**Facções Conectadas: A Ascensão do Crime Organizado Digital e os Caminhos da Ciberinteligência no Brasil**

**Autores:** Marcelo Branquinho e Plataforma Safer

07/11/2025

**Resumo:** O avanço tecnológico transformou radicalmente a atuação das facções criminosas brasileiras. Grupos como o Comando Vermelho, o Primeiro Comando da Capital e o Terceiro Comando Puro passaram a utilizar ferramentas digitais avançadas como comunicações criptografadas, drones armados, redes sociais para recrutamento e propaganda, spoofing e plataformas financeiras digitais para ampliar seu poder operacional, influência social e capacidade de evasão do Estado.

Este artigo técnico analisa, com foco no contexto do Rio de Janeiro, como essas organizações exploram o ciberespaço para potencializar suas atividades ilícitas, inclusive em esquemas de lavagem de dinheiro que envolvem criptomoedas e fintechs clandestinas. Além disso, propõe uma abordagem integrada de enfrentamento por meio da ciberinteligência, com uso de OSINT, aprendizado de máquina, análise forense financeira, cooperação interagências e parcerias público-privadas.

O estudo inclui casos reais e evidencia que, para combater o crime organizado do século XXI, é preciso romper com estratégias tradicionais e adotar uma arquitetura de segurança baseada em dados, predição e resposta automatizada.

**Keywords:** Crime Organizado Digital, Ciberinteligência, Facções Criminosas, Comunicação Criptografada, Drones Criminosos, Lavagem de Dinheiro Digital, Fintechs e Criptomoedas, Segurança Pública e Tecnologia.

POWERED BY SAFER

## 1. Introdução: A Tecnologia a Serviço do Crime Organizado

Organizações criminosas brasileiras, como o Comando Vermelho (CV), Primeiro Comando da Capital (PCC) e Terceiro Comando Puro (TCP), historicamente construíram seu poder através da violência territorial e do controle de economias ilegais locais. Entretanto, nas últimas décadas, essas facções demonstraram notável capacidade de adaptação e **modernização digital**. Aos poucos compreenderam que os grandes lucros e vantagens estratégicas do século XXI não viriam apenas **"do cano de uma arma, mas do clique de um mouse"**. Esse movimento silencioso de metamorfose levou os grupos a incorporarem tecnologias **digitais e cibernéticas** em praticamente todos os aspectos de suas operações criminosas, desde comunicações internas até a lavagem internacional de dinheiro.

O resultado é uma mudança de paradigma na segurança pública. Se antes a imagem típica do crime organizado restringia-se a traficantes armados coordenando ações via rádio em favelas, hoje vemos faccionados utilizando **aplicativos de mensagem criptografada, redes sociais, drones militares improvisados e até moedas virtuais** para expandir seu alcance e dificultar a repressão estatal.

Essa transformação ficou evidente em episódios recentes. **No Rio de Janeiro, por exemplo, traficantes do CV empregaram drones equipados com câmeras de visão noturna e até lançadores de explosivos contra forças policiais durante operações**. Em paralelo, investigações financeiras descobriram a criação de **bancos digitais clandestinos** para movimentar bilhões de reais em esquemas sofisticados de lavagem de dinheiro envolvendo PCC e CV. Tais casos ilustram como a tecnologia potencializou a criminalidade, **elevando o poder de fogo e a abrangência dessas facções a níveis sem precedentes**.

Este artigo técnico analisa, com foco nacional e especial destaque para o estado do Rio de Janeiro, **como as principais facções brasileiras estão empregando ferramentas digitais em suas atividades ilícitas** – incluindo comunicação criptografada, uso de redes sociais, drones, spoofing (falsificação de sinais e identidades), plataformas financeiras digitais e outros mecanismos. Discutiremos também, de forma **técnica e embasada**, como estratégias de

**ciberinteligência** e segurança cibernética podem combater esse fenômeno. Serão exploradas iniciativas como análise de inteligência de ameaças, monitoramento de mídias sociais, uso de ferramentas de **OSINT** (open source intelligence), interceptação de comunicações digitais, algoritmos de *machine learning* e parcerias público-privadas, mostrando **como esses recursos podem mapear, prever e mitigar as ações dessas facções de maneira eficiente**.

Cada seção trará exemplos reais documentados em notícias, relatórios oficiais ou pesquisas acadêmicas, oferecendo um panorama atual e propostas de enfrentamento para formuladores de políticas, profissionais de segurança pública e especialistas em TI. Em suma, buscamos evidenciar que enfrentar o crime organizado no século XXI exige ir além do combate tradicional – é preciso **travar uma verdadeira "corrida armamentista" no domínio cibernético**, onde inteligência e tecnologia tornaram-se tão cruciais quanto viaturas e armamentos no terreno.

## 2. Ferramentas Digitais nas Mãos das Facções

As facções criminosas brasileiras incorporaram diversas tecnologias digitais em suas operações. Abaixo, destacamos as principais ferramentas e técnicas utilizadas por CV, PCC, TCP e outros grupos, ilustrando como cada uma serve aos objetivos criminosos:

- **Comunicações Criptografadas:** A troca de mensagens **protegidas por criptografia ponta a ponta** tornou-se padrão entre criminosos, dificultando a interceptação por autoridades. Aplicativos populares como WhatsApp e Telegram são amplamente usados por lideranças para comandar operações à distância com sigilo. No Rio de Janeiro, a investigação do MPRJ revelou **uso intensivo de grupos de WhatsApp pelo CV para gerenciar bocas de fumo, coordenar "plantões" armados, monitorar viaturas policiais e até ordenar execuções remotamente**. A criptografia forte desses apps impede acesso ao conteúdo das conversas sem autorização judicial e cooperação das empresas – o que levou, por exemplo, à tentativa extrema de bloqueio do WhatsApp no Brasil em casos ligados ao

PCC, devido à dificuldade de obtenção de provas. Facções maiores foram além do básico: o PCC passou a **operar redes próprias de comunicação criptografada**, após o desmantelamento de serviços usados pelo crime internacional. Em 2021, com a queda da plataforma canadense *Sky ECC* (cujo servidor foi apreendido pela Europol), membros do PCC migraram para um **novo sistema conhecido como N1BC**, baseado em *criptofones* especializados. Esses dispositivos desligam GPS, apagam mensagens automaticamente e utilizam aplicativos customizados, tornando **praticamente impossível para as autoridades acessarem seu conteúdo**. Segundo investigação da Polícia Federal (Operação **Mafiusi**), o N1BC era oferecido no mercado clandestino brasileiro a antigos usuários do Sky ECC, por cerca de **R$11 mil por licença**, e passou a ser adotado por traficantes do PCC que enviam cocaína à Europa. Ou seja, **as facções hoje dispõem de uma infraestrutura de comunicação tão ou mais segura que a de governos**, incluindo celulares criptografados próprios e até centrais clandestinas. Cabe notar que **não apenas o PCC e CV** usam tais táticas – **milicianos e facções menores como o TCP também investiram pesado em comunicações seguras**. Em 2024, a PF desmantelou um núcleo tecnológico do TCP que incluía **rádios de longa distância e comunicadores de alta tecnologia** para **garantir contato seguro entre membros da facção mesmo durante confrontos**. Isso mostra uma convergência: do chefe em um presídio passando recados em bilhetes, evoluiu-se para **redes cifradas e coordenação em tempo real**, dificultando a interceptação e exigindo contra-inteligência avançada por parte do Estado.

