RISP

REVISTA DE INTELIGÊNCIA DE SEGURANÇA PÚBLICA

Número 10
2025

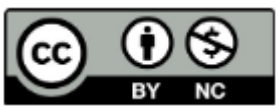
ISSN 2675-7168 ; 2966-0254

https://esisperj-ead.pcivil.rj.gov.br
https://www.policiacivil.rj.gov.br/publicacoesRisp
risp.esisperj@pcivil.rj.gov.br

RISP – Revista de Inteligência de Segurança Pública

Número 10 – 2025

ISSN 2675-7168 (Impressa); 2675-7249 (CD-Rom); 2966-0254 (Online)



EXPEDIENTE

Secretaria de Estado de Polícia Civil
Subsecretaria de Inteligência
Escola de Inteligência de Segurança Pública do Estado do Rio de Janeiro

Governador do Estado do Rio de Janeiro
Cláudio Bomfim de Castro e Silva

Secretário de Polícia Civil
Felipe Lobato Curi

Subsecretário de Inteligência
Flávio Marcos Amaral de Brito

Diretora-Geral da ESISPERJ
Carolina Salomão Albuquerque

Editora Chefe da RISP
Carolina Salomão Albuquerque

Editor Executivo da RISP
Leandro Martins de Paiva Passos

Revisores
Alessandra de Oliveira Rodrigues de Paiva Passos
Anderson Pereira Tavares
Maria Isabel Maia Marmello Henderson
Rafaela Silva Santos

Disponível em:
https://esisperj-ead.pcivil.rj.gov.br/login/index.php
https://www.policiacivil.rj.gov.br/publicacoesRisp

Escola de Inteligência de Segurança Pública do Estado do Rio de Janeiro
Rua do Lavradio, 162. Centro. Rio de Janeiro, RJ.
Tel: (21) 3132-3007 e 3132-3007. E-mail: esisperj@pcivil.rj.gov.br

RISP
REVISTA DE INTELIGÊNCIA DE SEGURANÇA PÚBLICA
ISSN 2675-7168 ; 2966-0254

Revista de Inteligência de Segurança Pública [online] [impressa] [CD-Rom]/Escola de Inteligência de Segurança Pública do Estado do Rio de Janeiro, Subsecretaria de Inteligência, Secretaria de Estado de Polícia Civil. Número 10 (2025). Rio de Janeiro: ESISPERJ, 2025.

Anual
ISSN 2675-7168(Impressa);2675-7249(CD-Rom);2966-0254 (Online).

1. Inteligência – periódicos. 2. Segurança Pública – periódicos. 3. Segurança e Defesa – periódicos. 4. Educação Profissional e Inteligência – periódicos. Secretaria de Estado de Polícia Civil, Subsecretaria de Inteligência, Escola de Inteligência de Segurança Pública do Estado do Rio de Janeiro.

CDD 300

Dados internacionais de catalogação na publicação (CIP)

Sumário

RISP
REVISTA DE INTELIGÊNCIA DE SEGURANÇA PÚBLICA
ISSN 2675-7168 ; 2966-0254

EDITORIAL

Caros leitores, é com entusiasmo e orgulho que celebramos a publicação da décima edição da RISP. Chegar na edição número dez é o resultado tangível de cinco anos ininterruptos de produção editorial voltada à Inteligência de Segurança Pública, à divulgação do conhecimento e ao fomento do debate sobre o tema. Olhamos para trás e vemos uma jornada marcada por publicações que não apenas ecoaram em seus campos de estudo, mas que, de fato, impulsionaram a fronteira do saber.

Esta edição não é somente um compilado de artigos; é um testemunho da solidez e da relevância que nossa revista alcançou na Comunidade de Inteligência. Nosso agradecimento caloroso vai a cada autor, revisor, conselheiro e leitor, que confia no trabalho da ESISPERJ.

O primeiro artigo, de Alessandra Paiva, é intitulado "Ensino de Inteligência de Segurança Pública: Aplicação da Taxonomia dos Objetivos Educacionais e Metodologias Ativas de Aprendizagem". Nele, a autora avalia a aplicabilidade e a eficácia dessas estruturas pedagógicas para o planejamento didático e o processo de aprendizagem na formação eficiente de profissionais de Inteligência de Segurança Pública (ISP).

O segundo artigo, “Análise Holística do Uso do Domínio Cibernético pelo Crime Organizado no Brasil”, de autoria de João Augusto Barros, aborda a crescente adaptação e o uso estratégico do domínio cibernético por organizações criminosas ligadas ao tráfico de drogas no Brasil. A análise detalha como as facções utilizam redes sociais, *dark web*, criptomoedas e inteligência artificial para aprimorar diversas etapas de suas operações, como recrutamento, logística, vendas e lavagem de dinheiro.

O autor André Galvão, no terceiro artigo desta edição, “Modernização das Agências Centrais de Inteligência de Segurança Pública: *Business Intelligence* como Instrumento Estratégico para o Assessoramento do Tomador de Decisão”, propõe o uso de *Business Intelligence* como ferramenta de modernização para a atividade de Inteligência, visando aprimorar o assessoramento e a eficiência das ações. Através de revisão bibliográfica, análise de casos e experiência prática, o trabalho demonstra o impacto positivo do BI na produção de conhecimento para a segurança pública.

Marcelo Martins é o quarto autor a abrilhantar a nossa décima edição. Com o artigo, “Perspectivas de Retorno para Brasileiros Voluntários na Guerra da Ucrânia: Motivação Tática e Formação em Operações com Drones”, alerta sobre a importância da Inteligência monitorar os voluntários brasileiros da Guerra da Ucrânia, que retornam ao Brasil, treinados em táticas avançadas, diante da possibilidade de recrutamento de alguns desses indivíduos por organizações criminosas.

Boa leitura e celebre conosco!

Carolina Salomão
Editora-chefe da RISP

RISP
REVISTA DE INTELIGÊNCIA DE SEGURANÇA PÚBLICA
ISSN 2675-7168 ; 2966-0254

ENSINO DE INTELIGÊNCIA DE SEGURANÇA PÚBLICA: Aplicação da Taxonomia dos Objetivos Educacionais e Metodologias Ativas de Aprendizagem

Alessandra de Oliveira Rodrigues de Paiva Passos[*]

RESUMO

A capacitação dos profissionais de Inteligência de Segurança Pública (ISP) é doutrinária e comumente motivada na comunidade de inteligência. Atualmente, algumas Agências de Inteligência de Segurança Pública (AISP) do estado do Rio de Janeiro e de outras Unidades Federativas brasileiras possuem setores de ensino ou realizam treinamentos para seu efetivo. Este estudo, fundamentado em uma revisão sistemática da literatura disponível, objetiva analisar a aplicabilidade e a eficácia das Metodologias Ativas e da Taxonomia dos Objetivos Educacionais nas instruções de ISP. A análise se aprofunda nos desafios específicos da atividade, buscando compreender como o planejamento pedagógico e didático, bem como a prática docente, podem resultar em um processo de aprendizagem mais ativo. Neste processo, o aprendiz assume o protagonismo e desenvolve habilidades de níveis cognitivos superiores, necessárias à profissão, tendo o instrutor como mediador e facilitador.

Palavras-chave: Inteligência de Segurança Pública; capacitação; metodologias ativas de aprendizagem; Taxonomia dos Objetivos Educacionais; ensino de Inteligência de Segurança Pública.

PUBLIC SECURITY INTELLIGENCE TEACHING: Application of the Taxonomy of Educational Objectives and Active Learning Methodologies

ABSTRACT

The training of Public Security Intelligence professionals is doctrinal and commonly motivated in the intelligence community. Currently, some Intelligence Agencies in the state of Rio de Janeiro and other Brazilian Federative Units have teaching or training sectors for their effectiveness. This study, based on a systematic review of the available literature, aims to analyze the applicability and effectiveness of Active Methodologies and the Taxonomy of Educational Objectives in PSI instructions. The analysis delves into the specific challenges of the activity, seeking to understand how pedagogical and didactic planning, as well as teaching practice, can result in a more active learning process. In this process, the learner assumes the leading role and develops higher cognitive skills, allowing the profession, with the instructor as a mediator and facilitator.

Keywords: Public Security Intelligence; training; active learning methodologies; Taxonomy of Educational Objectives; teaching Public Security Intelligence.

[*] Terceiro-sargento da Polícia Militar do Estado do Rio de Janeiro. Letróloga e Pedagoga. Especialista em Gestão e Docência do Ensino Superior. Coordenadora Pedagógica e de Ensino de Inteligência na Escola de Inteligência de Segurança Pública do Estado do Rio de Janeiro. Endereço eletrônico: alessandrapassos@pcivil.rj.gov.br

INTRODUÇÃO

A espécie Inteligência de Segurança Pública (ISP), oriunda da Inteligência Clássica (DISPERJ, 2015, p.4), compreende uma atividade peculiar com áreas de atuação específicas, intelectuais e/ou operacionais cada vez mais técnicas. Ela é indispensável para a produção de conhecimento e assessoramento de tomadores de decisão em seus variados níveis. Uma atividade com intensa atuação e evolução impõe constantes capacitações visando ao aperfeiçoamento dos recursos humanos das Agências de Inteligência de Segurança Pública (AISP), a fim de acompanhar as demandas contemporâneas da sociedade. A Doutrina de Inteligência de Segurança Pública do Estado do Rio de Janeiro (DISPERJ), com última atualização em 2015, categoriza como uma das dez características da ISP as Ações Especializadas:

> Ações Especializadas constituem a característica da ISP que, em face da metodologia, ações, técnicas e linguagem próprias e padronizadas, exige dos seus integrantes uma formação específica, idealmente acadêmica, complementada por longos anos de especialização, de treinamento e de experiência, conseguidos pela capacitação continuada e permanência na função. (DISPERJ, 2015)

Criada em 1995 no Rio de Janeiro, a ISP expandiu-se para outros estados brasileiros no final do século XX. Com isso, as capacitações da atividade ganharam destaque nas AISP (Ferreira, 2020, p.23).

Algumas dessas AISP atuam com órgãos/setores de ensino que promovem essas capacitações, seja em menor escala, com instruções internas para o efetivo orgânico; seja em maior escala, como a Escola de Inteligência de Segurança Pública do Estado do Rio de Janeiro (ESISPERJ), primeira escola de ISP do Brasil (Ferreira, 2020, p.24). A ESISPERJ pertence à Agência Central do Sistema de Inteligência de Segurança Pública do Estado do Rio de Janeiro (SISPERJ), conforme Decreto Estadual n.º 46.633, de 04 de abril de 2019 e, desde 2004, capacita os profissionais das AISP do Sistema e agências congêneres.

Em face da necessidade de instruir, torna-se necessário atentar para as metodologias de ensino aplicadas. Considerando as habilidades que os analistas e agentes de ISP precisam adquirir e os desafios inerentes à profissão, principalmente nos estados com significativo crescimento das organizações criminosas, o ensino tradicional pode ser menos adequado para preparar os alunos, podendo limitar a construção ativa do próprio conhecimento uma vez que se centraliza somente na transmissão de conteúdo, priorizando a aprendizagem passiva com foco na transmissão e repetição, impedindo o alcance de objetivos que visam preparar o profissional para a autonomia da atividade nas AISP. O ensino tradicional, em qualquer ação educativa, pode acarretar ausência de estratégias que possibilitem erros

e acertos, prejudicando a aprendizagem efetiva.

