



São Paulo, Brazil
October 29-30, 2018

The Tenth International Conference on
FORENSIC COMPUTER SCIENCE and CYBER LAW

www.ICoFCS.org

DOI: 10.5769/C2018012 or <http://dx.doi.org/10.5769/C2018012>

Brasil como principal alvo de ataques cibernéticos

Paulo Quintiliano¹, Coriolano Camargo², and Anthony Reyes³

(1) IPOG and QUINTILIANO ADVOCACIA

Email: paulo.quintiliano@hotmail.com, www.quintiliano.adv.br

(2) FIESP and OAB

Email: coriolanoaurelio@uol.com.br

(1) HTCIA International

Email: anthony.reyes@htcia.org

Abstract: Neste artigo são apresentados os cenários atuais dos crimes cibernéticos, bem como a evolução dessas condutas e as razões que levaram essa modalidade criminosa a aumentar de forma vertiginosa, especialmente no Brasil. Também são apresentados cenários prospectivos para os crimes cibernéticos, em função da evolução até então observada. São apresentadas as alternativas existentes para o enfrentamento dessa modalidade criminosa, bem como alternativas mais eficazes, baseadas em procedimentos ágeis e sem burocracias, com a finalidade de se levar a bom termo a investigação e toda a persecução penal dos crimes cibernéticos, especialmente aqueles com efeitos globais. São discutidas as possibilidades da criação de um tribunal criminal internacional para a persecução dos crimes cibernéticos com efeitos globais.

Key words: Crimes cibernéticos, investigação cibernética, cooperação internacional, crimes globais, tribunal criminal internacional para crimes cibernéticos.

I. Introdução

A sociedade como um todo está, dia após dia, fazendo uso da internet de forma cada vez mais intensa. Os recursos da alta tecnologia são utilizados por todas as pessoas, quer sejam crianças ou idosas, em suas atividades diárias. Dentre outras finalidades, a internet é utilizada para o entretenimento, trabalho, compra e venda de produtos, em que são movimentadas quantidades estratosféricas de recursos financeiros.

Observa-se claramente esse mesmo movimento com relação aos criminosos, eles também estão fazendo intenso uso dos recursos tecnológicos em suas práticas criminosas. Atualmente, o

principal objetivo do criminoso do espaço cibernético é a obtenção de vantagens financeiras de forma ilícita. Ele procura esse meio tecnológico para as suas práticas criminosas, em decorrência da possibilidade de gozar do suposto anonimato, desta forma procurando mitigar os riscos e maximizar a lucratividade.

A legislação brasileira precisa ser atualizada para que os órgãos encarregados da persecução penal desses crimes possam promover um enfrentamento mais eficaz dessa modalidade criminosa. É necessária a previsão de penas mais severas para os crimes cometidos por meio do espaço cibernético, pois seu poder ofensivo é muito maior, podendo uma mesma conduta atingir milhões de pessoas ao mesmo tempo.

2. Cenário atual dos crimes cibernéticos

No cenário atual dos crimes cibernéticos pode ser observada uma forte migração das atividades criminosas para o espaço cibernético. Inicialmente, os crimes federais, mais complexos, como corrupção e lavagem de dinheiro, começaram a fazer uso dos recursos tecnológicos como ferramenta, em suas práticas delitivas.

Contudo, atualmente todos os crimes, por mais simples que sejam, em decorrência da ampla popularização da alta tecnologia, podem ser praticados com a utilização desses recursos tecnológicos como ferramentas de apoio à prática criminosa. Até mesmo os simples “ladrões de galinha” usam recursos tecnológicos em suas práticas criminosas, no mínimo utilizam o aplicativo *WhatsApp* para acertar detalhes do crime com seus comparsas. Nesse sentido, as provas são digitais e demandam tratamento especializado em sua obtenção, salvaguarda e processamento.