- **Redes Sociais e Plataformas Públicas:** As facções exploram ativamente **redes sociais abertas (Facebook, Instagram, TikTok, YouTube)** para diversos fins. Uma frente é a **propaganda e ostentação**: perfis ligados ao crime expõem armas, carros de luxo, dinheiro e até tutoriais criminais. Um levantamento mostrou que **contrabandistas e traficantes exibem nas redes carregamentos ilícitos, ensinam "a arte de contrabandear" e dão dicas de rotas para fugir da fiscalização**. Em vídeos no

TikTok/Instagram, criminosos **não demonstram receio de serem identificados**, chegando a **gerar provas contra si mesmos** ao ensinar como cometer crimes ou incitando à ilegalidade. Hashtags e músicas de fundo glorificam o tráfico e a violência, num esforço claro de normalização e recrutamento. Essa presença digital serve para **atrair jovens** perfis como "menorescobar044" (alusão a Escobar) exibem adolescentes envolvidos no contrabando, muitos dos quais **abandonam a escola para ganhar status e salário no crime**. Em regiões de fronteira, facções utilizam essas plataformas para cooptar mão-de-obra e **organizar verdadeiras redes de colaboradores online**. Outro uso das redes sociais é a **intimidação e controle social**: em comunidades dominadas, circulam vídeos de punições ou mensagens dos "tribunais do tráfico" para espalhar medo. A inteligência policial já monitora essas atividades o Fórum Nacional de Combate à Pirataria estima que boa parte dos **R$410 bilhões anuais perdidos com contrabando no Brasil** seja fomentada pela **propagação criminosa nas redes sociais**, que ampliou os mercados ilícitos. O monitoramento tem levado a ações: autoridades conseguem identificar perfis e **remover conteúdos ou perfis ligados ao crime**, embora muitos voltem a surgir rapidamente. Em resumo, **as facções tratam redes sociais como ferramentas de negócio e guerra psicológica**, aproveitando o amplo alcance dessas mídias para **ostentar poder, disseminar desinformação (como no caso de "fake news" sobre operações policiais ou novas leis) e até aplicar golpes em massa** (tema adiante). Essa presença online amplia a influência das facções além de seus territórios físicos e dificulta o trabalho policial, que precisa vasculhar um volume enorme de dados públicos em busca de evidências e planos criminosos.

- **Drones e Guerra Eletrônica:** O uso de **veículos aéreos não tripulados (drones)** por facções **deixou de ser novidade e tornou-se realidade concreta e perigosa**. Nos últimos anos, multiplicaram-se casos de criminosos usando drones tanto para **vigilância** quanto para **ataques ativos**. No Rio de Janeiro, integrantes do CV *planejaram e executaram uma estratégia de "controle do espaço aéreo" em favelas*: mensagens

interceptadas mostram líderes discutindo a compra de **drones com câmeras termais e visão noturna** para monitorar incursões policiais à noite. De fato, **durante a megaoperação policial nos Complexos da Penha e do Alemão (outubro de 2025)**, traficantes **usaram drones comerciais adaptados para lançar granadas sobre efetivos policiais**, numa tática inédita no Brasil. Imagens divulgadas pela Polícia Civil flagram **drones sobrevoando equipes e arremessando explosivos de forma coordenada** uma escalada bélica que resultou em baixas e evidenciou a necessidade de respostas tecnológicas das autoridades. Esses drones improvisados carregavam um **mecanismo de garra mecânica** (similar ao de máquinas de pegar brinquedos) para soltar artefatos explosivos, e tiveram seus firmwares **desbloqueados para ultrapassar limites de altitude e zonas de exclusão aérea** (como proximidades de aeroportos). Ou seja, além de usar o drone em si, os criminosos **hackearam o software** para expandir seu raio de ação. Não por acaso, **facções rivais também adotaram essa tecnologia ofensiva**: investigações da PF apontam que o TCP adquiriu **"drones lançadores de granadas" para atacar comunidades do CV**, tendo inclusive comprado um modelo por R$ 30 mil via contrabando. A mesma facção mantinha unidades de drones para **espionar movimentações policiais e rivais**, aproveitando a vantagem de observar de cima sem expor integrantes em campo.

Frente a esse novo teatro de operações, os criminosos **também investem em contramedidas de guerra eletrônica**. Em julho de 2024, um aliado de Peixão (líder do TCP) foi preso portando um **fuzil antidrone de origem ucraniana (modelo "Tryzub")** instalado em um sótão na comunidade de Acari (RJ). Esse equipamento militar de contramedida eletrônica, com alcance de até 7 km, estava ativo para **interferir e derrubar drones das forças de segurança** na região, bloqueando seus sinais de rádio e GPS. A apreensão levantou **suspeitas de contrabando de dispositivos militares por facções e domínio de técnicas avançadas de guerra eletrônica** pelo crime organizado. De fato, o TCP estruturou uma *linha de suprimentos tecnológica* onde importava **equipamentos normalmente restritos às Forças Armadas** para uso criminal. Entre os itens adquiridos estavam

**bloqueadores de sinal (jammers)** para interromper comunicações GPS/celular/Wi-Fi de rastreadores e policiais, além de **interceptadores de comunicações policiais** capazes de captar rádio da polícia – ou seja, *espionagem ativa das operações das autoridades*. Na mesma operação, a PF apreendeu **outro fuzil antidrone** comprado sob ordens de Peixão e financiado pela cúpula do TCP. Esses exemplos revelam que a disputa entre facções e polícia **também ocorre no espectro eletromagnético**: drones, contra-drones, jammers e interceptadores configuram uma **guerra tecnológica paralela** nas comunidades. As forças de segurança começaram a reagir: o governo do RJ investiu R$ 27 milhões em **80 fuzis antidrone** para PM, Polícia Civil e administração penitenciária, capazes de neutralizar drones derrubando a conexão com o operador. Esses "canhões eletrônicos" emitem ondas de rádio direcionais que forçam o *drone* inimigo a pousar ou retornar automaticamente. Além disso, o RJ incluiu no seu pacote de segurança tecnológica câmeras com reconhecimento facial e leitura de placas, para melhorar o monitoramento terrestre e compensar a vigilância aérea dos criminosos. Apesar dessas medidas, fica claro que **as facções largaram na frente no uso ofensivo de drones**, transformando comunidades em zonas de conflito vertical e impondo uma nova fronteira de preocupação para a segurança pública.

- **Spoofing, Fraudes Digitais e Engenharia Social:** Não só no combate armado as facções inovaram elas também **descobriram no ciberespaço novas fontes de renda**. Golpes digitais diversos, que antes eram praticados por estelionatários isolados, foram incorporados ao *portfólio* do crime organizado. As primeiras investidas foram simples: faccionados passaram a aplicar **golpes de clonagem de WhatsApp**, sequestrando contas de usuários para então solicitar dinheiro aos contatos das vítimas (fingindo ser elas mesmas). Trata-se de uma modalidade de estelionato eletrônico que explodiu no Brasil, alimentada pela ampla base de usuários do WhatsApp e pela engenharia social. Em seguida, vieram os **"golpes do PIX"** esquemas que exploram o popular sistema brasileiro de pagamento instantâneo. Milhares de pessoas foram induzidas, via mensagens fraudulentas e páginas falsas (phishing), a transferir dinheiro acreditando em promessas enganosas ou em situações de emergência

