Crimes cibernéticos e seus efeitos internacionais

Paulo Quintiliano da Silva
Serviço de Perícia de Informática da Polícia Federal
Email: quintiliano.pqs@dpf.gov.br

***Abstract* — Neste artigo, os crimes cibernéticos são contextualizados no cenário internacional, apresentando as principais características desses crimes e as dificuldades encontradas em sua investigação. São abordadas as iniciativas dos principais organismos internacionais referentes ao enfrentamento desses crimes. As alternativas de combate a esses crimes, a reestruturação das agências policiais e a cooperação policial internacional direta entre essas agências são apresentadas.**

***Index Terms* — Crimes cibernéticos, organismos internacionais, perícia, agências policiais.**

I. Introdução

UMA das características dos crimes cibernéticos que mais dificulta as investigações é o fato de não existirem fronteiras no espaço cibernético. Assim, a mesma ação criminosa pode ter efeito em vários países, de forma simultânea, podendo atingir até milhões de pessoas, como é o caso da disseminação de programas maliciosos. Além disso, os vestígios que poderiam permitir a identificação e a localização dos autores desses crimes podem se perder definitivamente em pouco tempo. O criminoso pode estar em qualquer parte do planeta e, mesmo assim, pode conseguir atingir alvos em quaisquer localidades, por mais longínquas que estejam. Na verdade, o espaço cibernético conseguiu juntar virtualmente todo o planeta, transformando-o numa teia acessível por todos, de qualquer parte. Aproveitando-se desse fato, muitas quadrilhas que atuavam da forma tradicional estão migrando suas atividades criminosas para o espaço cibernético, por julgarem correr menos riscos e por obterem maiores ganhos financeiros em menor espaço de tempo. Esses criminosos estão cooptando jovens com conhecimentos de informática para fazerem parte de suas quadrilhas, com atuação na parte mais técnica, que exige maior experiência no assunto [1, 2, 3, 4, 5, 6, 7, 8].

Muitas dessas quadrilhas têm atuação internacional, são compostas por membros residentes em vários países. Usam as técnicas mais modernas e eficazes na consecução de suas atividades criminosas. Eles compartilham informações sem qualquer burocracia, disseminam conhecimentos, descobertas, dados e programas obtidos.

Vários organismos internacionais tomaram, ou estão tomando, medidas sérias para o combate a esses crimes. O G8, grupo dos oito países mais industrializados, criou e mantém a Rede 24x7. O Conselho da Europa criou a Convenção dos Crimes Cibernéticos. A Organização dos Estados Americanos (OEA), a Organização das Nações Unidas (ONU), o Banco Mundial e outros organismos internacionais vêm discutindo o assunto de forma recorrente, gerando grande quantidade de documentos. As agências policiais de todo o mundo estão preocupadas com o assunto e estão tomando as medidas que julgam corretas e pertinentes.

A Rede 24x7 do G8 é bastante ágil, contudo suas ações e abrangência são muito limitadas. Essa rede funciona bem para a solicitação da preservação das informações que poderão ser usadas para a comprovação da materialidade e autoria dos crimes, até que se consigam as necessárias cartas do MLAT (*Mutual Legal Assistance Treaty*) ou Cartas Rogatórias. Contudo, essas cartas demoram muito e por isso não se prestam para serem utilizadas em casos de crimes cibernéticos, pois os vestígios são muito voláteis e podem se perder em pouco tempo. Além disso, em se tratando de crimes cibernéticos, os incidentes acontecem muito rapidamente, necessitando de ações imediatas.

A Convenção dos Crimes Cibernéticos do Conselho da Europa deve dar bons resultados a médio prazo, quando um grande número de nações a tiver ratificado e ela já estiver operando em muitos países. Por enquanto, os resultados práticos dessa convenção ainda são isolados e de pouco expressividade, até mesmo porque sua operação iniciou há muito pouco tempo, com um número reduzido de países, e movimentação no espaço cibernético não muito significativa.