Além de tudo, os criminosos do espaço cibernético exigem segurança da informação, criptografia forte, backup nas nuvens, dentre outros, com relação aos recursos tecnológicos utilizados. Seguramente, se o aplicativo *WhatsApp* sofresse o *downgrade* desejado por alguns membros do Poder Judiciário, os criminosos imediatamente deixariam de utilizá-lo e procurariam outro aplicativo concorrente, com segurança forte.

De fato, os criminosos, a exemplo do que ocorre com a sociedade como um todo, estão totalmente dependentes dos recursos tecnológicos, especialmente da internet, para a prática de suas atividades criminosas. Com certeza, possíveis quedas do serviço de internet prejudicariam muito as suas atividades ilícitas.

Ultimamente, esses criminosos têm buscado atuação multinacional, por meio de parcerias firmadas entre eles. Dessa forma, podem perpetrar golpes estratosféricos, com efeitos globais, podendo atingir milhões de vítimas em dezenas de países e auferindo bilhões de dólares de lucros, de forma ilícita. Como exemplo desse

tipo novo de atuação, pode-se citar os ataques de ransomware.

São golpes complexos, em que as evidências que poderiam comprovar a materialidade e principalmente a autoria dos crimes podem estar armazenadas em países distantes. Definitivamente, a investigação é muito complexa, sendo necessária a cooperação judiciária internacional para ser viável a persecução penal desses crimes.

As vantagens ilícitas obtidas são pagas por meio de criptomoedas, o que dificulta e, às vezes, até impossibilita o rastreamento e a localização dos criminosos. São utilizadas criptomoedas cada vez mais difíceis de serem rastreadas, como a Monero.

Nesse atual cenário, os criminosos cibernéticos são pessoas com maior familiaridade com os recursos da alta tecnologia, visto que já nasceram na era da Informática, desde crianças já usavam recursos tecnológicos. Em decorrência, o uso da alta tecnologia na prática criminosa vem se consolidando como regra.

Para enfrentar esse cenário que deve piorar drasticamente, o Estado, principalmente os órgãos encarregados da persecução penal, precisa se preparar melhor, por meio do treinamento de seus membros, aquisição de equipamentos e softwares específicos para o apoio de suas atividades. Somente dessa forma, o Estado poderá promover um enfrentamento mais eficaz do crime cibernético.

3. Evolução do crime Cibernético

Com a popularização da internet, em que as pessoas passaram a utilizar esse recurso tecnológico como apoio às suas atividades, inclusive aquelas que envolvem pagamentos de produtos ou transferências bancárias, surgiram os crimes cibernéticos. São atividades ilícitas praticadas por meio do espaço cibernético.

Nos primórdios, os autores dessa conduta ilícita tinham como principal objetivo tão-só comprovar que eram os bons, que conseguiam burlar todos os mecanismos de segurança das vítimas. Enfim, o objetivo era mais romântico, mais exibicionista, sem maiores pretensões. Contudo, atualmente o

objetivo desses criminosos está focado na obtenção de vantagens financeiras ilícitas.

Especialmente depois das duas últimas ondas de automação bancária – *home banking* e *mobile banking*, em que o uso de telefones celulares inteligentes se tornou muito comum na realização de operações bancárias e outras igualmente sensíveis, os criminosos passaram a contar com essa grande facilidade e oportunidade para a prática de suas condutas ilícitas. Essa mobilidade permitiu que os criminosos pudessem agir com mais facilidade, de qualquer lugar que estejam.

De fato, os criminosos buscam os meios tecnológicos, incluindo-se a internet, para suas práticas criminosas com a finalidade de mitigar os riscos e maximizar os lucros de seus negócios ilícitos. Os criminosos não querem enfrentamento armado com a polícia, preferem se esconder no suposto anonimato proporcionado pela internet, bem como auferir lucros maiores em menor espaço de tempo.

Segundo o relatório da empresa Symantec, denominado “2017 Norton Cyber Security Insights Report Global Results”, 62,21 milhões de pessoas no Brasil se tornaram vítimas de criminosos do espaço cibernético, no ano de 2017. Segundo esse relatório, somente a China (352,70 Mi), Índia (186,44 Mi) e Estados Unidos (143,70 Mi) ficaram à frente do Brasil.