Educador brasileiro e crítico do ensino tradicional, Paulo Freire defendia que a educação deve ser um processo dialógico, que estimule a reflexão crítica e a autonomia dos aprendizes: "A educação não pode ser considerada um 'ato de depositar', em que os educadores depositam conhecimentos em recipientes vazios" (Freire, 1981, p.94). Existe uma necessidade de compreender melhor as estratégias pedagógicas, avessas ao ensino tradicional, que podem oferecer qualificações profissionais com foco nos atributos que, no caso, analistas e agentes de ISP precisam ter, bem como o papel do instrutor na aquisição do saber. Diante disso, como o ensino de ISP pode propiciar um processo de aprendizagem efetivo, resultante em uma mudança significativa e duradoura no conhecimento, nas habilidades e nas atitudes dos profissionais de inteligência, sendo dinâmico e influenciado por estratégias pedagógicas que tornem o aluno protagonista desse processo?

O ensino de Inteligência de Segurança Pública neste estudo é compreendido como um processo dialógico, reflexivo e formativo, no qual o educador atua como facilitador da construção do conhecimento, estimulando o desenvolvimento de competências cognitivas, técnicas e éticas. Essa abordagem está alinhada aos pressupostos de Dewey (2023), Freire (2019) e Bloom (2001), que defendem o protagonismo do aprendiz e a indissociabilidade entre teoria e prática no processo educativo.

Tendo em vista a importância do desenvolvimento profissional em ISP, esta pesquisa tem como objetivo geral analisar a aplicabilidade e a eficácia de dois elementos fundamentais no campo da educação, no contexto da formação dos recursos humanos das AISP: a Taxonomia dos Objetivos Educacionais (Bloom, 1972) e as metodologias ativas de aprendizagem. Ambas são abordagens pedagógicas promissoras que, mesmo com naturezas e funções distintas no processo de ensino-aprendizagem, superam as limitações do modelo tradicional.

Para tanto, serão considerados os seguintes objetivos específicos: (1) Revisar a literatura sobre a Taxonomia dos Objetivos Educacionais e as metodologias ativas, identificando as principais características, benefícios e aplicações no ensino de ISP; (2) Identificar o principal desafio no planejamento das instruções de ISP, analisando como as metodologias ativas e essa taxonomia podem contribuir para superar tal dificuldade; (3) Analisar as habilidades cognitivas exigidas para a atuação em ISP, comparando-as com os níveis cognitivos da Taxonomia dos Objetivos Educacionais; (4) Demonstrar como essas abordagens pedagógicas podem ser integradas ao ensino de ISP, visando o desenvolvimento de

competências desejadas; (5) Discutir as possíveis implicações da adoção de metodologias ativas e dessa taxonomia para a formação de analistas e agentes de inteligência, analisando os possíveis benefícios e desafios dessa abordagem para a prática pedagógica e para a formação dos profissionais de ISP.

Esta pesquisa apresenta tópicos que possibilitarão a cadência lógica do assunto tratado, permitindo a concepção das abordagens pedagógicas propostas, no contexto da educação profissional de inteligência. Seu teor considera as nuances da atividade de ISP, a necessidade e desafios da capacitação e, tendo em sua conclusão uma síntese dos possíveis resultados do estudo. A relevância da pesquisa é prática — uma vez que esses resultados podem ser aplicados para melhorar os processos de aprendizagem da ISP — e social, pois a qualificação e formação de profissionais de segurança pública impacta significativamente no serviço oferecido à sociedade e na elaboração de políticas públicas.

1 A TAXONOMIA DOS OBJETIVOS EDUCACIONAIS E SUA APLICAÇÃO NO ENSINO DE ISP

As formas de aprender e ensinar seguem em constante evolução, buscando novos meios de tornar o aprendizado mais eficaz e significativo, inclusive na educação profissional. Duas ferramentas que ganham destaque nesse contexto são a Taxonomia dos Objetivos Educacionais e as Metodologias Ativas de Aprendizagem que, combinadas, promovem maior engajamento dos alunos e consolidação do conhecimento ativamente.

Os objetivos educacionais e de aprendizagem[1] são declarações claras e concisas do que se espera que os alunos aprendam como resultado de uma experiência educacional (Tyler, 2013). Seja na educação regular ou na educação profissional, a definição dos objetivos é indispensável para o planejamento pedagógico, por serem eles que fornecem direção para o processo de ensino aprendizagem. Os objetivos de aprendizagem não só organizam e direcionam o instrutor, mas também esclarecem aos instruendos o propósito da ação educativa, o que estão destinados a aprender e como seu progresso será avaliado. Sendo assim, objetivos educacionais e de aprendizagem bem estruturados garantem uma experiência eficaz e significativa.

José Carlos Libâneo, em sua obra Didática (1994, p.120), escreve que "podemos dizer que não há prática educativa sem objetivos". Destaca que eles devem ser

[1] Objetivos educacionais são declarações mais amplas que descrevem as metas que um curso, programa educacional ou instituição busca alcançar. Enquanto objetivos de aprendizagem são declarações mais específicas que descrevem o que os alunos devem ser capazes de fazer ao final de uma aula, unidade ou atividade de aprendizagem. Alinhar os objetivos de aprendizagem com os objetivos educacionais garante que o ensino contribua para o desenvolvimento integral dos alunos. (Tyler, 2013)

claros, específicos e alcançáveis, devendo estar alinhados com as realidades e necessidades dos alunos, contribuindo para o desenvolvimento de competências e habilidades relevantes para suas vidas.

> (...) a prática educacional se orienta, necessariamente, para alcançar determinados objetivos, por meio de uma ação intencional e sistemática. Os objetivos educacionais expressam, portanto, propósitos definidos explícitos quanto ao desenvolvimento das qualidades humanas que todos os indivíduos precisam adquirir para se capacitarem para as lutas sociais de transformação da sociedade. (LIBÂNEO, 1994, p.132)

Diante desta perspectiva, os objetivos são uma exigência à prática docente, tendo os órgãos/setores de ensino de ISP, junto aos instrutores, o desafio de defini-los no planejamento didático. Na realidade do ensino de Inteligência de Segurança Pública, os objetivos educacionais devem ser definidos para cada curso, enquanto os objetivos de aprendizagem devem ser definidos para cada aula. É nesse contexto que a Taxonomia dos Objetivos Educacionais, conhecida como a Taxonomia de Bloom, atua como ferramenta para facilitar tais definições.

Ela foi criada em 1956, pelo psicólogo e pedagogo norte-americano Benjamin Samuel Bloom e sua equipe de estudiosos e atualizada por outro grupo em 2001, liderado por um antigo aluno de Bloom, Lorin W. Anderson. De origem grega, formada pela junção taxis (ordem, ordenação) e nomos (lei, norma), a palavra taxonomia remete a sistema de ordens (Murakami, 2021), ou seja, a Taxonomia de Bloom sistematiza os objetivos hierarquicamente e organiza os diferentes níveis de pensamento, desde o mais simples (lembrar de fatos) até o mais complexo (criar algo), ajudando professores e pedagogos no planejamento de atividades e avaliações que desenvolvam o raciocínio dos discentes em diferentes profundidades.

A Taxonomia de Bloom apresenta três domínios principais da aprendizagem que abrangem as diferentes maneiras pelas quais os indivíduos aprendem e se desenvolvem: o cognitivo, relacionado às capacidades intelectuais, ou seja, como o indivíduo processa informações, aprende, resolve problemas e pensa; o afetivo, que trata dos valores e apreciações, não apenas do que o indivíduo sabe, mas de como se sente em relação à informação e como valoriza as coisas; e o psicomotor, que aborda os movimentos corporais, habilidades motoras e da coordenação física, envolvendo aprender a realizar tarefas que exigem o uso do corpo (Bloom apud Batista, C.; Medeiros, L. M. S., 2016, p.52). Para este estudo, vamos considerar somente o domínio cognitivo, que engloba habilidades como análise e avaliação, sendo essencial para desenvolver competências para a atividade de ISP.

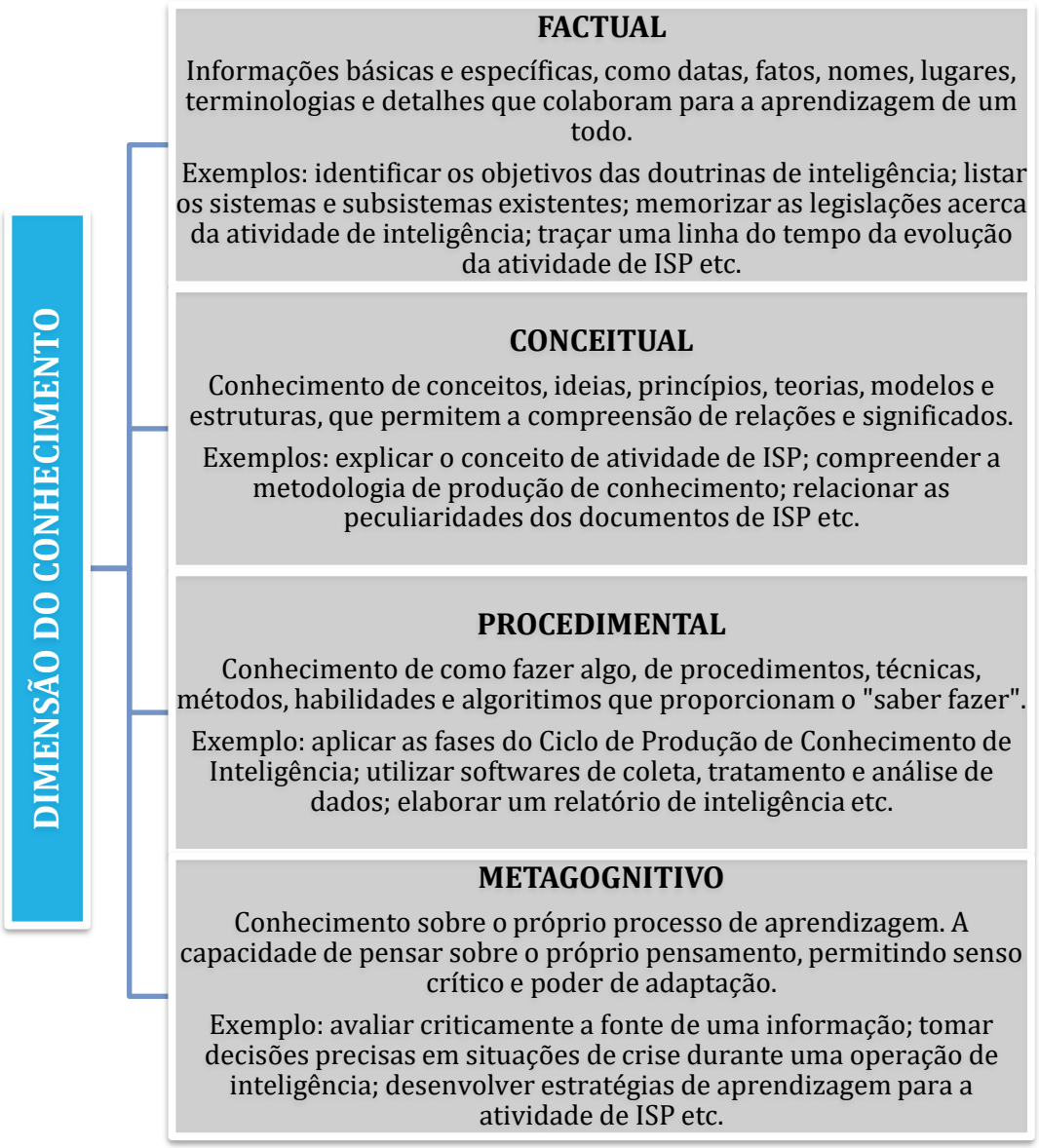
Com a revisão da Taxonomia de Bloom em 2001, o domínio cognitivo passou a ser composto por duas dimensões que se

complementam e se interligam: dimensão do conhecimento e dimensão dos processos cognitivos.

