Crimes Cibernéticos

1. Artigo: Atuando para deter o Cibercrime

- *Publicado em 30/04/2018*
- *Atualizado em 30/04/2018*

Em artigo de opinião, o chefe do Escritório das Nações Unidas sobre Drogas e Crime (UNODC), Yury Fedotov, lembra que o custo global dos cibercrimes já chega a 600 bilhões de dólares. Dirigente defende fortalecimento da cooperação entre os países e entre os setores público e privado, para promover capacitação dos atores envolvidos no combate a essas violações.

Por Yury Fedotov, diretor-executivo do Escritório das Nações Unidas sobre Drogas e Crime (UNODC)

Ciber. É o prefixo inevitável que atualmente define nosso mundo. Desde a privacidade das pessoas até as relações entre Estados, o termo "ciber" domina as manchetes e as discussões – tanto é assim que nos arriscamos a sermos paralisados pela magnitude dos problemas que enfrentamos.

Apesar das muitas perguntas pendentes sobre o futuro da cibersegurança e da governança, devemos tomar em conta que a cooperação internacional é o elemento essencial para fazer frente às ameaças cada vez maiores do cibercrime.

A exploração on-line e o abuso de meninas e meninos; os mercados negros cibernéticos para a compra e venda de drogas ilícitas e armas de fogo; os ataques *ransomware* e os traficantes de pessoas fazendo uso das redes sociais para atrair vítimas. O alcance sem precedentes do cibercrime – cruzando fronteiras, em nossos lares, escolas, negócios, hospitais e outros provedores de serviços vitais – somente amplifica as ameaças.

Um estudo recente estimou o custo global dos cibercrimes em 600 bilhões de dólares. O dano infligido ao desenvolvimento sustentável, à segurança, à igualdade de gênero e à proteção – as mulheres e meninas são prejudicadas desproporcionalmente pelo abuso sexual on-line – é imenso.

Manter as pessoas on-line mais seguras é uma tarefa enorme e nenhuma entidade ou governo tem a solução perfeita. Não obstante, há muito que podemos fazer para intensificar a prevenção e melhorar a reposta aos cibercrimes, por exemplo:

- Construir capacidades, principalmente de aplicação da lei para cobrir possíveis brechas jurídicas, particularmente em países em desenvolvimento;
- E fortalecer a cooperação internacional e o diálogo – entre governos e Nações Unidas, assim como com outras organizações internacionais e regionais, a INTERPOL, as empresas e a sociedade civil.

Os crimes relacionados ao crime cibernético, como a propagação de *malware*, *ransomware* e *hacking*, o uso de outros programas para o roubo de dados financeiros, a exploração sexual infantil on-line e o abuso, todos têm algo em comum além do termo "ciber": todos são crimes.

A polícia, os fiscais e os juízes necessitam compreender esses crimes e devem contar com as ferramentas adequadas, que lhes permitam investigá-los e perseguir os criminosos, assim como proteger as vítimas. Devem ser capazes também de processar e judicializar os casos.

No Escritório das Nações Unidas sobre Drogas e Crime (UNODC), estamos trabalhando em mais de 50 países, por meio da prestação da capacitação necessária para aprimorar as habilidades de investigação, o rastreamento de criptomoedas como parte das investigações financeiras, assim como o uso de software para detectar o abuso on-line e perseguir os agressores.

Como resultado direto do fortalecimento de capacidades nos países, um pedófilo de alto risco com mais de 80 vítimas foi preso, julgado e condenado. Ministramos sessões de capacitação em colaboração com o Centro Internacional para Crianças Desaparecidas e Exploradas (ICMEC) e o Facebook. Esse é só um exemplo de como o fortalecimento de capacidades, em coordenação com as organizações da sociedade civil e o setor privado, pode garantir que os criminosos estejam atrás das grades e que as crianças em situação de vulnerabilidade fiquem protegidas.

Em trabalho realizado com a Fundação de Vigilância da Internet (IWF), foram lançados portais para denunciar casos de abuso sexual infantil – mais recentemente em Belize – para que os cidadãos possam tomar iniciativa e reportar imagens de abuso, protegendo as meninas e os meninos da exploração on-line.

Com parceiros como Thorn e Pantallas Amigas, estamos fortalecendo a proteção on-line e educando pais, responsáveis e crianças sobre os riscos cibernéticos, por meio da aproximação com as escolas e as comunidades locais. A prevenção é a chave da questão.

A capacitação do UNODC – focada principalmente na América Central, no Oriente Médio, no Norte e no Leste da África e no Sudeste Asiático – está ajudando também a identificar evidência digital sobre o tráfico ilícito de drogas, a confrontar o uso da *darknet* com fins criminosos e de terrorismo e a melhorar a coleta de dados para abordar melhor as ameaças.

Uma base fundamental para todos nossos esforços é a cooperação internacional. Nosso trabalho – que é inteiramente financiado pelos governos doadores – tem demonstrado que, apesar das diferenças políticas, os países podem se unir para se opor às ameaças dos cibercrimes.

