Cibercrime

PETER GRABOSKY

Crimes relacionados aos computadores, como os crimes em geral, podem ser explicados pela conjugação de três fatores: motivação, oportunidade e ausência de efetiva vigilância e guarda. As motivações irão variar de acordo com a natureza do crime em questão, mas podem incluir ganância, desejo, vingança, desafio ou aventura. As oportunidades estão se expandindo rapidamente com a rápida proliferação e penetração da tecnologia digital. Desafios significativos são colocados pela natureza transnacional da maior parte dos crimes computacionais. As estratégias mais apropriadas para o controle dos crimes relacionados aos computadores compõem-se de soluções legais[1] (*law enforcement*), tecnológicas e oriundas do mercado (*market-based*). A busca de uma agenda estritamente sancionadora é, na maioria, não eficaz por causa da capacidade limitada do Estado. Excesso de regulação também pode obstruir o desenvolvimento comercial e tecnológico. Argumenta-se que, em alguns contextos, o mercado pode providenciar soluções mais efi-

1. *Law enforcement* é uma expressão de difícil tradução porque conjuga, no mínimo, dois conceitos: vigência (ou seja, existência válida de leis aprovadas) e eficácia (ou seja, o fato delas serem cumpridas). Também agrega, usualmente, a utilização de um sistema de justiça, que vai desde a vigilância policial até a punição dos infratores (N.T.).

cientes, para o problema dos crimes relacionados aos computadores, do que seriam as intervenções estatais.

Introdução

A teoria de que o crime é causado pela oportunidade estabeleceu-se fortemente na criminologia; redução das oportunidades se tornou um dos princípios fundamentais da prevenção ao crime. Mas há muito mais no crime do que oportunidade. O crime requer uma oferta de perpetradores motivados e uma ausência do que os criminólogos poderiam chamar de "vigilância capaz", ou seja, alguém para se preocupar com a loja, podemos dizer.

Estes princípios básicos da criminologia se aplicam aos crimes relacionados aos computadores não menos do que se aplicam ao roubo de bancos e furto de lojas. Eles aparecerão de tempos em tempos pela discussão que se segue. Nem todos estes fatores são amenizados pelo controle estatal, somente. Ocorre, entretanto, que uma variedade de instituições serão necessárias para controlar os crimes relacionados aos computadores.

Este artigo discute formas atuais e emergentes de ilegalidades relacionadas aos computadores. Analisam-se doze formas genéricas de ilegalidades envolvendo sistemas informacionais como instrumentos (meios) ou como alvos de crimes. Também discutem-se tópicos oriundos do alcance global dos sistemas informacionais. Tenta-se descrever os modos pelos quais os computadores, em sentido figurado, tornaram o mundo num lugar menor. O potencial para ofensas trans-jurisdicionais criará desafios formidáveis para a manutenção da lei (*law enforcement*). Para alguns crimes será necessária a busca de soluções alternativas.

As próximas páginas sugerirão que boa parte da ilegalidade relacionada aos computadores está além da atual capacidade de persecução judiciária (*law enforcement*) e regulatória de controle de órgãos isolados. E que a segurança no ciberespaço dependerá dos esforços de uma ampla gama de instituições e, também, de um grau

de auto-proteção das potenciais vítimas de cibercrime. Estes tópicos são explorados, com mais detalhes, em duas obras (GRABOSKY e SMITH, 1998; GRABOSKY, SMITH, DEMPSEY, 2001).

A conjunção ideal de instituições deve diferir, dependendo do crime em questão, mas provavelmente deve convergir com uma mistura de soluções de persecução judiciária (*law enforcement*), soluções tecnológicas e de mercado. Antes, porém, de iniciarmos uma revisão das várias formas de criminalidade envolvendo sistemas de informação como instrumentos e/ou alvos – e os meios mais apropriados de controlá-los – vamos analisar as questões de motivação e oportunidade.

1. Motivações dos criminosos informáticos

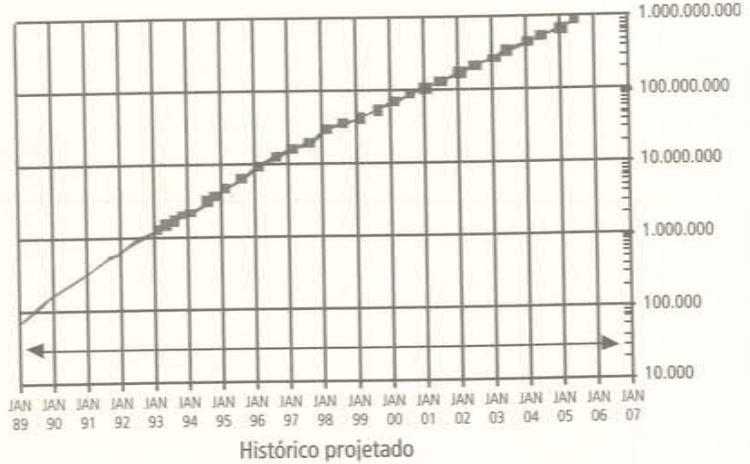
As motivações daqueles que cometem crimes relacionados aos computadores são diversas, mas dificilmente novas. Criminosos informáticos são impulsionados por motivações tradicionais. As mais óbvias delas são ganância, desejo, poder, aventura, busca por celebridade (ou notoriedade) e vontade de experimentar o "fruto proibido". O desejo de infligir perda ou dano no próximo. Ou, ainda, ideologia, quando algum se defronta com uma página eletrônica de uma instituição considerada por ele como detestável. Muito da atividade na "fronteira eletrônica" engloba um elemento de aventura, a exploração do desconhecido. O fato central de que algumas atividades no ciberspaço possam gerar reprovação oficial já é suficiente para atrair os desviantes, os rebeldes e os irredutivelmente curiosos. Considerado o grau de competência técnica requerida para cometer a maior parte dos crimes relacionados aos computadores, há uma outra dimensão motivacional digna de nota, aqui. Ela é, por certo, o desafio intelectual de dominar sistemas complexos.

Nenhuma destas motivações é nova. O elemento de novidade reside na capacidade, sem precedentes, da tecnologia de facilitar a ação em prol destas motivações.

2. Ampliando oportunidades para crimes relacionados aos computadores

Mudanças anteriores e recentes na tecnologia emergente da convergência de comunicações e computação são realmente de tirar o fôlego e, também, já têm um significativo impacto em muitos aspectos da vida. Operações bancárias e comerciais, controle de tráfego aéreo, telefonia, energia elétrica e um grande grupo de instituições de saúde, bem-estar e educação são definitivamente dependentes das tecnologias de informação e telecomunicações para sua operação. Chegamos ao ponto em que é possível estatuir que "tudo depende do *software*" (EDWARDS, 1995). O crescimento exponencial da tecnologia digital, o aumento na sua capacidade e acessibilidade e o decréscimo de seu custo trouxeram mudanças revolucionárias no comércio, comunicações, entretenimento e educação. Junto com esta grande capacidade, entretanto, vem maior vulnerabilidade. A tecnologia da informação começou a prover oportunidades criminosas sem precedentes.

Figura 1. *Servidores de Internet - evolução geral.*



Fonte: M. Lottor, Internet Software Consortium <www.isc.org>

Estatísticas sobre uso de computadores e conectividade são notoriamente evanescentes. Elas estão ultrapassadas antes de serem impressas. As informações que estão, porém, na Figura 1, dão um sentido geral do crescimento e penetração da tecnologia digital em anos recentes.