1.1 Entendendo a Dimensão do Conhecimento

Dimensão do conhecimento, também conhecida como "dimensão do conteúdo", refere-se ao "o que" do aprendizado, ou seja, o tipo de informação que o aluno, no caso o profissional de ISP, deve aprender. Abrange quatro categorias de conhecimento: factual, conceitual, procedimental e metacognitivo, como especificado na figura 1.

FIGURA 1: CATEGORIAS DA DIMENSÃO DO CONHECIMENTO E EXEMPLOS DE APLICAÇÕES NO ENSINO DE ISP



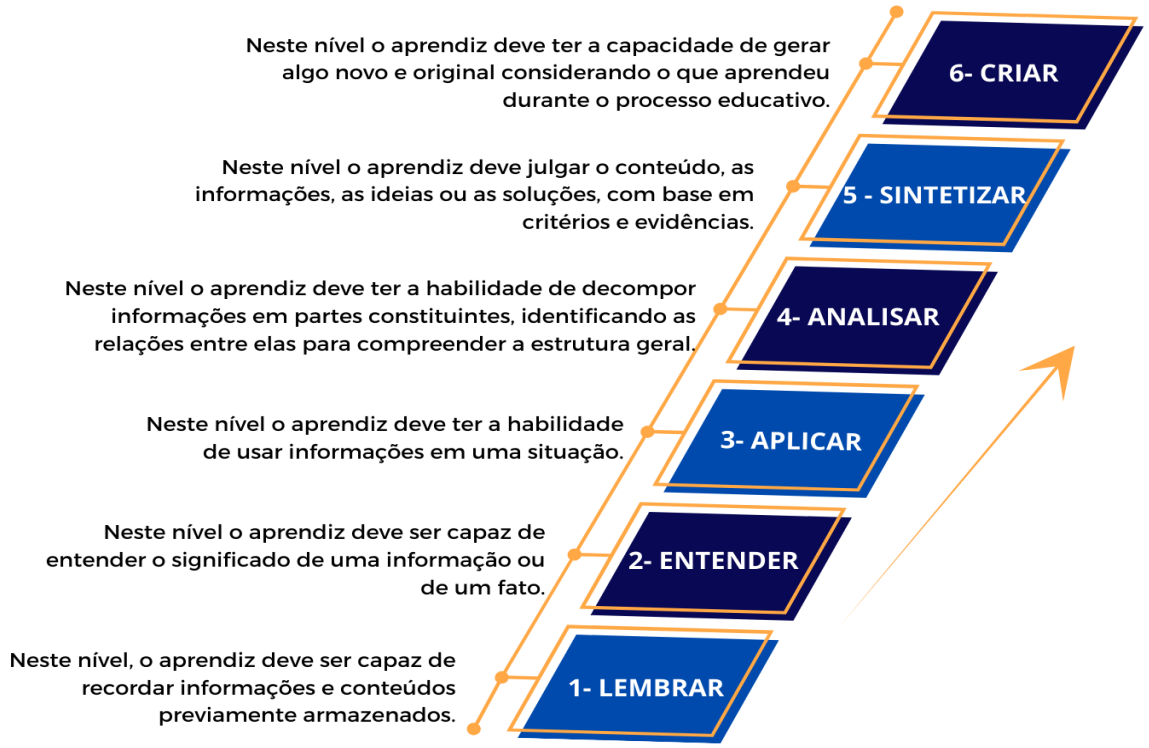
Fonte: elaborada pela autora, com base em Anderson, L. W. et tal (2001) e DISPERJ (2015), 2025.

No planejamento pedagógico de um curso de inteligência e temáticas afins de interesse à atividade, deve-se considerar qual o tipo (ou tipos) de conhecimento que se deseja que os aprendizes adquiram ao término do curso. Da mesma forma, ao planejar as aulas do mesmo curso, os instrutores devem considerar qual tipo (ou tipos) de conhecimento ele deseja que os alunos adquiram ao final de cada aula, em consonância com o objetivo geral da capacitação. Essa escolha influenciará na forma como o conteúdo será apresentado, nas atividades que serão propostas e nos critérios de avaliação, podendo identificar se os objetivos foram alcançados.

1.2 Entendendo a Dimensão dos Processos Cognitivos

Dimensão dos processos cognitivos, também conhecida como "dimensão das habilidades", refere-se ao "como" do aprendizado, ou seja, como o aprendiz pensa sobre a informação, como a processa e a utiliza. É o tipo de operação mental que o aluno realiza com o conhecimento. Essa dimensão envolve habilidades intelectuais que os alunos podem alcançar, como fases de progressão a serem conquistadas, que indicam a profundidade com que um indivíduo compreende um determinado conteúdo, dando sentido a ele e adquirindo competências, como representado na figura 2.

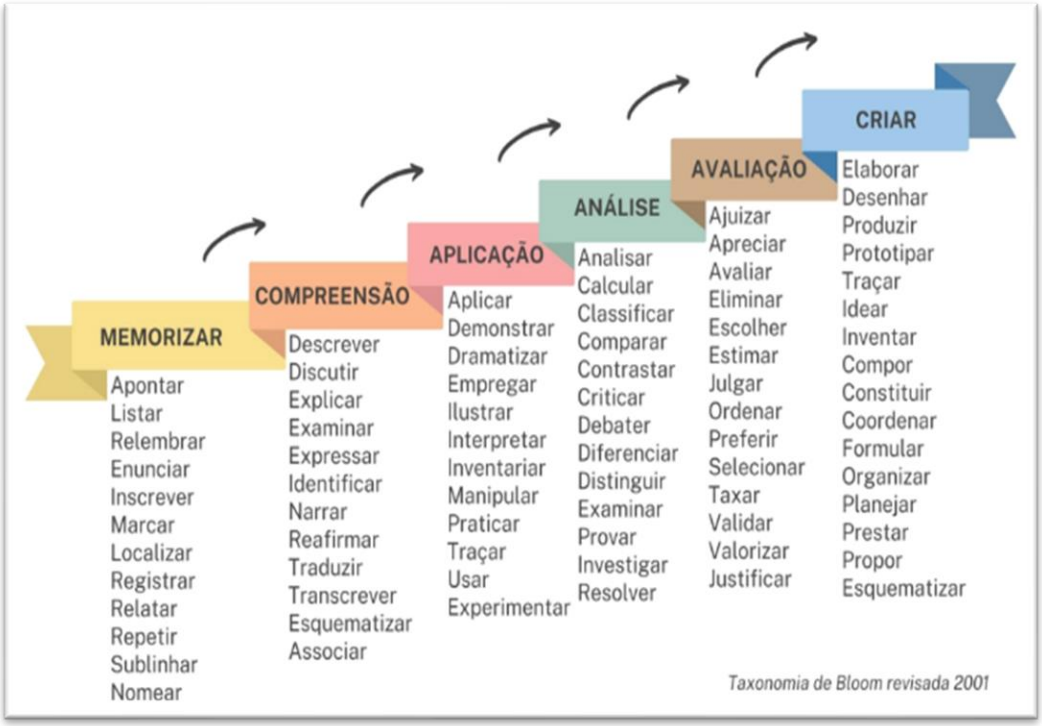
FIGURA 2: CATEGORIZAÇÃO DA TAXONOMIA DE BLOOM REVISADA



Fonte: elaborada pela autora, com base em Anderson, L. W. et tal. (2001), 2025.

Esses níveis, que apresentam sinônimos em várias literaturas, auxiliam os instrutores a entender como a mente humana processa a informação, desde a simples memorização (lembrar) até a aplicação mais complexa de conhecimentos (criar). Para elaborar os objetivos, usam-se verbos de ação conforme o nível desejado, como alguns exemplos expostos na figura 3. Entender de que forma o indivíduo aprende auxilia a planejar a prática docente, utilizando objetivos focados em diferentes aspectos do desenvolvimento.

FIGURA 3: VERBOS DE AÇÃO QUE PODEM SER UTILIZADOS PARA DEFINIR OBJETIVOS EDUCACIONAIS E DE APRENDIZAGEM



Fonte: Verbos de Taxonomia de Bloom Revisada, de Isadora Souza (2024), 2025.

1.3 A complementação das duas dimensões

Segundo Anderson, L.W. et tal. (2001), há uma relação intrínseca entre o tipo de conhecimento que se busca aprender e como o cérebro processa e utiliza esse conhecimento. Em outras palavras, o conteúdo a ser aprendido influencia a maneira como pensamos sobre ele, e a maneira como pensamos sobre ele molda a forma como o aprendemos e aplicamos. Por isso, ao elaborar os objetivos, consideram-se ambas as dimensões, sopesando o que se deseja que o aluno aprenda e o tipo de operação mental que se espera.

Em um curso de inteligência, quando se almeja que o aluno possa recordar quais as leis que regulam a atividade de ISP (conhecimento factual), por exemplo, o processo cognitivo envolvido será o **lembrar**,

então o objetivo pode ser: espera-se que os alunos sejam capazes de **listar** as principais legislações que regulam a atividade de ISP, a nível federal e estadual. Ao alcançar esse objetivo, com a mediação do instrutor, o aprendiz memorizará as leis e a execução da atividade de ISP na legalidade como um todo, o que é fundamental para o próximo tipo de conhecimento (conceitual) que ele pode seguir e para o próximo nível cognitivo (compreender) que ele pode alcançar, o qual vai entender conceitos fundamentais da atividade.

É necessário que os gestores do ensino e os instrutores considerem a hierarquia dos níveis do processo cognitivo ao elaborar os objetivos, visto que, geralmente, níveis mais complexos dependem da aquisição dos níveis mais básicos. O aprendizado comumente se dá gradualmente, com o aprendiz progredindo à medida que adquire conhecimento e desenvolve habilidades. Portanto, para o aprendiz alcançar o nível de produzir (criar) um relatório de inteligência, é necessário que ele lembre, entenda, pratique, analise e avalie alguns fundamentos e aspectos que vão fornecer as competências necessárias para produzir tal relatório. Como, por exemplo, os Estados da Mente, os Trabalhos Intelectuais e os Tipos de Conhecimentos (DISPERJ, 2025, p. 15 e 16).