Do mesmo modo, estamos reforçando a cooperação internacional por meio do Grupo Intergovernamental de Especialistas, que se reúne na sede do UNODC, em Viena.

O Grupo de Especialistas, criado por meio de resolução da Assembleia Geral, reúne diplomatas, responsáveis de políticas e especialistas do mundo todo para discutir os desafios mais urgentes do cibercrime. Essas reuniões demonstram o desejo e a vontade dos governos para buscar uma cooperação pragmática, com vistas a melhorar os mecanismos de prevenção e fomentar a confiança.

Como passo seguinte, necessitamos aumentar tais esforços, proporcionando mais recursos para apoiar os países em desenvolvimento que, frequentemente, possuem usuários de Internet mais recentes e defesas mais fracas contra o cibercrime.

As empresas tecnológicas são um aliado indispensável na luta contra o cibercrime. Precisamos fortalecer a relação do setor público com o setor privado de forma a abordar preocupações comuns, melhorando também a educação e detendo a disponibilidade de material de abuso online.

Neutralizar o cibercrime pode salvar muitas vidas, aumentar a prosperidade e construir a paz. Ao reforçar as capacidades de aplicação da lei e criar alianças com empresas de modo que possam ser parte da solução, podemos avançar para assegurar que a Internet seja uma força para o bem.

(Fonte: https://nacoesunidas.org/artigo-atuando-para-deter-o-cibercrime/, data de acesso: 12/08/2020)

2. Criminalidade Cibernética: panorama atual e perspectivas

José Mariano Araujo Filho

Publicado em 09/2019. Elaborado em 09/2019.

DIREITO PENAL

Os cibercrimes têm alcançado um volume significativo nos últimos anos, o que leva a necessidade de um enfrentamento muito mais efetivo por parte das Autoridades de todo mundo. Mas qual a perspectiva no combate aos crimes cibernéticos no Brasil?

Segundo um relatório produzido em 2016 pela empresa de pesquisa em cibersegurança "Cybersecurity Ventures" (http://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016), com sede nos Estados Unidos, até 2021, o custo do cibercrime no mundo deve chegar a US$ 6 trilhões por ano – um valor 15 vezes maior do que o registrado em 2015, de US$ 400 bilhões.

Este tipo de informação é apenas mais uma no universo de dados espalhados pela internet que procuram traçar um panorama sobre as ameaças que cercam a utilização da tecnologia pela população mundial, especialmente aquelas relacionadas a internet.

A maioria dos dados coletados sobre ameaças e crimes praticados por meios eletrônicos, especialmente com a utilização da internet, são produzidos por empresas que comercializam produtos e serviços destinados a proteção cibernética, ou entidades não governamentais.

Por si só, esta situação remete a uma constatação sobre a realidade dos cibercrimes no mundo inteiro: a inexistência de estatísticas oficiais, produzidas através de dados coletados por órgãos de governo com base em dados oficiais.

Longe de lançar algum tipo de polemica sobre a credibilidade das informações coletadas por empresas privadas e entidades não governamentais, esta situação apenas revela o total desinteresse dos órgãos governamentais em conhecer mais sobre a cibercriminalidade e o seu alcance.

Estrategicamente falando, como é possível o combate aos crimes praticados por meios eletrônicos sem que os órgãos responsáveis tenham informações adequadas sobre o "modus operandi" utilizado pelos criminosos, cifras envolvidas, perfis de vítima e outras informações relevantes? Seria algo como combater uma ameaça sobre a qual nada se sabe.

Episódios relacionados ao uso da tecnologia da informação para a prática de delitos tem expandido e, evidentemente, a quantidade de vítimas tem se multiplicado de forma exponencial, enquanto todas as esferas da administração pública no país têm se quedado inerte.

Interessante observarmos que o cibercrime tem se mostrado como um crime que compensa, motivo pelo qual um grande número de criminosos tem se dando ao luxo de comercializar seus conhecimentos para interessados no ingresso a este mundo de possibilidades de ganhos fáceis.

O que descrevemos acima tem levado a uma situação contrastante na qual dois lados intransigentes se opõem: organizações avançadas de cibercriminosos especializados, de um lado, e instituições internacionais com pesquisadores altamente competentes, incluindo profissionais do direito e tecnólogos, de outro. A tecnologia é a mesma, mas é o uso indevido da mesma que separa as boas intenções daquelas condenáveis.

Investigar o cibercrime é um processo cheio de desafios, no qual especialistas em computadores caçam outros especialistas em computadores, o que, evidentemente, remete a necessidade de profissionais cada vez mais preparados para este tipo de enfrentamento.

O trabalho é extremamente intensivo no que diz respeito aos recursos necessários e, mesmo com investigadores competentes, a falta de condições adequadas para investigações pode levar a ações policiais infrutíferas.

Os criminosos conhecedores de computador são bem versados em explorar os benefícios de um mundo onde as fronteiras físicas e virtuais são muito mais difusas do que antes.