Em termos volume de prejuízos causados pelo crime cibernético, em 2017 o Brasil aparece em 2º lugar, com prejuízos de U\$ 22,5 bilhões. Em primeiro lugar, aparece a China com U\$ 66,3 bilhões.

Conforme as investigações reportadas pelo relatório denominado *Economic Impact of Cybercrime — No Slowing Down*”, emitido pelas empresas McAfee e *Center for Strategic and International Studies* (CSIS), o Brasil possui um dos ecossistemas de crimes cibernéticos mais exclusivos do mundo, contando com grande quantidade *hackers black-hat*, em que seriam oferecidos até mesmos cursos online sobre spam e desenvolvimento de malware.

Esse mesmo relatório assegura que 54% dos ataques cibernéticos registrados no Brasil são originários do próprio país, bem como que o crime financeiro mais comum no Brasil é praticado por

meio da internet contra Bancos e instituições financeiras, em que 95% das perdas sofridas pelos bancos brasileiros são originadas de ataques cibernéticos.

Esse relatório da McAfee também informa que no Brasil mais da metade de todas as transações bancárias são feitas por meio de dispositivos conectados à Internet e que a falta de leis fortes contra o cibercrime torna o Brasil um dos alvos preferidos dos ataques online.

De fato, as leis brasileiras contra os crimes cibernéticos são muito frágeis. A Lei Nº 12.737/2012, conhecida como Lei Caroline Dieckmann, incluiu o artigo 154A no Código Penal. Este dispositivo prevê penas de reclusão de 3 meses a um ano para os crimes de invasão de dispositivo informático alheio, produção ou disseminação de código malicioso, podendo a pena ser aumentada a até 2 anos, em casos específicos. Assim, no Brasil, esses crimes cibernéticos próprios são considerados infrações penais de menor potencial ofensivo, conforme o artigo 61 da Lei Nº 9.099/1995. Assim, tais crimes são de competência dos Juizados Especiais Criminais.

Esse tratamento leniente e tolerante com o crime cibernético certamente motiva os criminosos a escolherem o Brasil como alvo preferido de seus ataques. Nos Estados Unidos a pena para a invasão de sistemas informáticos alheios pode chegar até 15 anos de reclusão, sendo que na China as penas são ainda mais rigorosas.

Em decorrência dessa tolerância, o Brasil vem sistematicamente subindo no ranking dos países preferidos pelos criminosos cibernéticos. Se nada mudar, a tendência é que em um período de dois a cinco anos o Brasil supere a China, tornando-se o principal alvo dos ataques cibernéticos no mundo.

Quando os ataques são provenientes de outros países, a investigação se torna mais complexa, são necessárias cooperações judiciais internacionais para a busca das provas, o criminoso deve ser julgado com base nas leis de seu país. Contudo, conforme o relatório da McAfee, 54% dos ataques sofridos no Brasil são originários do próprio país. Tal fato

indiscutivelmente facilita em muito a investigação e a persecução desses crimes. Ainda assim, o índice de sucesso nas investigações é muito baixo, em decorrência da frágil legislação e da falta de melhor estruturação e treinamento dos órgãos encarregados da persecução penal.

Se o país não consegue prover um enfrentamento contundente contra o crime cibernético praticado dentro do território nacional, muito pior desempenho terá com relação aos crimes praticados a partir de outros países. Tal perspectiva sinaliza para uma total impunidade, com relação a esses ataques estrangeiros.

4. Cenário prospectivo do crime cibernético

A tendência é que os criminosos do espaço cibernético continuem a atuar no formato de quadrilhas organizadas, muitas vezes com seus membros espalhados em vários países, para envidar esforços na aplicação de golpes com efeitos globais, em que os lucros serão auferidos por meio de criptomoedas, a exemplo dos ataques de *ransomware*. Seguramente, novas modalidades e variantes desse tipo de ataque surgirão. As criptomoedas, em decorrência da dificuldade de rastreamento do dinheiro, sempre deverão ser utilizadas nos novos golpes.

