O Crime Organizado e as Novas Tecnologias: uma Faca de Dois Gumes

Helena Carrapiço
Investigadora no Instituto da Defesa Nacional. Doutoranda no Instituto Universitário Europeu, Florença.

Resumo

O benefício que determinados Estados retiram das novas tecnologias é incalculável. Contudo, não são os únicos a tirar partido dessas vantagens. O crime organizado, e em especial o cibercrime, aproveita as vulnerabilidades dos sistemas de informação, em que as nossas sociedades estão baseadas, para lucro próprio. Apesar dos conhecimentos que já possuímos sobre este tipo de criminalidade, os nossos esforços não têm conseguido travar o número crescente de ataques cibernautas, nem evitar o aumento das perdas das empresas e dos particulares. Não devemos, no entanto, cair no erro pessimista de pensar que não existe nenhuma forma eficiente de combater o cibercrime. Existe todavia, muito trabalho por desenvolver. Desde a consciencialização da população, para os perigos inerentes à Internet, até à formação de recursos humanos mais qualificados, passando pela investigação e a cooperação entre sectores, há sem dúvida muito ainda por fazer. Adoptámos as novas tecnologias, resta-nos agora aceitar por completo as responsabilidades que elas acarretam.

Abstract

Numerous States have largely benefited from new technologies. They are, however, not the only one to have done so. Organized Crime, and cibercrime in particular, have also taken advantage of the vulnerabilities of the information system – which constitutes the basis for the functioning of our societies – for their own profit. Although we have managed to gather a considerable amount of knowledge concerning this issue, our efforts have been unsuccessful in controlling the growing number of cyber-attacks and their consequent losses for companies and individuals. Nevertheless, we should not adopt the pessimistic view, according to which there is no efficient way to handle this type of criminality. Naturally, much work remains to be developed: populations have to become more aware of the dangers related to Internet and its consequences; there is a growing need for skilled technicians; research lacks real investment; and the different sectors of society have to deepen their cooperation. After promptly embracing all the benefits that new technologies could foster, we are now confronted with the fact of having to accept, as well, its negative consequences.

Introdução

O crime organizado não é um fenómeno recente, mas a sua constante capacidade de adaptação e de sobrevivência permitiu-lhe acompanhar as mudanças das sociedades, alterando a sua forma e os seus métodos. Tendo mantido o lucro como objectivo principal, o crime organizado está já longe da imagem do tradicional *gangster* dos filmes americanos. Aprendeu a dominar as novas tecnologias e a utilizá-las a seu favor, facilitando assim o desenvolvimento das suas actividades ilícitas. A evolução das comunicações permitiu-lhe actuar à distância e estabelecer contactos a nível internacional, enquanto que a informática possibilitou a criação de novos métodos e, até, de novos tipos de crime. À medida que as sociedades foram integrando tecnologias inovadoras no seu quotidiano, foram-se criando igualmente novas fragilidades: estes avanços tecnológicos tornaram-se indispensáveis para o bom funcionamento das instituições-chave dos países, assim como para o dia-a-dia dos cidadãos. Neste sentido, e tendo em consideração que o acesso aos conhecimentos e materiais informáticos é cada vez mais fácil, a possibilidade das sociedades virem a ser vítimas do seu próprio progresso deve ser considerada com alguma seriedade. Da mesma forma, como estas criaram os instrumentos para melhorar a qualidade de vida dos seus cidadãos, forneceram ao crime organizado e ao terrorismo as capacidades para as destruírem.

Contudo, e tal como veremos ao longo deste artigo, a tecnologia é uma faca de dois gumes: se pode ser manipulada no âmbito de actividades ilícitas, também pode ser utilizada para combater estas últimas. Por forma a demonstrar este pressuposto, iremos tentar compreender, em primeiro lugar, o que é o crime organizado e quais as suas formas de actuação mais tradicionais, para em seguida analisarmos em maior detalhe a forma como as novas tecnologias influenciaram a sua evolução. Por fim, pretende-se referir alguns dos esforços desenvolvidos no sentido de controlar este problema, nomeadamente o papel que a tecnologia pode ter no combate ao crime organizado, assim como reflectir sobre o que resta ainda fazer.

I – Definição e Caracterização do Crime Organizado

O fenómeno do crime organizado é alvo de estudo de numerosas obras, sendo algumas mais fictícias do que outras. Dado que se trata de uma área em que é difícil fazer a distinção entre as informações verdadeiras e as falsas, e onde as obras com

rigor científico são raras, optou-se por basear este trabalho nas definições oficiais das Nações Unidas e da União Europeia. De acordo com esta última, "a Criminal Organization means a structured association, established over a period of time, of 2 or more persons, acting in a concerted manner with a view to committing offences which are punishable by deprivation of liberty or a detention order (...) whether such offences are an end in themselves or a means of obtaining material benefits and, where appropriate, of improperly influencing the operation of public authorities"[1]. A descrição das Nações Unidas, embora apresente algumas diferenças, segue as mesmas linhas gerais: "a group activities of 3 or more persons, with hierarchical links or personal relationships, which permit their leaders to earn profits or control territories or markets, internal or foreign, by means of violence, intimidation or corruption, both in furtherance of criminal activity and in order to infiltrate the legitimate economy"[2].