Usando a tecnologia da computação, indivíduos com o conhecimento adequado ou grupos de especialistas em computação podem executar atos criminosos em escala colossal.

Isto significa a prática de atos que podem ameaçar a segurança de uma nação, causar estragos financeiros, organizar atividades terroristas ou paralisar redes nacionais vitais, sem nos esquecermos que muitos criminosos acabaram por se especializar na prática de crimes de proporções menores, como furto de identidade, "bullying", fraudes em "e-commerce" e distribuição de pornografia infantil, práticas estas que podem causar muitos danos.

A Internet é hoje o principal canal de negociação de pornografia adulta e de pornografia infantil, com o incremento de sua proliferação decorrente da mudança da distribuição analógica para a digital.

Mas o fato de que o uso sofisticado dos meios de comunicação anônima pode dificultar a identificação do infrator é motivo de grande preocupação para as unidades de investigação de cibercrimes, principalmente em relação ao intercâmbio de pornografia infantil online.

O substancial incremento da pornografia infantil online foi suportado pelo preço decrescente dos dispositivos e serviços técnicos utilizados na produção e comercialização deste tipo de crime, como equipamentos de gravação e serviços de hospedagem se tornando comuns e baratos.

Estes tipos de serviços estão abertos a cerca de dois bilhões de usuários da Internet, o que levou a um aumento significativo do número de clientes em potencial.

Mas a grande preocupação está no fato de que o acesso facilitado acabou atraindo pessoas que não desejavam correr o risco de serem pegos tentando obter pornografia infantil fora da Internet.

Com a mudança da mídia analógica para a digital, um número crescente de imagens de pornografia infantil foi descoberto por intermédio de investigações.

Outro aspecto que provavelmente apoiou esse desenvolvimento é o fato de que a informação digital pode, em geral, ser duplicada sem perda de qualidade.

No passado os consumidores de pornografia infantil que desejassem duplicar e comercializar o material acabavam prejudicados pela perda da qualidade de reprodução, sendo que atualmente um arquivo baixado pode se tornar a fonte de mais e mais duplicações.

Uma das consequências desse desenvolvimento é que, mesmo quando o infrator que produziu o material no primeiro lugar é preso e seus arquivos são confiscados, ainda sim, é uma tarefa muito difícil "remover" os arquivos depois de negociados na Internet.

Em contraste com opiniões diferentes sobre a pornografia adulta, a pornografia infantil é amplamente condenada e os delitos relacionados à esta são amplamente reconhecidos como atos criminosos.

Organizações Internacionais estão engajadas na luta contra a pornografia infantil on-line, devendo ser destacado os avanços proporcionados pela Convenção das Nações Unidas sobre os Direitos da Criança, de 1989, Conselho da União Europeia sobre o combate à exploração sexual de Crianças e Jovens e a Convenção do Conselho da Europa de 2007 para a Proteção das Crianças contra a Sexualidade, Exploração e Abuso sexual, dentre outros.

Infelizmente, essas iniciativas que buscam controlar a distribuição digital de pornografia infantil têm um efeito pouco dissuasivo para criminosos que usam a Internet para se comunicar e trocar pornografia infantil, até por conta do aumento da largura de banda

para acesso à internet que proporcionou uma melhoria na troca de filmes e arquivos de imagens.

E este é apenas um dos diversos crimes praticados com o uso da tecnologia.

Um exemplo bastante atual de fraude cibernética é a fraude bancária na Internet, realizada através da utilização de sofisticados programas de computador, onde a prática delituosa é realizada através de intensivo trabalho de equipe onde alguns membros são especializados em diferentes áreas da operação.

Assim, alguns criminosos são os responsáveis pelo desenvolvimento e atualização de "malware", enquanto outros produzem e espalham vírus, enquanto outros são responsáveis pelo recrutamento de "laranjas" que forneceram suas contas corrente para o recebimento dos valores fruto da expropriação dos ativos financeiros das vítimas.

Outro exemplo ao qual a maioria das pessoas está exposta é o furto de identidade, ação na qual a principal característica é que alguém finge ser outro.

Algo extremamente comum para o possuidor de uma conta de correio eletrônico é o recebimento de um e-mail em que o remetente é supostamente um banco respeitável que precisa verificar os dados pessoais dos clientes, técnica conhecida como "phishing", e onde os criminosos geralmente conseguem obter as informações que desejam por conta da ação do próprio recebedor da mensagem que, inadvertidamente, acaba clicando em algum "link" da mensagem e possibilitando a instalação e execução de programas maliciosos.

Um dos principais desafios são as disparidades entre as regras nacionais em matéria de cibercrime. Apesar de uma maior harmonização da legislação de vários países, permanecem diferenças significativas em escala global.

Toda esta situação torna cada vez mais difícil reprimir atos criminosos cometidos através do território brasileiro, não sendo demasiado afirmar que os cibercriminosos conhecem e exploram as falhas legais e a excessiva burocracia que envolve o combate ao cribercrime.