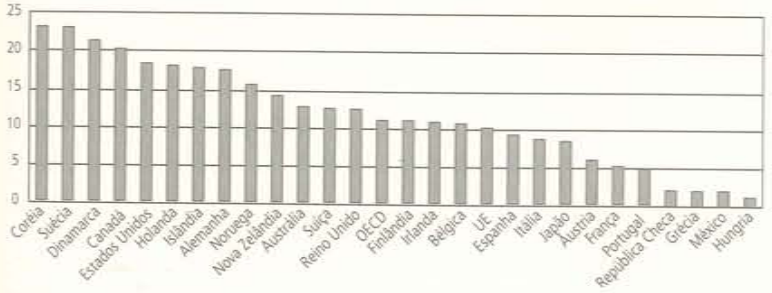
E também na Figura 2, abaixo:

Figura 2. *Comércio eletrônico – gastos.*

Fonte: Real Numbers Behind "Net Profits 1999", ActivMedia, Research LLC 1999.

Ainda, na Figura 3, abaixo:

Figura 3. *Assinantes de Internet por 100 habitantes, por países (jan. 2000).*



Fonte: Base de dados da OCDE, jun. 2001.

Pode notar-se que o uso da Internet, em geral, e o volume do comércio eletrônico estão crescendo exponencialmente, mas este crescimento tem sido desigual entre as nações, com as industrializadas experimentando maior uso das novas tecnologias. Recentemente, estimou-se que o Brasil possui cerca de 20 milhões de usuários de Internet e 50 provedores.[2] Mas não apenas o aumento da conectividade incrementa o número de vítimas potenciais de crimes relacionados aos computadores. Ela também aumenta o número de possíveis infratores.

4. Variedade de crimes relacionados aos computadores

A variedade de atividades criminosas que podem ser cometidas com ou contra sistemas de informação é surpreendentemente diversa. Algumas destas não são realmente novas em substância. Apenas o meio é novo. Outras, entretanto, representam novas formas de ilegalidades. As formas genéricas de ilegalidade que seguem envolvem sistemas de informação como instrumentos e/ou alvos de crimes. Elas não são mutuamente excludentes, nem a lista é exaustiva.

4.1 Furto de serviços de telecomunicações

Os *phone phreakers* de três décadas atrás estabeleceram o precedente do que se tornou uma grande indústria criminal. Ao ganhar acesso ao quadro de telefone (*switchboard*, PBX) de uma organização, indivíduos ou organizações criminosas podem obter acesso aos circuitos de entrada e saída (*dial-in* e *dial-out*) e, então, fazer suas próprias ligações e vender tempo de conexão para terceiros (GOLD, 1999). Infratores podem conseguir acesso ao quadro disfarçando-se de técnicos, obtendo fraudulentamente um código de acesso de um empregado ou usando *softwares* disponíveis na Internet. Formas adicionais de furto de serviços de telecomunicações incluem: a captura de detalhes de um cartão de ligações; a venda de ligações debitadas na conta do cartão de ligações que chama; e a falsificação ou reprogramação ilícita dos valores guardados nos cartões telefônicos.

Foi sugerido que, desde 1990, falhas de segurança em um grande sistema de telecomunicações trazem custos de aproximadamente £290 milhões. E, mais recentemente, que até 5% dos lucros totais da indústria foram perdidos por fraudes (SCHIECK, 1995:02-05; NEWMAN, 1998). Custos para assinantes individuais também podem ser significativos. Em um caso, *hackers* nos Estados Unidos obtiveram ilegalmente acesso à rede telefônica da Scotland Yard e realizaram ligações internacionais no valor de £620.000, pelas quais o órgão foi responsabilizado (TENDLER e NUTTALL, 1996).

4.2 Acesso não autorizado aos sistemas de computador

Próximo ao fim do ano de 1995, Julio Cesar Ardita, que residia em Buenos Aires com seus pais e três irmãos mais novos, usou o seu PC e o sistema da Telecom Argentina para obter acesso não autorizado de contas do sistema de computadores da Universidade de Harvard. Ardita conseguiu isto instalando um programa "buscador" (*sniffer*) que capturou a identificação e senhas de usuários de Harvard. Ele então fez uso destas contas para acessar outros sistemas, incluindo os da NASA, do Departamento de Defesa dos Estados Unidos e do Laboratório Nacional de Los Alamos, entre outros. Mesmo não tendo conseguido acesso a material altamente sigiloso, Ardita viu e copiou informações relevantes sobre tecnologias de radar e desenhos industriais de aeronaves. Quando sua invasão se tornou aparente, as agências que foram alvos tiveram que despender valores substanciais para refazer a segurança de seus sistemas. As atividades de Ardita dificilmente foram as únicas. O desafio de invadir sistemas de computadores alheios se mostrou irresistível para muitos. O dano causado por algumas destas invasões será mencionado posteriormente.

2. http://cyberatlas.internet.com/big_picture/geographics/article/0,1323,5911_151151,00.html (acesso em 01 maio 2003).

4.3 Comunicações visando a realização de conspirações criminosas

Tanto quanto as organizações legalizadas nos setores privado e público baseiam-se em sistemas de informações para comunicações e manutenção de arquivos, também as atividades de organizações criminosas são ampliadas pela tecnologia. Há evidência de que equipamentos de telecomunicações vêm sendo usados para facilitar o tráfico organizado de drogas, jogo, prostituição, lavagem de dinheiro, pornografia infantil e tráfico de armas (nas jurisdições nacionais onde estas atividades são ilegais). O uso de tecnologia criptográfica pode colocar as comunicações criminosas além do alcance da persecução judiciária (*law enforcement*).

O uso de tecnologia digital por organizações terroristas já foi mencionado. Bem antes de 11 de setembro de 2001, o Diretor da CIA, George Tenet, testemunhou que grupos terroristas "incluindo o Hezbollah, Hamas, a organização Abu Nedal e a organização Al Qaeda, de Osama Bin Laden estavam usando arquivos computadorizados, correio eletrônico e criptografia para apoiar suas operações" (apud FREEH, 2000).

4.4 Pirataria de informação, falsificação e contrafação

A tecnologia digital permite reproduções perfeitas e fácil disseminação de imagens, gráficos, sons, vídeos e combinações de multimídia. A tentação de reproduzir material protegido por direitos autorais para uso pessoal, venda a preços baixos ou, também, para distribuição gratuita se provou irresistível para muitos. Indústrias norte-americanas de bens protegidos por direitos autorais estimam a perda de cerca de 20 a 22 bilhões de dólares, anualmente, por causa da pirataria mundial (INTERNATIONAL INTELLECTUAL PROPERTY ALLIANCE, 2002).

A associação da indústria de *software* e informação norte-americana (*Software and Information Industry Association*, SIIA) calculou perdas de lucros globais, por causa da pirataria no mercado de aplicativos comporativos de computador, em 1999, de 12 bilhões de dólares. Isso foi atribuído somente às empresas e outras organizações que utilizam programas corporativos ilegalmente. A pirataria de aplicativos corporativos, nos Estados Unidos, em 1999, ocasionou a perda, por parte de empresas de *software*, de mais de 3,6 bilhões de dólares em vendas (SIIA, 2000). Quando criadores de um produto, em qualquer mídia, são inviabilizados de lucrar com suas criações, poderá haver um efeito deprimente no esforço criativo, em geral, adicional à perda financeira.

O furto de identidade se tornou um assunto de grande relevância para os países ao redor do globo. Isto foi facilitado, também, pela tecnologia digital, que permite perfeita reprodução de documentos como registros de nascimento e outros. Estes, por sua vez, podem ser utilizados para construir uma identidade falsa para uso em uma variada gama de atividades criminosas. A tecnologia digital também facilitou a falsificação de moedas e outros papéis monetários negociáveis.