2 METODOLOGIAS ATIVAS DE APRENDIZAGEM

As metodologias ativas são abordagens pedagógicas que colocam o discente como protagonista do processo de ensino-aprendizagem, incentivando sua participação ativa e autonomia na construção do próprio conhecimento. Em vez de somente receber informações passivamente, os alunos são estimulados a interagir, colaborar, questionar e aplicar os conhecimentos em diferentes situações (Dewey, 2023). Elas surgiram como resultado de um conjunto de ideias e práticas pedagógicas que colaboraram para seu desenvolvimento e, com sua eficiência aliada aos estudos de vários filósofos, educadores, psicólogos e pedagogos, foram se popularizando.

Por meio de trabalhos em grupo, debates, resolução de problemas e outras atividades que estimulem o aprendiz a pensar, questionar e construir, as metodologias ativas proporcionam maior engajamento dos alunos, desenvolvimento de habilidades essenciais, aprendizado mais significativo e melhora do desempenho. O instrutor, por sua vez, considerando sua especialidade e vasto conhecimento, assume o papel de mediador, oferecendo suporte, orientação e feedback. No ensino de ISP, essas metodologias são bem-vindas, visto que as abordagens pedagógicas que vão além da mera transmissão de informações são fundamentais, já que a atividade demanda

profissionais com habilidades analíticas, pensamento crítico e capacidade de adaptação, que serão mais bem analisadas na seção quatro desta pesquisa.

São muitas as estratégias que abrangem as metodologias ativas de aprendizagem e que podem ser utilizadas no contexto de ISP:

- Aprendizagem Baseada em Problemas (ABP) – surgiu na década de 1960, idealizada pelo médico e educador Howard S. Barrows, na Faculdade de Medicina de McMaster, no Canadá. Através do desafio para resolver problemas reais ou simulados, essa metodologia estimula o desenvolvimento do pensamento crítico, da capacidade de análise e da tomada de decisões sob pressão, habilidades cruciais para um profissional de inteligência (Barrows, 1999).

- Aprendizagem Baseada em Projetos (ABJ) – surgiu no movimento da educação progressista dos Estados Unidos e foi sistematizada por William Heard Kilpatrick em 1918. De forma estruturada, desenvolve projetos significativos, práticos e/ou científicos, que ocasionam um produto a apresentar. Permite a aplicação de conhecimentos em situações reais, desenvolvendo habilidades de planejamento, organização, trabalho em equipe, observação e comunicação, fundamentais ao profissional de ISP (Kilpatrick, 2011).

- Sala de Aula Invertida – surgiu nos Estados Unidos na década de 2000, idealizada por Jonathan Bergmann e Aaron Sams, professores de química do ensino médio em Colorado. Estudo de conteúdo teórico de forma autônoma, fora do ambiente escolar, antes da aula, utilizando-se o tempo em sala para discussões, debates, resolução de dúvidas e atividades práticas. Promove um aprendizado mais ativo e engajador, permitindo que os alunos aprofundem seus conhecimentos e desenvolvam habilidades de argumentação e pensamento crítico. Poder ser aplicado em disciplinas que demandam um estudo mais profundo e demorado (Bergmann; Sams, 2016).

- Estudo de Caso – surgiu no início do século XX na Harvard Business School. Trata-se de análise de casos reais, identificando os pontos fortes e fracos, os desafios enfrentados e as lições aprendidas (Garvin, 2002). Permite o aprendizado com a experiência de outros profissionais, desenvolvendo habilidades de análise, avaliação e tomadas de decisão. Pode ser inserido perfeitamente no ensino de ISP, trabalhando a percepção da aplicabilidade da atividade e suas características.

- Simulação – inspirada nos princípios do aprendizado experiencial de John Dewey (2023), refere-se à participação em simulações de cenários, onde precisam aplicar seus conhecimentos e habilidades para lidar com diferentes situações, como crises,

ataques cibernéticos ou operações. Permite a vivência de situações complexas e desafiadoras, desenvolvendo habilidades de tomada de decisões sob pressão, observação, memorização e trabalho em equipe e liderança.

• Aprendizagem Baseada em Equipe (ABE) – desenvolvida por Larry K. Michaelsen, na década de 1970, e fundamentada em princípios da teoria sociocultural de Vygotsky. Funciona de forma estruturada e sequencial, combinando estudo individual e trabalho colaborativo. O objetivo é maximizar o aprendizado ativo, a interação e a aplicação prática do conhecimento. Estruturada em etapas, inicia-se com estudo individual, seguido de testes individuais e em equipe, discussão em grupo e atividades práticas aplicadas. Essa abordagem promove o compartilhamento de ideias, pensamento crítico, liderança e integração, sendo especialmente eficaz para contextos complexos, como a Inteligência de Segurança Pública (Michaelsen; Sweet, 2014).

Esses são só alguns exemplos de metodologias ativas que podem ser empregadas, muitas outras contribuem para uma prática docente mais dinâmica, porém, mesmo sendo o aprendiz o ator principal da aprendizagem, a aplicação dessas metodologias ativas precisa ser bem planejada pelo instrutor e gestor. É necessário estudar o público-alvo e considerar suas peculiaridades e experiências prévias, usar um ambiente de aprendizagem colaborativo e utilizar recursos apropriados. As técnicas empregadas precisam estar associadas aos objetivos definidos no planejamento didático, para poderem levar o aluno a alcançá-los. Aplicá-las sem sentido e planejamento, apenas para evitar a monotonia na sala de aula, pode levar o processo de ensino-aprendizagem ao fracasso e desconexão com os desígnios pretendidos, causando até desinteresse dos instruendos.

A Andragogia, arte e ciência de ajudar adultos a aprender, diz que esses estão mais propensos a aprender quando sentem que o conhecimento será útil e relevante para suas necessidades profissionais (Knowles, 2005). Portanto, é necessário explicar aos discentes da atividade de ISP como funcionam as metodologias que serão aplicadas, o assunto que elas explorarão e a quais objetivos estão associadas, para verem sentido na proposta. Avaliar o processo também é uma preocupação que o instrutor deve ter ao aplicar as metodologias ativas, acompanhando e verificando o desenvolvimento, oferecendo correções construtivas e ajustando as estratégias quando necessário.

3 A CONEXÃO DA TAXONOMIA DE BLOOM COM AS METODOLOGIAS ATIVAS DE APRENDIZAGEM APLICADAS NO ENSINO DE ISP

As metodologias ativas oferecem ferramentas e estratégias para que os discentes desenvolvam as habilidades cognitivas propostas pela Taxonomia de Bloom, daí a relação entre as duas abordagens.

Para atingir, por exemplo, a dimensão do processo cognitivo aplicar, da Taxonomia de Bloom, metodologias ativas, como a Aprendizagem Baseada em Problema (ABP), permitem que os alunos utilizem seus conhecimentos para praticar soluções para problemas reais. Para atingir o nível analisar, o Estudo de Caso é uma das metodologias ativas que oferece aos alunos a oportunidade de examinar situações complexas, identificar padrões e tirar conclusões. A Sala de Aula Invertida, por sua vez, pode ser utilizada para preparar os alunos para níveis mais altos dessa taxonomia, como avaliar e criar, permitindo que eles cheguem à aula com o conteúdo já estudado e prontos para debates e atividades mais desafiadoras.

Na tabela 1 abaixo, é possível analisar a relação e aplicação dessas abordagens no contexto do ensino de ISP, como na disciplina Produção de Conhecimento:

TABELA 1: EXEMPLOS DE UTILIZAÇÃO DA TAXONOMIA DE BLOOM E METODOLOGIAS ATIVAS DE APRENDIZAGEM NA DISCIPLINA PRODUÇÃO DE CONHECIMENTO DE ISP

Dimensão do conhecimento ou do conteúdo ("o que")	***Dimensão do processo cognitivo ou das habilidades ("como" / níveis) e exemplos de verbos de ação***	***Exemplos de objetivos gerais de aprendizagem (Operação mental que se espera que o aluno realize com o conhecimento adquirido.)***	***Exemplos de metodologias ativas***
Factual	**Lembrar**: listar, recitar, relembrar, memorizar, selecionar, pesquisar, categorizar, apontar, localizar, marcar, inscrever, nomear, sublinhar, apontar etc.	**Apontar** os principais conceitos, termos e definições relacionados à produção de conhecimento. **Memorizar** as etapas do ciclo de produção do conhecimento de inteligência e suas	**Gamificação** quizz rápidos com perguntas objetivas sobre os conteúdos factuais, no formato de jogo com *score*.

		respectivas finalidades.	
Conceitual	**Compreender**: explicar, entender, parafrasear, reafirmar, exemplificar, resumir, comparar, interpretar, discutir, descrever, examinar, identificar, associar, esquematizar etc.	**Explicar** a diferença entre dado, informação e conhecimento no contexto de ISP, bem como os estados da mente e tipos de conhecimento. **Interpretar** o significado e a importância do ciclo de produção do conhecimento para a atividade de inteligência.	**Aprendizagem Baseada em Equipe:** desafios individuais e em grupo para identificar em relatórios de inteligência os conceitos trabalhados, com ênfase nos estados da mente e tipos de conhecimento.
Procedimental	**Aplicar**: demonstrar, dramatizar, empregar, ilustrar, interpretar, inventariar, manipular, praticar, traçar, usar, experimentar, aplicar, calcular, resolver, ilustrar, executar, apresentar, determinar etc.	**Empregar** o ciclo de produção de conhecimento. **Utilizar** ferramentas e técnicas de coleta de dados e técnicas acessórias de análise.	**Simulação de Cenários:** através de uma denúncia, os alunos simularão uma aplicação introdutória das fases do ciclo de produção de conhecimento. Outra opção é utilizar ferramentas das técnicas acessórias para coletar dados sobre a denúncia.
Metacognitivo	**Analisar**: classificar, decompor, categorizar, analisar, diagramar, calcular, classificar, comparar, contrastar, criticar, debater, diferenciar, distinguir, examinar, provar, investigar, resolver etc.	**Analisar** criticamente diferentes fontes de informação, avaliando sua credibilidade, relevância e potencial de viés. **Avaliar** a qualidade de conhecimentos produzidos, considerando sua precisão, confiabilidade e utilidade para a tomada de decisões.	**Estudo de Casos:** avaliar fontes e relatórios de inteligência produzidos em diversos casos no contexto de ISP.

Metacognitivo	**Avaliar**: escolher, apoiar, relacionar, determinar, defender, julgar, qualificar, comprar, contrastar, argumentar, justificar, convencer, selecionar, avaliar, apreciar, eliminar, escolher, estimar, ordenar, preferir, validar, valorizar, justificar, ajuizar etc.	**Avaliar** a eficácia das técnicas acessórias de análise e das fontes para reunião de dados para a produção de conhecimento de inteligência. **Validar** a importância da análise e do desenvolvimento do senso crítico e analítico na produção de conhecimento.	**Análise de Cenários:** apresentação de diferentes cenários para que os alunos avaliem os riscos, as ameaças, o avanço do crime, os vínculos e as oportunidades, justificando suas escolhas e refletindo sobre a utilidade das técnicas acessórias.
Metacognitivo/Procedimental	**Criar**: projetar, formular, construir, inventar, modificar, desenvolver, criar, elaborar, desenhar, produzir, traçar, idear, inventar, compor, constituir, coordenar, organizar, planejar, prestar, propor, esquematizar etc.	**Produzir** conhecimento original e relevante no contexto de ISP. **Elaborar** planos e projetos de inteligência que integrem diferentes fontes de informação e técnicas de análise.	**Aprendizagem Baseada em Projeto:** produção de relatório de inteligência com base num problema social real designado pelo instrutor, utilizando metodologias, ferramentas e técnicas trabalhadas anteriormente.

