RELAÇÃO ENTRE FACÇÕES CRIMINOSAS E CRIMES CIBERNÉTICOS

Eliezer de Souza Batista Junior
Doutorando em Ciências Militares pelo Instituto Meira Mattos/ECEME

Cristiano Rolim Pereira
Mestre em Ciberdefesa, pela Universidade de Alcalá (Madri, Espanha)

Henrique de Queiroz Henriques
Mestrando em Ciências Militares pelo Instituto Meira Mattos/ECEME

Há vários grupos criminosos organizados de Norte à Sul do país, sendo os principais exemplos: Primeiro Comando da Capital (PCC), Comando Vermelho (CV), Amigos dos Amigos (ADA), Terceiro Comando Puro (TCP), Primeiro Comando Mineiro (PCM), Paz, Liberdade e Direito (PLD), Comando Norte/Nordeste e Família do Norte (FN) (BITTAR).

As facções criminosas no Brasil remontam da década de 70. Desde o início, essas facções se especializaram em crimes, sendo que a sustentação econômica advém principalmente do tráfico de drogas. Adicionam-se também outras atividades como roubos, sequestros e assaltos (HARTMANN).

Com a chegada da Era da Informação, houve a necessidade do crime organizado se reinventar para auferir mais lucro. Para tanto, crimes foram inovados dentro do ambiente cibernético. Nesse ínterim, surgem os crimes cibernéticos que são caracterizados por atividade criminosa que tem como alvo ou faz uso de um computador, uma rede de computadores ou dispositivo conectado em rede, infringindo algum dispositivo tipificado em uma lei. Isso mostra que essa derivação de crime não é praticada somente por hackers, mas também por pessoas ou organizações (KASPERSKY).

Uma das formas de implementação foi modificar a forma de venda de ilícitos, na qual traficantes passaram a vender de forma online, por meio da *deep*[1] e *dark web*[2], sendo incluído o serviço de entrega até usuário final. Essa modificação no modo de venda talvez seja responsável pelo maior boom econômico das organizações narco criminosas, pois conseguiram atingir maior público e, portanto, maximizou lucros (LACERDA, 2018).

Usando os lucros da venda de drogas, as principais facções brasileiras revertem esse dinheiro para compra de armas com fins da autoproteção do grupo criminoso e ampliação da sua área de venda (CORDEIRO, 2019). A deep e dark web também facilitaram o tráfico internacional ilegal de armas (COX, 2017).

Os crimes não ficaram apenas na parte de vendas. Alastrou-se, tornando-se uma base para operações contra alvos. Um exemplo ocorreu quando houve monitoramento de agentes de segurança que trabalhavam no presídio federal de Catanduvas–PR. A consequência foi a morte de Melissa de Almeida Araújo[3] em uma emboscada, supostamente, por ser a responsável pela transferência do traficante Marcola[4] para o presídio federal em Rondônia. As investigações concluíram de que Melissa foi seguida por membros da facção PCC, utilizando as redes sociais da ex-psicóloga (COSTA, 2017).

Investigações oficiais apontam que o PCC possui técnicas avançadas de investigação social com pesquisas aprofundadas em redes sociais, como Facebook, Snapchat, Instagram, Twitter e fontes oficiais, utilizando-se de cadastros e dados publicados em páginas oficiais nos mais diversos órgãos públicos. De posse dessas informações, realizam ameaças contra agentes e trabalhadores, como magistrados, promotores, repórteres e servidores de segurança pública (PAZ, 2019).

A utilização das redes sociais também serve para divulgação e promoção de atividades, contribuindo com a projeção do poder e disseminação do medo na sociedade. Os criminosos usam imagens de suas ações, exibem armas e escolhem suas próximas vítimas. Um exemplo ocorreu com Luyan Roges, quando seu assassinato foi gravado, postado em uma rede social e enviado aos familiares. Esse crime teria sido executado após julgamento e ordem dos "Tribunais do Crime"[5] (ARAUJO, 2019).

Com a maior adoção de comunicações pelo meio digital, a polícia tem interceptado conversas e ordens emanadas por facções. Entretanto, esse é um trabalho difícil, pois quando a justiça solicita informações para as empresas detentoras de serviços de comunicações, esbarram em recusas fundamentadas na privacidade do cliente[6]. Tal situação leva a intermediação do poder judiciário que pode ou não continuar com o procedimento investigatório (THOMAS, 2016).

Outro crime comum por parte de integrantes do crime organizado é a clonagem de cartões de crédito. As técnicas são variadas, podendo se levar a cabo com a instalação de uma simples câmera com a finalidade de filmar os dados do cartão até a

instalação de chips em leitores (LAVORENTI E SILVA, 2000).

Há pessoas que não se envolvem diretamente com o crime organizado (chamados de simpatizantes pela causa), mas que têm realizado um ciberativismo[7] para legalização de ilícitos (SILVA e ROSA, 2019), corroborando com a percepção de poder das facções no ciberespaço. Há registros de que essas pessoas estejam levando discussões para legalização das drogas, tendo como um dos argumentos o poderio das facções, tentando levar terror à sociedade.

O crime organizado também passou a vislumbrar as criptomoedas como fonte de recursos, principalmente nas situações de sequestros. Existem relatos de exigências de pagamentos de resgate utilizando bitcoins, o que dificulta a atuação das delegacias especializadas (PAGNAN, 2017). Outra forma foi verificada pelo uso de mineradoras de bitcoins[8]. Dessa forma, os criminosos usando o lucro advindo de ativos virtuais podem comercializar armas. Esse procedimento é dificilmente rastreado pelos órgãos responsáveis, por conta pouca gama de dados de rastreabilidade nas transações comerciais utilizando-se as criptomoedas (BARBOSA, 2019).