fabricadas. Essa **epidemia de fraudes eletrônicas** é reflexo da percepção das facções de que golpes online oferecem **alto retorno financeiro com baixo risco físico e legal**. Um dado marcante: já em 2024, **os registros de estelionato eletrônico superaram os de roubos presenciais no país**, indicando que o "crime digital" não é apenas um apêndice, mas está se tornando o **core business** para muitas facções. O PCC, por exemplo, profissionalizou essas práticas a ponto de estabelecer **"centrais de golpe"**: em dezembro de 2023, a polícia desmantelou em São Paulo um **call center criminoso operado pelo PCC**, no qual 24 pessoas se passavam por atendentes de empresa para enganar clientes e cobrar por serviços inexistentes. Esse caso comprovou que as organizações criminosas montam **verdadeiros escritórios de telemarketing do crime**, com divisão de tarefas, treinamento e metas de lucro, tal como empresas legítimas. As facções também diversificaram suas fraudes: outro golpe disseminado foi o da **"falsa garota de programa"**, no qual **quadrilhas (associadas ao PCC) criavam perfis falsos em redes sociais para atrair vítimas e depois as extorquiam se passando por membros da facção**, alegando que a vítima desrespeitou uma suposta garota de programa protegida pelo grupo. Um manual detalhado de extorsão para esse crime chegou a ser apreendido, mostrando um nível de organização preocupante dos golpistas. Ademais, **há indícios de utilização futura de técnicas mais avançadas, como deepfakes de voz ou vídeo, para tornar extorsões e fraudes ainda mais convincentes** – um desenvolvimento que autoridades já veem no horizonte. Em suma, **o crime organizado brasileiro abraçou a economia do crime cibernético**, aplicando spoofing e engenharia social em larga escala. Essas fraudes virtualizam práticas tradicionais (estelionato, extorsão), permitindo atingir milhares de vítimas em diversas localidades a partir de um *notebook* na mão de um preso ou comparsa remoto. A lucratividade é tamanha que financia outras atividades ilícitas e diminui a dependência de atividades de alto risco (como grandes assaltos ou tráfico explícito), ao mesmo tempo em que **fortalece as facções financeiramente e expande sua influência para além do território que controlam fisicamente**.

- **Plataformas Financeiras Digitais e Criptomoedas:** Por fim, uma das áreas de maior inovação criminosa está na **lavagem de dinheiro e movimentação financeira digital**. As grandes facções estruturaram esquemas complexos para **ocultar e "esquentar" recursos ilícitos** aproveitando brechas tecnológicas e regulatórias. Um caso emblemático foi revelado em abril de 2025: **uma aliança financeira entre PCC e CV** para lavar dinheiro do tráfico, que envolveu a criação de **uma fintech clandestina atuando como banco digital paralelo**. Essa investigação da Polícia Civil do RJ (Operação *Contention*) mapeou transações suspeitas – depósitos semanais em dinheiro vivo, em pequenas cédulas, feitos por dezenas de pessoas ligadas a comunidades do CV – que convergiam para uma empresa de fachada em São Paulo (uma perfumaria fictícia). Surpreendentemente, essa única empresa (registrada em nome de uma mulher de baixa renda) **movimentou R$ 200 milhões em um ano**. A seguir, o dinheiro era pulverizado em **dezenas de outras empresas fantasmas** (floriculturas, transportes, consultorias etc.) e finalmente consolidado em uma plataforma financeira chamada **Fortbank** – um *banco digital* criado em 2020 pelo PCC (sob o codinome "4TBank") e adotado também pelo CV. Essa fintech operava **sem autorização do Banco Central**, servindo exclusivamente aos interesses das facções. Em apenas 12 meses, **cerca de R$ 6 bilhões transitaram por empresas de fachada e pelo Fortbank**, beneficiando as duas facções. O Fortbank tinha estrutura profissional: usava contas de laranjas (incluindo beneficiários de programas sociais) e sistemas on-line para realizar pagamentos e transferências internacionais sem levantar suspeitas. A sócia formal da fintech – uma jovem de 24 anos – sacou R$ 15 milhões em 3 dias, mas os investigadores identificaram que o controle real era exercido por um policial civil de SP, que atuava como CEO a serviço do PCC. Esse **"engenheiro financeiro" infiltrado** foi preso, e as autoridades descobriram conexões dessa rede com 15 países, incluindo paraísos fiscais e fronteiras por onde o dinheiro servia para comprar armas e drogas. Uma parte dos recursos voltava ao RJ para alimentar um *"fundo previdenciário"* do CV – caixa usado para apoiar famílias

de membros presos ou mortos, evidenciando a sofisticação administrativa das facções.

Além das fintechs, as facções **aproveitam a falta de regulação rigorosa em fintechs e moedas virtuais**. Em 2020-2024, organizações criminosas abriram inúmeras contas em bancos digitais e apps de pagamento para lavar dinheiro longe do escrutínio. A Receita Federal indicou que, após boatos infundados de "taxação do Pix" levarem à revogação de novas regras de monitoramento sobre fintechs, **os criminosos passaram a usar essas instituições de pagamento como "bancos paralelos" para transitar grandes somas sem rastreamento**. De fato, operações recentes (*Carbono Oculto*, *Quasar* e *Tank*, em 2025) identificaram **milhares de estabelecimentos comerciais e postos de gasolina que movimentaram R$ 52 bilhões ilícitos via fintechs** em esquemas ligados ao PCC. A ausência de obrigatoriedade de reportar movimentações suspeitas (que bancos tradicionais têm há décadas) facilitou essa opacidade. Em paralelo, **criptomoedas** entraram na equação. Relatórios de inteligência revelaram que o PCC opera carteiras de criptomoedas vinculadas a suas fintechs para transferir valores ao exterior e até **financiar atividades de grupos terroristas internacionais**, segundo alerta do governo de Israel em 2025. Esse comunicado indicou que cerca de **R$ 450 milhões (US$ 82 milhões)** saíram do PCC para contas ligadas a terrorismo em dois anos. Embora detalhes dessas conexões não tenham sido totalmente abertos, a denúncia levou autoridades brasileiras a investigar a fundo as operações financeiras digitais do PCC e suas parcerias obscuras pelo mundo. Outro exemplo do uso de criptoativos é interno: em São Paulo, uma operação policial em 2024 encontrou uma **mineradora de Bitcoin clandestina num bairro nobre (Tatuapé)** usada pelo PCC para lavar dinheiro de tráfico. O local, ligado a membros milionários da facção, tinha máquinas de alto consumo elétrico (indicando intensa mineração) e aparece associado a um chefe do PCC (conhecido como "Cara Preta") que teria investido R$ 200 milhões nesse esquema. A mineração de criptomoedas permite converter dinheiro do crime em Bitcoins "limpos" que depois podem ser vendidos como se fossem resultado de atividade de mineração lícita, dificultando a comprovação de origem. Essas iniciativas mostram que **PCC e CV não apenas usam o sistema financeiro: eles**

criam **seu próprio sistema**, com bancos digitais próprios, redes de empresas de fachada (de perfumarias a contabilidades), *laranjas* em massa e uso integrado de criptomoedas para driblar mecanismos tradicionais de controle. Tal arranjo clandestino e profissionalizado levou investigadores a concluem que **há uma espécie de "holding financeira" do crime organizado**, uma teia de negócios aparentemente legítimos que dá cobertura a bilhões de reais ilícitos. Mais impressionante, **há cooperação entre facções rivais nesse campo**: PCC e CV, apesar de inimigos no varejo de drogas, estabeleceram **uma trégua digital pragmática** onde compartilham infraestrutura de lavagem e conhecimentos financeiros em prol do lucro. A utilização conjunta do 4TBank/Fortbank e de redes de empresas permitiu maximizar ganhos para ambos os lados, num volume estimado de R$ 6 bilhões/ano somente nessa parceria. Essa aliança insólita reforça que **no mundo digital o que impera é a racionalidade econômica**, criando um *nexo* onde facções aprendem umas com as outras e até cooperam quando mutuamente vantajoso. Para as autoridades, esse é um jogo do "gato e rato" em que identificar, rastrear e bloquear essas operações financeiras é um desafio tremendo, exigindo capacidades investigativas além do convencional.

Em resumo, **as facções brasileiras potencializaram sua criminalidade com tecnologia**. Suas comunicações ficaram mais seguras e integradas, sua propaganda e influência se amplificaram via redes sociais, sua capacidade tática incorporou drones e contramedidas eletrônicas, seus golpes virtuais geram fortunas silenciosamente e sua lavagem de dinheiro tornou-se um empreendimento global e de alta tecnologia. A seguir, discutiremos como isso altera o panorama de comparação entre a criminalidade tradicional e essa nova criminalidade potencializada pela tecnologia, para então avançarmos nas respostas de *ciberinteligência* necessárias para enfrentá-la.