A consequência desta situação é que um número cada vez maior de criminosos está transferindo suas operações para países onde as leis são menos rigorosas e onde é mais fácil fugir da ação dos órgãos policiais.

Exemplo disto está no fato de que a lei de crimes cibernéticos é muito fraca e quase inexistente em países asiáticos e outros do continente africano.

O cibercrime não tem fronteiras por natureza, o que torna as investigações mais complicadas para as autoridades policiais. Para combater efetivamente o cibercrime, são necessárias disposições transfronteiriças adequadas, a cooperação internacional e a assistência mútua na aplicação da lei.

Mas também é oportuno mencionarmos que muitos criminosos utilizam a seu favor recursos de anonimato oferecidos por provedores de serviço da internet com a certeza de que a burocracia que gira em torno da obtenção internacional de informações, no mínimo,

retardará por prazo indeterminado o aceso a informações essenciais para a elucidação de seus crimes.

A realidade está a demonstrar que os órgãos de investigação em nosso país não dispõem de informações e de recursos mínimos necessários para o combate a uma ameaça tão atual como a cibercriminalidade.

Mesmo com avanços legislativos importantes no Brasil como é o caso da Lei Geral de Proteção de Dados, o que pode ser constatado é o pouco progresso no combate ao cibercrime no Brasil.

Fato é que, apenas a existência de legislação destinada ao combate de vazamentos de dados, elemento importante no combate a ação dos cibercriminosos, não representa qualquer tipo de garantia na aplicação da justiça e muito menos na proteção das pessoas, sendo necessário um esforço concentrado no sentido de dar efetividade aos dispositivos legais tornando mais efetiva a responsabilização daqueles que contribuem direta ou indiretamente para a ação dos criminosos.

Também deve ser mencionado que até mesmo os próprios criminosos estão mudando uma vez que eles se tornaram mais especializados, formando uma economia subterrânea organizada.

Os criminosos são especializados em diferentes serviços individuais, como recrutar laranjas para uso de contas correntes que garantem o acesso a instituições financeiras, distribuição de códigos malicioso através de mensagens com bastante credibilidade, manutenção de “Botnets”, etc.

E mais: este tipo de delinquentes tecnológicos passaram a vender esses serviços a outros criminosos, o que tem acarretado na atualidade a desnecessidade do conhecimento técnico necessário para a execução de ações delituosas, pois os mesmos passaram a disponibilizar o modelo "Crime como serviço", onde a atividade de criminosos cibernéticos é mais fácil de executar e o suporte técnico é fornecido pelo próprio criminoso vendedor.

E como consequência de todo o aperfeiçoamento que a indústria do cibercrime está passando, está o fato de que na atualidade existe um interesse cada vez maior por parte dos criminosos na engenharia social, até pelo fato de ser uma técnica muito mais simples e extremamente eficaz.

Há também uma maior alavancagem de dados furtados que circulam na “Darkweb” ou em sites de vazamento de dados, contendo dados com senhas de pessoas que podem ser usadas para obter acesso não autorizado a vários tipos de contas, tais como correio eletrônico, lojas online, sites de mídia social, contas bancárias, etc.

O acesso a essas contas pode ser útil para coletar informações para fins de engenharia social, fraude ou para a prática de delitos diversos.

Incontroverso é que as pessoas costumam usar a mesma senha para várias contas; portanto, se uma senha for furtada de um site, todas as outras contas poderão ser acessadas.

Se as contas de correio eletrônico estiverem comprometidas, também será mais fácil solicitar redefinições de senha para outras contas.

Desponta daí o fato de que apenas a existência da lei de proteção de dados não terá o condão de modificar todo o panorama exposto, uma vez que, na atualidade, muitos dos casos de vazamentos de dados pessoais não são divulgados e nem mesmo são objeto de investigação.

Fato é que conjuntos de dados furtados são absorvidos pelos "mercados negros "que alimentam um ecossistema de furto de identidade, sendo que, ao final, por uma falta de uma ação mais efetiva no que tange aos vazamentos de dados, a vítima nem mesmo toma conhecimento da divulgação de suas informações pessoais.

A falta de conscientização do usuário, quando combinada com um aumento significativo na atividade criminosa (e táticas aprimoradas), deu origem a várias violações em larga escala do setor público e privado que resultaram em uma epidemia global de problemas envolvendo confidencialidade, integridade e disponibilidade de dados e serviços.

E o resultado não poderia ser outro senão a constatação de que o conjunto de dados comprometidos são absorvidos pelos mercados negros que alimentam um ecossistema de furto de identidade e fomentam a prática de novos crimes.

Os criminosos também estão aproveitando novas tecnologias para lavagem de dinheiro e anonimização, aumentando o rol de possibilidades para a prática de cibercrimes.

O uso de criptomoedas está se tornando um método popular de pagamento, especialmente em casos de ataques de "ransomware", extorsão e DD4BC (DDoS for BitCoin).

A facilidade com que cibercriminosos estão tendo com o uso de criptomoedas e outras técnicas para lavagem de dinheiro torna mais difícil para os investigadores seguirem o dinheiro.