A partir destas duas definições, é já possível destacar um conjunto de características que têm surgido, de forma recorrente, na literatura sobre este tema. Em primeiro lugar, é de realçar a dedicação a actividades que são ilegais; actividades estas, que são levadas a cabo por mais do que um indivíduo com o intuito de obter lucro[3]. Outra característica importante reside na organização interna destes grupos, descrita como hierarquicamente definida e estruturalmente semelhante à de uma empresa. Desta forma, obtêm a flexibilidade necessária à sua constante adaptação e expansão da sua actividade a novas áreas geográficas e mercados. Ainda no que diz respeito à caracterização deste fenómeno, será relevante sublinhar a questão dos métodos utilizados. Estes têm como principal objectivo destruir os obstáculos à actividade criminosa e passam habitualmente pelo uso de violência selectiva ou de outros meios de intimidação, assim como pelo exercício de influência na política, nos média, na economia e no meio judicial.

Apesar de existirem numerosas teorias relativamente ao aparecimento do crime organizado, e mais recentemente do crime organizado transnacional, é possível apontar-se elementos comuns aos vários autores. Sabe-se, por exemplo, que este fenómeno teve a sua origem em pequenos grupos de tipo gang ou clã, de base étnica, nacional ou familiar[4].

1 Joint Action 98/733/JHA of 21 December 1998, adoptada pelo Conselho com base no artigo K.3 do Tratado da União Europeia; http://europa.eu.int/scadplus/leg/en/lvb/133077.htm

2 United Nations Convention on Transnational Organised Crime (entry into force 29th September 2003).

3 A obtenção de lucro como objectivo primordial do crime organizado é uma característica extremamente relevante para alguns autores, como David Whittaker e Bruce Hoffman, que consideram ser essa a diferença fundamental relativamente aos grupos terroristas.

4 Ingeborg Schroeder, Transnational Organised Crime, Illicit Trade and European Security in Illicit Trade and Organised Crime – new threats to economic security? p. 82.

Graças ao desenvolvimento de um contexto muito específico, esses grupos puderam tornar-se mais sólidos e expandir a sua actividade. As mudanças políticas, económicas, sociais, jurídicas e tecnológicas que o mundo sofreu nos últimos anos constituem uma parte fulcral desse contexto. Tomemos o exemplo da União Europeia: no que diz respeito às primeiras alterações, é de sublinhar, nomeadamente, a desagregação da União Soviética e a consequente degradação das condições de vida nessa região. Naturalmente, o crime organizado que opera na Europa não vem apenas de Leste. Neste sentido, é igualmente relevante tomar em consideração as medidas políticas da União Europeia relativamente à redução das barreiras dentro do espaço europeu. Da mesma forma, não é possível compreendermos o crescimento exponencial deste fenómeno, nesta área geográfica, se não analisarmos igualmente outros factores como a crise de valores nas democracias europeias e a desilusão com a classe política, os quais poderão estar na origem de sociedades menos reactivas em relação à corrupção e ao crime. No que diz respeito às mudanças económicas, é importante referir o aumento drástico das trocas comerciais e da globalização da economia. Com o acesso facilitado a novos mercados, o crime organizado foi gradualmente adquirindo métodos mais profissionais e evoluindo para formas mais complexas (como é o caso do crime organizado transnacional). O resultado desta mutação traduziu-se numa maior dificuldade em detectar as actividades ilegais e em controlar os movimentos dos grupos em questão. Novamente, o Mercado Único surge como um bom exemplo da expansão da disrupção provocada pelo crime organizado. A nível das mudanças sociais, a crescente mobilidade dos cidadãos veio permitir um maior número de contactos a nível internacional e facilitar a exportação das actividades ilícitas para outros países. Ligadas a esta evolução estão também as alterações tecnológicas, em especial nos meios de transporte e de comunicação, que possibilitaram a adopção de métodos de actuação mais sofisticados e anónimos. Por fim, é ainda de mencionar que as mudanças jurídicas também influenciam a actuação do crime organizado, na medida em que este tira partido das diferenças, ainda acentuadas, entre as legislações nacionais.

No que diz respeito às actividades desenvolvidas, é possível observar a existência de, pelo menos, seis áreas distintas: o narcotráfico, os crimes financeiros, o tráfico de seres humanos, a ajuda à imigração, os crimes tecnológicos e o tráfico diverso. De entre estes sectores, o da droga será de longe o mais lucrativo, apresentando um lucro estimado pelas Nações Unidas em 400 biliões de dólares por ano[5]. Seguem-se o tráfico de seres

5 United Nations Office for Drug Control and Crime Prevention, World Drug Report 2000, Oxford University press, Oxford, p. 55.