Fonte: elaborado pela autora, 2025.

A Taxonomia de Bloom e as metodologias ativas se complementam. A taxonomia oferece um mapa dos objetivos de aprendizagem, enquanto as metodologias ativas oferecem o caminho para alcançar esses objetivos. Ambas são ferramentas flexíveis que servem para conduzir e facilitar o planejamento dos instrutores e gestores, podendo ser adaptadas à realidade dos cursos e dos aprendizes. Aplicadas no ensino de ISP, podem proporcionar um envolvimento maior dos alunos ocasionando aprendizagens mais significativas e permanentes onde seja possível experimentar os desafios e nuances da atividade.

4 TAXONOMIA DE BLOOM E A INTELIGÊNCIA DE SEGURANÇA PÚBLICA: habilidades cognitivas em foco com uso de metodologias ativas

A atividade de ISP, tanto em suas

ações de Inteligência quanto de Contrainteligência, consiste em um trabalho contínuo e organizado de ações especializadas. O objetivo primordial é identificar, avaliar e monitorar ameaças, sejam elas concretas ou apenas potenciais, que possam impactar a segurança pública. A finalidade precípua é produzir conhecimento e proteger informações cruciais que sirvam de base para as decisões. Tais informações são essenciais para o planejamento e a implementação de políticas eficazes, bem como para a execução de ações que visem prever, prevenir, neutralizar e reprimir atividades criminosas de qualquer natureza (DISPERJ, 2015, p.9).

Pelo exposto, a ISP, desde a sua criação, tem sido de extrema relevância para a garantia da segurança pública. Diante dessa importância e das especificidades da atividade, entende-se que, para executá-la, é necessário um conjunto de destrezas cognitivas. Robert M. Clark, em sua obra "Análise de Inteligência: uma abordagem centrada no alvo - estratégias para uma análise eficaz e colaborativa" (2024), argumenta que a análise de inteligência é um processo complexo que exige habilidades de pensamento crítico, raciocínio lógico e uma abordagem científica e que, por isso, os analistas devem ser objetivos, metódicos e curiosos, buscando sempre novas informações e desafiando as existentes. Ao combinar essas habilidades com uma ampla perspectiva e apreciação pelo contexto histórico, os analistas podem produzir conhecimento de inteligência de alta qualidade, que pode ser utilizado para a tomada de decisões estratégicas na área de segurança pública.

Já a DISPERJ (2015), especifica não só o analista, mas também os agentes como profissionais de inteligência. São classificados como os recursos humanos da AISP que devem possuir "um perfil adequado ao bom desempenho da atividade de ISP e que engloba os valores, os requisitos e os atributos" (p.39). Portanto, verifica-se que são necessárias qualidades e desenvolturas específicas, algumas que podem ser adquiridas em capacitações e a maioria através da experiência. Outras são próprias do caráter individual, como os valores.

> **Atributos dos analistas:** objetividade, apreensão, perspicácia, método, poder de análise, poder de síntese, atenção, curiosidade intelectual, imaginação criadora, imparcialidade, comunicação e humildade intelectual.
> **Atributos dos agentes:** espírito de aventura, criatividade, versatilidade, adaptabilidade, dissimulação, dinamismo, equilíbrio emocional, coragem física, habilidade no trato com pessoas, resistência e espírito de sacrifício. (DISPERJ, 2015, p.30. Grifo nosso)

A Doutrina Nacional de Inteligência de Segurança Pública (DNISP, 2016) descreve os profissionais de ISP como aqueles que exercem funções de análise e aqueles que, adicionalmente, se dedicam às Operações de Inteligência (OPISP),

ressaltando que, embora ambos compartilhem qualidades essenciais, os profissionais dedicados às OPISP devem possuir um conjunto adicional de características.

> Os analistas deverão se destacar, ainda, pela objetividade e pela capacidade intelectual e analítica (curiosidade intelectual, capacidade de apreensão, imaginação criadora e disciplina intelectual).
> Os que se dedicam às Operações de Inteligência deverão possuir ainda adaptabilidade, flexibilidade, habilidade no trato, iniciativa, criatividade, determinação, dinamismo, coragem, controle emocional, paciência e resistência à tensão. (DNISP, 2016, p.51-52)

O ensino de ISP pode instruir e fomentar nesses profissionais a maioria desses atributos, por meio de estratégias que foquem na prática dessas habilidades, com um ambiente de aprendizagem dinâmico e profícuo. A Taxonomia de Bloom e as metodologias ativas colaboram ao definir os objetivos educacionais e de aprendizagem bem estruturados, relacionados a atividades que promovem o protagonismo dos aprendizes.

Esta seção propõe uma analogia entre os níveis da dimensão do processo cognitivo e os atributos necessários a analistas e agentes de inteligência, já que a Taxonomia de Bloom fornece uma organização clara e útil para compreender e desenvolver habilidades essenciais. Ao comparar esses níveis com os atributos, conforme tabela 2, é possível identificar quais desenvolturas são cruciais para cada função e em qual nível de complexidade elas podem se encontrar.

TABELA 2: ANALOGIA DOS NÍVEIS COGNITIVOS DA TAXONOMIA DE BLOOM COM OS ATRIBUTOS DOS PROFISSIONAIS DE INTELIGÊNCIA.

Nível da dimensão do processo cognitivo e dimensão do conhecimento	***Alguns Atributos***	***Analogias***
LEMBRAR (FACTUAL) Neste nível, é importante ter conhecimento básico e ser capaz de reproduzi-lo.	**ANALISTA:** ATENÇÃO	Capacidade de se concentrar, memorizar detalhes e se ater às minúcias.
	AGENTE: HABILIDADE NO TRATO COM AS PESSOAS	Capacidade de conseguir e armazenar informações de diferentes pessoas agindo de acordo com elas.
COMPREENDER (CONCEITUAL) Neste nível, é importante entender o significado da informação e ser capaz de interpretá-la.	**ANALISTA:** OBJETIVIDADE	Capacidade de ver as coisas como elas são, sem distorções e influências.
	AGENTE: ADAPTABILIDADE	Capacidade de entender e se adaptar a novas situações.

APLICAR (PROCEDIMENTAL) Neste nível, é importante ser capaz de aplicar o conhecimento na prática para resolver problemas específicos.	**ANALISTA:** MÉTODO	Capacidade de aplicar métodos lógicos para análise de dados e informações.
	AGENTE: VERSATILIDADE/ RESISTÊNCIA	Capacidade de aplicar diversas habilidades e conhecimentos, dependendo da situação. Capacidade de suportar cargas físicas e psicológicas
ANALISAR (METACOGNITIVO E PROCEDIMENTAL) Neste nível, é importante ser capaz de analisar informações, identificar padrões e tirar conclusões.	**ANALISTA:** PODER DE ANÁLISE/ PERSPICÁCIA	Capacidade de dividir informações complexas em componentes e identificar interconexões. Capacidade de ver conexões ocultas e entender as intenções de outras pessoas.
	AGENTE: DISSIMULAÇÃO	Capacidade de analisar a situação e agir de forma discreta e eficaz.
AVALIAR (METACOGNITIVO) Neste nível, é importante ser capaz de avaliar as informações, fazer julgamentos e tomar decisões.	**ANALISTA:**PODER DE SÍNTESE/ HUMILDADE INTELECTUAL	Capacidade de combinar diferentes elementos de informação em um todo unificado. Capacidade de reconhecer a limitação de seu conhecimento e estar aberto a novas informações.
	AGENTE: EQUILÍBRIO EMOCIONAL	Capacidade de manter a calma e tomar decisões sob pressão.
CRIAR (METACOGNITIVO E PROCEDIMENTAL) Neste nível, é importante ser capaz de criar conhecimentos, gerar ideias e encontrar soluções originais e inovadoras.	**ANALISTA:** CURIOSIDADE INTELECTUAL	Capacidade de buscar por novos conhecimentos e descobertas.
	AGENTE: ESPÍRITO DE AVENTURA E CRIATIVIDADE	Capacidade de prontidão para correr riscos, explorar o novo, criar estórias, situações e encontrar abordagens e soluções não convencionais.

Fonte: elaborado pela autora, com base na Taxonomia de Bloom revisada (2021) e DISPERJ (2015), 2025.

As analogias apresentadas reforçam que a atividade bem-sucedida na área da ISP requer um complexo de aptidões cognitivas desenvolvidas, que correspondem a diferentes níveis da Taxonomia de Bloom. Ao mesmo tempo, há uma variação no conjunto de qualidades necessárias, dependendo se a função é de analista ou agente.

As metodologias ativas contribuem com essa dinâmica na promoção de atividades que facilitem a aprendizagem das habilidades pertinentes aos profissionais de inteligência.

M. Clarck (2024) disserta que a análise de inteligência é um processo colaborativo e ao construir relações com diversos atores de interesse e entre si, os analistas de inteligência podem transformar dados em conhecimento estratégico, contribuindo para a segurança pública e para a tomada de decisões mais assertivas.

> Como a análise é um processo colaborativo, os analistas devem ser adeptos do trabalho em equipe. Devem conhecer bem a cultura, os processos e os problemas dos parceiros de equipe. Especificamente, os analistas devem conhecer os coletores e trabalhar em estreita colaboração com eles para obter inteligência e avaliar o processo de coleta. Devem manter uma rede de colegas analistas dentro e fora da agência em que exista uma convergência de interesses. (M. CLARK, p. 127, 2024)

A obtenção de dados muito se faz através da colaboração, respeitando sempre o princípio da compartimentação. Assim como na aprendizagem, quando em equipe, é muito mais produtiva. A integração é uma forte aliada na atividade de ISP e as capacitações são grandes oportunidades de promovê-la entre AISP e entre profissionais de inteligência. A adoção das metodologias ativas nessas capacitações proporciona ainda mais a colaboração e integração entre profissionais, uma vez que incentiva a aprendizagem em equipe.

A cooperação é a base tanto da análise de inteligência quanto das metodologias ativas, já que o trabalho em equipe, a troca de informações e a construção do conhecimento são elementos centrais em ambos os contextos. Profissionais de ISP em agências, assim como alunos em grupos de trabalho, enriquecem reciprocamente, seja através da aprendizagem, durante as capacitações, seja através da produção de conhecimento de ISP, na laboração em suas AISP, respeitando sempre a necessidade de conhecer determinado assunto ou dado.

5 PRINCIPAL DESAFIO NO PLANEJAMENTO DIDÁTICO DO ENSINO DE ISP: como as metodologias ativas e a Taxonomia de Bloom podem contribuir para superá-lo?