O aumento do uso do "Bitcoin" e de outras moedas criptográficas tornou possível, seguro e fácil exigir e receber pagamentos e transferir dinheiro anonimamente.

Isso teve um impacto dramático sobre o número e o tipo de oportunidades para a prática de crimes cibernéticos, pois enquanto houver uma maneira dos cibercriminosos serem pagos, com risco limitado, os crimes continuarão a aumentar exponencialmente.

Mais uma vez forçoso é concluirmos que não existe uma política eficaz para o combate de crimes cibernéticos financeiros hoje, o que nos leva a constatação de que as organizações precisam aumentar suas defesas e se tornar mais resilientes, pelo simples fato de não existir solução de curto prazo para a crescente epidemia de crimes cibernéticos, o que leva a necessidade de que as grandes empresas se tornem tão ágeis quanto seus atacantes.

E o que não faltam são recursos tecnológicos empregados por criminosos para aperfeiçoar as formas de praticarem os seus delitos e comprometer cada vez mais a segurança digital das pessoas.

Apenas como exemplo, podemos mencionar que os trojans bancários mais atuais estão usando a rede "TOR" para hospedar seus servidores de comando e controle (Retefe, por exemplo).

O uso do TOR, não apenas para anonimizar o acesso do cliente, mas também para destinos de servidor, aumenta a dificuldade de investigação e interrupção de ações criminosas.

Em relação ao crime cibernético, há evidência de que os infratores se associam em ambientes virtuais, principalmente através do uso de fóruns subterrâneos online, disto resulta o fato de que a compreensão dos caminhos que levam a associação dos infratores pode permitir que a sociedade considere as maneiras mais apropriadas de desviá-los da prática de crimes.

Fóruns clandestinos servem como um ponto de entrada no crime cibernético para possíveis infratores, sendo que estes locais também permitem que atores não técnicos aprendam a delinquir e desenvolver suas habilidades.

Nestes fóruns, os participantes mais ativos fornecem a outros membros informações sobre seus interesses e experiência, o que de certa forma, demonstra a facilidade com que informações e técnicas utilizadas para a prática de cibercrimes circulem com tanta rapidez e facilidade.

A análise da evolução do envolvimento de criminosos menos experientes em fóruns clandestinos, pode permitir considerar abordagens de intervenção precoce, com o objetivo de impedir seu envolvimento em atividades criminosas, facilitando ainda o entendimento de quem são os principais atores no cenário local da cibercriminalidade e quais novas ferramentas eles fornecem, o que, simplisticamente falando, pode ser útil para o rápido desenvolvimento de novas formas de defesa e de investigação contra este tipo de delito.

Mas, na atualidade, não existe no Brasil nenhuma iniciativa que promova a utilização de informações provenientes de fóruns clandestinos de informações para a prática de cibercrimes e muito menos de identificação de cibercriminosos que promovam a divulgação e utilização de informações e ferramentas para práticas criminosas.

Exemplo maior do que estamos mencionando está no fato de que não há qualquer notícia nos últimos 20 (vinte) anos de algum tipo de campanha pública governamental (federal, estadual ou municipal) visando alertar a população sobre os perigos a que os cidadãos estão expostos num ambiente virtual.

A natureza assimétrica do crime cibernético exige novas abordagens para uma ação mais eficiente, além do emprego de novas tecnologias voltadas a inteligência policial.

Tradicionalmente, as ameaças às fronteiras nacionais levam à concentração de agentes da lei ou militares nas passagens de fronteira e nos pontos de entrada. Da mesma forma, muitas ameaças criminais são atendidas com o envio de policiais extras em um bairro. Agora, dado o acesso e a facilidade da Internet, qualquer pessoa que possua um computador, um Smartphone ou qualquer outro dispositivo que possa se conectar à Internet é um ponto

potencial de entrada em um país, o que demonstra inequivocamente o nível de ameaça que o cibercrime representa.

Como enfatizam organizações como as Nações Unidas, o crime organizado transnacional abrange fronteiras nacionais e étnicas; e as jurisdições policiais locais também devem estar atentas aos cibercriminosos que operam nas linhas estaduais e regionais. As autoridades de segurança e as unidades de investigação de cibercrimes devem colocar uma nova ênfase na inteligência preventiva para localizar fontes de possíveis ameaças cibernéticas para as organizações e as pessoas que eles devem proteger.

Também é relevante notarmos que os crimes cibernéticos são relativamente novos, o que acarreta a necessidade de respostas mais rápidas por parte dos legisladores e das autoridades policiais.

Um dos problemas críticos enfrentados por todas as organizações policiais é o aumento exponencial de vários tipos de evidências digitais que estas unidades precisam coletar e armazenar, incluindo relatórios, fotos, vídeos e outros registros eletrônicos.

Os departamentos de polícia devem proteger evidências digitais para garantir a integridade da autenticidade das informações, além de fornecer acesso que ofereça responsabilidade verificável.