## 3. Comparativo: Criminalidade Tradicional vs. Criminalidade Potencializada por Tecnologia

A incorporação de recursos tecnológicos pelas facções transformou características centrais do crime organizado. A tabela a seguir resume as diferenças em diversos aspectos entre a

**criminalidade tradicional** (operações sem apoio tecnológico significativo) e a **criminalidade potencializada por tecnologia**, conforme observado atualmente em grupos como PCC, CV e TCP:

| **Aspecto** | **Crime Organizado Tradicional** | **Crime Organizado Potencializado por Tecnologia** |
|---|---|---|
| **Comunicação & Coordenação** | Comunicação **local e limitada** – uso de celulares convencionais, rádios FM ou bilhetes. Coordenação dependente de presença física ou contatos diretos. Interceptações policiais são mais fáceis (ligações não criptografadas, rádios monitoráveis). | Comunicação **instantânea e segura** – uso de aplicativos **criptografados** (WhatsApp, Telegram) e redes dedicadas. Lideranças coordenam ações remotamente de dentro e fora do país, em tempo real. Interceptação é difícil sem quebras de sigilo ou exploits avançados. Facções implementam até **centrais virtuais** (grupos online) para emitir ordens simultâneas a múltiplos subordinados. |
| **Inteligência & Vigilância** | Informações obtidas por **campanas físicas, informantes locais** ou corrupção de agentes. Vigilância do território restrita a olheiros nas ruas. Pouco alcance além da área de influência direta. | **Espionagem eletrônica e vigilância remota** – uso de **drones com câmera** para monitorar policiais e rivais à distância. Hackeio de comunicações de rivais e até da polícia (ex: facções captando rádio da PM). Uso de **redes sociais e databases vazados** para coletar dados de alvos (inclusive possíveis delatores ou autoridades). Maior **consciência situacional** graças a imagens aéreas e monitoração online constante, cobrindo áreas amplas sem presença física. |

| | | |
|---|---|---|
| **Armamento & Logística** | Arsenais consistem em armas de fogo tradicionais, explosivos improvisados e veículos terrestres. Tecnologia limitada a rádios comunicadores e alguns equipamentos como coletes. **Ataques diretos e presença física** são necessários para confrontar rivais ou polícia. | **Tecno-arsenal sofisticado** – além de armas comuns, facções dispõem de **drones armados** (granadas aéreas), **dispositivos eletrônicos** como *jammers* para sabotar sinal de rastreadores e celulares, e **fuzis antidrone** para neutralizar equipamentos policiais. Logística otimizada: uso de GPS e apps de comunicação para planejar rotas de tráfico em tempo real, clonagem eletrônica de veículos, etc. Possibilidade de **ações ofensivas remotas** (ex: lançar explosivos via drone sem expor membros). Maior poder de fogo efetivo e **defesas eletrônicas** contra operações policiais (ex: bloqueio de comunicação dos agentes). |
| **Finanças & Lavagem** | Fluxo financeiro baseado em **dinheiro vivo, comércio local e algumas empresas de fachada simples**. Lavagem via compra de imóveis, veículos de luxo, e negócios em nome de laranjas, porém em volume menor e de forma compartimentada regionalmente. Rastreabilidade maior – depósitos | **Finanças digitalizadas e globalizadas** – uso intensivo de **fintechs, criptomoedas e estruturas empresariais complexas** para diluir e ocultar recursos. Criação de **"bancos paralelos" on-line** para operações bancárias internas. Redes transnacionais de lavagem enviam valores a diversos países quase instantaneamente. Micro-transações fragmentadas (como múltiplos PIX pequenos) driblam alertas convencionais. Maior dificuldade de rastreamento – exigem-se auditorias digitais e cooperação internacional para seguir o |

| | | |
|---|---|---|
| | suspeitos em banco tradicional podem gerar alerta. | rastro do dinheiro. O volume de recursos ilícitos movimentados cresce exponencialmente com essas técnicas (bilhões de reais em um ano, no caso PCC-CV). |
| **Alcance & Capilaridade** | Atuação concentrada nos territórios dominados (favelas, rotas específicas). Dificuldade de expandir sem presença física ou alianças presenciais. **Crimes afetando vítimas próximas** (ex: tráfico local, roubo a banco regional). | **Atuação nacional e até internacional via internet** – as facções podem **operar golpes em todo o país** a partir de um computador, vitimando pessoas de estados onde nem têm presença física. Conexões com mafias estrangeiras facilitadas (comunicação criptografada e transações financeiras globais). Reclutamento de colaboradores em diferentes regiões via redes sociais. **Menor dependência da proximidade física** para exercer poder criminoso. |
| **Riscos e Exposição** | Integrantes expostos a confrontos diretos com forças de segurança. Comunicação desprotegida sujeita a escutas telefônicas e infiltrações presenciais. Atividades ilícitas mais **visíveis** (bocas de fumo, roubo armado), permitindo | Criminosos **mais protegidos e anônimos**: líderes podem operar de longe (até do exterior ou de presídios) sem se expor em campo, transmitindo ordens por meios seguros. Parte dos crimes acontece de forma silenciosa (ciberfraudes) sem violência explícita, dificultando a detecção imediata. **Provas digitais voláteis** e criptografadas tornam investigações forenses complexas. Maior capacidade de **dispersar operações** – por exemplo, um call center de golpes pode mudar de local rapidamente, e fundos ilícitos |

| | | |
|---|---|---|
| | reação policial imediata. | transitam por incontáveis contas virtuais, frustrando bloqueios. Em contrapartida, quando pegos, os criminosos tecnológicos deixam registros digitais que podem ser analisados retroativamente – porém isso exige perícia avançada. |

*Tabela 1: Comparação entre características do crime organizado tradicional e do crime potencializado pela tecnologia.*

Observa-se que **a tecnologia aumentou a escala, o sigilo e a eficiência das atividades criminosas**, criando uma disparidade entre a capacidade ofensiva das facções e a prontidão defensiva das forças de segurança convencionais.

Essa comparação evidencia a urgência de evoluir as estratégias de combate. A seguir, exploraremos como a **ciberinteligência** pode tornar-se uma arma fundamental para equilibrar essa equação, analisando primeiro as lacunas atuais do aparato de segurança pública perante o crime digital e depois propondo soluções técnicas para fortalecê-lo.

## 4. Ciberinteligência como Arma de Combate

Diante da transformação digital do crime organizado, torna-se indispensável uma resposta à altura por parte do Estado: **a ciberinteligência**. Podemos defini-la, em linhas gerais, como o conjunto de técnicas, ferramentas e análises que **transformam dados do mundo digital em informação acionável para prevenir e reprimir delitos**. No contexto das facções criminosas, a ciberinteligência consiste em **monitorar comunicações on-line, rastrear atividades em redes sociais e na darknet, analisar transações financeiras digitais, identificar padrões via algoritmos de aprendizado de máquina e integrar informações de múltiplas fontes** (policiais, financeiras, tecnológicas) para **mapear as redes criminosas e antecipar suas ações**. Diferente da inteligência tradicional muitas

vezes baseada somente em informantes e vigilância física, a ciberinteligência opera em um domínio onde os alvos **deixam rastros digitais** e **se comunicam em sistemas globais**, exigindo capacidades técnicas e jurídicas inovadoras das agências de segurança. Nesta seção, discutiremos as **lacunas atuais** que dificultam essa resposta e, em seguida, **propostas técnicas de fortalecimento** que envolvem ferramentas, procedimentos e parcerias interinstitucionais.

