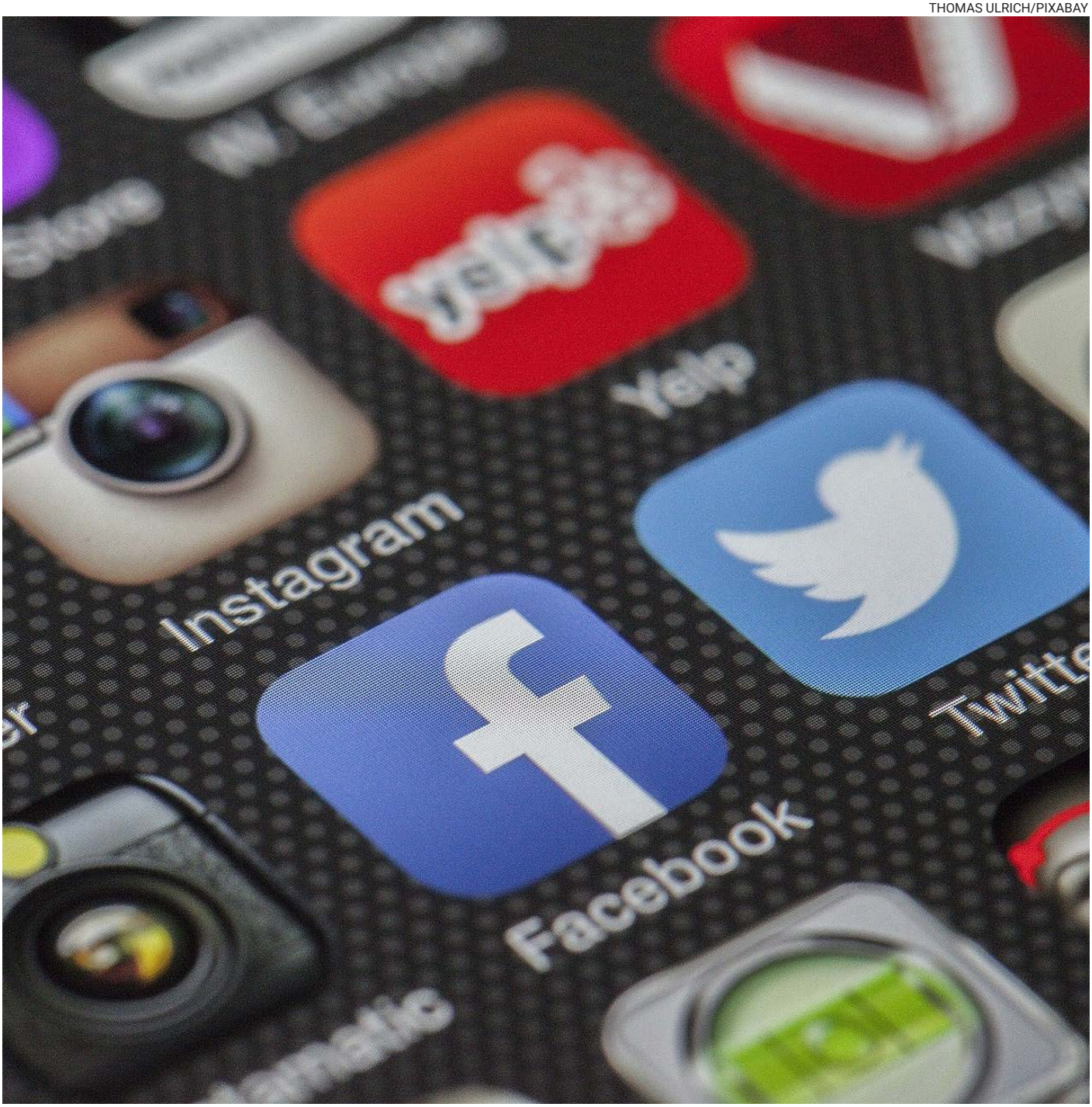
ECONOMIA E SEGURANÇA

Os desafios de investigar a criminalidade cibernética

Cibercriminosos são livres das fronteiras nacionais, enquanto os esforços das agências policias são limitados às jurisdições locais. Problema requer uma resposta com parcerias globais

José Mariano de Araujo Filho
24 de setembro de 2019

THOMAS ULRICH/PIXABAY



As mídias sociais ainda são uma ferramenta de investigação valiosa para ajudar na aplicação da lei e no rastreamento da identidade dos cibercriminosos

Um relatório produzido em 2016 pela empresa de pesquisa em cibersegurança "Cybersecurity Ventures" menciona que, 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.

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

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, cooperação internacional e assistência mútua na aplicação da lei.

Os criminosos são especializados em diferentes serviços individuais, e passaram a vender serviços a outros criminosos, o que leva a uma dispensa do conhecimento técnico necessário para a execução de ações delituosas. Isso porque os mesmos passaram a disponibilizar o modelo "Crime como serviço", em que a atividade de criminosos cibernéticos é mais fácil de executar e o suporte técnico é fornecido pelo próprio criminoso vendedor.

Desponta daí o fato de que apenas a existência de leis, como a 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.

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).

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.

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.

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. 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.

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.

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.

No Brasil, lamentavelmente 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.

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.

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. Cabe às polícias 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.

José Mariano de Araujo Filho
Delegado da Polícia Civil do Estado de São Paulo

---

https://backup.forumseguranca.org.br/economia-e-seguranca/-bfbfn