As discussões e os documentos da OEA, da ONU, do Banco Mundial e de outros organismos internacionais ainda não geraram resultados práticos que pudessem contribuir de forma efetiva para o combate aos crimes cibernéticos. Com certeza, as iniciativas desses organismos internacionais são de grande relevância, a expectativa é surjam bons resultados a partir dessas ações.

II. Situação atual

Considerando os procedimentos rotineiros utilizados de forma geral, normalmente são necessárias Cartas Rogatórias para possibilitar o afastamento dos sigilos telemáticos e a obtenção dos dados das pessoas investigadas junto aos Provedores de Serviços de Internet localizados no exterior. Devido à grande morosidade desses procedimentos, quando são concluídos, os provedores de serviços de Internet responsáveis pela guarda dos dados já liberaram as mídias magnéticas que continham os dados de interesse, tornando os vestígios perdidos.

Sabe-se que grande parte dos provedores de serviços de Internet mantém as suas cópias com os *logs* dos acessos e demais vestígios por, no máximo, noventa dias e, às vezes, por período ainda menor, visto que ainda não existem leis que regulamentam suas atividades, obrigando-os a preservarem os dados por mais tempo. Considerando a atual forma de trabalho, com a necessidade de Cartas Rogatórias e demais procedimentos, este prazo não é suficiente, o que inviabiliza todo o trabalho de investigação.

Há vários casos trabalhados em que criminosos brasileiros, fazendo uso do espaço cibernético, atacaram sítios de entidades governamentais estrangeiras, causando danos sérios. Quando o processo chega no momento de serem realizadas as investigações e as perícias, já se passaram seis meses, um ano ou até mais, não havendo como descobrir a autoria do crime, pois os dados já se perderam.

De forma semelhante, quando são solicitados dados que estão armazenados em provedores de serviços de Internet no exterior, para efeito de identificação e de localização de suspeitos, a solicitação muitas vezes sequer chega a ser feita, em decorrência da grande morosidade dos procedimentos. Isso acontece porque, quando se trata de crimes cibernéticos, não é possível esperar os prazos exigidos pelos procedimentos feitos por meio das Cartas Rogatórias.

Houve casos em que foram feitas tentativas junto aos provedores estrangeiros de serviços de Internet com representação no Brasil, no sentido de buscar informações de criminosos brasileiros, com base em ordens judiciais. A informação recebida foi de que os dados estavam armazenados em computadores localizados no exterior, e que apenas o Poder Judiciário daquele país poderia autorizar a quebra do sigilo telemático. Essa ordem judicial somente poderia ser obtida por meio de uma Carta Rogatória.

III. Cenário dos crimes cibernéticos nos próximos anos

O espaço cibernético está sendo utilizado cada vez mais para a prática de crimes. A tendência assinalada é de crescimento das atividades criminosas por meio do espaço cibernético. Dessa forma, questiona-se como seria o cenário mundial no ano de 2020, a respeito desse tipo de atividade criminosa. Para tentar responder a essa questão, é importante lembrar que há 15 anos esse tipo de crime era muito incipiente ou quase inexistente, e que nesse espaço de tempo ele experimentou um vertiginoso crescimento e um aperfeiçoamento incomparáveis.

Pode-se inferir que ocorrerá daqui a 15 anos um cenário em que os criminosos terão muito mais conhecimentos e habilidades no uso da informática e na prática dessa modalidade de crime, visto que esses infratores nasceram ou terão nascido na era da cibernética e da inclusão digital. Além disso, os pacotes de softwares utilizados para a prática dos crimes estão sendo comercializados pela Internet a custos acessíveis, ou que até podem ser obtidos gratuitamente. Assim, é possível prever que nesse cenário esses criminosos deverão fazer uso da Internet, de computadores e de outros recursos da Informática como ferramentas para a prática de suas atividades criminosas.