Nos crimes cibernéticos a coleta da prova com a mais absoluta rapidez é fator de extrema importância para a definição de autoria e comprovação de materialidade delitiva, levando em consideração o fato de que a maioria dos elementos probatórios são extremamente voláteis.

Não havendo uma coleta rápida das provas aumenta a probabilidade do desparecimento destas e da ação dos próprios criminosos no sentido de acobertarem seus crimes, uma vez que muitos dados que registram as técnicas empregadas para a prática delitiva podem ser apagados ou alterados, sem qualquer margem para recuperação.

Ferramentas legislativas adequadas à obtenção de informação, levando em consideração o arcabouço das tecnologias empregadas pelos cibercriminosos, devem ser objeto de respostas através de ações políticas efetivas, isto em todos os níveis do governo.

Exemplo do que estamos a tratar pode ser encontrado na legislação dos Estados Unidos, país onde existem mais de cinquenta estatutos federais que abordam direta ou indiretamente diferentes aspectos da cibersegurança e do cibercrime.

Interessante notarmos que o rol de legislação daquele país voltado para o combate ao cibercrime, incluem a Lei de Dispositivos de Acesso Falsificado e Fraude e Abuso de Computador, de 1984, a Lei de Pesquisa e Desenvolvimento de Segurança Cibernética de 2002 e a Lei de Governo Eletrônico de 2002.

Além disso, várias agências federais norte americanas criaram centros para lidar com ameaças cibernéticas, tais como o "Centro de Crimes Cibernéticos de Defesa" do Departamento de Defesa, o "Centro de Denúncias de Crimes na Internet" do F.B.I., e o

“Centro de Crimes Cibernéticos” do Serviço de Imigração e Alfândega, sendo que outras agências federais atuam na investigação de tipos específicos de cibercrime, como aconteceu na tentativa do D.E.A. de enfrentar o problema das vendas ilegais on-line de medicamentos controlados por meio de farmácias falsas.

As agências policiais de todo o mundo têm procurado responder ao avanço da cibercriminalidade com a expansão do seu conhecimento das mídias sociais, utilizando-as para resolver crimes.

Neste ponto, convêm destacarmos que as mídias sociais continuam a ser uma ferramenta de investigação valiosa para ajudar na aplicação da lei e no rastreamento da identidade dos cibercriminosos.

O desafio é enorme, porque os cibercriminosos são livres das fronteiras nacionais, enquanto os esforços das agências policiais são limitados às jurisdições locais.

Diante da ameaça constante que o cibercrime representa e dos ataques praticados por organizações criminosas altamente organizadas, a pergunta que surge é se as forças policiais do Brasil, com poucos recursos materiais e humanos, não estariam travando uma batalha perdida?

Poucos deixariam de concordar que apenas a existência de legislação por si só e a ausência de recursos financeiros, técnicos ou de mão-de-obra especializada, por parte da maioria das unidades policiais que investigam cibercrimes no Brasil é suficiente para causar um impacto real no crime cibernético.

O denominador comum de todo crime cibernético são os serviços de hospedagem na web que formam uma parte crítica da infraestrutura de TI da economia subterrânea.

Esses serviços fornecem um link vital para a Internet em prol dos cibercriminosos que os utilizam para hospedar mecanismos de comando e controle de “botnets” de computadores sequestrados, armazenar dados furtados e atacar suas vítimas.

Decorre daí que o papel de todas as esferas de governo do país no combate ao cibercrime é fundamental, pois se for criada uma legislação adequada para controlar os provedores de hospedagem e de serviços, isso ajudará bastante a restringir as atividades dos criminosos cibernéticos.

Também é de vital importância entender que o cibercrime é um problema global compartilhado e requer uma resposta global, pois nenhum país ou empresa opera no vácuo e o mundo como um todo precisa construir uma nova geração de parcerias entre entidades transnacionais, nacionais e corporativas.

O déficit de imposição do combate ao cibercrime está sendo causado, em grande parte, pelas dificuldades de conduzir investigações sobre invasores que operam frequentemente no exterior, contra sistemas técnicos diversos e díspares usando de tecnologia de comunicações que torna qualquer ataque desta natureza global por padrão.

Sem a identificação e submissão dos criminosos à justiça, as defesas técnicas tão somente deslocam as ameaças para alvos mais fáceis em novos setores, estados ou países.

Mas é primordial que seja reconhecido que investigar crimes cibernéticos é diferente de investigar tipos tradicionais de crimes, não sendo uma questão de capacidade das unidades policiais de investigação. Toda vítima, detentor de dados ou órgão de investigação, seja no setor público ou privado, faz parte de um ecossistema global cada vez mais conectado e dependente entre si.

As habilidades, capacidade e dados necessários para investigar estão dentro do domínio corporativo. Esse é um tipo de crime que opera em um ritmo diferente e, portanto, há uma necessidade muito maior de trabalhar sob estruturas e princípios comuns acordados em nível global e na velocidade da internet, o que inclui incentivar o compartilhamento e a colaboração de dados e definir funções e orientações claras para aproveitar os recursos uns dos outros.