Os cursos de ISP têm por finalidade o desenvolvimento de aptidões específicas, preparação de profissionais e contribuição para a segurança pública, integrando-se às dimensões do trabalho, da ciência e da tecnologia. Portanto, entende-se que o ensino de ISP pertence à educação profissional, estabelecida no artigo 39[1] da Lei de Diretrizes e Bases da Educação (Lei Federal n.º 9.394, de 20 de dezembro de 1996), constituído por capacitações informalmente conhecidas como cursos livres.

Considerando que a educação profissional não pertence aos níveis de ensino regulares (ensino fundamental, médio e

[1] A educação profissional e tecnológica, no cumprimento dos objetivos da educação nacional, integra-se aos diferentes níveis e modalidades de educação e às dimensões do trabalho, da ciência e da tecnologia. (BRASIL, 1996)

superior), não há a obrigação de formação didática para aquele que instrui, já que o objetivo é desenvolver habilidades e técnicas peculiares para o desempenho da atividade de ISP, ensinando o "como fazer" de forma prática e objetiva, realizada com maestria pelos instrutores. Portanto, o corpo docente dos cursos de ISP é constituído por instrutores com alto nível de conhecimento, experiência, expertise e formações em suas áreas de atuação, geralmente profissionais ativos das Agências de Inteligência por período considerável, zelando pelo princípio da permanência.

O professor possui um papel abrangente na educação, responsabilizando-se pelo planejamento, avaliação e acompanhamento pedagógico do aprendizado. Já o instrutor direciona seu trabalho para a transmissão prática de habilidades específicas. Contudo, mesmo com essa ênfase prática, o instrutor tem sua atividade muito peculiar a do professor, pois também precisa planejar sua aula para assegurar que os alunos atinjam os objetivos de aprendizagem estabelecidos.

Considerando que a formação acadêmica em licenciaturas não é um requisito para atuar na educação profissional, especialmente em cursos de qualificação, alguns instrutores menos familiarizados com o planejamento didático podem enfrentar desafios na organização de sua prática docente. A Taxonomia de Bloom é uma grande aliada nesta construção, já que ela permite que o instrutor visualize os níveis cognitivos que os alunos precisam alcançar conforme o que pretende ensinar, servindo como um guia do processo. As metodologias ativas também são eficazes, uma vez que dispõem ao instrutor uma gama de abordagens que ele pode escolher para levar seus alunos a alcançar o que ele almeja.

Cabe à gestão do ensino de ISP da agência orientar e treinar o corpo docente quanto ao uso dessas ferramentas, além da priorização da interdisciplinaridade e multidisciplinaridade em todas as aulas. É necessário que os instrutores sejam conscientizados quanto aos objetivos educacionais estipulados para os cursos, de modo que compreendam os objetivos de aprendizagem que precisam estabelecer para suas aulas, utilizando ferramentas e técnicas que facilitem este planejamento.

CONCLUSÃO

O processo de ensino-aprendizagem de ISP pode ser dinâmico e influenciado por estratégias pedagógicas que coloquem o aluno no papel ativo e central de sua própria jornada de conhecimento, com foco nas aptidões necessárias, através da integração pensada de abordagens pedagógicas atuais. A Taxonomia dos Objetivos Educacionais (Taxonomia de Bloom) e as metodologias ativas de aprendizagem podem ser adaptadas às especificidades da atividade ISP e propiciar

uma aprendizagem resultante em uma mudança significativa no conhecimento, nas habilidades e nas atitudes dos profissionais de inteligência.

Ambas são ferramentas do contexto educacional valiosas, muito utilizadas e bem aproveitadas no planejamento didático da educação regular. São flexíveis e adaptadas a qualquer contexto que vise o alcance de competências a serem adquiridas, inclusive na educação profissional e técnica. A união entre essas ferramentas pode configurar um progresso importante no ensino de ISP.

A analogia da Taxonomia de Bloom com os atributos dos profissionais de inteligência demonstra uma lógica no seu uso, ao explorar cada nível consoante os atributos dos profissionais. Ao estruturar o aprendizado em níveis cognitivos, essa taxonomia oferece um roteiro claro para o desenvolvimento de habilidades essenciais aos profissionais de ISP. Com seu uso, os instrutores podem definir objetivos mensuráveis, evitando a ambiguidade e garantindo que o ensino seja focado em resultados específicos. Ela oferece um padrão simples e fácil de usar, que pode ser adaptado a diferentes contextos e disciplinas, facilitando o planejamento de aulas, atividades e avaliações, mesmo para instrutores sem experiência em design instrucional. Permite, também, a visualização mais clara dos níveis cognitivos, proporcionando a possibilidade de sequenciar o conteúdo e as atividades de forma lógica, garantindo que os alunos progridam gradualmente em seu aprendizado, consolidando-o de maneira eficaz e duradoura.

A Taxonomia de Bloom também auxilia na seleção de avaliações e estratégias de ensino adequadas e, por isso, integra-se com as metodologias ativas, colocando o aluno no centro do processo de aprendizagem, incentivando a participação ativa, a colaboração e o desenvolvimento de habilidades como pensamento crítico e adaptação a variadas situações. Com uma variedade de técnicas, as metodologias ativas permitem que os instrutores adaptem o ensino às especificidades da ISP, aproximando os alunos da realidade profissional. A troca de informações, o trabalho em equipe e a construção coletiva do conhecimento enriquecem a experiência de aprendizagem e preparam os profissionais para os desafios da atividade.

REFERÊNCIAS

ANDERSON, L. W., KRATHWOHL, D. R., AIRASIAN, P. W., CRUIKSHANK, K. A., MAYER, R. E., PINTRICH, P. R.& WITTROCK, M. C. (2001). *A taxonomy for learning, teaching, and assessing: A revision of Bloom's taxonomy of educational objectives. New York: Longman*. 2001.

BATISTA, Cristina Jardim; MEDEIROS, Ligia Maria Sampaio de. Três Domínios da Taxonomia de Objetivos Educacionais no Ensino Básico de Desenho. Revista Brasileira de Expressão Gráfica. Vol. 6, No. 2, p. 52 – 55. 2018. Disponível em: file:///D:/Usu%C3%A1rios/4401238/Downloads/artigo60.pdf. Acesso em: 05 dez.2024.

BLOOM, Benjamin S. (et al). Taxonomia dos objetivos educacionais: domínio cognitivo. Porto Alegre: Globo, 1972.

BRASIL. Lei nº 9.394, de 20 de dezembro de 1996. Estabelece as diretrizes e bases da educação nacional. Diário Oficial da União, Brasília,1 DF. 1996. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9394.htm. Acesso em: 05 dez. 2024.

CLARK, Robert M. Análise de Inteligência: Uma abordagem centrada no alvo - estratégias para uma análise eficaz e colaborativa. ISBN 978-65-5757-051-7. Biblioteca do Exército. 2024.

DEWEY, J. Experiência e Educação. Patrópoli, RJ. 2023.

DISPERJ. Doutrina de Inteligência de Segurança Pública do estado do Rio de Janeiro. Rio de Janeiro (RJ). Secretaria de Estado de Segurança Pública. 2015.

DNISP. Doutrina nacional de Inteligência de Segurança Pública. Brasília (DF). Ministério da Justiça. 2016.

FERRAZ, Ana Paula do Carmo Marcheti; BELHOT, Renato Vairo. Taxonomia de Bloom: revisão teórica e apresentação das adequações do instrumento para definição de objetivos instrucionais. Gestão & Produção, São Carlos, v. 17, n. 2, p. 421-431. 2010. Disponível em: file:///D:/Usu%C3%A1rios/4401238/Downloads/Taxonomia_de_Bloom_revisao_teorica_e_apresentacao_.pdf. Acesso em: 25 jan. 2025.

FERREIRA, Romeu Antônio. A Criação da ISP. Revista de Inteligência de Segurança Pública. v. 1, n. 1, p. 11-28. 2020. Disponível em: https://esisperj-ead.pcivil.rj.gov.br/pluginfile.php/377/mod_resource/content/11/RISP%20n%201%20v%201%202020.pdf. Acesso em: 16 out. 2024.

FREIRE, Paulo. Pedagogia do Oprimido. Rio de Janeiro: Paz e Terra. 1981.

GONÇALVES, Jonisvaldo Brito. Atividade de Inteligência e Legislação Correlata. Niterói (RJ): Impetus. 2018.

KNOWLES, M., & Associates. Andragogia em Ação. Aplicando princípios modernos de educação de adultos. San Francisco: Jossey Bass. 2005.

KRATHWOHL, D. R.; BLOOM, B. S.; & MASIA, B. B. *Taxonomy of educational objectives: The classification of educational goals*, Handbook II: The affective domain. New York: David McKay Co., Inc. 1964.

LIBÂNEO, José Carlos. Didática. São Paulo: Cortez. 1994.

MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA. Matriz Curricular Nacional para a Formação dos Profissionais de Segurança Pública. DF. 2014. Disponível em: https://www.gov.br/mj/pt-br/assuntos/sua-seguranca/seguranca-publica/ensino-e-pesquisa/site-novo/copy_of_matrizcurricularnacional_versaofinal_2014.pdf. Acesso em: 20 mar. 2025.

MURAKAMI, Roberto. O que é a Taxonomia de Bloom? Ensino bilíngue e educação, Gestão e Desenvolvimento. 2021. Disponível em: https://www.youbilingue.com.br/blog/o-que-e-a-taxonomia-de-bloom/. Acesso em: 23 fev. 2025.

RIO DE JANEIRO. Decreto nº 40.254 de 30 de outubro de 2006. Cria sem aumento de despesa, na estrutura organizacional básica da Secretaria de Estado de Segurança Pública – SSP, como órgão de ensino, a Escola de Inteligência de Segurança Pública – ESISP – e inclui, nos subitens 2 e 3, do Anexo I ao Decreto nº 33.503, de 03 de julho de 2003, que dispõe sobre a referida estrutura, os subitens 2.7 e 3.13, respectivamente, e dá outras providências. Disponível em: https://l1nq.com/decreto40256-2006. Acesso em: 13 mar. 2025.

RIO DE JANEIRO. Decreto nº 46.633, de 3 de abril de 2019. Dispõe sobre a estrutura do Sistema de Inteligência de Segurança Pública do Estado do Rio de Janeiro (SISPERJ). Leis Estaduais, Rio de Janeiro, 3 abr. 2019. Disponível em: https://l1nq.com/decreto46633-2019. Acesso em: 13 mar. 2025.

RIO DE JANEIRO. Resolução SESEG nº 737, de 30 de dezembro de 2013. Dispõe sobre a reorganização e implementação da Escola de Inteligência de Segurança Pública do Estado do Rio de Janeiro ESISPERJ. Diário Oficial do Estado do Rio de Janeiro nº 002 de 03 de janeiro de 2014.

SILVA, Maria Aparecida de Souza e. A Taxonomia de Bloom como instrumento para o planejamento didático-pedagógico no ensino de engenharia. Revista Brasileira de Ensino de Engenharia, v. 19, n. 1, p. 11-22. 2015. DOI: 10.1590/1806-96392015191011. Disponível em: https://www.scielo.br/j/gp/a/bRkFgcJqbGCDp3HjQqFdqBm/?lang=pt. Acesso em: 16 out. 2024.