humanos e o apoio à imigração ilegal. Embora por vezes estreitamente ligadas, estas duas actividades devem ser claramente distinguidas: se a segunda se pode definir como uma prestação de serviços a indivíduos, a primeira implica a existência de uma vítima. De acordo com a Casa Branca, "trafficking in persons is often related to organized crime, and the profits from trafficking entreprises help fuel other illegal activities"[6]. Os crimes financeiros estão classificados como uma actividade de tipo clássico, embora o relatório da Europol de 2004 chame a atenção para o facto de estarem actualmente em franco crescimento devido à utilização de novas tecnologias[7]. No sector do tráfico diverso é possível enquadrar actividades desde o contrabando de bebidas alcoólicas e de tabaco, ao tráfico de armas, passando pelo roubo de veículos. Na conjuntura actual, uma das maiores preocupações é naturalmente a circulação de armas e a sua potencial compra por parte de grupos terroristas. Tendo em consideração o tema deste trabalho, os crimes tecnológicos serão analisados em maior detalhe numa segunda parte.

Ao fazer uma retrospectiva dos últimos anos, e tal como foi mencionado na introdução, é possível afirmar que houve uma evolução do crime organizado no sentido de este se adaptar às mudanças do ambiente político, económico, social, legal e tecnológico em que se encontra. Paralelamente, também se pode observar uma diversificação da panóplia de actividades desenvolvidas. Diversificação esta que passa, não só pela escolha de outras actividades ilegais, mas também pelo desenvolvimento de negócios lícitos com o objectivo de branquear capitais. Ao alcançar um nível de poder antes reservado exclusivamente a Estados, este fenómeno adquiriu a capacidade de desestabilizar económica, social e politicamente os países onde opera. Consequentemente, o crime organizado deixou de ser um simples problema da economia de mercado para passar a ser uma ameaça que diz respeito à sobrevivência dos próprios países e dos seus cidadãos.

II – A influência das novas tecnologias na actuação do crime organizado

As oportunidades criadas pelas novas tecnologias permitiram às sociedades em geral, e ao comércio em particular, melhorar as suas capacidades e reduzir os seus custos. As últimas décadas representaram um avanço extraordinário na área das tecno-

6 The White House, Fact Sheet: trafficking in Persons National Security Presidential Directive, February 25th 2003, http://usinfo.state.gov/topical/global/traffic/03022502.htm

7 2004 EU Organised Crime Report, Europol.

logias de informação e telecomunicações, o que levou a uma maior aproximação dos indivíduos e a uma alteração da forma como estes interagem. Actualmente, a quase totalidade das sociedades ocidentais funciona com base em sistemas de informação, que são utilizados nas mais variadas áreas. Contudo, da mesma forma como as trocas lícitas foram beneficiadas, não devemos esquecer que também as ilegais foram favorecidas com esta evolução: "comme toute invention humaine porteuse de progrès, elle engendre dês comportements déviants et une nouvelle forme de délinquance: la cybercriminalité"[8].

A enorme capacidade de adaptação do crime organizado permitiu-lhe tirar partido do progresso tecnológico, tendo-se tornado até um dos seus principais beneficiários. O desenvolvimento em áreas como as comunicações, os transportes e o ciberespaço aumentaram de forma exponencial o campo em que estes grupos podem operar: "the spread of e-business and the possibility of creating so-called virtual identities facilitates and obscures criminal activities and actors by providing anonymity"[9]. Outra consequência relevante é a constituição de parcerias e a cooperação entre grupos de crime organizado de diferentes regiões do globo: "rather than treat each other as rivals, many criminal organizations are sharing information, services, resources, and market access according to the principle of comparitive advantage. By doing so, they can reduce their risks and costs and are better able to exploit illicit criminal opportunities"[10]. Para além deste aspecto, as inovações tecnológicas a nível de software e de impressão permitiram ainda melhorar a produção de moeda, documentos falsos e até cartões de crédito. Como é possível observar, o conceito de novas tecnologias é extremamente abrangente, não se esgotando apenas no campo de actuação do chamado cibercrime ou crime de alta tecnologia. No entanto, parece-nos indicado colocar a ênfase desta segunda parte neste último, tendo em consideração a ameaça que este representa para o estilo de vida das nossas sociedades.

O cibercrime é a denominação dada a um conjunto específico de crimes relacionados com a utilização de computadores e de redes informáticas. Esta expressão pode igualmente ser empregue no que refere à facilitação de actividades ilegais tradicionais através do recurso a meios informáticos. De acordo com o Conselho da Europa, o cibercrime pode ser definido como "criminal activity including offences against computer data and systems, computer-related offences, content offences and copyright offences"[11]. Outra definição, mais completa, poderá ser encontrada no recente artigo do General Claude

8 Claude DeChamps, Cybercriminalité, in Defense Nationale, Avril 2005, p. 99.
9 2004 EU Organised Crime Report, Europol.
10 US Government Interagency Working Group, International Crime Threat Assessment, 2000.
11 Council of Europe, Cybercrime Treaty, EST nº185.

DeChamps: "la cybercriminalité est un terme générique qui peut se definir comme l'ensemble des exactions commises par un moyen lié aux nouvelles Technologies, principalement Internet, permettant par réseau filaire, hertzien ou satellite, de voler, détourner, paralyser, contrefaire, modifier, détruire des données ou se procurer, diffuser et échanger des contenus illégaux"[12]. Neste sentido, podem ser identificados três tipos principais de cibercrime: actividades contra indivíduos, contra a propriedade e contra o Estado.