### 4.1 Lacunas Atuais da Segurança Pública frente ao Crime Digital

Apesar de avanços pontuais, as forças de segurança brasileiras ainda enfrentam diversas **deficiências estruturais e técnicas** para enfrentar o crime organizado em sua vertente tecnológica. Entre as principais lacunas identificadas, destacam-se:

- **Dificuldade na obtenção de Provas Digitais:** A natureza efêmera e protegida dos dados digitais cria um cenário de **"prova volátil"**. Mensagens criptografadas podem se autodestruir ou estar armazenadas em servidores no exterior; transações em criptomoedas podem ocultar identidades; vídeos de redes sociais podem ser deletados antes da apreensão. A necessidade de rápida coleta e preservação de evidências digitais nem sempre é atendida, seja por **falta de ferramentas forenses especializadas**, seja por limitações legais de acesso. Além disso, técnicas de anonimização (VPNs, *Tor*, perfis falsos) e criptografia ponta a ponta **garantem aos criminosos um grau de invisibilidade frente aos mecanismos tradicionais de escuta e vigilância**. Muitas investigações esbarram na impossibilidade de quebrar criptografia robusta ou de atribuir atividades on-line a indivíduos específicos, gerando o que se chama de *"lacuna de atribuição"* sabe-se que crimes acontecem na esfera digital, mas nem sempre é possível provar quem os cometeu.
- **Carência de Pessoal Especializado:** A segurança pública carece de **recursos humanos capacitados em cibersegurança e análise de dados**. Poucos policiais e peritos dominam técnicas de investigação digital avançada, e estes poucos geralmente estão concentrados em unidades federais (como a PF) ou capitais. Essa **falta de capilaridade técnica** impede, por

exemplo, que delegacias regionais desvendem esquemas de fraude online ligados a facções, ou que polícias estaduais aproveitem plenamente dados de inteligência cibernética. Conforme salientado em estudo do Fórum Brasileiro de Segurança Pública, há **déficit de pessoal qualificado e infraestrutura defasada**, o que faz com que as facções evoluam em velocidade "vertiginosa" enquanto as forças legais lutam para acompanhá-las. Investigações financeiras complexas exigem analistas de alto nível (contadores forenses, data scientists), mas muitas equipes são enxutas e com treinamento insuficiente nessa área, resultando em subutilização de informações que poderiam levar a cúpulas criminosas.

- **Fragmentação e Falta de Integração de Informações:** No Brasil, as polícias civis estaduais, polícias militares, PF, PRF, Ministério Público e outros órgãos **ainda operam de forma relativamente isolada** em termos de bases de dados e inteligência. Não há um sistema nacional unificado que consolide dados sobre membros de facções, suas conexões, bens apreendidos, contas investigadas etc. Isso significa que **informações críticas não fluem rapidamente**: por exemplo, um suspeito monitorado por aplicar golpes em São Paulo pode não ser imediatamente associado a uma facção atuando no Rio de Janeiro, porque as evidências estão em inquéritos distintos, sem cruzamento automático. O caso da aliança PCC-CV ilustra isso – só após um relatório do Ministério da Justiça alertar o Rio é que se confirmou a movimentação conjunta de dinheiro por facções de SP e RJ. A falta de integração também se manifesta na **inteligência de sinais**: não há, até onde divulgado, um centro unificado que trate de interceptações eletrônicas multi-estado para crime organizado, o que gera esforços duplicados e "pontos cegos" quando criminosos cruzam fronteiras estaduais.

- **Legislação e Procedimentos Desatualizados:** As leis penais e processuais muitas vezes não acompanham o ritmo das inovações criminosas. Determinados delitos cibernéticos caem em zonas cinzentas ou possuem penas brandas em comparação a crimes tradicionais equivalentes. Por exemplo, até recentemente estelionatos massivos on-line podiam ser

enquadrados como crimes de informática ou de falsidade ideológica com penas inferiores às de roubos armados, apesar do enorme prejuízo causado. Além disso, **procedimentos legais para obtenção de dados telemáticos internacionais são lentos e burocráticos**. A cooperação jurídica com provedores estrangeiros (como operadoras de e-mail, redes sociais ou empresas de hospedagem) depende de acordos como o MLAT, que podem levar meses "uma eternidade no tempo da internet". Criminosos se beneficiam dessas demoras para apagar vestígios ou migrar suas operações. Outro ponto é a **soberania digital**: diferenças entre ordenamentos jurídicos e preocupações nacionais dificultam ações coordenadas, e criminosos exploram jurisdições mais fracas em regulação como "santuários" para seus servidores ou contas. No âmbito doméstico, ainda há debates acerca de privacidade e sigilo que, às vezes, impedem maior compartilhamento de dados entre agências (por exemplo, restrições no acesso a bases da Receita ou Banco Central por órgãos investigativos). Em síntese, **o arcabouço jurídico-operacional não foi pensado para enfrentar organizações descentralizadas operando em rede global**, criando brechas aproveitadas pelas facções digitais.

- **Subfinanciamento e Infraestrutura Insuficiente:** Tecnologias de combate – desde sistemas de análise de big data até equipamentos de vigilância eletrônica – **são caros e exigem atualização constante**. Muitas polícias enfrentam orçamento limitado para inovação tecnológica, priorizando necessidades básicas e emergenciais. O resultado é que **ferramentas essenciais faltam**: laboratórios forenses sem software para quebrar criptografia ou analisar celulares em grande volume, departamentos de inteligência sem acesso a plataformas de *analytics* modernas, delegacias sem acesso expedito a registros de IP ou mecanismos de rastreamento de criptomoedas. O subfinanciamento também impede a **expansão de unidades especializadas**. Por exemplo, a PF possui núcleos de combate a crimes cibernéticos, mas em número aquém da demanda nacional; polícias civis de alguns estados têm delegacias de crimes virtuais, porém focadas em golpes comuns, e não

necessariamente estruturadas para investigar facções. A carência de recursos financeiros compromete inclusive a **capacitação contínua** dos agentes – em um campo que evolui todo mês, investigadores precisam de treinamento constante em novas técnicas (sejam elas de OSINT, análise de blockchain, ciência de dados, ou uso de inteligência artificial aplicada). Essa lacuna orçamentária foi destacada no contexto da lavagem de dinheiro: **investigações financeiras complexas são cruciais para desmontar estruturas econômicas das facções, mas exigem tempo e investimento** que nem sempre estão disponíveis para as forças-tarefa convencionais.

- **Uso estratégico da desinformação pelos criminosos:** Uma dimensão menos tangível, mas real, é como as facções **exploram falhas de comunicação entre Estado e sociedade para se beneficiar**. Vimos isso no caso das **fake news sobre a "taxação do Pix"**, que geraram pressão popular e política para revogar medidas de controle sobre fintechs – exatamente o cenário que os criminosos desejavam. Grupos ligados ao crime se aproveitaram dessa brecha regulatória para ampliar seus "bancos digitais" e dificultar o rastreamento de recursos. Esse episódio expõe uma fraqueza: **a ausência de estratégias de contrapropaganda governamental eficaz** em temas de segurança cibernética e financeira. Enquanto a Receita Federal tentava implementar salvaguardas, uma campanha de desinformação online (espalhada em parte via redes sociais e aplicativos) minou a iniciativa. Ou seja, as forças de segurança não enfrentam apenas obstáculos técnicos, mas também **batalhas narrativas no espaço informacional**, onde carecem de presença proativa. A inteligência em segurança pública ainda engatinha no monitoramento e reação a campanhas de informação maliciosas que favorecem o crime.

Essas lacunas combinadas produzem um cenário preocupante: **enquanto as facções correm com criatividade e recursos no âmbito digital, a resposta estatal segue aquém, fragmentada e lenta**. Como descrito por analistas, vive-se uma espécie de **"corrida armamentista assimétrica"**, em que o lado ilegal se mostra ágil e inovador, e o lado legal, pesado e reativo. Isso não significa que a batalha está perdida

mas evidencia que é necessário **repensar e reforçar profundamente a estratégia de combate, incorporando de vez a ciberinteligência** como componente central. No próximo tópico, apresentamos propostas técnicas e operacionais para fortalecimento da resposta estatal, cobrindo desde melhorias em ferramentas até modelos de cooperação que buscam superar as deficiências mapeadas.