SOUZA, Isadora. Verbos da Taxonomia de Bloom Revisada. Start Educação. 2024. Disponível em: https://www.starteducacao.com/post/verbos-taxonomia-de-bloom-revisada. Acesso em: 25 jan.2025.

TYLER, Ralph W. Basic principles of curriculum and instruction. 1. ed. rev. Chicago: University of Chicago Press, 2013.

RISP
REVISTA DE INTELIGÊNCIA DE SEGURANÇA PÚBLICA
ISSN 2675-7168 ; 2966-0254

ANÁLISE HOLÍSTICA DO USO DO DOMÍNIO CIBERNÉTICO PELO CRIME ORGANIZADO NO BRASIL

J. A. A. de Barros[*]

RESUMO

Este artigo explora a crescente adaptação e o uso do domínio cibernético por organizações criminosas ligadas ao tráfico de drogas no Brasil. Analisa-se como as facções empregam redes sociais, *dark web*, criptomoedas e inteligência artificial para otimizar suas operações, incluindo recrutamento, logística, vendas e lavagem de dinheiro. Discute-se o uso de *frameworks* consagrados para planejar e prevenir ações maliciosas pelos adversários do crime, dando aos ambientes policial e judicial soluções para o enfrentamento à evolução criminosa no espaço cibernético. O trabalho indica que, apesar da lacuna na documentação pública detalhada, as evidências indicam uma sofisticação substancial do cibercrime organizado, exigindo uma abordagem integrada que combine inteligência, tecnologia, legislação e cooperação nacional e internacional.

Palavras-chave: crime organizado; crimes cibernéticos; tráfico de drogas.

HOLISTIC ANALYSIS OF THE USE OF CYBER DOMAIN BY ORGANIZED CRIME IN BRAZIL

ABSTRACT

This paper investigates the increasing appropriation of the cyber domain by drug trafficking organizations in Brazil. It analyzes how criminal factions utilize social media platforms, the dark web, cryptocurrencies, and artificial intelligence to enhance operational capabilities in recruitment, logistics, illicit sales, and money laundering. Drawing on established cybersecurity and threat modeling frameworks, the study outlines preventive strategies against malicious actions and proposes actionable insights for law enforcement and judicial responses. Despite limited open documentation, available evidence reveals a growing sophistication in organized cybercrime, highlighting the urgent need for integrated approaches combining intelligence, technological tools, legal mechanisms, and both national and international cooperation.

Keywords: organized crime; cybercrime; drugs traffic.

[*] Engenheiro eletricista pelo Instituto Militar de Engenharia e Especialista em Políticas e Estratégias Cibernéticas pela Escola Superior de Guerra. Endereço eletrônico: augusto.barros@idciber.org

INTRODUÇÃO

A dinâmica nas ações do crime organizado no Brasil tem sido caracterizada por grandes transformações nos últimos anos, movendo-se do “mundo físico” para uma atuação cada vez mais intensa do domínio cibernético. A antiga máxima de que "o crime não para" ressoa com particular pertinência diante da crescente atualização tecnológica das organizações criminosas, principalmente aquelas envolvidas no tráfico de drogas.

Apesar da percepção de que facções criminosas se valem de tecnologia, inclusive as emergentes, em suas atividades ilícitas, a formalização e o detalhamento desses casos em relatórios públicos ou acadêmicos ainda são escassos. Essa lacuna na documentação pública representa um desafio para pesquisadores, formuladores de políticas e forças de segurança, que buscam uma compreensão aprofundada da dinâmica e do impacto dessa evolução.

Cabe destacar que a escassez de dados confirmados e documentados não equivale à ausência de tais atividades. Diversos fatores contribuem para essa limitação, como a natureza sensível das investigações, que frequentemente envolvem sigilo para proteger táticas e fontes utilizadas pelas forças de segurança. Adicionalmente, a complexidade inerente às investigações de crimes cibernéticos, que demandam expertise técnica, cooperação internacional e, por vezes, tratamento de comunicações criptografadas, retarda a apresentação de narrativas conclusivas ao público.

O relatório do Conselho Internacional de Controle de Narcóticos (INCB) publicado em março de 2024, órgão ligado à Organização das Nações Unidas, alerta para o aumento do tráfico de drogas *online*, destacando o uso de plataformas de mídia social como facilitador do tráfico de substâncias ilícitas. O estudo observa que, além da *dark web*, criminosos estão explorando redes legítimas para expandir o mercado de drogas, tornando mais difícil o controle e aumentando os riscos à segurança pública. Pode-se afirmar que o Brasil também faz parte desse uso tecnológico criminoso, visto que o país, segundo o World Drug Report emitido pela United Nations Office on Drugs and Crime (UNODC), é um dos principais países onde ocorre a passagem de cocaína, devido à sua extensa fronteira com países produtores da droga, como Colômbia, Peru e Bolívia. Tal fato é corroborado pelo alto índice de apreensões.

Quando se trata de inteligência de ameaças, em seu aspecto tático, cabe destacar a rápida obsolescência de algumas informações identificadas e coletadas no cenário cibernético. Além disso, cabe observar os limites jurisdicionais, visto que o cibercrime, em muitos casos, não respeita ou se limita a fronteiras. Aspecto que também complica os processos legais e probatórios

necessários para relatórios públicos detalhados.

Para contextualizar dados disponíveis e direcionar pesquisas e estratégias de combate ao crime, torna-se inegável a necessidade de elaboração de métodos e técnicas que superem os óbices citados.

O presente artigo contribui demonstrando a aplicabilidade de *frameworks* relacionados à matéria de inteligência de ameaças para construção de análises que permitam não apenas relatar as ações, mas também identificar pontos, onde a ação policial possa vir a prevenir, interromper ou elucidar casos. Cabe destacar que não é objetivo deste trabalho realizar uma Operação de Inteligência, portanto, na coleta de dados, iremos nos ater a notícias disponíveis em mídias abertas, as quais estarão relacionadas nas referências.

1 CONCEITOS E FUNDAMENTOS

No intuito de identificar e caracterizar os processos no domínio cibernético envolvidos nos atos criminosos do tráfico de drogas, torna-se necessário compreender os fundamentos de *Cyber Threat Intelligence* (CTI).

Em essência, conforme tratado na Conference on Semantic Technology for Intelligence, Defense, and Security (STIDS), CTI é o conhecimento baseado em evidências sobre ameaças cibernéticas existentes ou emergentes que pode ser usado para promover as decisões. Diferente de dados brutos ou informações isoladas, a CTI é contextualizada, analisada e acionável, permitindo que as forças de segurança antecipem e respondam a ações por parte dos criminosos no ambiente cibernético.

Para produção de inteligência útil aos objetivos, utiliza-se do ciclo da inteligência de ameaças, que é representado por fases. Inicialmente, realiza-se o planejamento. Nessa fase, são definidos os objetivos para coleta de inteligência, observadas as demandas das partes interessadas e as ameaças. O Planejamento impacta em todas as demais fases, pois trata, inclusive, de como aquele produto de inteligência será atualizado ou dito como obsoleto.

Em seguida, a operação do ciclo envolve a realização da coleta, com a aquisição de dados brutos de diversas fontes. No caso do crime organizado, isso pode incluir o monitoramento de redes sociais de envolvidos ou suspeitos, fóruns da *dark web*, comunicações criptografadas e dados de transações de criptomoedas.

Os dados coletados são tratados na fase de processamento para construção de um padrão utilizável. Essa fase envolve filtragem, revalidação e organização dos dados, visando alcançar dados estruturados.

Com os dados processados, analistas de inteligência examinam as informações

para identificar padrões, tendências, motivações e capacidades dos adversários. Por vezes, nessa fase, demandam novos dados a serem coletados e processados.

A partir desse ciclo, os analistas transformam informações em inteligência acionável, respondendo à pergunta: "O que isso interessa para nós?".

A fase de análise permite a emissão de relatórios, que representam a disseminação da inteligência, utilizados para comunicar às partes interessadas de forma oportuna e compreensível.

A inteligência disseminada é avaliada em relação à sua utilidade e precisão, e o *feedback* é usado para refinar as fases anteriores do ciclo, como retroalimentação deste. Nesse momento, assemelha-se ao chamado ciclo PDCA (*Plan, Do, Check, Act*), pois o *feedback* permite a melhoria contínua do ciclo de inteligência.

O ciclo de Inteligência completo permite trabalhar o dado e o relacionar com outros dados. Esse tratamento depende de processos “internos” ou “auxiliares” ao ciclo em si. Para compor essas rotinas, cabe fazer uso de boas práticas ou *frameworks* consolidados.

O National Institute of Standards and Technology (NIST) desenvolveu um dos *frameworks* mais observados pelos analistas de CTI, pois oferece um conjunto de diretrizes e melhores práticas para tratar riscos e incidentes de segurança cibernética e se baseia em cinco funções principais: Identificar, Proteger, Detectar, Responder e Recuperar.

O NIST Cybersecurity Framework favorece a identificação de riscos de ativos ou processos em redes vulneráveis a ações maliciosas, assim como possibilita a proposição de soluções de resposta. Tal abordagem permite não apenas a proteção contra táticas criminosas, mas também a detecção de atividades ilícitas, a resposta ao uso indevido e a recuperação de danos ocorridos.

O Center for Internet Security (CIS) apresenta um conjunto de controles, objetivando à segurança cibernética. Cabe observar que o *framework* do CIS é o atualmente aplicado pela Secretaria de Governo Digital do Governo Federal e recomendado pelo Tribunal de Contas da União para os órgãos públicos federais em geral. Os CIS Controls permitem uma abordagem prática, que pode ser adaptada para a definição de aspectos de coleta, processamento e análise do ciclo de inteligência.

Quando se trata de Inteligência de Ameaças em seu aspecto operacional, a principal ferramenta utilizada nas definições de Técnicas, Táticas e Procedimentos (TTPs) dos adversários são as estabelecidas no MITRE ATT&CK. Podemos considerar como uma base de conhecimento acessível de táticas e técnicas adversárias baseadas em

observações de incidentes e tendências. O ATT&CK pode ser usado para estruturar os dados na fase de processamento do ciclo de inteligência, pois, ao mapear as TTPs, favorece a simplicidade na construção da informação a ser tratada pelos analistas para compor a Inteligência a ser disseminada. Outro modelo muito útil em CTI é o Diamond Model of Intrusion Analysis. Esse modelo recai sobre a fase de análise, pois permite avaliar os dados coletados e processados em quatro elementos: Adversário, Capacidade, Infraestrutura e Vítima.

Os elementos do Modelo Diamante favorecem a concatenação das ideias a serem contempladas pelos analistas para compor a inteligência, pois permitem uma compreensão holística da operação da ameaça.

Para o contexto do crime organizado, o Diamond Model pode ajudar a entender os passos atuais e futuros das facções (Adversários), as ferramentas digitais que utilizam ou utilizarão (Capacidades), as plataformas e redes que exploram ou potencialmente exploráveis (Infraestrutura) e os prováveis alvos atuais e futuros (Vítima).

Embora não seja um *framework* técnico, quando comparado ao proposto pelo NIST ou MITRE, o UNODC Global Programme on Cybercrime, proposto pela United Nations Office on Drugs and Crime, apresenta diretrizes para o incremento das capacidades no combate à cibercriminalidade e, consequentemente, ao crime organizado transnacional.