Diante do quadro assinalado, de um lado as autoridades governamentais, responsáveis pela persecução penal dessas atividades criminosas e sensíveis aos problemas cibernéticos, devem adotar, desde já, medidas eficazes para o combate dessas condutas, pois o espaço cibernético poderá se tornar muito inseguro, vulnerável e de baixa confiabilidade, comprometendo o avanço das atividades responsáveis que vêm sendo conduzidas por meio da Internet, tanto nos campos científico e comercial, como na área de governo.

De outro lado, as polícias têm que se preparar adequadamente, por meio do treinamento de seus policiais, da aquisição de ferramentas, da formação de doutrinas, da cooperação policial internacional e da adequação e modernização de sua estrutura de combate aos crimes cibernéticos, de forma a se tornar uma única grande unidade especializada em investigação de crimes cibernéticos, pois praticamente todos os crimes estarão fazendo uso do espaço cibernético, de computadores e de outros recursos da informática para a prática de suas condutas criminosas [4, 5, 6, 7, 8].

Nesse sentido, urge que os policiais, no mais curto prazo possível, sejam habilitados, por meio de treinamentos específicos, a investigar os crimes de suas respectivas áreas de competência também quando praticados dentro do espaço cibernético. As agências policiais, da mesma forma, devem buscar procedimentos céleres de cooperação policial internacional, com a utilização de redes conectando o maior número possível de países, que possibilitem o estabelecimento de intercâmbio de informações de investigação, em consonância com a velocidade que experimentam os crimes cibernéticos.

Dessa forma, poder-se-á garantir uma atuação policial efetiva no combate aos crimes cibernéticos, mesmo nos casos em que os efeitos dos crimes são espalhados em vários países, estando os criminosos muitas vezes localizados em países distintos e distantes entre si, de forma organizada em quadrilhas internacionais.

IV. Estrutura das agências policiais

Os chamados “crimes cibernéticos” normalmente podem ser enquadrados em crimes já tipificados na legislação penal brasileira, pois estão sendo cometidos os crimes já existentes, apenas utilizando a informática e o espaço cibernético como uma ferramenta adicional às atividades criminosas. Um exemplo típico dessa assertiva é a ação do estelionatário, que é muito criativo e sempre encontra no espaço cibernético uma fonte inesgotável de possíveis vítimas.

Observa-se que os crimes cibernéticos estão ocorrendo dentro de várias áreas de atuação da polícia. Por meio do espaço cibernético, são cometidos crimes de tráfico de drogas, de exploração sexual de crianças, de lavagem de dinheiro, de colarinho branco, de dano, de falsificação de documentos públicos, de estelionato, de apologia de crime ou fato criminoso, crimes fazendários, e muitos outros [8].

Vale ressaltar que as atividades criminosas estão fazendo e continuarão a fazer cada vez mais uso da informática e do espaço cibernético na consecução dos objetivos criminosos. Nesse contexto, é possível que em breve chegue o momento em que todas as áreas operacionais das polícias terão que estar aptas a também fazerem as suas investigações no espaço cibernético.

Dessa forma, as várias áreas de atuação das polícias terão que se estruturar para atuarem e investigarem os crimes de suas respectivas competências também quando praticados no espaço cibernético. Isso pode ser feito por meio da criação de setores específicos de repressão aos crimes cibernéticos dentro de cada uma dessas áreas, para que atuem no combate aos crimes de suas competências respectivas, praticados dentro e fora do espaço cibernético.

É importante que todas as áreas de atuação das polícias tenham seus próprios setores de repressão aos crimes cibernéticos, visto que dessa forma certamente serão evitadas possíveis sobreposições de atribuições, pois tais unidades especializadas somente atuariam na repressão dos crimes de suas respectivas competências. Assim, possibilitar-se-ia a especialização dos policiais nos crimes de suas áreas de atuação, bem como seria evitada a duplicidade de esforços e as possíveis invasões de atribuição entre as várias áreas das agências policiais.