4.5 Disseminação de materiais ofensivos

Há conteúdos considerados por algumas pessoas como censuráveis em abundância no ciberespaço. Isto inclui, entre outros, materiais sexualmente explícitos, propaganda racista, páginas eletrônicas de jogo e roteiros para a fabricação de dispositivos incendiários e explosivos. O que é de relevo, aqui, são as diferenças, ao redor do mundo, com o que os vários Estados soberanos denominam como agressivo. O que é objetável em um país pode ser agradável em outro. O mundo pode, em algum sentido, ser descrito como uma vila global, mas as diferenças de valores persistem. Ainda pode haver profundas diferenças em um mesmo país sobre o que é agressivo e o que não é. Como pode-se imaginar, isto configura significativos impedimentos para cooperação internacional.

O uso de redes de computadores para produzir e distribuir pornografia infantil se tornou um assunto de crescente atenção. Hoje, esses materiais podem ser copiados e transportados por entre fronteiras nacionais na velocidade da luz (GRANT, DAVID, GRABOSKY, 1997).

4.6 Rastreamento

Sistemas de telecomunicações também podem ser usados para comunicações assediadoras, ameaçadoras e invasivas, que vão desde a tradicional ligação telefônica obscena até a contemporânea manifestação de ciber-rastreamento (*cyber-stalking*), na qual subseqüentes mensagens são enviadas para um destinatário que não as deseja (OGILVIE, 2000).

Um homem em Déli (Índia) relatou ter acessado (*logged on*) uma sala de bate-papo (*chat*) usando a identidade de uma mulher. O agressor alegadamente usou uma linguagem sugestiva e disponibilizou o número telefônico da mulher. Ela conseqüentemente recebeu ligações telefônicas assediadoras, de lugares tão distantes como o Kuwait. O perpetrador foi localizado pelo endereço de IP usado no contato com a sala de bate-papo e foi, depois, preso (DUGGAL, 2001).

Em outro caso, um pretendente rejeitado publicou convites na Internet no nome de uma mulher de 28 anos, a provável destinatária de sua afeição, que relatava que ela tinha fantasias sexuais de estupro e sexo coletivo. Ele, então, comunicou-se, por correio eletrônico, com homens que responderam suas solicitações e forneceu informações pessoais sobre a mulher, incluindo seu endereço, telefone, detalhes de sua aparência física e como ultrapassar o seu sistema de segurança residencial. Homens estranhos apareceram na casa dela em seis ocasiões diferentes e ela recebeu muitos telefonemas obscenos. Apesar de a mulher não ter sido fisicamente atacada, ela não atendia ao telefone, tinha medo de sair de casa e perdeu seu emprego (MILLER e MAJARAJ, 1999).

Um então estudante universitário da Califórnia utilizou o correio eletrônico para assediar 5 estudantes em 1998. Ele comprou informações na Internet sobre elas usando o cartão de crédito de um professor e, então, enviou-lhes 100 mensagens incluindo ameaças de morte, descrições gráficas de atividades sexuais e referências sobre as atividades diárias delas. Ele aparentemente fez as ameaças em resposta às implicâncias recebidas contra sua aparência física (ASSOCIATED PRESS, 1999).

4.7 Extorsão

As redes de computadores podem ser também utilizadas na busca de extorsão. O The Sunday Times, de Londres, publicou, em 1996, que mais de 40 instituições financeiras na Grã-Bretanha e nos Estados Unidos foram atacadas eletronicamente durante os três anos anteriores. Na Inglaterra, instituições financeiras relataram ter pagado significativas quantidades para criminosos computacionais sofisticados que ameaçaram apagar seus sistemas eletrônicos (THE SUNDAY TIMES, 02 jun. 1996). O artigo citava quatro incidentes entre 1993 e 1995, nos quais um total de £42,5 milhões foram pagos por executivos seniores das instituições envolvidas, que foram convencidos pela capacidade dos extorquidores de destruir seus sistemas (DENNING, 1999:233-234).

Um caso, que ilustra o alcance internacional dos extorquidores, envolveu um grupo de *hackers* alemães, que comprometeram o sistema de um provedor de serviços de Internet no sul da Flórida desabilitando oito das dez máquinas. Os perpetradores obtiveram informações pessoais e detalhes dos cartões de crédito de 10.000 assinantes e, comunicando-se por correio eletrônico por uma das contas capturadas, demandaram que 30 mil dólares fossem enviados por correio até a Alemanha. A cooperação entre autoridades americanas e alemães resultou na prisão dos criminosos (BAUER, 1998).

Explorando a vulnerabilidade de *software* de um dos mais comuns dos sistema operacionais do mundo, Vasily Gorshkov e Alexey Ivanov, residentes de Chelyabinsk (Rússia), detonaram uma série de invasões em provedores de serviços de Internet, bancos on-line e páginas de comércio eletrônicos nos Estados Unidos. Os transgressores

tiveram sucesso em furtar mais de 56.000 números de cartões de crédito e informações pessoais financeiras sobre os clientes das páginas. Eles, então, buscaram extorquir dinheiro das vítimas ameaçando publicar os dados dos consumidores e danificando os computadores das empresas (US DEPARTAMENT OF JUSTICE, 2001).

4.8 Lavagem eletrônica de dinheiro e evasão fiscal

Por algum tempo, atualmente, a transferência eletrônica de fundos ajudou a ocultar e movimentar o dinheiro adquirido pelos crimes. Tecnologias emergentes vão, em grande medida, apoiar o encobertamento da origem ilícita de ganhos. Renda legitimamente conseguida também pode ser mais facilmente escondida das autoridades tributárias. Grandes instituições financeiras não vão mais ser as únicas com capacidade de realizar transferências eletrônicas de fundos por várias jurisdições nacionais na velocidade da luz. O desenvolvimento de instituições bancárias informais e sistemas bancários paralelos pode permitir que a supervisão de bancos centrais seja ultrapassada, mas também pode facilitar os requisitos de informações de evasão de transações monetárias, nas nações que os possuem. Bancos subterrâneos tradicionais, que floresceram em países asiáticos há séculos vão usufruir de mais capacidade, ainda, pelo uso das telecomunicações.

Com a emergência e a proliferação das várias tecnologias de comércio eletrônico, pode-se facilmente intuir como as medidas protetivas tradicionais contra lavagem de dinheiro e evasão de tributos deverão, em breve, ser de limitado valor. Eu poderei brevemente vender para o leitor uma quantidade de heroína, recebendo por uma transferência não-detectável de valor no meu *smart-card*, que eu, então, poderei baixar (*dowload*), anonimamente, para minha conta corrente numa instituição financeira situada numa jurisdição estrangeira (*oversea*), que proteja a privacidade dos seus correntistas. Eu poderei discretamente usar estes fundos como e quando eu quiser, baixando-os, de novo, para o meu cartão de débitos (WAHLERT, 1996).

4.9 Vandalismo eletrônico e terrorismo

Como nunca antes, a sociedade industrial ocidental depende de complexos sistemas de processamento de dados e de telecomunicações. Danificá-los – ou interferir neles – pode significar conseqüências desastrosas. Sejam motivadas por curiosidade ou vingança, invasões eletrônicas causam inconvenientes, na melhor das hipóteses, e têm o potencial de infringir danos maciços (HUNDLEY e ANDERSON, 1995; SCHWARTAU, 1994; DENNING, 2000).

A maior parte dos leitores experimentou algum inconveniente como resultado de vírus do tipo ILOVEYOU, Melissa e/ou Code Red. Ou, então, deve ter ouvido falar sobre os ataques desferidos para tirar do ar feitos contra a Amazon.com, Yahoo e outros proeminentes sítios de comércio eletrônico em fevereiro de 2000 (*denial of service attacks*). Estas atividades foram mais que um inconveniente para alguns. Perdas coletivas, em negócios ao redor do mundo, excederam centenas de milhões de dólares americanos.