No que diz respeito ao primeiro género, a pornografia, nomeadamente a infantil, será sem dúvida a questão mais premente. A proliferação de *sites Internet* contendo imagens e vídeos de crianças é uma ameaça crescente na União Europeia, especialmente dada a evolução dos sistemas de pagamento electrónicos que permitem, cada vez mais, manter o anonimato, quer do comprador, quer do fornecedor: "le caractére virtuel des échanges sur l'*Internet* et le semblant d'anonymat favorisent le franchissement des barrières de l'illégalité, les internautes pensant que les normes morales ou légales du monde réel ne s'appliquent pas dans ce cyberespace"[13]. Existe um aumento dos casos de aliciamento de menores através de salas de conversação virtuais, onde estes não estão protegidos contra a possibilidade de serem abordados por pedófilos ou outro tipo de criminosos: "As noted by the FBI, chat rooms may also provide the pedophile with na anonymous means of identifying and recruiting children"[14]. As vítimas costumam ter uma média de idades que ronda os 13 – embora seja cada vez mais frequente o aparecimento de casos envolvendo crianças mais novas – sendo a sua maioria angariada junto de jovens sem abrigo. De acordo com o relatório da Europol de 2004, a grande maioria das vítimas e do material ilegal que circula no interior da UE é originário dos países da antiga União Soviética, do Sul-Este da Ásia e da América do Sul. Outros países de destino como o Canadá e os Estados Unidos não diferem muito quanto à origem das crianças em questão. O tráfico de mulheres, que tem como objectivo a prostituição forçada ou a escravatura, é igualmente fonte de séria preocupação. As novas tecnologias têm também um papel preponderante na angariação de indivíduos para estes fins. Numerosos homens e mulheres são levados a acreditar que irão aceder a melhores mercados de trabalho e a um nível de vida com que sempre sonharam, sendo posteriormente arrastados para esquemas de prostituição e violência.

12 Claude DeChamps, Cybercriminalité, in Defense Nationale, Avril 2005, p. 100.
13 Idem.
14 Jay Albanese, Commercial Sexual Exploitation of Children, in Transnational Crime, International Studies in Social Sciences, Sitter Publications, 2005.

Os crimes contra indivíduos incluem ainda a extorsão, a fraude e o assédio, sendo que qualquer uma destas três actividades pode ser realizada facilmente através da Internet e de correio electrónico. Será ainda relevante mencionar um último tipo de crime contra o indivíduo, o do roubo de dados pessoais: "defined as the unauthorized collection and use of personal information, usually for criminal purposes. […] The criminal assumes the victim's identity to take advantage of his or her established credit rating"[15]. Os casos mais comuns estão ligados a pagamentos electrónicos efectuados através de canais pouco seguros, resultando na captura de informações que poderão ser utilizadas, posteriormente, no financiamento de operações criminosas. Outro método recente, já utilizado em larga escala para a obtenção de dados relativos a cartões de crédito, consiste no envio de mensagens através de correio electrónico. Numa tentativa de se fazer passar por uma entidade bancária, o crime organizado pede aos destinatários das mensagens determinadas informações, alegando estar a proceder a uma reestruturação dos sistemas informáticos. De acordo com a Comissão Federal de Comércio Norte-Americana, das 516,740 queixas apresentadas por cidadãos em 2003, 41% corresponderam a roubo de dados pessoais[16].

Tal como já foi referido, o segundo tipo de cibercrime tem como objectivo atentar contra a propriedade. Embora seja possível apontar inúmeras actividades passíveis de serem desenvolvidas neste âmbito, optou-se por se referir apenas as principais: o vandalismo informático e a intercepção de dados. Esta última actividade inclui o desvio de informações comerciais e crimes financeiros, dos quais as empresas são geralmente as vítimas mais comuns. Segundo inquéritos realizados a empresas americanas pelo Computer Security Institute do Federal Bureau of Investigation, foram relatadas perdas nos Estados Unidos, com origem em cibercrime, de $124 milhões em 1999. Este número tem vindo a subir gradualmente, tendo atingido os $266 milhões, em 2000, e os $378 milhões em 2001[17]. Este crescimento deve-se, nomeadamente, ao facto deste tipo de crime ser facilmente posto em prática, de ser acessível a um número importante de indivíduos e da aplicação das legislações, quer nacionais, quer internacionais, ser extremamente insuficiente. No que diz respeito ao primeiro tipo de actividade, o

15 Criminal Intelligence Service Canada, Technology and Crime, 2001, p. 3, http://www.cisc.gc.ca/AnnualReport2001/Cisc2001/technology2001.html

16 Tony Aeilts, Defending Against Cybercrime and Terrorism: a new role for universities, FBI Law Enforcement Bulletin, Jan. 2005.