Esse tipo de ação criminosa, por ser mais complexa e ter efeitos globais, muitas vezes torna a investigação e a persecução penal inviáveis. Essa impunidade certamente ocorre em países que não possuem estrutura de investigação adequada.

O Brasil, em decorrência da fragilidade atual da legislação, se não ocorrerem atualizações significativas nas leis e melhores estruturações dos órgãos estatais, dentro de dois a cinco anos certamente o Brasil terá que conviver com a incômoda situação de ser o principal alvo dos criminosos do espaço cibernético. O país terá que enfrentar fortes ondas de ataques complexos, perpetrados por criminosos espalhados em diversos outros países.

Para que se possa prover um enfrentamento eficaz a um cenário mais complexo que se aproxima, medidas urgentes são necessárias. Além da atualização da legislação nacional e melhor estruturação das polícias, também é imprescindível o estabelecimento de mecanismos de cooperação internacional entre os órgãos encarregados da persecução penal desses crimes dos países envolvidos.

Para se levarem a bom termo as investigações dos crimes cibernéticos com efeitos globais, é necessário o estabelecimento de cooperação policial internacional específica, ágil e sem burocracias. É necessário que tais cooperações sejam concebidas com a mesma visão dos hackers, de forma a ser rápida e eficaz, sem o uso de burocracias incompatíveis com a velocidade dos crimes cibernéticos.

Há uma proposta de criação de um Tribunal Criminal Internacional específico para julgar os crimes cibernéticos com efeitos globais, na ONU. Essa proposta parece ser uma ótima opção para se buscar um enfrentamento mais eficaz dessa modalidade criminosa. Naturalmente haveria a necessidade de adesão dos países a esse tribunal, garantindo-se a sua competência para o julgamento dos crimes cibernéticos com efeitos globais.

5. Necessidade de atualização da legislação nacional

A legislação penal brasileira atual está em vigor desde datas anteriores ao início da Informática, sendo o Código Penal de 1940 e Código de Processo Penal de 1941. Dessa forma, é necessária a atualização desses diplomas legais, de forma que se tornem compatíveis com as características e complexidades dos crimes praticados por meio do espaço cibernético.

Como o Direito Penal não admite analogia, os novos bens jurídicos surgidos em decorrência da alta tecnologia precisam ser protegidos pelo Direito Penal, por meio da criação de novos tipos penais, com previsão de penas altas, compatíveis com o poder ofensivo das condutas que infringem tais bens jurídicos. Essa assertiva se aplica aos

crimes cibernéticos puros, com relação aos novos bens jurídicos.

No que se refere aos crimes cibernéticos impuros, em que os bens jurídicos já são protegidos pelo Código Penal, como o estelionato, os crimes contra a honra e outros, a legislação precisa ser atualizada para aumentar as penas desses crimes quando praticados por meio da internet. Essa majoração é imprescindível, visto que quando o crime é praticado por meio do espaço cibernético o seu poder ofensivo aumenta de forma astronômica, podendo atingir até milhões de vítimas, como é o caso do estelionato praticado pela internet.

Nesses casos, os criminosos podem obter vantagens financeiras ilícitas em volumes estratosféricos, em tempo muito reduzido e com pouco risco, haja vista que se escondem atrás de teclados, usando softwares maliciosos, em busca de suposto anonimato e da impunidade.

Ademais, quando o criminoso perpetra ataque por meio do espaço cibernético contra alvos localizados em outros países, a persecução penal se torna complexa. Nesses casos, como não houve nenhum efeito do crime no território nacional, as polícias judiciárias brasileiras não tomam conhecimento do fato criminoso, sendo que seria necessário um pedido de cooperação judiciária internacional, normalmente por meio de cartas rogatórias. Contudo, normalmente esses mecanismos são muito morosos e normalmente demoram tempo superior à obrigatoriedade dos provedores de acesso à internet de preservarem os registros de acesso à internet, que é de um ano. Assim, torna-se inviável a persecução penal desses crimes.