Se fosse criado apenas um setor ou uma diretoria de crimes cibernéticos dentro da polícia, esse fato poderia gerar, além da sobreposição de atribuições com relação aos órgãos operacionais das polícias, uma grande concentração de atividades nesses novos órgãos especializados em crimes cibernéticos, podendo até inviabilizar suas atividades, pois é grande o crescimento da incidência de crimes praticados no espaço cibernético ou com a utilização de computadores e outros recursos de informática.

Entende-se que as principais unidades operacionais e centrais das agências policiais devem ser contempladas com treinamentos e ferramentas específicos, preferencialmente à criação de setores formais especializados na repressão aos crimes cibernéticos. Assim, os policiais devem ser habilitados a investigarem os crimes de suas respectivas áreas de atuação também quando praticados com a utilização da informática e do espaço cibernético. Dessa maneira, todas as unidades da polícia poderiam continuar trabalhando em suas áreas de atuação, sem haver sobreposição de atribuições nas investigações e o grupo de policiais especializados em crimes cibernéticos poderia estar inserido numa estrutura formal para a atuação nas investigações dos crimes de suas respectivas competências, quando praticados no espaço cibernético.

Dessa forma, as agências policiais, com o objetivo de enfrentar o cenário previsto neste trabalho, tornar-se-iam uma grande e moderna unidade policial de crimes cibernéticos, preparada para investigar todos os crimes de sua competência, praticados dentro ou fora do espaço cibernético, com ou sem a utilização de computadores e de outros recursos da informática. Estariam preparadas para enfrentar talvez um dos maiores desafios e uma das maiores ameaças da criminalidade neste século XXI. Esses desafios e ameaças estão vindo e continuarão a vir pelo espaço cibernético, estão atingindo e continuarão a atingir alvos de toda a sociedade moderna.

V. Cooperação policial internacional direta

O mundo está se convencendo de que a cooperação policial internacional para o combate aos crimes cibernéticos, por meio da adoção de mecanismos céleres, é imprescindível para se levar a bom termo a persecução criminal dessa nova modalidade de ilícitos. As ações de combate aos crimes cibernéticos, principalmente quando dois ou mais países estão envolvidos, não podem esperar os prazos dilatados dos mecanismos convencionais de cooperação internacional. Os mecanismos mais comuns para a busca e a validação de vestígios provenientes do exterior são a tradicional Carta Rogatória, as cartas do *Mutual Legal Assistance Tready* (MLAT) e as solicitações da Rede 24x7 do G8.

A Carta Rogatória precisa passar pelas supremas cortes dos países envolvidos, após a adoção de vários procedimentos morosos, como a tradução juramentada e o encaminhamento de um país para outro, normalmente necessitando de prazos superiores a dois ou três anos para a sua conclusão. Certamente essa medida não se presta para a utilização em casos de crimes cibernéticos, que exigem atuação imediata dos órgãos governamentais [8].

O MLAT, embora possa ser mais célere do que outros mecanismos, também é bastante burocrático e lento. Além disso, o MLAT é um acordo bilateral entre os Estados Unidos e vários outros países. Assim, somente é possível utilizar o MLAT com os Estados Unidos, nos casos em que seja necessária a cooperação com outras nações, esse canal não está disponível.

A Rede 24x7, organizada e mantida pelo *Subgroup on High-Tech Crime* do grupo dos 8 países mais industrializados, identificado como G8, é bastante célere, as comunicações entre os pontos de contatos são feitas por telefone ou por mensagens eletrônicas, garantindo a maior rapidez possível, durante 24 horas por dia e 7 dias por semana. Esse é o espírito da Rede, a partir do qual decorre o seu nome. No entanto, a Rede 24x7 ainda é bastante limitada, tanto em termos de quantidade de países membros (atualmente há pouco mais de 40 países filiados), como de sua reduzida atuação. Hoje, a Rede 24x7 somente se presta para que os países-membro sejam acionados sejam acionados para solicitarem aos Provedores de Serviços de Internet (PSI) a preservação dos vestígios relativos aos crimes praticados por meio do espaço cibernético, evitando a perda dessas informações. Contudo, para que essas informações realmente sejam obtidas pelo país solicitante, é necessário que o requerimento seja feito por meio de um acordo de cooperação jurídica, como o MLAT, ou por meio de Cartas Rogatórias.