17 Dorothy E. Denning, "Information, Technology and Security", in Grave New World, Edited by Michael E. Brown, p. 93.

vandalismo informático, este consiste na propagação de vírus susceptíveis de danificar seriamente os computadores e os site Internet visados: "many attacks are extremely costly. According to Computer Economics of Carlsbad, California, the *ILOVEYOU* virus and its variants, which crippled computers in May 2000, were estimated to have cost $8.5 billion in damages, vastly exceeding the damages from any previous virus"[18]. É importante sublinhar que para além de provocar danos directos às suas vítimas, este tipo de ataque também constitui uma ameaça à economia global no sentido em que mina a confiança pública no comércio electrónico e nas novas tecnologias em geral. É, no entanto, curioso observar que nem o vandalismo informático, nem a intercepção de dados constam da lista de ameaças do mais recente relatório da Europol sobre crime organizado.

Os Estados podem igualmente ser vítimas de vandalismo informático, de fraude ou de intercepção de dados, pois o processo utilizado é exactamente o mesmo. Tal como foi referido na primeira parte, o crime organizado interessa-se tradicionalmente pelo lucro e não por questões políticas. Qual o seu interesse, então, em atacar Estados? É verdade que os Estados têm recursos financeiros que podem ser mais aliciantes que os dos indivíduos; contudo, estes constituem apenas uma parte das motivações do crime organizado. O factor mais importante reside no facto dos governos disporem de informações preciosas que, se interceptadas, podem ser uma mais-valia para outros Estados ou terroristas, mais-valia esta, que se traduz em remunerações extremamente elevadas. Contudo, o acto de visar Estados acarreta consequências muito diferentes. Um ataque dirigido contra uma instituição governamental, civil ou militar, pode afectar gravemente a segurança nacional, especialmente se estiverem em causa informações confidenciais. O exemplo apresentado por Dorothy E. Denning no seu artigo é revelador: "Before and during the Gulf War, [...] hackers from the Netherlands penetrated computer systems at thirty-four American military sites on the Internet, including sites that were directly supporting Operations Desert Storm and Desert Shield. They browsed through files and obtained information about the exact location of US troops, the types of weapons they had, the capabilities of the Patriot missile, and the movement of American warships in the gulf region"[19]. Este episódio, que mais parece saído de um filme, é, no entanto, apenas uma pequena parte da realidade. Segundo a Joint Task Force Computer Network Operations do Departamento da Defesa Americano, o número de tentativas para entrar

18 Idem.

19 Dorothy E. Denning, "Information, Technology and Security", in Grave New World, Edited by Michael E. Brown, p. 95.

no sistema deste último, em 2000, foi de 28 106, das quais 369 foram bem sucedidas[20]. Um ataque deste tipo a infra-estruturas chave de um Estado (central eléctrica ou rede de distribuição da água) teria, portanto, consequências devastadoras para toda a sua população. Naturalmente, tentativas como esta não são comuns, mas só o facto de esta possibilidade existir leva-nos a reflectir seriamente sobre o nosso nível de preparação para fazer frente a esta ameaça.

III – O papel das novas tecnologias na luta contra o crime organizado

O ciberespaço e, em especial a Internet, são habitualmente encarados como um mundo virtual sem ligação ao real, com um espaço e um tempo próprios, sem fronteiras nem regras e, consequentemente, sem segurança. Esta visão, embora tenha alguns traços de verdade, não é totalmente correcta. Os pontos de acesso a este mundo virtual, os computadores, têm uma existência física e como tal podem ser controlados de determinadas formas. No entanto, seria alimentar uma falsa esperança pensar-se que é possível vencer o crime organizado, de forma definitiva, no campo da informática. Nenhum sistema é totalmente inviolável e, como tal, existe sempre a possibilidade de alguém o poder aceder: "The bottom line is that we will never have secure systems. The underlying technology will always have vulnerabilities and people will always make mistakes. […] Thus an important component of any security program is the capability to detect and respond to security breaches that do occur"[21]. Tendo em consideração estas duas visões, analisemos quais as possíveis estratégias de combate ao crime organizado.

De acordo com Dorothy E. Denning, a capacidade reactiva das autoridades é um dos seus poucos meios de acção para fazer frente a futuros ataques. Na sequência de uma brecha na segurança de um sistema, é desenvolvido um outro mais avançado, em que as fragilidades do anterior são colmatadas. Seguem-se novas tentativas, por parte do crime organizado, para aceder ao sistema desejado. Assim que este é penetrado, as autoridades voltam a concentrar os seus esforços para melhorar os pontos fracos,

20 Defense Information and Electronics Report, JTF-CNO Battles Surging Tide of More Destructive Computer Attaks, 7 de Set. 2001, http://delphi.dia.ic.gov/admin/EARLYBIRD/010910/s20010910jjtf.htm