Normalmente, as evidências que podem comprovar a materialidade, a dinâmica e a autoria dos crimes estão armazenadas em computadores localizados em outros países, fato que dificulta sobremaneira a investigação cibernética e a apuração dos fatos.

6. Conclusões

Atualmente, a sociedade como um todo vem fazendo intenso uso da internet em suas atividades diárias, tornando-se totalmente

dependentes desses recursos tecnológicos. Esse mesmo movimento ocorre com os criminosos, inclusive com os membros das quadrilhas tradicionais de assalto a bancos.

Os novos golpes perpetrados por meio do espaço cibernético apresentam cada vez maior nível de sofisticação, fazendo uso de novas tecnologias e buscando vantagens financeiras ilícitas em criptomoedas.

Atualmente, o Brasil ocupa o segundo lugar no ranking dos países mas afetados pela criminalidade cibernética, atrás apenas da China. Contudo, em decorrência da fragilidade das leis nacionais e da frágil atuação dos órgãos nacionais encarregados da persecução penal dessa modalidade criminosa, a expectativa é que dentro de 2 a 5 anos o Brasil pode se tornar o principal alvo do crime cibernético.

Referências

- [1] BRITO, Auriney. Direito Penal Informático. Editora Saraiva, 2013. ISBN 978-85-02-20942-8.
- [2] CASSANTI, Moisés de Oliveira. Crimes Virtuais, Vítimas Reais. Editora Brasport Livros e Multimídia Ltda. 2014.
- [3] DE LUCA, Newton (obra coletiva). Direito & Internet. Editora Quartier Latin do Brasil. 2ª edição, 2005.
- [4] MALAQUIAS, Roberto Darós. Crime Cibernético e prova: A investigação Criminal em Busca da Verdade. ISBN 978-85-362-5383-1. Curitiba: Editora Juruá, 2ª edição revista e atualizada, 2015.
- [5] PINHEIRO, Patricia Peck. Direito Digital. São Paulo: Editora Saraiva, 6ª edição: 2016. ISBN 978-85-02-63561-6.
- [6] PINHEIRO, Patrícia Peck (obra coletiva). Direito Digital Aplicado 2.0. São Paulo: Editora Thomson Reuters, 2ª edição: 2016. ISBN 978-85-203-6864-0.
- [7] REYES, Anthony (obra coletiva). Cyber Crime Investigations. Editora Amorette Pedersen, 2007. ISBN 978-1-59749-133-4.
- [8] SCHJOLBERG, Stein. A global framework on cybersecurity and cybercrime, and a contribution for peace, security and justice in cyberspace. A Geneva Convention or Declaration for Cyberspace. VFAC Review, No. 12, October 2016, Korean Institute of Criminology.

[9] SCHJOLBERG, Stein. An International Criminal Tribunal for Cyberspace. 13th International Criminal Law Congress in Queenstown. November 11, 2012. The IT Countrey Justice Cybercrime

[10] W. Kraft, and STREIT, Claudia. Ideas on the Establishment of an International Court for Cyber Crime. WCLF 2011.



Paulo Quintiliano, *Ph.D.*

Presidente HTCIA Brazil Chapter
Advogado especialista em
Direito Cibernético
(www.quintiliano.adv.br)
paulo.quintiliano@hotmail.com



Coriolano Camargo, *Ph.D.*

Diretor Titular Adjunto do
Departamento Jurídico da FIESP
e Conselheiro Estadual da
OAB/SP
Advogado especialista em
Direito Digital
(www.almeidacamargo.com.br)
coriolano@almeidacamargo.com.br



Anthony Reyes

Presidente da HTCIA
Internacional
www.arc.com
anthony.reyes@htcia.org