### 4.2 Propostas Técnicas de Fortalecimento – Ferramentas, Procedimentos e Parcerias

Para enfrentar facções cada vez mais tecnológicas, a segurança pública precisa **adotar uma postura inovadora e integrada**, combinando recursos de diversas áreas. Abaixo estão propostas e diretrizes técnicas que podem fortalecer o combate ao crime organizado digital, alinhadas às melhores práticas internacionais e lições aprendidas nos casos recentes:

- **Criação de Unidades Especializadas em Ciberinteligência:** Assim como no passado foram formadas delegacias anti-drogas ou grupos de combate a crime organizado (GAECOs), hoje impõe-se a criação de **núcleos dedicados à inteligência cibernética** dentro das polícias e do MP. Essas unidades seriam responsáveis por **monitorar atividades on-line de facções 24/7**, reunindo analistas de TI, peritos forenses digitais, especialistas financeiros e investigadores experientes. Elas fariam varreduras constantes em busca de sinais de atividade criminosa digital: desde **análise de dados de WhatsApp obtidos judicialmente** (como no caso do MPRJ, que precisou gerenciar milhares de mensagens interceptadas), até o rastreamento proativo de redes sociais suspeitas e sites na dark web onde facções podem estar atuando. Para operar com eficiência, esses núcleos devem estar equipados com **plataformas de análise de big data e** machine. learning capazes de identificar padrões em volumes massivos de dados. Por exemplo, sistemas de *analytics* podem correlacionar depósitos bancários atípicos com geolocalização de usuários de redes sociais em áreas faccionadas, apontando esquemas de lavagem. Já algoritmos de aprendizado de máquina podem varrer conversas públicas e indicar gírias ou códigos novos usados pelo crime organizado para driblar detecções. Inspirando-se em

Centros de Fusão de Inteligência (Fusion Centers) utilizados em outros países, a ideia é concentrar e *correlacionar informações de fontes diversas (policiais, financeiras, tecnológicas)* em um só lugar – superando a fragmentação atual. Em nível federal, a **PF e a PRF** podem ampliar seus centros já existentes, integrando-os a um **centro nacional de ciberinteligência contra o crime organizado**, que alimentaria também os estados.

- **Monitoramento Sistemático de Redes Sociais e Mídias Digitais:** É fundamental **automatizar e ampliar o monitoramento de conteúdo aberto** na internet associado às facções. Ferramentas de **OSINT** podem rastrear hashtags, perfis e grupos públicos onde haja apologia ao crime, ostentação de armas ou coordenação de atos ilícitos. Um exemplo bem-sucedido vem do próprio trabalho do FNCP e da PF na fronteira: ao **mapear perfis de TikTok/Instagram de contrabandistas**, foi possível identificar quadrilhas e até iniciAR operações repressivas. Essa prática deve ser expandida para contextos urbanos: **mapas do ecossistema digital criminoso** no Rio, São Paulo e demais estados podem ser construídos, identificando influenciadores do tráfico nas redes, canais de comunicação usados para avisos ("sintonias" via Facebook, etc.) e eventuais **tentativas de recrutamento online**. Uma medida concreta seria firmar parcerias com as próprias **plataformas de mídia social**: memorandos de entendimento para **fluxo ágil de denúncias e solicitações**. Por exemplo, grupos no Facebook onde se vendem armas ou drogas podem ser detectados por sistemas internos da plataforma e sinalizados para as autoridades (que então podem pedir judicialmente os dados dos administradores). O **uso de IA** aqui também é valioso: algoritmos de visão computacional podem varrer imagens postadas publicamente buscando elementos ilícitos (armas de fogo, grande quantidade de drogas ou dinheiro) e sinalizar automaticamente para análise humana. Além disso, **combater a desinformação** faz parte do monitoramento: órgãos como Polícia Federal e Receita Federal devem aprimorar sua presença nas redes para **desmentir boatos nocivos** (como os do Pix) e **educar a população** para não cair em golpes (reduzindo assim o lucro fácil das facções com

estelionato). Importante frisar que esse monitoramento deve respeitar limites legais – focado em informação pública ou obtida com ordem judicial –, evitando violações de privacidade de cidadãos comuns. Com transparência e técnica, a análise de mídias digitais pode antecipar movimentações de facções (por exemplo, identificar quando criminosos combinam pelas redes invadir certa área ou realizar um "bondão" de resgate) e também auxiliar na **identificação de integrantes** que se expõem online, facilitando futuras prisões.

- **Aprimoramento da Interceptação e Contraespionagem Digital:** Embora a criptografia seja um obstáculo real, ainda há formas de obter inteligência a partir de comunicações dos criminosos. Uma frente é investir em **capacidades de infiltração**: assim como agentes conseguiram infiltrar-se em grupos de mafiosos na Europa para quebrar o sigilo do Sky ECC, as forças brasileiras podem adotar táticas semelhantes. Isso inclui desde **infiltrados humanos em chats fechados** (policiais disfarçados ou informantes que tenham acesso a grupos de WhatsApp/Telegram das facções) até **operações ciber-ofensivas controladas**, como a instalação de *malware* ou *spyware* em dispositivos de líderes (mediante ordem judicial, nos moldes de um "Mandado de Busca e Apreensão eletrônico"). Em vários países, agências de aplicação da lei têm utilizado vulnerabilidades em apps ou enviado mensagens isca para induzir criminosos a revelarem informações – no Brasil, isso precisa ser legalmente e tecnicamente estruturado. Outra medida é **explorar metadados**: mesmo sem ler o conteúdo de mensagens criptografadas, a inteligência pode analisar padrões de comunicação (quem fala com quem, em que horários, de onde geograficamente) para mapear redes. O afastamento de sigilo telemático concedido por justiça no RJ permitiu descobrir a **hierarquia do CV via grupos de WhatsApp**, pelos membros e frequência de interações. Esse tipo de análise de rede social (SNA – *social network analysis*) pode revelar líderes ocultos ou conexões interestaduais antes desconhecidas. Além disso, para comunicações de voz, **tecnologia de interceptação e quebra de cifra em tempo real** deve ser buscada: por exemplo, investir em

equipamentos capazes de decodificar rádios digitais usados por facções (há registros de milícias usando rádios digitais criptografados), com apoio de órgãos como Anatel para localizar e desligar emissões clandestinas. No campo da **contraespionagem**, a polícia deve proteger melhor suas comunicações: a apreensão de interceptadores de comunicação pelo TCP indica que facções podem estar ouvindo a polícia. Portanto, PM e Polícia Civil no RJ e outros lugares precisam adotar **criptografia nas suas próprias rádios** e rotinas de mudança de frequência/senha, bem como varreduras frequentes anti-grampos nos quartéis e centrais.