21 Dorothy E. Denning, "Information, Technology and Security", in Grave New World, Edited by Michael E. Brown, p. 102.

criando-se, desta forma, um círculo vicioso. O problema da capacidade reactiva é, tal como o seu nome o indica, o facto de ser posterior à acção ilegal e, portanto, de não ser capaz nem de a prever, nem de a evitar. Esta asserção leva-nos a questionar-nos se não será realmente possível fazer mais a nível preventivo. Contrariamente a Dorothy E. Denning, Peter Grabosky do Australian Institute of Criminology defende que sim, que as tecnologias de vigilância, detecção e bloqueio podem ser uma grande mais-valia neste campo[22]. Da mesma forma como passaram a existir, por exemplo, detectores de metais nos aeroportos, deverão ser cada vez mais comuns os mecanismos de prevenção da criminalidade no ciberespaço. Nos últimos anos, tem-se desenvolvido toda uma indústria dedicada a esta área: criptografia, biometria, programas antivírus e bloqueadores de intrusos, têm custos cada vez mais acessíveis ao cidadão comum, cuja consciência do problema parece estar a aumentar. A vigilância é outro aspecto da prevenção no qual as autoridades têm investido de forma considerável. Perante a actual situação, os serviços de segurança nacionais optaram por formar agentes cuja única função é patrulhar a Internet, permitindo assim a detecção de pornografia infantil ou de outro tipo de actividade ilegal. Outra aplicação das novas tecnologias no combate contra o cibercrime é a utilização da Internet como canal de comunicação privilegiado entre a população e as autoridades. Estas últimas podem agora mais facilmente fazer passar mensagens relevantes sobre vírus em expansão ou informar os indivíduos sobre a quem recorrer em caso de serem vítimas de crime. As populações têm igualmente a possibilidade de cooperar neste esforço através da denúncia de sites ilegais com os quais tenham deparado: "Online hotlines now facilitate the reporting of activities as diverse as fraud and child pornography"[23].

No que diz respeito ao enquadramento destas iniciativas, vários países têm vindo a desenvolver estratégias de combate ao cibercrime, dada a crescente preocupação com este problema. Os Membros do Conselho da Europa, por exemplo, desenvolveram uma convenção internacional apenas dedicada a este tema, cujo texto final foi assinado, por 26 países, a 23 de Novembro de 2001[24]. Estes países pretendiam, desta forma, encorajar uma abordagem comum a este tipo de crime. A União Europeia, por seu lado, deu igualmente um passo relevante neste campo ao adoptar o eEurope Action Plan 2002 e, posteriormente, o eEurope Action Plan 2005, ambos com o objectivo de desen-

22 Peter Grabosky, Technology & Crime, in Trends and Issues in Crime and Criminal Justice, nº78, January 1998.

23 Idem.

24 International Convention on Cyber Crime.

volver – com base numa infra-estrutura de informação segura – serviços públicos presentes na Internet, assim como um ambiente dinâmico para o comércio electrónico com acesso de banda larga, a preços competitivos[25]. Os Estados Unidos, por seu lado, têm vindo a desenvolver elementos mais especificamente no âmbito do combate ao cibercrime. Note-se, em especial, a criação do Protection Board (Outubro de 2001) – um órgão que coordena os programas de protecção dos sistemas de informação pertencentes às instituições vitais do país[26] – e do FBI's Cyber Crimes Program, que inclui iniciativas como o InfraGard, uma cooperação entre esta agência e o sector privado, e a **Innocent Images National Initiative, cujo objectivo é controlar os crimes sexuais informáticos contra crianças**. É ainda de sublinhar, apesar de já não ser recente (1997), a iniciativa do grupo G8 que consistiu na compilação de dez princípios a ser seguidos no combate ao crime de alta tecnologia e na proposta de um plano de acção com base nestes últimos. Este mesmo grupo de países está neste momento a analisar uma proposta conjunta da França, Irlanda, Suécia e Reino Unido sobre a retenção de dados relativos ao tráfico em geral.

Estas iniciativas têm sido, no entanto, ainda muito limitadas, sendo necessário desenvolver mais esforços por forma a garantir que as novas tecnologias possam evitar mais crimes do que facilitam. Neste sentido, propõe-se o seguinte conjunto de recomendações: em primeiro lugar, é necessário reconhecer que não existe ainda uma perfeita consciência, por parte do público em geral, dos perigos das novas tecnologias e, em especial da Internet. Muitos utilizadores são vítimas de crimes que poderiam ser facilmente evitados se estivessem correctamente informados: "The negative phenomenon of misusing information technologies is very often enabled by the lack of preparedness of the society for the ever more intensive linkage between ordinary activities and new technology"[27]. Por forma a colmatar esta falta, deverão ser investidos mais fundos em campanhas de alerta, tendo em atenção que um número crescente de cibernautas são adolescentes e até crianças. Essas campanhas deverão, contudo, ser bem adaptadas ao público-alvo para evitar cair-se no ridículo de produzir, por exemplo, brochuras informativas extremamente detalhadas para regiões com elevadas taxas de iliteracia. A responsabilidade pela divulgação da informação não deverá, no entanto, recair,

25 http://europa.eu.int/information_society/eeurope/2005/index_en.htm

26 Dorothy E. Denning, "Information, Technology and Security", in Grave New World, Edited by Michael E. Brown, p. 107.

27 Czech Ministry of the Interior, Strategy of Combating Crime in the Area of Information Technology, June 2001, Prague, p. 2. http://www.mvcr.cz/odbor/bezp_pol/english/dokument/konc_eng.html

como é habitual pensar, apenas nos ombros dos Estados. Só serão atingidos bons resultados se toda a sociedade se sentir envolvida neste processo, o que implica recorrer igualmente a empresas, instituições privadas não comerciais e até indivíduos. Aliás, a maioria dos especialistas informáticos não se encontra ao serviço do Estado (muito pelo contrário), sendo portanto uma mais-valia poder contar com o seu apoio.