Nas sociedades industriais ocidentais, em geral, e de modo crescente ao redor do globo, boa parte das infra-estruturas nacionais é privada, o que usualmente impossibilita o controle centralizado do Estado. Independentemente da propriedade, a infra-estrutura conectada à Internet é potencialmente acessível aos *hackers* habilidosos. Isto significa que alguns sistemas, que mantêm serviços essenciais em sociedades industriais avançadas, são vulneráveis aos ataques. Apesar destes ataques não terem ainda ocorrido de forma sustentada e difundida, vimos exemplos de danos significativos ocasionados por ataques isolados. O termo "ciber-terrorismo" foi cunhado para referir-se ao potencial catastrófico de danos resultante dos ataques contra infra-estruturas (GRABOSKY e STOHL, 2003).

Enquanto este potencial não se realiza, um número de indivíduos e grupos de protesto já invadiu (*hacked*) as páginas eletrônicas oficiais de várias organizações governamentais e empresas

(VATIS, 2001).[3] Já foram feitas tentativas de quebrar os sistemas de computador do governo de Sri Lanka (ASSOCIATED PRESS, 1998) e da Organização do Tratado do Atlântico Norte (OTAN), durante o bombardeio de Belgrado, em 1999 (BBC, 1999). Em março de 2001, *hackers*, situados na Coréia do Sul, causaram a queda (*crash*) de sítio eletrônico do Ministério da Educação do Japão em protesto contra um novo livro didático de História (BBC, 2001).

Estrategistas, na área de defesa, ao redor do mundo, estão investindo substancialmente em guerra informacional (*information warfare*) como meios de destruir a infra-estrutura de tecnologia da informação de sistemas de defesa (STIX, 1995; DENNING, 1999).

4.10 Fraude em vendas e investimentos

À medida que o comércio eletrônico se torna mais prevalente, a aplicação de tecnologia digital para os esforços fraudulentos será cada vez maior. É comum o aumento do uso de telefone para pontos de venda inexistentes, falsas solicitações de caridade ou ofertas falsas de novas oportunidades de investimento. O ciberespaço sobeja agora com uma ampla variedade de oportunidades de investimentos que vão desde os tradicionais títulos, ações e bônus, até oportunidades exóticas como fazendas de coco, a venda e leasing (*leaseback*) de caixas bancários eletrônicos e loterias telefônicas internacionais (CELLA e STARK, 1997:837-844). Ainda, a era digital está sendo acompanhada de oportunidades, sem precedentes, para desinformação. Agora, fraudadores usufruem de acesso direto a milhões de vítimas potenciais ao redor do mundo, instantaneamente e a um custo mínimo.

Uma das características distintivas da Internet e tecnologias baseadas em rede é a enorme capacidade que elas colocam nas mãos de indivíduos medianos. Uma pessoa com pouca habilidade no uso

3. Cf. http://www.2600.com/hacked_pages (acesso em 05 maio 2003).

de um computador pode se comunicar com milhões de outras, imediatamente e com ínfimo custo.

Esquemas clássicos de pirâmides e "oportunidades excitantes e com baixo risco" não são inusuais. A tecnologia da *world wide web* é idealmente preparada para estes convites de investimento. Nas palavras de dois membros do SEC: "A um baixo custo, na privacidade de um escritório caseiro ou da sala de estar, o fraudador pode produzir uma página eletrônica que parece melhor e mais sofisticada que a de uma empresa que figura na lista das 500 da Fortune" (CELLA & STARK, 1997:822).

Exploração fraudulenta de leilões virtuais se tornou uma fonte de preocupação para as autoridades de proteção dos consumidores pelo mundo. A fraude do convite à contribuição pelo "Avanço da Nigéria", antes entregue pelo correio, hoje segue por e-mail.

4.11 Interceptação ilegal de telecomunicações

O desenvolvimento nas telecomunicações criou novas oportunidades para bisbilhotagens eletrônicas. A interceptação de telecomunicações tem crescido em aplicações para atividades que vão desde as tradicionais, como a vigilância de um cônjuge infiel, até as mais novas formas de espionagem política e industrial. Aqui, novamente, os desenvolvimentos tecnológicos criaram novas vulnerabilidades. Os sinais eletromagnéticos, emitidos por um computador, isoladamente, podem ser interceptados. Cabos podem servir como antenas de transmissão. A legislação existente não previne o monitoramento remoto de radiação dos computadores.

Foi relatado que o conhecido *hacker* americano Kevi Poulsen foi capaz de ganhar acesso a dados do sistema eletrônico de persecução criminal e segurança nacional anteriores à sua prisão em 1991 (LITTMAN, 1997). Em 1995, *hackers*, a soldo de uma organização criminosa, atacaram o sistema de comunicações da polícia de Amsterdam. Os *hackers* tiveram sucesso em adquirir informações da inteligência operacional da polícia e em intrometer-se nas comu-

nicações policiais (RATHMELL, 1997). Mais recentemente, o acesso não autorizado ao código fonte da Microsoft, em outubro de 2000, indicava a vulnerabilidade das empresas à espionagem industrial (ASSOCIATED PRESS, 2000).

4.12 Transferências fraudulentas de fundos eletrônicos

Os sistemas de transferência eletrônica de fundos começaram a proliferar e, com isso, aumentou o risco de tais transações serem interceptadas e desviadas. Números de cartão de créditos válidos podem ser interceptados eletronicamente, bem como fisicamente; a informação digital armazenada num cartão pode ser contrafeita.

Em 1994, um *hacker* russo, Vladimir Levin, operando de São Petersburgo, acessou os computadores da rede central do departamento de transferências do Citibank. E transferiu fundos de contas de grandes empresas para contas que haviam sido abertas por seus comparsas nos Estados Unidos, nos Países Baixos, Finlândia, Alemanha e Israel. Representantes de uma das empresas vitimadas, localizada na Argentina, notificaram o banco e as contas suspeitas, em São Francisco, foram congeladas. Aquele comparsa foi preso. Outro foi pego tentando retirar fundos de uma conta em Roterdã. Apesar de a legislação russa impedir a extradição de Levin, ele foi capturado durante uma visita aos Estados Unidos e, então, preso (DENNING, 1999:55).

* * *

As formas de crime mencionadas acima relacionadas aos computadores não são necessariamente excludentes e não precisam ocorrer isoladamente. Tanto como um assaltante armado pode roubar um carro para facilitar sua rápida fuga, também, podem-se furtar serviços de telecomunicações e usá-los para fins de vandalismo, fraude ou apoio de uma conspiração criminosa. Crimes relacionados aos computadores podem ser compostos, por natureza, combinando duas ou mais das formas genéricas arrazoadas anteriormente.

Adicionalmente, uma quantidade de temas percorre cada uma destas formas de ilegalidade. Previamente a estas, estão as tecnologias para dissimular o conteúdo das comunicações (DENNING, 1999). Tecnologias de criptografia podem limitar o acesso, pelos agentes de persecução criminal (*law enforcement*), às comunicações mantidas em atenção de uma conspiração ou para a disseminação de material censurável entre partes consensuadas.

Também são importantes as tecnologias para esconder a identidade de uma parte na comunicação. Despersonalização eletrônica, coloquialmente chamada de *spoofing*,[4] pode ser utilizada para a tentativa de realização de uma variedade de atividades criminosas, incluindo fraude, conspiração criminosa, assédio sexual e vandalismo. As tecnologias do anonimato visam complicar a tarefa de identificar um suspeito.

Além da previamente mencionada relutância das vítimas em relatar, as tecnologias de segredo e anonimato, tratadas antes, geralmente fazem a detecção do agressor ser extremamente difícil. Aqueles que procuram mascarar sua identidade em redes de computadores são usualmente aptos a fazê-lo trocando-a (*looping*) ou alterando-a (*weaving*) por meio de múltiplos sítios eletrônicos em uma variedade de nações. Re-enviadores de e-mails e dispositivos de encriptação podem bloquear alguém do escrutínio de todos, mesmo das mais determinadas e tecnologicamente sofisticadas agências regulatórias e de persecução criminal. Alguns crimes não resultam em detecção ou dano até pouco tempo antes de sua realização. Tempo considerável pode passar antes do momento anterior à ativação de um vírus de computador ou entre a inserção de uma "bomba lógica" e sua detonação.