- **Análise Avançada de Dados Financeiros e Blockchain:** Para combater a engenharia financeira das facções, propõe-se montar **equipes conjuntas entre forças de segurança e órgãos de supervisão financeira** (COAF, Receita, Banco Central). Essas equipes utilizariam **ferramentas de análise de grandes volumes de transações (Big Data analytics)** para vasculhar o sistema financeiro em busca de padrões característicos de lavagem. Por exemplo, o esquema CV-PCC exposto no RJ tinha como padrão **depósitos frequentes em dinheiro vivo de baixo valor feitos por muitos CPF distintos**. Um algoritmo pode identificar aglomerações de depósitos assim em contas de fintechs e emitir alertas automáticos. O Banco Central, com a implementação do PIX, poderia colaborar disponibilizando dados agregados (preservando privacidade individual) para detecção de anomalias – similar ao que se faz no combate ao terrorismo financeiro. Outro foco é **rastrear criptomoedas**: apesar do anonimato relativo, há empresas especializadas em análise de blockchain (blockchain analytics) que conseguem seguir o rastro de criptos associadas a crimes, identificando endereços suspeitos e ligando-os a exchanges conhecidas. O governo brasileiro já sinalizou a intenção de **integrar exchanges de criptomoedas à futura moeda digital (Drex)** e exigir maior transparência. A curto prazo, **forçar a compliance das exchanges** que operam no país – exigindo KYC rigoroso e colaboração em investigações – é essencial. Ferramentas como o *CipherTrace* ou *Chainalysis* podem ser licenciadas para uso das agências, permitindo montar

um **mapa das movimentações em Bitcoin/Monero** possivelmente vinculadas às facções (por exemplo, monitorar se carteiras conhecidas de faccionados recebem grandes somas após operações financeiras suspeitas). Importante também é **retomar e aprimorar a regulamentação das fintechs e pagamentos**: a Instrução Normativa que foi derrubada pelas fake news do Pix deve ser rediscutida com participação ativa de órgãos de segurança, para fechar brechas usadas como "bancos paralelos". Isso pode incluir reduzir limites de transações anônimas, melhorar a troca de informações sobre clientes suspeitos entre fintechs e COAF, e criar canais de denúncia anônima para funcionários dessas empresas reportarem movimentações atípicas. Outra proposta é **instituir forças-tarefa permanentes de combate à lavagem digital**, a exemplo da Operação Contenção, reunindo delegados, promotores, auditores fiscais e analistas do BC que, de forma contínua, vão "seguindo o dinheiro" e bloqueando bens. A Operação Contenção conseguiu bloquear R$ 6 bilhões em ativos de PCC/CV e desmantelar 30 empresas de fachada esse modelo pode ser replicado em outras regiões e mantido como ação preventiva (não só reativa a um crime já ocorrido). O uso de **machine learning** nessas forças-tarefa pode ajudar a *prever* tendências de lavagem: por exemplo, modelos que indiquem setores econômicos emergentes onde criminosos podem investir (como aconteceu com o setor de postos de combustível no caso Carbono Oculto). Compreender e **antecipar a próxima "moda" de ocultação de capital ilícito** (seja ouro ilegal, criptoativos de privacidade, *crowdfunding* falso, etc.) dará vantagem às autoridades.

- **Cooperação Público-Privada e Internacional Intensiva:** Uma lição clara dos casos recentes é que **nenhuma agência sozinha consegue mapear toda a extensão das atividades digitais das facções**. É crucial estreitar parcerias tanto **entre setor público e empresas privadas** quanto **entre o Brasil e órgãos internacionais**:
    - *Setor financeiro e de tecnologia:* Instituições financeiras – bancos tradicionais, fintechs, empresas de meio de

pagamento – devem atuar lado a lado com investigadores. Pode-se criar um **Grupo de Trabalho intersetorial** onde bancos compartilham sinais de alerta com a polícia (resguardado o sigilo legal), e a polícia informa bancos sobre contas e chaves PIX associadas a criminosos para que sejam vigiadas. Do lado de empresas de tecnologia, acordos com provedores de e-mail, hospedagem em nuvem e telecomunicações podem **agilizar respostas a ordens judiciais** (diminuindo de meses para dias a entrega de dados críticos). Um exemplo de boa prática foi o papel de um banco brasileiro que notou transações suspeitas numa fintech e alertou autoridades, desencadeando a descoberta do financiamento ao terrorismo via PCC. Esse tipo de vigilância corporativa deve ser incentivado por meio de marcos regulatórios (exigindo relatórios de operações suspeitas também de fintechs) e **canais seguros de comunicação** entre compliance bancário e inteligência policial.

- *Academia e Pesquisa:* Universidades e centros de pesquisa em segurança cibernética podem contribuir desenvolvendo novas soluções sob demanda das forças de segurança. Por exemplo, algoritmos de processamento de linguagem natural (PLN) treinados para identificar gírias de facções em interceptações, ou estudos sobre comportamento de faccionados on-line para auxiliar na detecção precoce de recrutamento de jovens. Projetos de P&D financiados pelo governo em parceria com academia poderiam focar, por exemplo, em **sistemas preditivos** que combinem dados socioeconômicos e atividade em redes para prever quais áreas estão em risco de "tomada digital" por facções (como golpes do motoboy, fraudes do PIX, etc. associados a certo grupo).
- *Cooperação entre órgãos de segurança:* Internamente, aprimorar o compartilhamento de inteligência entre PF, polícias estaduais, ABIN, COAF e até Forças Armadas (no que tange a contrabando internacional, por exemplo). Isso pode ser formalizado com um **Centro Nacional de**

**Inteligência contra o Crime Organizado Tecnológico**, integrado por representantes de cada órgão, que se reúnam regularmente para trocar informações e delinear estratégias conjuntas. Uma agência pode dispor de informação vital (por exemplo, a ABIN coletar dados sobre compra de equipamentos de guerra eletrônica entrando via fronteira) que precisa chegar à polícia local a tempo de flagrar o uso desses equipamentos. Estruturas de comando e controle unificadas durante grandes operações (como a do Complexo da Penha) devem incluir células dedicadas à guerra eletrônica, com especialistas monitorando sinais de drones, rádio e telefone em tempo real para orientar as tropas e neutralizar dispositivos – essa integração operacional ainda engatinha.

- *Parcerias internacionais:* O crime organizado brasileiro já tem tentáculos no exterior (drogas, lavagem, armas) e agora conexões digitais globais. Portanto, ampliar a colaboração com agências estrangeiras é primordial. O alerta do Ministério da Defesa de Israel ao Brasil sobre uso de criptomoedas pelo PCC evidenciou uma **nova dimensão de parceria** – envolvendo inteligência financeira internacional. O Brasil deve aproveitar canais como Interpol, Ameripol e acordos bilaterais para **troca rápida de informações sobre criptowallets suspeitas, empresas offshore ligadas a facções, e transitórios internacionais**. A participação em forças-tarefa globais de combate a *ransomware* e tráfico humano digital pode também beneficiar o país, pois técnicas desenvolvidas lá fora podem ser adaptadas aqui. Ademais, vale considerar **operações conjuntas**: por exemplo, se identificar que facção brasileira está enviando drogas via portos europeus com apoio de mafias locais, planejar ações sincronizadas com polícias europeias (como foi o caso de **megaoperações na Bélgica e Itália resultantes da infiltração no Sky ECC**). Outro ponto crítico é a **aceleração de tratados**: o Brasil deve implementar o **Segundo Protocolo Adicional à Convenção de**

**Budapeste** (de cooperação em crimes cibernéticos), que permite acesso mais ágil a provas eletrônicas transnacionais. Com isso, agilizamos investigações que envolvem servidores em outros países e reduzimos a janela em que os criminosos podem esconder rastros.

- **Capacitação e Atualização Contínua das Forças de Segurança:** Todas as medidas anteriores requerem pessoal bem treinado. Portanto, investir em **capacitação massiva** é uma proposta transversal. Isso inclui desde cursos de curta duração para delegados e promotores sobre procedimentos de preservação de evidências digitais, até formação aprofundada de peritos em análise de malware, criptografia e rastreamento de blockchain. Parcerias com empresas (como treinamentos oferecidos por gigantes de tecnologia em suas ferramentas), intercâmbio de profissionais (mandar policiais para estágios em unidades de combate ao cibercrime no exterior) e criação de uma **academia específica de crimes cibernéticos** dentro das forças (por exemplo, uma escola nacional nos moldes da Academia da PF, dedicada à ciberinvestigação) são caminhos. Ao melhorar o capital humano, aumenta-se a capacidade de usar efetivamente as novas ferramentas adquiridas e de desenvolver *insights* investigativos a partir delas. Um perito bem treinado, por exemplo, pode descobrir que um determinado *malware* encontrado em celular de traficante se comunica com um servidor, e dessa pista extrair a localização de um líder no exterior – algo que passaria despercebido sem conhecimento especializado.