Em segundo lugar, existe outra área em que a cooperação entre o sector privado e o sector público deveria ser reforçada: "One of the challenges [...] is that industry has been reluctant to share information out of concern for its confidentiality. In particular, companies are concerned that sensitive information provided voluntarily might not be adequatly protected"[28]. É necessário que as empresas compreendam que a segurança da sociedade deve estar acima dos seus interesses particulares e que um sistema de maior partilha de informações só as poderá beneficiar a longo termo. Naturalmente, esta cooperação deverá ser desenvolvida por forma a não sacrificar a competitividade das indústrias. É igualmente importante que tomem consciência da verdadeira capacidade policial neste campo, assim como da existência de respostas adequadas aos seus problemas. Muitas empresas evitam informar as autoridades de que foram vítimas de crimes de alta tecnologia pois não acreditam, por um lado, que estas estejam dotadas com os instrumentos necessários à resolução das ocorrências e, por outro, porque receiam que os seus casos sejam tratados com alguma ligeireza, levando assim a uma diminuição do seu prestígio junto do público: "consequently, agencies may not adequatly capture cyber-related crime statistics, and the gross impacto of this type of crime, generally, may appear understated"[29].

Por fim, deve ser referido o problema dos recursos humanos. Só é possível combater o cibercrime se houver especialistas em segurança informática. Por esta razão, deve ser incentivada (através, por exemplo, de bolsas) a entrada de jovens em cursos universitários e profissionais passíveis de lhes dar uma formação adequada. Ligadas a esta questão estão ainda o reduzido investimento na área da investigação, sem a qual não poderão surgir novas tecnologias menos vulneráveis, e a falta de material moderno nas instituições responsáveis pelo combate deste tipo de criminalidade. São já numerosos os autores que sugerem cooperações com instituições universitárias com vista, quer à obtenção de apoio especializado, quer como fonte de recrutamento para os seus

28 Dorothy E. Denning, "Information, Technology and Security", in Grave New World, Edited by Michael E. Brown, p. 108.

29 Tony Aeilts, Defending Against Cybercrime and Terrorism: a new role for universities, FBI Law Enforcement Bulletin, Jan. 2005, p. 16.

quadros: "law enforcement administrators should identify university faculty and staff as a significant training resource, as well as one in support of high-tech criminal investigations"[30].

Conclusão

O benefício que determinados Estados retiram das novas tecnologias é incalculável. Contudo, não são os únicos a tirar partido dessas vantagens. O crime organizado, e em especial, o cibercrime, aproveita as vulnerabilidades dos sistemas de informação, em que as nossas sociedades estão baseadas, para lucro próprio. Apesar dos conhecimentos que já possuímos sobre este tipo de criminalidade, os nossos esforços não têm conseguido travar o número crescente de ataques cibernautas, nem evitar o aumento das perdas das empresas e dos particulares. Não devemos, no entanto, cair no erro pessimista de pensar que não existe nenhuma forma eficiente de combater o cibercrime. Existe todavia, muito trabalho por desenvolver. Desde a consciencialização da população, para os perigos inerentes à Internet, até à formação de recursos humanos mais qualificados, passando pela investigação e a cooperação entre sectores, há sem dúvida muito ainda por fazer. Adoptámos as novas tecnologias, resta-nos agora aceitar por completo as responsabilidades que elas acarretam.

Bibliografia

Jay Albanese, *Commercial Sexual Exploitation of Children*, in *Transnational Crime*, International Studies in Social Sciences, Sitter Publications, 2005.

Barnett, N.; *The Criminal threat to Stability in the Balkans*, in Janes's Intelligence Review, Vol.14, number 4, April 2002.

Bauer, A. & Raufer, X.; *La Guerre ne fait que commencer*; Folio Documents; Gallimard; 2002.

Boniface, P.; *Les Guerres de Demain*; Editions du Seuil; 2001.

30 Tony Aeilts, Defending Against Cybercrime and Terrorism: a new role for universities, FBI Law Enforcement Bulletin, Jan. 2005, p. 17.

Brown, M. (editor); *Grave New World – Security Challenges in the 21st Century*; Georgetown University Press; Washington; 2003.

Cárter, F. & Tullett, T.; *The Sharp End – the fight against organised crime*; The Bodley Head London; 1988.

Conselho da Europa; *Cybercrime Treaty*, EST nº185.

Concelho da União Europeia; *EU Actions against Organised Crime in the Western Balkans*; Ref. 14768/03 CRIMORG 79; 2 de Dezembro de 2003; Bruxelas.

Courmont, B.; *L'emergence de nouveaux acteurs asymétriques*, in La Revue Internationale et Stratégique, nº51, automne 2003.

