005;
- SANTOS, P; BESSA, R; PIMENTEL, C. *Cyberwar – O Fenómeno, as Tecnologias e os Actores.* Lisboa: FCA – Editora Informática, 2008;
- VALENTE, M. *Teoria Geral do Direito Policial. 2ª Ed*. Coimbra: Almedina, 2009.
- VERDELHO, P; BRAVO, R; ROCHA, M. *Leis do Cibercrime Volume 1.* Lisboa. 2003;
- YAR, M. *Cybercrime and Society. 2ªEd*. London. 2006.

Webgrafia

- Acórdão do STJ de 11/12/2009, Proc. nº 200/06.0JAPTM.E1.S1: http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/a553479b09d64bf0802576880033961a?OpenDocument
- APAV Cibercrime: https://apav.pt/cibercrime/
- Conceito Estratégico de Defesa Nacional: https://www.idn.gov.pt/conteudos/documentos/CEDN_2013.pdf
- Comunicação da Comissão ao Parlamento Europeu e ao Conselho: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52010DC0673&from=PT
- Comunicação da Comissão do Comissão da U.E (Rumo a uma política geral de luta contra o cibercrime): https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=LEGISSUM:l14560&from=EN
- Convenção da ONU contra a Criminalidade Organizada: Transnacional: http://gddc.ministeriopublico.pt/sites/default/files/documentos/instrumentos/convencao_nu_criminalidade_organizada_transnacional.pdf
- Decisão-Quadro 2008/841/JAI do Conselho da U.E: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32008F0841&from=EN
- Definição de ORTMEIER: http://www.organized-crime.de/organizedcrimedefinitions.htm

- Discurso de Abertura do Ex-Secretário-Geral da O.N.U: http://www.unodc.org/unodc/en/about-unodc/speeches/speech_2000-12-12_1.html

- Entrevista do Eng LINO Santos à Renascença: https://rr.sapo.pt/2019/06/27/pais/ciberataques-em-portugal-a-questao-nao-e-saber-se-vai-acontecer-mas-quando/noticia/155956/

- ESCORREGA, L. (Nº 2491/2192 - Agosto/Setembro de 2009). *A segurança e os "novos" riscos e ameaças: perspectivas várias*. Revista Militar: Revista mihttps://www.revistamilitar.pt/artigo/499

- Estratégia Nacional de Segurança do Ciberespaço: https://www.cncs.gov.pt/content/files/rcm_36-2015.pdf

- Lei n.º 5/2002 de 11 de Janeiro - Medidas de combate à criminalidade organizada: http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=147&tabela=leis

- SANTOS, Lino (2015). "*Regulação do ciberespaço: cesuristas e tradicionalistas*". *JANUS.NET e-journal of International Relations*, Vol. 6, N.o 1, Maio-Outubro 2015: observare.ual.pt/janus.net/pt_vol6_n1_art6

- Projecto de conclusões do Conselho sobre o desenvolvimento de uma Estratégia de Segurança Interna da U.E renovada: http://data.consilium.europa.eu/doc/document/ST-15670-2014-INIT/pt/pdf

- RAMALHO, D. *A Investigação Criminal na Dark Web,* in Revista de concorrência e regulação, Coimbra, a.4n.14-15, Abr.-Set.2013 (download do PDF): https://www.academia.edu/31146150/A_investigação_criminal_na_Dark_Web

- Relatório da O.N.U (2004) - *A more secure world: our shared responsibility:* https://documents-dds-ny.un.org/doc/UNDOC/GEN/N04/602/31/PDF/N0460231.pdf?OpenElement

- Regulamento (UE) 2016/794: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0794&from=pt

- UNODC, United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime,* Draft, February 2013, United Nation, New York, 2013: https://www.unodc.org/documents/organized-crime/cybercrime/CYBERCRIME_STUDY_210213.pdf