Outro ponto que dificulta o processo investigatório é que, infelizmente, os registros de crimes cibernéticos arquivados nas polícias especializadas não possuem fidedignidade. Não há unificação dos procedimentos relativos às investigações dos crimes cibernéticos e, dessa forma, cada delegacia possui um modus operandi próprio[9]. A criação de delegacias, núcleos técnicos e grupos especializados, com treinamento e capacitação periciais poderiam mitigar essa vulnerabilidade (MPF, 2016).

Verifica-se que as facções criminosas brasileiras já se inseriram na "Era da Informação". Pode-se dizer que, aparentemente, ainda estão em um estágio inicial, visto que utilizam tecnologias que estão disponíveis a todo o público. Entretanto, caso haja investimentos massivos, esses grupos podem representar grave ameaça contra a democracia e ao Estado de Direito, uma vez que podem direcionar suas ações às infraestruturas estratégicas e causar estragos substanciais à sociedade brasileira.

1 *Deep web* são sites não indexados, ou seja, que não podem ser encontrados por canais de busca, como o Google, Bing e Yahoo. Possui características de criptografia que deixam a identidade do usuário ocultada (BARROS, 2018)

2 *Dark web* possui criptografia mais complexa, permitindo que apenas usuários avançados ou alguns curiosos sortudos consigam chegar até os servidores. A URL dos sites possui várias letras e números aleatórios, não fazendo sentido para um usuário comum (BARROS, 2018). Alguns autores dividem a dark web em três subníveis: internet restrita (necessidade de alteração do servidor de conexão, ou *proxy*), internet mais restrita (necessidade de utilizar navegadores com distribuição de acesso Tor) e internet secreta (necessidade de alterar um hardware para que a comunicação ocorra) (AGUIAR, 2018)

3 Psicóloga morta pelo PCC que atendia presos no presídio de Catanduvas – PR (COSTA, 2017).

4 Um dos maiores líderes do PCC (COSTA, 2017).

5 São julgamentos que são realizados em cada facção criminosa por meio de debates realizados por aproximadamente oito ou nove chefes de quadrilha que podem ou não estar encarcerados (na condição de juízes) e réus (chamados de credores) que possuem direito de defesa. Após o julgamento, com base na maioria dos votos, é estabelecido um veredicto, em que a pena máxima é a capital, ou seja, morte dolorosa (MENEGHETI, 2013)

6 Segundo Mark Khan, advogado-geral do Whatsapp: "Pouco importa se esse cliente é um criminoso. Priorizamos nossos usuários. Por isso, adotamos sistemas cada vez mais avançados de proteção de dados" (THOMAS, 2016).

7 Utilização das tecnologias digitais como ferramenta para comunicação, informação e mobilização para o enfrentamento político, social e cultural (MILHOMENS, 2009).

8 A mineradora de *Bitcoin* é um computador ou hardware específico que se conecta à rede baseada em pares da criptomoeda (não há um servidor central), formando um nó e agregando poder de processamento para validar informações de transações envolvendo essa moeda e garantindo a segurança na troca de dados. Em troca pelo processamento, a rede paga em *bitcoin* uma quantia relativa a esse esforço (SCHIAVON, 2018).

9 Inclui-se nesse escopo a definição de crime cibernético e a tipificação de cada tipo de crime (MPF, 2016).

Rio de Janeiro - RJ, 21 de junho de 2021

.

Como citar este documento:

BATISTA JUNIOR, Eliezer Souza; PEREIRA, Cristiano Rolim; HENRIQUES, Henrique de Queiroz. Relação entre facções criminosas e crimes cibernéticos. **Observatório Militar da Praia Vermelha**. Rio de Janeiro: ECEME. 2021.

Referência:

AGUIAR, Andrey J. Qual é a diferença entre Dark Web e Deep Web? Disponível em: https://www.tecmundo.com.br/internet/128029-diferenca-entre-dark-web-deep-web.htm. Acessado em 10 de abril de 2020.

ARAUJO, Ismael. Facções usam internet na divulgação de seus crimes. Disponível em: https://imirante.com/oestadoma/noticias/2019/07/13/faccoes-usam-a-internet-na-divulgacao-de-seus-crimes/. Acessado em 03 de abril de 2020.

BARBOSA, Soraia. PM de São Paulo apreende mineradora usada pelo PCC. Disponível em: https://guiadobitcoin.com.br/noticias/pm-sao-paulo-apreende-mineradora-pcc/. Acesso em 21 de fevereiro de 2020.

BARROS, Evelin. Saiba a diferença entre Surface Web, Dark Web e Deep Web, e entenda o lado obscuro da internet. Disponível em: https://blog.maxieduca.com.br/saiba-a-diferenca-entre-surface-web-dark-web-e-deep-web-e-entenda-o-lado-obscuro-da-internet/. Acessado em 10 de abril de 2020.

BITTAR, Paula. Especial Presídios – a história das facções criminosas brasileiras. Disponível em: https://www.camara.leg.br/radio/programas/271725-especial-presidios---a-historia-das-faccoes-criminosas-brasileiras--05--50--. Acessado em 21 de fevereiro de 2020.

CORDEIRO, Tiago. Como facções como PCC e Comando Vermelho controlam o contrabando no Brasil. Disponível em: https://www.gazetadopovo.com.br/republica/como-faccoes-como-pcc-e-comando-vermelho-controlam-o-contrabando-no-brasil/. Acessado em 10 de abril de 2020.