O tamanho do problema

Estimar a incidência, prevalência, custo ou alguma outra medida acerca dos crimes relacionados aos computadores é um desafio

4. Em português, seria algo próximo de paródia ou troça (nota do tradutor).

difícil. Diferentemente de assaltos aos bancos ou acidentes fatais com veículos automotivos, crimes relacionados aos computadores tendem a desafiar quantificação. Alguns dos mais hábeis crimes realizados com ou contra sistemas de informação não são nunca detectados, nem pelas vítimas. Dos que o são, alguns são escondidos das autoridades porque sua revelação poderia se provar embaraçosa ou comercialmente inconveniente para as vítimas.

A quantificação também pode ser mascaradora. O que parece ser uma questão trivial pode, de fato, ser um indício da ponta do *iceberg*. Uma imagem clássica, provida por Stoll (1991), é a que a busca por um erro na contabilidade de 0,75 de dólar, numa conta de computador, pode indicar um círculo de espionagem internacional.

Mesmo descrições qualitativas podem ser ilusórias. Muitas pessoas, independentemente de suas motivações, estão inclinadas a acentuar o problema, incluindo *hackers* orgulhosos, empreendedores morais, vítimas ou entidades comerciais com capital investido, sem mencionar a mídia jornalística.

Algumas tentativas estão sendo feitas para desenvolver uma análise sistemática da incidência de crimes no ciberespaço. A Câmara Internacional de Comércio (*International Chamber of Commerce*, ICC) abriu uma nova divisão para auxiliar cerca de 7.000 empresas associadas, ao redor do mundo, a proteger-se contra os crimes relacionados aos computadores. Além de identificar como e onde os ataques ocorrem, a Câmara procura providenciar informação sobre segurança para os seus membros. A nova unidade de cibercrime da ICC está desenvolvendo uma base de dados sobre atividades criminais no ciberespaço e vai facilitar a troca de informações entre o setor privado e os órgãos de persecução criminal (*law enforcement*).[5]

5. Cf. http://www.iccwbo.org/ccs/menu_cybercrime_unit.asp (acesso em 05 maio 2003).

5. O desafio de controlar o crime relacionado aos computadores

5.1 Controlando fatores contributivos - motivações

Lembremos da discussão anterior de que o crime pode ser explicado, em parte, em termos de uma oferta de criminosos motivados. Dada a diversidade dos crimes relacionados aos computadores, não é surpreendente que vários tipos de comportamentos, discutidos antes, brotem de uma quantidade de motivos. Como notamos, alguns deles são tão antigos como a sociedade humana, incluindo ganância, desejo, vingança e curiosidade. A vingança, nos tempos modernos, pode decorrer de uma dimensão ideológica. De considerável significado, se não único, para os crimes relacionados aos computadores, é o desafio intelectual de derrotar um sistema complexo. Motivações, seja pelo lado dos indivíduos, seja no todo, são muito difíceis de alterar. Por este motivo, as investidas estrategicamente vantajosas, para os crimes relacionados aos computadores, estarão preocupadas com a redução das oportunidades e com a melhor qualidade da vigilância (*guardianship*).

5.2 Oportunidades

Enquanto as motivações tendem a não se alterar, a variedade e número de oportunidades para crimes informáticos estão proliferando. O crescimento exponencial da conectividade, na computação e comunicações, cria oportunidades paralelas para potenciais agressores e riscos paralelos para vítimas potenciais. Ao passo que a Internet se transforma mais e mais em um meio de comércio, também se tornará mais um meio de fraude.

O modo mais eficiente de eliminar oportunidade para o crime on-line é simplesmente arrancar o soquete da parede. Isto é, claro, irreal. As nações ricas do mundo estão, agora, altamente dependen-

tes das tecnologias da informação. Para as nações pobres, a tecnologia da informação é provavelmente um caminho, se não completamente, necessário para o desenvolvimento econômico. Então, o desafio está em gerenciar o risco de modo a alcançar o máximo de benefícios, extraídos das novas tecnologias, e minimizar a possibilidade de revés. Um comerciante pode analisar detalhadamente cada transação com cartão de crédito para drasticamente reduzir o risco de fraude, mas no processo pode perder clientes honestos. Num nível mais geral, as nações ao redor do mundo estão no processo de forjar políticas públicas de onde possam definir a linha sobre questões fundamentais como o equilíbrio entre a privacidade dos cidadãos e os imperativos da persecução criminal. E, também, da liberdade de expressão versus a proteção de certos valores culturais.

Existem muitas tecnologias que reduzem a oportunidade de cometimento de crimes relacionados aos computadores. Considerado que grande parte dos crimes relacionados aos computadores depende de acesso não autorizado aos sistemas de informação, as tecnologias de controle de acesso e autenticação se tornaram essenciais. Dispositivos sofisticados e produtos para prevenção de crimes computacionais são providos por uma das indústrias mundiais com maior crescimento atualmente, nomeada de segurança de computadores.

Denning (1999) oferta um inventário completo das tecnologias para a redução das oportunidades para crimes computacionais. Ela descreve tecnologias de criptografia e anonimato, que permitem o ocultamento do conteúdo das comunicações (como os detalhes sobre o cartão de crédito de um consumidor) ou da identidade da parte na comunicação (nem todos os participantes em um grupo de discussão sobre saúde reprodutiva desejam mostrar suas identidades). Denning também delineia as tecnologias de autenticação, que vão desde as senhas básicas até dispositivos biométricos como impressão digital ou tecnologia de reconhecimento de voz e análise de imagem da retina. Todas aumentam em muito a dificuldade de obtenção de acesso não autorizado aos sistemas de informação.

Detectores de vírus podem identificar e bloquear códigos maliciosos de computador; programas de bloqueamento e filtragem podem procurar por conteúdo não desejável. Uma rica variedade de *softwares* comerciais já opera com esta capacidade de bloquear o acesso a certos sítios eletrônicos (VENDITTO, 1996).

5.3 Vigilantes (guardians)

O terceiro fator básico que explica os crimes relacionados aos computadores é a ausência de vigilância eficiente. Esta tem evoluído ao longo da história humana. Do feudalismo até a aparição do Estado e da proliferação das instituições estatais de controle social, até a era pós-moderna, na qual empregados de serviços privados de segurança superam vastamente em números absolutos os policiais em muitas das democracias industriais. Aqui, novamente, pode ser instrutivo comparar os crimes relacionados aos computadores com tipos mais convencionais de crimes.

Vigilância contra o crime convencional envolve esforços preventivos no campo das vítimas potenciais, contribuições por membros do público, em geral, ou de terceiras partes comerciais, bem como das atividades das agências de persecução criminal. De fato, usualmente apenas quando os esforços privados em prevenção do crime falham é que os procedimentos criminais são mobilizados. Assim é que proprietários de veículos automotivos são encorajados a trancar seus carros em todos os momentos, que contratos de seguros podem oferecer descontos especiais para clientes com medidas protetivas como alarmes de roubo e que alguns estacionamentos de veículos têm vigilância por câmeras de vídeo ou guardas de segurança de plantão. Normalmente, é apenas quando estes sistemas falham que a ajuda da polícia é buscada.