O estabelecimento de princípios claros para o combate a cibercriminalidade é cada vez mais importante em uma época em que as preocupações com a privacidade, o compartilhamento de dados e a interpretação de legislação como a lei de proteção de dados estão inadvertidamente e potencialmente prejudicando o compartilhamento de informações valiosas.

As empresas geralmente mantêm dados críticos, mas não se sentem capazes de compartilhá-los devido a preocupações com a privacidade dos dados, a confidencialidade do cliente ou a divulgação de informações a empresas rivais.

Novas ferramentas e plataformas que usam tecnologias como criptografia homomórfica serão necessárias para ajudar a construir modelos mais sustentáveis para proteger as vítimas e permitir investigações globais, respeitando o direito à privacidade.

Definir princípios e estruturas de harmonização para a resposta cibernética entre vítimas, provedores de serviços cibernéticos, órgãos policiais, setores de T.I. de empresas privadas e instituições transnacionais são exemplos importantes de como fechar as margens de cooperação nas quais os cibercriminosos operam.

A solução do déficit cibernético exigirá uma integração e diálogo transnacional mais profundo entre os governos, tanto do ponto de vista de políticas a serem criadas quanto de capacidade de enfrentamento de ameaças, requerendo também uma integração muito mais estreita entre as unidades de investigação e o setor privado.

Isso oferece uma oportunidade única de criar confiança entre entidades e concordar com valores comuns, a partir dos quais uma nova arquitetura global de combate a ciberameaças emergirá.

Se isso não puder ser alcançado, corremos o risco de minar a economia digital, bem como as instituições tradicionais que são confiáveis para fornecer segurança e confiança em toda a sociedade, desacreditando todos os órgãos de proteção cibernética do país.

Mas isto é apenas uma parte do esforço necessário ao combate de criminosos cibernéticos.

Para investigar e processar crimes cibernéticos, as unidades policiais precisam de investigadores qualificados, peritos forenses atualizados e Promotores de Justiça com familiaridade com crimes cibernéticos.

Lamentavelmente no Brasil o número de policiais qualificados é limitado porque os que investigam ou examinam crimes cibernéticos devem ser especialistas altamente treinados, exigindo habilidades técnicas e conhecimento aprofundado de técnicas de investigação, incluindo conhecimento de vários hardwares e softwares de TI e ferramentas forenses.

O problema assume sua verdadeira proporção quando um outro fator é adicionado: o tempo de treinamento de um policial especializado.

Depois que um investigador decide se especializar em crimes cibernéticos, o aperfeiçoamento de suas habilidades pode levar mais de 01 (um) ano para que ele ou ela se torne proficiente o suficiente para gerenciar totalmente as investigações.

Poucos departamentos de polícia do Brasil são formados por pessoas capazes ou dispostas a lidar com investigações que envolvem computadores e formas altamente avançadas de tecnologia.

Devido aos recursos limitados e à falta de um conhecimento suficientemente amplo dos crimes cibernéticos como um problema que cresce rapidamente pode ser solucionado?Neste ponto uma abordagem mais lógica é justamente a criação de forças-tarefa multiagência, com o envolvimento de todas as esferas de governo de nosso país.

Além de compartilhar conhecimentos entre unidades policiais, a abordagem multiagência também resolve muitos problemas jurisdicionais.

Mas como selecionar candidatos adequados a este tipo de atuação em equipe? O que deve ser procurado em um membro em potencial?

Em primeiro lugar: interesse. Se houver interesse, ele ou ela pode ser treinado, muito embora é importante ressaltarmos que a competência também é um fator essencial, uma vez que um candidato a integrar um força-tarefa deve demonstrar boas habilidades de investigação, necessitando ser tecnicamente proficiente e também um bom investigador em assuntos policiais.

Mas dentro da realidade policial brasileira, frequentemente não há ninguém para escolher, interessado ou não, pois a maioria dos órgãos policiais estão com um nível muito baixo de pessoal; o que acarreta que num processo de recrutamento elas se recusam a comprometer uma pessoa com uma força-tarefa, pois não podem poupar ninguém, mesmo reconhecendo os benefícios da participação neste tipo de trabalho especializado.

Os desafios colocados pelo crime cibernético são vividos intensamente em nosso país por conta da transformação digital: à medida que o nível de conectividade aumenta, também aumenta o potencial de furto, fraude e abuso online.

Assim, forçoso é reconhecer que o cibercrime é um fenômeno generalizado em nosso país, e todas as esferas de governo devem trabalhar para limitar seu impacto, criando uma economia geral resiliente e unidades de investigações sólidas, equipando-as adequadamente para enfrentar seus novos desafios.

No decorrer de nossa exposição procuramos destacar alguns dos problemas enfrentados pela sociedade moderna decorrente do uso indevido da tecnologia da computação e do ciberespaço.