- **Uso Ético de Inteligência Artificial e Automação em Larga Escala:** Por fim, deve-se incorporar **IA de forma ética** para lidar com o volume de dados. Chatbots de IA poderiam auxiliar triando denúncias anônimas e até conversas interceptadas, resumindo e destacando trechos potencialmente relevantes para o caso (sempre com revisão humana posterior). Sistemas de visão por computador podem monitorar **câmeras de segurança urbanas** com reconhecimento facial para identificar deslocamentos de suspeitos conhecidos (lembrando do cuidado com vieses e a necessidade de calibragem para evitar falsos positivos). A

**automação de tarefas repetitivas** libera policiais para atividades analíticas mais complexas: por exemplo, *scripts* que automaticamente reúnem todas as informações de diversas bases sobre um CPF ou CNPJ suspeito, gerando um dossiê inicial em minutos, em vez de dias de pesquisa manual. A IA também pode ser empregada na **previsão preditiva de violência**: combinando históricos de tiroteios, menções em redes sociais a conflitos e ocorrências, modelos podem indicar onde uma facção pode tentar expandir território ou quando há risco de rebelião coordenada em presídios via comandos digitais. Evidentemente, toda adoção de IA deve vir acompanhada de transparência, supervisão humana e respeito aos direitos fundamentais, para evitar abusos e garantir que a tecnologia sirva à justiça de forma confiável.

Implementar as propostas acima exige **vontade política, investimento e coordenação**. Felizmente, há sinais de progresso: em 2023, o Estado do Rio de Janeiro já investiu em infraestrutura anti-drones e tecnologias de vigilância inteligentes; em nível federal, operações integradas estão bloqueando fortunas criminosas; e debates sobre regulação de fintechs e criptos avançam. O passo seguinte é **sistematizar e ampliar essas iniciativas**, de modo que não sejam reativas e episódicas, mas sim parte de uma política permanente de segurança cibernética pública.

## 5. Conclusão

O crime organizado brasileiro vive um processo de transformação impulsionado pela tecnologia, incorporando ferramentas digitais para ampliar seu alcance, lucro e proteção contra a lei. Facções como PCC, CV e TCP demonstraram uma capacidade notável de **evolução estratégica**, combinando violência tradicional com cibercrime e guerra eletrônica. Esse novo patamar de ameaça coloca desafios inéditos para a segurança pública: **diante de inimigos que se comunicam por canais impenetráveis, atacam com drones e lavam dinheiro com um clique, as respostas clássicas operações táticas e prisões isoladas já não são suficientes**. Se a **RO.CB.BR-01** (rotina obrigatória de cibersegurança do setor elétrico) estudada no artigo modelo precisava

de complementos para enfrentar ataques de IA, podemos traçar um paralelo na segurança pública: **as rotinas tradicionais de policiamento e investigação precisam ser complementadas por inteligência artificial defensiva, monitoramento comportamental e plataformas inteligentes**. Em outras palavras, é imperativo travar no campo da lei e da ordem a mesma **dinamicidade, predição e integração** que caracterizam os ataques modernos.

Este artigo explorou as várias facetas dessa questão – das **ferramentas digitais nas mãos das facções** às **propostas de ciberinteligência para combatê-las** baseando-se em casos concretos recentes. Ficou evidente que **as facções já deixaram de ser entes puramente "analógicos"**; hoje elas operam **redes virtuais complexas**, verdadeiras corporações clandestinas globalizadas. Em resposta, **o Estado precisa se reinventar tecnologicamente**. As recomendações apresentadas investir em unidades especializadas, monitorar sistematicamente o ciberespaço, integrar bancos de dados, atualizar leis, intensificar parcerias e capacitar efetivos apontam um caminho viável e moderno para recuperar a vantagem nessa luta assimétrica.

Os exemplos de sucesso, embora pontuais, nos dão esperança: a apreensão de um arsenal tecnológico do TCP antes que causasse mais estragos; a identificação e bloqueio de um banco clandestino que movimentava bilhões; a neutralização de drones criminosos por novos equipamentos da polícia. Cada vitória dessas resulta de **inteligência bem aplicada e cooperação efetiva** exatamente os pilares a serem fortalecidos.

Concluímos, portanto, que **ciberinteligência não é mais acessória, mas central na segurança pública contemporânea**. A tecnologia, que tantas vantagens trouxe ao crime organizado, pode e deve ser usada igualmente a favor da lei. Se criminosos dispõem de "copilotos cibernéticos" para o mal, as forças de segurança precisam de **copilotos cibernéticos para o bem**, como plataformas de SIEM com UEBA, sistemas de resposta automatizada e análise preditiva. Somente com esse aporte tecnológico-intelectual será possível **mapear, prever e mitigar** as ações das facções no nível necessário. Em última instância, a batalha contra o crime organizado no Brasil do

século XXI será vencida não apenas nas ruas e vielas, mas também nos servidores, nos algoritmos e nas salas de *war room* digital. O investimento nessa frente, aliado ao esforço tradicional, promete **reduzir a vantagem comparativa que hoje as facções detêm** e assegurar que a sociedade e o Estado retomem o controle no mundo físico e no cibernético.

**6. Referências formatadas**


1. CNN BRASIL. Denúncia que embasou operação no RJ usou mensagens de WhatsApp e drones. *CNN Brasil*, 2025.
2. RIO DAS OSTRAS JORNAL. Drones noturnos: CV planejava espionar polícia com tecnologia avançada. *Rio das Ostras Jornal*, 2025.
3. GAZETA DO POVO. Conheça o equipamento que pode combater ataques a drones por facções criminosas. *Gazeta do Povo*, 2025. Autor: Bruno Maffi.
4. METRÓPOLES. Peixão coordena tecnologia bélica e faz espionagem com itens da China. *Metrópoles*, 2025. Autora: Mirelle Pinheiro.
5. CNN BRASIL. PCC e CV: relatório aponta ligação entre facções no Rio de Janeiro. *CNN Brasil*, 2025. Autor: Cleber Rodrigues.
6. FONTE SEGURA – FBSP. A metamorfose digital: como as facções brasileiras estão trocando o fuzil pelo phishing. *Fonte Segura*, 2025. Autor: Roberto Uchôa.
7. CNN BRASIL. “Fake news sobre Pix ajudaram crime organizado”, diz secretário da Receita. *CNN Brasil*, 2025. Autora: Cristiane Noberto.
8. GAZETA DO POVO; BNEWS. Fake news sobre PIX contribuíram para lavagem de dinheiro por grupos criminosos. *BNews*, 2025.
9. GAZETA DO POVO. Contrabandistas usam redes sociais para aumentar ganhos e ostentar ilícitos. *Gazeta do Povo*, 2023. Autora: Juliet Manfrin.

10. METRÓPOLES. PCC usa até mineradora de criptomoedas para lavar milhões do crime. *Metrópoles*, 2024. Autor: Artur Rodrigues.

11. GAZETA DO POVO. Governo de Israel acusa PCC de usar banco digital e criptomoedas para financiar terrorismo. *Gazeta do Povo*, 2025. Autora: Juliet Manfrin.

12. EDUARDO MAURICIO ADVOCACIA; ESTADÃO. Operação da PF mostra novo esquema de comunicação criptografada do PCC e da máfia. *Blog Eduardo Mauricio Advocacia / Estadão*, 2025.

13. CNN BRASIL. Veja momento em que drone do CV arremessa bomba durante megaoperação no RJ. *CNN Brasil*, 2025.

14. CNN BRASIL. Entenda como Operação Contenção se tornou a mais letal da história do RJ. *CNN Brasil*, 2025.

15. O GLOBO. PCC e CV unidos? Lavagem de dinheiro é o elo entre facções, aponta Polícia Civil do Rio. *O Globo*, 2025. (Citado via Fonte Segura).

16. ESTADÃO. 'Call center do golpe': polícia prende 24 pessoas suspeitas de esquema em SP. *Estadão*, 2024. Autor: Okumura.