Tecnologia pode, também, aumentar a vigilância. Denning (1999) descreve várias tecnologias para detecção de tentativa de invasões em sistemas de informação. Alarmes podem indicar quando sucessivas tentativas de acesso (*login*) falham, por causa das senhas

incorretas. Ou quando acesso é tentado fora do horário normal de trabalho. Outros dispositivos de detecção de anormalidade vão identificar padrões de uso dos sistemas, incluindo destinação atípica e duração das ligações telefônicas. Ou, ainda, padrões de consumo inusuais no uso de cartões de crédito.

A vigilância também pode ser expandida pelas forças de mercado. Atualmente, um mercado está emergindo para provedores de serviços de Internet especializados em conteúdos adequados para consumo familiar, garantidos por serem livres de sexo, violência e difamação. As forças de mercado podem gerar, ainda, influências secundárias de controle. Quando grandes organizações começam a analisar suas vulnerabilidades ao furto eletrônico ou vandalismo, elas podem securitizar-se contra perdas potenciais. É muito adequado ao interesse das companhias de seguro requerer precauções de segurança por parte de seus segurados.

Logo, decisões sobre aceitação dos seguros e sobre os preços podem depender das práticas de segurança dos potenciais segurados. Subcontratadores podem, também, ter que possuir programas rígidos de integridades da tecnologia da informação como condição para realização dos negócios.

A preocupação dos cidadãos acerca da disponibilidade de conteúdo indesejável deu ensejo ao monitoramento privado e vigilância no ciberespaço. O Centro Simon Wiesenthal, cuja linha-direta (*hotline*) de ciber-vigilância solicita notificações sobre materiais anti-semitas e racistas, está dentre as mais proeminentes organizações envolvidas nesta guarda.[6]

A cooperação dos cidadãos pode complementar as atividades levadas a termo pelas agências estatais. Um exemplo de esforço na colaboração público-privado, na empreitada de controlar conteúdo objetável é a linha-direta holandesa contra a pornografia infantil na Internet, uma iniciativa da Fundação de Provedores de Internet Holandeses (*Foundation for Dutch Internet Providers*, NLIP), do

6. Cf. http://www.wiesenthal.com/watch/whotline.htm.

Serviço de Inteligência Criminal Nacional Holandês (*Dutch National Criminal Intelligence Service*, CRI), usuários da Internet e do Bureau Nacional contra o Racismo (*National Bureau against Racism*, LBR). Usuários que encontrem pornografia infantil originada nos Países Baixos, identificável pelo nome de domínio terminado em "nl", são incitados a relatar isto ao endereço "meldpunt@xs4all.nl"" O emissor é avisado sobre o material publicado e é solicitado a abandonar quaisquer atividades futuras do gênero. Se o aviso é ignorado, então a linha-direta vai encaminhar (*forward*) qualquer informação disponível para o esquadrão da polícia local.

O policiamento do espaço territorial agora é uma empreitada muito mais plural e, assim também, o é o policiamento do ciberespaço. A responsabilidade pelo controle da criminalidade computacional será, similarmente, dividida entre os agentes do Estado, os especialistas em segurança da informação do setor privado e o usuário individual. No ciberespaço, hoje, assim como no espaço territorial dois milênios antes, a primeira linha de defesa será a autodefesa. Em outras palavras: será cuidar do seu quintal (*minding one's own store*).

Questões legislativas

Está ficando cada vez mais claro que o bem-estar econômico dos países depende da sua integração à economia global. Como o ciberespaço se caracteriza como meio dominante para o comércio, torna-se crescentemente relevante que haja uma plataforma legal segura para o comércio eletrônico.

Para que qualquer jurisdição possa proteger-se contra crimes relacionados aos computadores, é necessária uma base legal básica. Isto envolve leis criminais, o direito de busca e apreensão e o direito das provas. Por causa da natureza global do ciberespaço e da natureza trans-jurisdicional de grande parte da criminalidade computacional, é desejável um grau de harmonia e consistência, se não de uniformidade, entre as nações.

As leis de alguns países são relativamente vagas e capazes de alcançar novas circunstâncias sem precisarem ser emendadas. Outros sistemas legais são muito rígidos, requerendo mudanças para novas formas de crimes. No mundo da *common law*, por exemplo, consideramos transgressões relacionadas à obtenção fraudulenta de coisas valiosas por meio de mentiras. Estas englobam o envolvimento da mente de uma vítima humana. Onde a fraude é executada contra um sistema eletrônico (como um caixa bancário eletrônico) será necessária uma nova legislação. Similarmente, as leis sobre furto ou dano em alguns países podem alcançar apenas bens tangíveis (bens corpóreos). Ou seja, pode não ser crime furtar ou danificar propriedade em forma digital.

De forma mais fundamental, a lei criminal substantiva deve providenciar o seguinte:

- Acesso não autorizado aos computadores ou sistemas computacionais;
- Interferência com o uso lícito de um computador ou sistemas computacionais;
- Destruição ou alteração de informação num sistema computacional;
- Furto de propriedade intangível;
- Obtenção de valores por fraude (incluindo sistemas eletrônicos).

De forma similar, as leis acerca de provas e procedimentos devem acomodar buscas e apreensões no ambiente eletrônico e devem permitir a admissibilidade de provas eletrônicas nos procedimentos judiciais.

Questões extraterritoriais

Um dos aspectos mais significativos da criminalidade relacionada aos computadores é o seu alcance global. Enquanto as transgressões internacionais são, por todos os sentidos, parte de um

fenômeno moderno único, a natureza global do ciberespaço aumenta significativamente a habilidade dos perpetradores de cometerem crimes em um país, que afetarão indivíduos em uma quantidade de outros países. Isto configura grandes desafios para a detecção, investigação e persecução dos transgressores.

Surgem dois problemas em relação à persecução de crimes por telecomunicações que possuem um aspecto inter-jurisdicional: primeiro, a determinação de onde o crime ocorreu, de forma a decidir qual lei será aplicada; segundo, a obtenção de provas e garantia de que o criminoso poderá ser localizado e poderá ser levado ao julgamento. Ambas levantam problemas jurídicos complexos de conflitos de jurisdição e extradição (LANHAM, WEINBERG, BROWN, RYAN, 1987). Se um jornal eletrônico financeiro (*newsletter*), originado nas Bahamas, contém especulação fraudulenta sobre as expectativas de uma empresa cujas ações são negociadas no mercado de ações australiano, onde ocorreu o crime?

Mesmo que alguém determine qual lei será aplicada, podem surgir dificuldades futuras na aplicação daquela lei. Numa jurisdição unitária, como a da Nova Zelândia, onde há mais uma lei e uma agência de persecução criminal, determinar e aplicar a lei aplicável já é uma tarefa difícil. Atividades criminais cometidas ao redor do globo, entretanto, apresentam problemas ainda maiores. Se governos soberanos estão considerando difícil exercer controle sobre o comportamento on-line de seu país natal, imagine no estrangeiro. Um residente de Chicago que seja vítima de um esquema fraudulento de telemarketing originado da Albânia, por exemplo, pode esperar por pouca ajuda das agências de persecução criminal de ambas as jurisdições. Como conseqüência, a regulação por normas baseadas territorialmente pode provar-se pouco apropriada para estes tipos de transgressões (POST, 1995).

Os custos de persecução criminal extraterritorial também são proibitivos. O tempo, dinheiro e incerteza necessários para as investigações internacionais e, se bem sucedidas, os procedimentos de extradição, podem ser tão altos que excluam a atenção para todos as

transgressões, excepcionadas as mais graves. Ainda, usualmente, a cooperação por sobre as fronteiras internacionais, nas tentativas destas persecuções, requer a conjunção de valores e prioridades que raramente ocorre. Excepcionando-se, por certo, no caso dos grandes temas em direção à globalização.