Que ninguém duvide que os cibercriminosos confiam no avanço constante da tecnologia e no quase anonimato no ciberespaço para atuar dentro e fora das fronteiras e jurisdições, o que cria problemas significativos para os usuários de tecnologia e aqueles que tentam impedir ataques cibernéticos.

O anonimato gerado pela internet torna extremamente difícil as investigações e a identificação de responsáveis por práticas criminosas.

A rápida evolução da internet permite que cibercriminosos operem em um mundo virtual sem fronteiras, utilizando do anonimato ou mesmo de identidades diferentes para não serem identificados e permanecerem impunes.

Governo, empresas e usuários devem manter-se atualizados com os desenvolvimentos tecnológicos na tentativa de proteger-se desta ameaça cada vez maior.

São vários os elementos diferentes para a implantação de uma política de sucesso na repressão aos crimes cibernéticos, conforme relatado no decorrer de nossa exposição.

As habilidades necessárias a um investigador de cibercrimes vêm do desenvolvimento de uma profunda experiência no combate a esta modalidade criminosa, até porque a experiência também é fator essencial para se obter sucesso no combate antidrogas, nos crimes contra a vida ou na investigação de crimes financeiros.

A competência cibernética é mais difícil de adquirir e diferentemente do que ocorre na investigação de outros tipos de crime bem menos passível de transferência.

O inexorável avanço da tecnologia cria pressões para renovação e atualização do conhecimento necessário para o enfrentamento dos crimes cibernéticos, gerando desafios complementares aos investigadores que se veem na necessidade de aumentar suas qualificações, pois as mesmas se tornam rapidamente desatualizadas.

Cabe às policiais brasileiras especializadas no combate a este tipo de crime otimizar suas perspectivas de formação efetiva de profissionais inclusive com a criação de forças-tarefa especializadas em crimes cibernéticos.

Mas o fato incontestável é que se o Brasil não adotar medidas eficazes e cooperativas para combater o cibercrime, a batalha será perdida e até mesmo o futuro tecnológico de nossa população poderá ser seriamente comprometido.

Autor

José Mariano Araujo Filho

-Bacharel em Direito pela Universidade Braz Cubas de São Paulo; -Pós-graduado em Direito Comercial pela Universidade São Paulo; -Técnico em Eletrônica pelo Escola Albert Einstein da Fundação Paula Souza; -Delegado da Polícia Civil de São Paulo desde de 1991, atuando atualmente como Delegado Assistente da Divisão de Investigações Sobre Infrações Contra a Saúde Pública do Departamento de Polícia de Proteção da Cidadania; -Foi titular durante 7 (sete) anos da 4ª. D.I.G. – Crimes Financeiros Praticados por Meios Eletrônicos; -Atuou na Unidade de Inteligência Policial do D.E.I.C. - Departamento de Investigações Sobre o Crime Organizado de São Paulo; -Professor concursado de Sistemas Policiais e Investigação de Crimes Praticados por Meios Eletrônicos da Academia da Polícia Civil de São Paulo; -Professor de Investigação de Cibercrimes no MBA de Direito Eletrônico da Escola Paulista de Direito; -Professor de Investigação de Cibercrimes no MBA de Forense Computacional da Faculdade Impacta de Tecnologia; -Atuou como Professor de Direito Comercial e Direito Penal na Graduação e na Pós-graduação da Universidade Camilo Castelo Branco e Universidade Bandeirantes na cidade de São Paulo; -Membro consultor da Comissão de Crimes de Alta Tecnologia da O.A.B. de São Paulo e da Comissão de Ciência e Tecnologia, ambas da Ordem dos Advogados do Brasil; -Professor convidado no Curso de aperfeiçoamento de Magistrados da Escola Paulista da Magistratura de São Paulo; -Graduado no Curso de Cybercrimes do Serviço Secreto dos Estados Unidos; -Graduado no Curso de Invasão de Computadores e Redes junto ao I.L.E.A. de El Salvador; -Graduado no Curso de Crimes Financeiros e Lavagem de Dinheiro junto ao I.L.E.A. de El Salvador; -Graduado no Curso de Interdição de Atividades Terroristas do Consulado dos Estados Unidos em São Paulo; -Foi Delegado da Divisão de Tecnologia da Informação do Departamento de Inteligência da Polícia Civil de São Paulo e Supervisor do Laboratório de Crimes Eletrônicos da Polícia Civil de São Paulo; -Associado da High Technology Crime Investigation Association (HTCIA), capítulo Brasília; -Membro da Ação de Número 8 do E.N.C.C.L.A. – Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro, que versa sobre a utilização de ativos virtuais para fins de lavagem de dinheiro e financiamento do terrorismo.

Textos publicados pelo autor

Fale com o autor

Informações sobre o texto

Este texto foi publicado diretamente pelo autor. Sua divulgação não depende de prévia aprovação pelo conselho editorial do site. Quando selecionados, os textos são divulgados na Revista Jus Navigandi.

(Fonte: https://jus.com.br/artigos/76742/criminalidade-cibernetica-panorama-atual-e-perspectivas, data de acesso: 12/08/2020)