Para tentar minimizar essas adversidades na condução das investigações, propõe-se a adoção da Cooperação Policial Internacional para o Combate aos Crimes Cibernéticos (*International Police Co-operation to Combat the Cyber Crimes – IPCCCC*).

Além do Conselho da Europa, várias outras organizações internacionais, como as Nações Unidas, a Organização dos Estados Americanos (OEA), a União Européia, a *European Police Office* (Europol) e a Interpol, também estão adotando suas medidas visando à cooperação policial internacional para o combate aos crimes cibernéticos.

Dadas as características dessa ação criminosa, em que muitas vezes as suas provas são perdidas em poucos meses ou semanas, para o seu combate efetivo é necessária a cooperação policial internacional entre os agentes públicos encarregados deste mister, que deve ser feita por meio de grupos organizados e estruturados em cada um dos países, objetivando adotar imediatamente todas as medidas necessárias. Dessa forma, em se tratando de crimes cibernéticos, é imprescindível que as ações sejam tomadas de forma extremamente célere, pois, de outra forma, perder-se-iam definitivamente todos os vestígios, inviabilizando-se o trabalho da investigação policial.

VI. IPCCCC

O IPCCCC consiste no estabelecimento de cooperação policial internacional, por meio da adoção de mecanismos ágeis no combate aos delitos cibernéticos, especialmente aqueles que têm repercussão internacional. Os mecanismos propostos procuram evitar, sempre que possível, todos os procedimentos burocráticos e morosos, incompatíveis com a velocidade que experimentam os crimes cibernéticos e com a agilidade dos criminosos [8].

No âmbito do IPCCCC, está sendo considerada a necessidade da "nacionalização" das provas produzidas no exterior, por meio dos procedimentos estabelecidos. Essa cooperação policial internacional para o combate aos crimes cibernéticos tem como pressuposto a existência de Grupos Técnicos formados por policiais especializados na investigação desses crimes, estruturados e organizados em cada um dos países participantes. Para que o IPCCCC funcione em sua totalidade, é necessária a adesão do maior número possível de países, para que essa cooperação se torne universal e possa alcançar todas as localidades conectadas na Internet. As ações e os mecanismos propostos serão adotados principalmente principalmente pelos Grupos Técnicos de cada país, da forma mais ágil possível e com o mínimo de formalidade.

Pode-se considerar a participação da Rede 24x7, organizada e administrada pelo G8, da qual o Brasil é membro. Essa Rede, também conhecida como "G8 24/7 *Computer Crime Network*", já possui pontos de contato, está estruturada em mais de 40 países, e pode ser utilizada na implantação do IPCCCC, com as devidas estruturações e adequações em alguns de seus pontos de contato, quando for o caso. Para tanto, é necessária a existência de policiais especializados em crimes cibernéticos em todos os países participantes, que funcionarão como os pontos de contato da Rede. É importante que os membros desses grupos sejam policiais com formação em Ciência da Computação ou com bastante conhecimento e experiência em crimes cibernéticos. O ideal é que esses grupos sejam criados em todos os países conectados na Internet, de forma que a cooperação seja universal e feita por todos, de maneira uniforme.

VII. Conclusões

Os crimes cibernéticos estão experimentando um grande crescimento nos últimos anos. Se tais atividades criminosas não forem combatidas com o devido vigor, pode haver grande prejuízo nas atividades lícitas que vêm sendo conduzidas por meio do espaço cibernético, tanto as atividades governamentais, como as comerciais e as científicas. Nos casos em que as atividades criminosas ultrapassam as fronteiras do país, é imprescindível que haja cooperação policial internacional, por meio dos grupos de cooperação formados pelos órgãos governamentais responsáveis, de modo a ser possível enfrentar com maior probidade essa nova face do crime do século XXI.