Adicionalmente, os custos associados com a assistência jurídica mútua são providos pela parte que fornece auxílio. Isto cria injustiça, pela qual os países menos providos, donde talvez nunca seja pedida assistência jurídica mútua por seu pedido, são instados a processar pedidos de países mais fornidos como o Reino Unido ou os Estados Unidos. Países mais pobres podem então ser obrigados, por tratados, a subsidiar os mais ricos.

Tradicionalmente, a jurisdição das cortes era local. Isto é, as cortes podem apenas acolher processos a respeito de crimes cometidos contra as leis locais, onde haja existido uma ligação entre o mesmo e a jurisdição em questão. Alguns países estão agora declarando sua jurisdição para fora das fronteiras. Na Austrália, a Lei de Cibercrime de 2001 (*Cybercrime Act*) demanda jurisdição nos casos em que:

- A conduta, que constitui a transgressão, ocorre parcialmente na Austrália ou a bordo de um navio ou aeronave australiana;
- O resultado da conduta, que constitui a transgressão, ocorre parcialmente na Austrália ou a bordo de um navio ou aeronave australiana;
- A pessoa que comete a transgressão é cidadã australiana ou uma empresa da Austrália.

O grau em que os crimes relacionados aos computadores sejam passíveis de efetividade para a persecução internacional dependerá do acordo na cooperação internacional. Experiências passadas, no caso de outras formas de criminalidade, sugerem que esta cooperação é difícil de acontecer. E, também, que há pouco interesse em reprimir alguns tipos criminais, exceto os relativamente infreqüentes, em que há amplo consenso internacional sobre a atividade em questão, como pornografia infantil ou fraudes em escala passível de desestabilizar mercados financeiros. Em muitos sentidos a extradição deve ser mais incômoda à medida que aumenta a distância cultural e ideológica entre os dois países (*parties*).

Mesmo assim, para tanto teríamos que considerar um homogêneo sistema mundial de Estados soberanos. Tal sistema não existe hoje e nem deve existir enquanto vivermos. Vácuos concernentes à persecução criminal e à regulação existem em algumas partes do mundo, certamente naqueles cenários onde o Estado efetivamente desmoronou. Mesmo onde o poder de Estado existe em força total, a corrupção de alguns regimes pode impedir a colaboração internacional.

Apesar de tudo, algum progresso excepcional foi realizado na ampliação da harmonização internacional de leis relativas aos crimes computacionais e sua investigação. Refiro-me ao trabalho das Nações Unidas, do Grupo dos Oito, da Organização para Cooperação e Desenvolvimento Econômico (OCDE), do Conselho da Europa e da INTERPOL. Como um exemplo do movimento em direção à consistência nas respostas legislativas, pode-se visualizar o rascunho da Convenção sobre Cibercrime do Conselho da Europa (*Council of Europe'a Draft Convention on Cybercrime*). Este arrazoado de Convenção contém partes gerais relacionadas às leis criminais substantivas, busca e apreensão de informações eletrônicas, jurisdição e assistência mútua.

Medidas a serem tomadas, em nível nacional, a respeito da lei criminal substantiva, incluem a adoção de atitudes para criminalizar: o acesso ilegal aos sistemas de computadores; a interceptação ilegal e/ou a interferência em dados; a produção, venda ou aquisição de ferramentas ou *software* de hackeamento; fraude e falsificação relacionadas aos computadores; atividades relacionadas à pornografia infantil; e transgressões relacionadas à violação de direitos autorais.[7]

7. Cf. http://conventions.coe.int (visited 5 May 2003).

Afora questões de criminalidade além das fronteiras, muitas das agências de persecução criminal, como as que conhecemos hoje, não possuem capacidade de controlar o crime relacionado aos computadores que ocorre dentro das suas próprias jurisdições.

Isto decorre de uma multiplicidade de fatores, dos quais o último é a restrição de recursos. Na maior parte das sociedades industriais ocidentais, as polícias estão sendo solicitadas a fazer mais com menos. O longo alcance das leis criminais e a abundância de atividades criminais significam que a polícia usualmente deve escolher o que deve perseguir e o que ignorar. Isto tem mais sentido, ainda, no caso de crimes eletrônicos internacionais do que nas atividades criminosas domésticas. Outra questão fundamental, pelo menos no momento histórico atual, é a dificuldade encontrada pelos serviços policiais em todo mundo de manter especialistas em crimes computacionais como investigadores. Assim como o sacerdócio, a polícia era uma vocação para a vida toda. Hoje, em muitos serviços policiais, investigadores treinados em crimes computacionais devem batalhar pelo equipamento que consideram necessário para realizar seu trabalho. O desenvolvimento da especialidade em perícia criminal sobre computadores, entretanto, pode requerer concentração e especialização que inibem o desenvolvimento de habilidades gerais necessárias para as promoções de carreira. Como junto às áreas tradicionais de alto status nas polícias (caso da investigação de homicídios) vieram se juntar outras de gerência geral, as perspectivas futuras para mobilidade ascendente por parte dos investigadores de crimes computacionais vêm sendo limitada.

Ao mesmo tempo, existem oportunidades muito atrativas no setor privado para pessoas com habilidade em perícia criminal em computadores. Um policial competente pode muito bem ser capaz de duplicar ou triplicar seu salário indo para a área privada, seja trabalhando para uma grande firma de auditoria multinacional ou para uma grande instituição financeira.

Ainda está para ser visto se esta fuga de cérebros vai continuar indefinidamente ou se deve diminuir quando o suprimento de indivíduos versados em computadores, tanto no setor público, quanto no privado, alcançar o equilíbrio com a demanda. Neste meio tempo, entretanto, a polícia não vai ser capaz de seguir sozinha. Ela vai continuar dependente do setor privado e de organizações sem fins lucrativos para combater o crime no ciberespaço.

Em geral, esta divisão do trabalho vai incluir elementos de auto-proteção por parte de vítimas potenciais de ilegalidade relacionadas às telecomunicações. Também deve incluir: soluções comerciais baseadas no mercado (*market-based*); iniciativas auto-regulatórias pelos regulados; persecução criminal ou intervenção regulatória estatal, tradicionais; e co-produção de vigilância por terceiros, como indivíduos isolados ou grupos de cidadãos.

6. Conclusão

Crime transnacional de natureza convencional se provou um desafio muito difícil para a persecução criminal. Crime relacionado aos computadores apresenta desafios ainda maiores. Poderá haver diferenças, entre as jurisdições envolvidas, sobre: se a atividade em questão ocorreu, ou não; se ela é criminosa, quem a cometeu; quem deve investigá-la; e, também, quem deve julgar e punir.

Ainda mais, há uma tensão fundamental entre o imperativo desregulamentador que caracteriza os países com economias mais avançadas e o desejo de controlar alguns dos cantos mais obscuros do ciberespaço. Há um perigo significativo de que intervenções regulatórias prematuras não apenas falhem em alcançar os efeitos desejados, mas também que tenham um impacto negativo no desenvolvimento das tecnologias de benefício geral. Extra-regulação – ou intervenções regulatórias prematuras – pode colocar em risco os delicados investimentos e inovação. Dada a natureza crescentemente competitiva do mercado global, os governos podem ser forçados a escolher entre imperativos paternalistas e aqueles de desenvolvimento comercial e crescimento econômico.

O desafio, que se apresenta àqueles que querem minimizar o crime relacionado aos computadores, é buscar o equilíbrio que poderá permitir um grau tolerável de ilegalidade em troca da exploração criativa da tecnologia digital. Pode ser útil aos indivíduos, grupos de interesse e governos, neste estágio recente da revolução tecnológica, articular suas preferências e deixar que sirvam como sinais ao mercado. Os mercados podem ser capazes de prover soluções mais eficientes do que intervenções estatais.