Criminal Intelligence Service Canada, *Technology and Crime*, 2001, p. 3
http://www.cisc.gc.ca/AnnualReport2001/Cisc2001/technology2001.html

Czech Ministry of the Interior, *Strategy of Combating Crime in the Area of Information Technology*, June 2001, Prague.
http://www.mvcr.cz/odbor/bezp_pol/english/dokument/konc_eng.html

DeChamps, C., *Cybercriminalité*, in Defense Nationale, Avril 2005.

Defense Information and Electronics Report, JTF – CNO Battles Surging Tide of More Destructive Computer Attaks, 7 de Set. 2001
http://delphi.dia.ic.gov/admin/EARLYBIRD/010910/s20010910jjtf.htm

Denning, D.; *Information, Technology and Security*, in *Grave New World*, Edited by Michael E. Brown.

Europol; *2003 EU Organised crime Report*; http://europa.eu.int.

Europol; *2004 EU Organised crime Report*; http://europa.eu.int.

Europol; *Trafficking of Human Beings: a Europol Perspective*; January 2004.

Europol; *Organised Illegal Immigration into the European Union*; January 2004.

Fiorentini, G. & Peltzman, S.; *The Economics of Organised Crime*; Centre for Economic Policy Research; Cambridge University Press; 1997.

Kaldor, M.; *New and Old Wars – organised violence in a global era*; Stanford University Press; 1998.

Galeotti, M.; *Albanian Gangs gain Foothold in European Crime undeworld*; in Jane's Intelligence Review; vol.13; number 11; Novembro de 2001.

Godson, R.; *Transnational Crime, Corruption and Security*, in *Grave New World – Security Challenges in the 21st Century*; 2003.

Grabosky, P.; *Technology & Crime*, in Trends and Issues in Crime and Criminal Justice, nº 78, January 1998.

Makarenko, T.; *Terrorism and Transnational Organised Crime: the emerging nexus*, in Paul Smith (ed), *Transnational Violence and Seams of Lawlessness in the Asia-Pacific: Linkages to Global Terrorism* (Hawaii: Asia Pacific Centre for Security Studies, Forthcoming). Disponível em www.st-andrews.ac.uk/academic/intrel/research/cstpv/pdffiles/APCSS%20%20**crime**%20terror%20contin.pdf

Makarenko, T.; *Tracing the Dynamics of the Illicit arms trade*, in Jane's Intelligence Review, September 2003.

Makarenko, T.; *A Model of terrorist-criminal relation*, in Jane's Intelligence Review, vol.15, nº8, Agosto 2003.

Margalho Carrilho, M. N. J.; *Narcotráfico e terrorismo* in Anais do Clube Militar Naval; 2001.

Nações Unidas, *United Nations Convention on Transnational Organised Crime*.

United Nations Office for Drug Control and Crime Prevention, *World Drug Report 2000;* Oxford University press; 2000.

Politi, A.; *Russian Organised and European Security* in *Illicit Trade and Organised Crime – New threats to economic security?*; European Commission-Directorate-General for External Relations; Office for Official Publications of the European Communities; 1998.

Pratt, A. N.; *Human Trafficking: the Nadir of an Unholy Trinity*; European Security; vol. 13; Spring-Summer 2004; numbers 1-2.

Proença Garcia, F. & Saraiva, M. F.; *O Fenómeno da Guerra no Novo Século – uma perspectiva*; Revista Negócios Estrangeiros; 2004.

Rotberg, R. (editor); *When States Fail – causes and consequences*; Princeton University Press; 2004.

Schmid, A. P.; *Links between terrorism and drug trafficking: a case of "narco-terrorism"*, in Turkish Policy Quaterly, vol.3, nº2, Summer 2004.

Schroeder, I.; *Transnational Organised Crime, Illicit Trade and European Security* in *Illicit Trade and Organised Crime – New threats to economic security?*; European Commission--Directorate-General for External Relations; Office for Official Publications of the European Communities; 1998.

Sum Tzu; The Art of War; Dover Publications; 2002.

US Government Interagency Working Group, *International Crime Threat Assessment*, 2000.

White, J. B.; *Uma Ameaça Diferente – Reflexões sobre a Guerra Irregular*; Military Review; Edição brasileira; 1st Quarter 2004.

Whittaker, D. (editor); The terrorism Reader; Routledge; 2001.

Referências Internet

Joint action 98/733/JHA of 21 December 1998, adoptada pelo Conselho com base no artigo K.3 do Tratado da União Europeia, http://europa.eu.int/scadplus/leg/en/lvb/l33077.htm

A common EU approach to the fight against organised transnational crime, http://europa.eu.int/comm/justice_home/fsj/crime/wai/fsj_crime_intro_en.htm

Justice and Home Affairs issues are an important feature of the Stabilisation and the Association Process. http://europa.eu.int/comm/justice_home/fsj/external/balkans/wai/fsj_external_balkans_en.htm

The White House, Fact Sheet: trafficking in Persons National Security Presidential Directive, February 25th 2003, http://usinfo.state.gov/topical/global/traffic/03022502.htm