Os criminosos estão, dia após dia, migrando suas atividades ilícitas para o espaço cibernético. Observando a tendência evidenciada e discutida neste artigo, em 15 anos, praticamente todos os criminosos estarão fazendo uso do espaço cibernético e/ou de computadores e outros recursos de informática na realização de suas atividades criminosas. Para se conviver nesse ambiente, as polícias têm que se preparar, adaptando-se a essa realidade mutante, para o enfrentamento dessa nova modalidade criminosa.

Neste artigo são propostas duas ações para um combate mais eficiente e eficaz desses crimes: a) modernização das investigações, incluindo o treinamento dos policiais, para que os mesmos possam investigar os crimes de suas respectivas competências dentro do espaço cibernético, bem como a criação de setores especializados na repressão dos crimes cibernéticos dentro da estrutura das várias áreas de atuação das polícias e; b) estabelecimento de cooperação policial internacional, por meio do IPCCCC, especialmente nos casos em que dois ou mais países estejam envolvidos na investigação e/ou na prática dos crimes.

Infere-se que a modernização proposta possibilitará uma ação mais efetiva da polícia, quando serão utilizados policiais já especializados em suas respectivas áreas de atuação, para que esses próprios especialistas também façam investigações no espaço cibernético. Dessa forma, serão evitadas possíveis duplicações de esforços e invasões de atribuições de uma área em relação às outras.

Quanto à cooperação policial internacional proposta – a IPCCCC –, ela permitirá que as investigações internacionais envolvendo dois ou mais países sejam eficazes e mais agilizadas. Serão evitados procedimentos morosos para a obtenção de vestígios estrangeiros, como as Cartas Rogatórias. O IPCCCC pode possibilitar ações imediatas, em tempos compatíveis com a velocidade que experimentam os crimes cibernéticos, com informalidade e rapidez semelhantes às das ações ilícitas dos criminosos do espaço cibernético.

Dessa forma, as ações propostas neste artigo podem permitir que as agências policiais se antecipem a esse cenário de mudança que as envolve e as limita, possibilitando o enfrentamento dessa modalidade criminosa, no momento adequado.

Referências Bibliográficas

[1] Ashcroft, John, "Electronic Crime Scene Investigarion: A Guide for First Responders", U.S. Department of Justice Office of Justice Programs, 93pp., 2001.

[2] Carrier, Brian, "Defining Digital Forensic Examination and Analysis Tools Using Abstraction Layers", In: International Journal of Digital Evidence, Winter 2003, Volume 1, Issue 4, 12pp, 2003.

[3] Cassey, Eoghan, "Error, Uncertainty, and Loss in Digital", In: International Journal of Digital Evidence, Summer 2002, Volume 1, Issue 2, 45pp, 2002.

[4] Silva, Paulo Quintiliano da, "Crimes Cibernéticos no Contexto Internacional", In: Anais do XIII Congresso Mundial de Criminologia, Rio de Janeiro-RJ, Brasil, 8pp., 2003.

[5] Silva, Paulo Quintiliano da. "Perícias em Crimes Cibernéticos", In: Anais do XVII Congresso Nacional de Criminalística, Londrina-PR, Brasil, 8pp., 2003.

[6] Silva, Paulo Quintiliano da. "Crimes Cibernéticos e seus Efeitos Multinacionais", In: Revista Perícia Federal, Brasil, 6pp., 2004.

[7] Silva, Paulo Quintiliano da. "Cooperação Policial Internacional no Combate aos Crimes Cibernéticos", In: Proceedings of ICCyber'2004 – First International Conference on Cyber Crime Investigation, 7pp, 2004.

[8] Silva, Paulo Quintiliano da, "Crimes Cibernéticos sob uma Abordagem Investigativa", Monografia do curso MBA em Gestão de Segurança Pública, FGV, Brasília-DF, Brasil, 60pp, 2005.