Com certeza, o ciberespaço é dificilmente o primeiro – ou o único – campo de políticas pública que se coloca além do controle de somente um Estado nacional. O tráfego aéreo internacional, o direito concernente aos mares, transferências de fundos e questões ambientais como a camada de ozônio e o aquecimento global, entre outros, têm demandado esforços internacionais organizados. Alguém poderia esperar que o desenvolvimento de arranjos internacionais em resposta aos crimes relacionados aos computadores vá ocorrer de uma forma não muito distinta daqueles concernentes a outras questões extraterritoriais que vão desde o tráfico de drogas até testes nucleares e caça às baleias. Veremos se o reino das telecomunicações vai ser capaz de conseguir um melhor registro de sucesso que estes outros resistentes problemas globais.

Referências bibliográficas

ASSOCIATED PRESS. *Microsoft acknowledges theft of source code.* The New York Times on the Web. 2000. Disponível em: http://channel.nytimes.com/aponline/technology/27MICROSOFT.html (acesso em 23 nov. 2000)

_____. *Man guilty of internet stalking.* 1999. Disponível em: http://www.bayinsider.com/news/1999/01/20/stalking.html (aceso em 01 jul. 1999)

_____. *First cyber terrorist action reported.* Nando.Net. 1998. Disponível em: http://www.techserver.com/newsroom/ntn/info/050698/info9_25501_noframes.html (acesso em 08 out. 2000)

BAUER, James. *Testimony to the subcommittee on technology, terrorism and government information.* Committee on the Judiciary, United States Senate, 20 maio 1998. Disponível em: http://www.securitymanagement.com/library/bauer.html (acesso em 05 maio 2003)

BBC. *Attack on Japan ministry website.* 2001. Disponível em: http://news.bbc.co.uk/hi/english/world/asia-pacific/newsid_1252000/1252965.stm (acesso em 02 maio 2003)

_____. *Nato under 'cyber attack'.* 1999. Disponível em: http://www.flora.org/flora.mai-not/10498 (acesso em: 24 abril 2003)

CELLA, Joseph F., STARK, John Reed. SEC *Enforcement and the Internet:* Meeting the Challenge of the Next Millennium - A Program for the Eagle and the Internet. 52 Bus. Law. 815, 1997.

DENNING, D. *Information warfare and security.* Boston: Addison Wesley, 1999.

_____. *Activism, hacktivism, and cyberterrorism:* the Internet as a tool for influencing foreign policy. 2000. Disponível em: http://www.nautilus.org/info-policy/workshop/papers/denning.html (acesso: 24 abr. 2003)

DUGGAL, S. *India's first cyberstalking case:* some cyberlaw perspectives. 2001. Disponível em: http://www.cyberlawindia.com/2CYBER27.htm (acesso: 29 mar. 2001).

EDWARDS, O. Hackers from hell. *Forbes,* 182. 09 out. 1995.

FREEH, L. *Statement before the Senate Judiciary Committee, Subcommittee for the Technology, Terrorism, and Government Information.* United States Senate, 28 mar. 2000. Disponível em: http://www.usdoj.gov/criminal/cybercrime/freeh328.htm (acesso: 24 abr. 2003).

GOLD, Steve. BT starts switchboard anti-hacking investigation. *Newsbytes,* 11 jan. 1999. Disponível em: http://www.infowar.com (acesso: 23 dez. 1999)

GRABOSKY, P., SMITH, R.G. *Crime in the digital age:* controlling telecommunications and cyberspace illegalities. New Brunswick, NJ: Transaction Publishers and Sydney: Federation Press, 1998.

_____, DEMPSEY, G. *Electronic theft:* crimes of acquisition in cyberspace. Cambridge: Cambridge University Press, 2001.

GRABOSKY, P., STOHL, M. Cyberterrorism. *Reform,* n. 82, p. 8-13, 2003.

GRANT, A., DAVID, F., GRABOSKY, P. Child pornography in the digital age. *Transnational Organized Crime*, n. 3/4, p. 171-188, 1997.

HUNDLEY, R., ANDERSON, R. Emerging challenge: security and safety in cyberspace. *IEEE Technology and Society Magazine*, v. 4, n. 14, p. 19-28, 1995.

INTERNATIONAL INTELLECTUAL PROPERTY ALLIANCE. *Press release*, 30 abr. 2002. Disponível em: http://www.iipa.com/pressreleases/2002_Apr30_USTR301.pdf (acesso: 01 maio 2003).

LANHAM, D., WEINBERG, M., BROWN, K. E., RYAN, G. *Criminal fraud*. Sydney: Law Book Co. Ltd, 1987.

LITTMAN, J. *The watchman*: the twisted life and crimes of serial hacker Kevin Poulsen. Boston: Little Brown, 1997.

MILLER, Greg, MAHARAJ, Davan. N. Hollywood man charged in 1st cyber-stalking case. *Los Angeles Times*, 22 jan. 1999. Disponível em: http://www.cs.csubak.edu/~donna/news/crime.html#stalking (acesso: 25 out. 2000).

NEWMAN, Keith. Phone call scams skim off millions. *New Zealand Herald*, 20 ago. 1998. Disponível em: http://www.infowar.com/ (acesso: 23 dez. 1999)

OGILVIE, Emma. Cyberstalking. *Trends and Issues in Crime and Criminal Justice*. n. 166. Canberra: Australian Institute of Criminology, 2000. Disponível em: http://www.aic.gov.au/publications/tandi/tandi166.html (acesso: 24 abr. 2003)

POST, D. G. Anarchy, state, and the internet: an essay on law-making in cyberspace. *Journal of Online Law*, art. 3. 1995.

RATHMELL, A. Cyber-terrorism: the shape of future conflict? *Royal United Service Institute Journal*, 40-46. out. 1997. Disponível em: http://www.kcl.ac.uk/orgs/icsa/rusi.htm#who (acesso: 21 dez. 1999)

SCHIECK, M. Combating fraud in cable and telecommunications. *IIC Communications Topics*, n. 13. London: International Institute of Communications, 1995.

SCHWARTAU, Winn. *Information warfare*: chaos on the electronic superhighway. New York: Thunder's Mouth Press, 1994.

SOFTWARE AND INFORMATION INDUSTRY ASSOCIATION. *Report on global software piracy 2000*. 2000. Disponível em: http://www.siia.net/piracy/pubs/piracy2000.pdf (acesso: 05 maio 2003)

STOLL, Clifford. *The cuckoo's egg*. London: Pan Books, 1991.

TENDLER, S., NUTTALL, N. Hackers leave red-faced yard with $1.29m Bill. *The Australian*, p. 37, 06 ago. 1996.

UNITED STATES DEPARTMENT OF JUSTICE. *Russian computer hacker convicted by jury*, 10 out. 2001. Disponível em: www.usdoj.gov/usao/waw/pr2001/oct/vasiliy.html (acesso: 24 abr. 2003)

VATIS, Michael *Cyber attacks during the war on terrorism*: a predictive analysis. Institute for Security Technology Studies, Dartmouth College, Hanover New Hampshire, 2001.

VENDITTO, G. Safe computing. *Internet World*, p. 48-58, set. 1996.

WAHLERT, G.) Implications for law enforcement of the move to a cashless society, p. 22-28. In: GRAYCAR, A., GRABOSKY, P. N. (Eds.). *Money Laundering*. Canberra: Australian Institute of Criminology, 1996.

Resumo

Este artigo fornece um panorama dos crimes relacionados aos computadores (computer related crimes). Doze variedades de crimes são consideradas: roubo de serviços; acesso não autorizado aos sistemas computacionais; comunicações objetivando conspirações criminosas; pirataria e falsificação de informação; disseminação de materiais com conteúdo ofensivo; [rastreamento cibernético]; extorsão; lavagem de dinheiro eletrônico; vandalismo e terrorismo eletrônico; fraude em telemarketing; interceptação ilegal; e fraude em transferências de recursos eletrônicos.