Os manuais e programas da UNODC podem fornecer orientações sobre coleta de dados e análise. Além disso, propõem a cooperação internacional como boa prática de combate ao ilícito nas redes.

Conforme observado para cada caso, o entendimento e a aplicação desses fundamentos, boas práticas e *frameworks* permitem uma abordagem estruturada para construção de inteligência, pois possibilita a inteligência acionável a partir de uma vasta quantidade de dados.

2 O USO DO ESPAÇO CIBERNÉTICO COMO ESTRATÉGIA PARA O CRIME ORGANIZADO

As ações de repressão ao crime e os novos processos de negócio, além da mudança do perfil de consumo da sociedade, impulsionam as ações das facções para o ciberespaço. Fica evidente que não se trata de uma mera conveniência, a "sobrevivência" do negócio reside em mudar a estratégia, quando a forma de operar anterior não permite mais a manutenção, tão pouco a expansão.

Segundo SÁ (2021), o problema público envolvendo o crime organizado é complexo, devido à natureza interdisciplinar do crime organizado e suas características de estrutura hierárquica, o uso da violência, o uso de tecnologia, a "lavagem de dinheiro", a multiplicidade de crimes, dentre outras. A

análise proposta corroborou com outros estudos, que permitiram caracterizar o "negócio" até então estruturado pelo crime organizado nas diversas Unidades da Federação. *Frameworks* específicos baseados em estudos e análises favoreceram a evolução dos métodos policiais e como ocorre a coordenação, focando em um arranjo interorganizacional formado para investigar essas organizações criminosas, possibilitando reflexões e propostas de intervenções.

Observados os processos de qualquer negócio, os métodos tradicionais do tráfico mostravam-se cada vez menos eficientes e mais suscetíveis à detecção pelas forças de combate ao crime. Essa afirmação se comprova pelas quantidades cada vez maiores de drogas e outros produtos do crime apreendidos. O "alto escalão" do crime organizado percebeu a necessidade de tornar suas operações mais eficientes. Cabe destacar que, como observado por FERRO (2006), a evolução dos planos de negócio e das estruturas do crime organizado não é uma novidade. No decorrer dos anos, mudanças têm ocorrido na estrutura das organizações, seja decorrente da modernização do seu *modus operandi* ou simplesmente como resposta a mudanças legais ou novas táticas de repressão praticadas pelas organizações de aplicação da lei.

As soluções do mundo virtual proporcionam anonimato relativo, pois permitem uma maior restrição dos dados relevantes da operação criminosa, ocultando identidades e localizações, além de limitar a identificação de seus usuários e vítimas.

Ao dominar as ferramentas disponíveis do ciberespaço, o crime organizado amplia seu alcance geográfico, tendo acesso a mercados antes não viáveis e facilitando o recrutamento de novos membros em larga escala para dar suporte a essa expansão.

A internet e o uso de soluções em rede incrementam a capacidade de comando e controle, pois aumentam a velocidade das transações e comunicações, agilizando as operações. Além disso, reduzem custos e riscos associados a atividades presenciais e abrem novas fontes de receita, através da exploração de vulnerabilidades na economia digital, como no caso de roubo de criptomoedas e lavagem de dinheiro.

As vantagens para os "negócios" do crime organizado, em particular para o tráfico de drogas, determinam que haja grandes mudanças na forma de combate a essas organizações, pois agora exige um forte componente de cibersegurança, adicionado às abordagens tradicionais.

Um estudo apresentado por YANG (2017) apresentou um *framework* para identificar postagens relacionadas a drogas, analisar padrões de comportamento e detectar contas de traficantes no Instagram. A conclusão indica que a abordagem proposta é eficiente para uso prático, podendo servir

como uma ferramenta eficaz para rastrear e combater o comércio ilícito de drogas nas redes sociais. Destaca-se que o paper expõe que os dados coletados precisam de uma seleção e análise preliminar para tornar a solução mais rápida e ter maior escala, o que poderia ser realizado com outras soluções ligadas à inteligência de ameaças. Outra medida para aplicação da proposta seria a automatização parcial do tratamento dos dados com o uso de Inteligência Artificial.

3 ANÁLISE HOLÍSTICA

Para análise dos exemplos e das teorias apresentadas até aqui, podemos entender que as operações do crime organizado no ambiente cibernético acontecem para o recrutamento ou a identificação de clientes, o planejamento das operações de tráfico e crimes relacionados, comando e controle, a comunicação efetiva, execução e logística do crime e, por fim, a lavagem de dinheiro e ocultação dos bens gerados. Nesse contexto, cabe observar ações recentes e disponíveis em fontes abertas, por exemplo, as operações "Cryptoscam" e "Wet Cleaning".

O uso do domínio cibernético pelo crime organizado brasileiro no contexto do tráfico de drogas aparentemente é multifacetado. Desde a produção, o transporte e o comércio das drogas, verificam-se processos bem arquitetados e completos.

A comunicação eficiente e sempre disponível é aspecto essencial para o devido comando e controle das operações de tráfico de entorpecentes. As soluções de mensageria legítimas, com dados criptografados de ponta a ponta, e massivamente utilizadas pela sociedade em geral permitem, não apenas a disponibilidade, mas a confidencialidade e integridade necessárias para uma comunicação eficiente e oportuna aos processos ilegais. Outras demandas logísticas e até a movimentação financeira encontram ferramentas, inclusive *open source* ou gratuitas, para fomentar as ações das facções. Por fim, com o uso de "laranjas" e criptoativos, a execução da lavagem de dinheiro passa a ser um ato bem mais difícil de identificar e impedir.

Como tratado anteriormente, são poucos dados disponíveis sobre nosso tema. Portanto, o uso do termo provável ou similar será uma constante durante a análise a seguir. Ao aplicar o Diamond Model, cada incidente ou padrão de atividade criminosa no ciberespaço pode ser desmembrado em seus componentes essenciais.

Nesse estudo, o adversário é representado pelas facções criminosas ligadas ao tráfico de drogas. Cabe incluir a Máfia Italiana Ndrangheta devido a sua aliança com organizações criminosas no Brasil, o que permitiu o fortalecimento das atividades criminosas da facção na Europa. Apesar de indícios da infiltração do crime organizado

em instituições públicas e privadas, a principal motivação do crime organizado brasileiro é o lucro. Visando aumentar a eficiência de suas operações, gerando mais valores, essas ameaças utilizam plataformas e serviços digitais populares, como serviços de mensageria e mídias sociais. No entanto, em diversas fontes verificam-se indícios de uso de tecnologias emergentes, como a inteligência artificial.

O adversário malicioso apresenta capacidade de atuar ativamente no uso corrente de redes sociais, particularmente para recrutamento e vendas diretas, aplicativos criptografados de mensageria para comunicação e logística, mercados na *dark web* para comércio de entorpecentes, criptomoedas para lavagem de dinheiro e financiamento, e até mesmo inteligência artificial para inteligência operacional e tática. Pode-se incluir nessas capacidades o uso de engenharia social, seja para o convencimento dos recrutados, seja para o uso discreto para alcançar novos usuários nas mídias sociais, principalmente para evitar os controles de conteúdo e rastreamentos tradicionais.

A infraestrutura envolvida inclui plataformas de mídias sociais legítimas, serviços de aplicativos de mensagens, uso de navegador Tor para transações na *dark web*, Virtual Private Network (VPN) para anonimização, plataformas de exchange de criptomoedas, e até mesmo infraestruturas de comunicação (GPS e rádio definido por *software*) para coordenação de operações. Os *endpoints*, devido ao caráter descentralizado das ações, indicam dispositivos móveis (celulares e tablets), além de notebooks e dispositivos de armazenamento portáteis. Não se descarta, apesar de não ser verificado nas fontes pesquisadas, que as facções façam uso de infraestruturas em nuvem ou mesmo *on premisse*.

Segundo VESSONI (2023), as organizações criminosas, ao atuarem à margem da lei e sem controle estatal efetivo, tornaram-se um fenômeno complexo e de abrangência nacional, espalhando-se por todas as unidades federativas do Brasil e ultrapassando fronteiras, configurando-se como uma ameaça à segurança pública e nacional. Tais organizações não se limitam a um tipo específico de crime nem a uma delimitação geográfica, estando presentes também em países como Bolívia e Paraguai. Suas práticas criminosas englobam, desde tráfico de drogas e armas até contrabando, homicídios, furtos, roubos, lavagem de dinheiro, grilagem de terras, extração ilegal de madeira e garimpo ilegal. Entre os principais grupos destacam-se o Primeiro Comando da Capital (PCC) e o Comando Vermelho (CV), ambos com atuação transnacional. Os maiores desafios à segurança pública estão na atuação dessas facções nas fronteiras, no fortalecimento de seus vínculos com produtores de drogas da

América Latina, na ampliação de suas redes a partir dos presídios e na internacionalização de suas operações. Diante desse cenário, torna-se imperativa a adoção de políticas públicas integradas e coordenadas entre os diversos órgãos de segurança pública, visando ao enfrentamento eficaz ao crime organizado e aos ilícitos transnacionais que o sustentam. Do exposto, como se trata de crime organizado ligado ao tráfico de drogas, a compreensão de "vítima" abrange a sociedade como um todo.

Com os dados apresentados observa-se que o processo criminoso proposto pelas facções do tráfico de drogas, necessariamente, envolve o emprego de tecnologia em seus processos finalísticos.

O uso de soluções populares favorece a rápida migração entre plataformas com baixo prejuízo no processo e com grande capacidade de burlar os esforços policiais de monitoramento, além disso, o tráfego de dados não se destaca no contexto geral.

A lavagem de dinheiro via criptoativos também se mostra bem eficaz, pela grande variedade disponível de carteiras digitais e criptomoedas disponíveis, o que permite, além de favorecer o anonimato, distribuir as transferências de valores em várias carteiras.

Em primeira análise, o elo fraco dessa corrente seria o usuário de drogas e os *street-level dealers* ou aviões, no jargão policial brasileiro, que têm menos expertise e cuidado com a tecnologia, sendo mais simples a sua identificação e o seu monitoramento.

A partir dos dados coletados para cada incidente ou padrão de atividade criminosa e os ligando a esses quatro pontos do diamante, os analistas podem construir uma imagem mais completa e interconectada das operações criminosas, identificando as relações entre os adversários, suas capacidades, a infraestrutura que exploram e quem são os afetados.

O *framework* MITRE ATT&CK permite identificar as Técnicas, as Táticas e os Procedimentos (TTPs) utilizadas pelo crime organizado no ambiente cibernético. Quando das pesquisas nas diversas fontes, podemos extrair vários pontos, como o caso da tática utilizada no desenvolvimento de recursos, visto que foi identificado que as facções buscam o recrutamento de novos membros, através de redes sociais. Cabe observar que a forma de abordagem e o próprio linguajar permitem identificar a facção, sub-facção ou o aliciador. A exploração de engenharia social para obter acesso inicial aos indivíduos mostra-se como outra tática óbvia, mas não menos importante, pois permite identificar o modo de agir dos grupos criminosos quando do engajamento com os recrutados ou consumidores de drogas.

Outro aspecto no uso da engenharia social pelo crime organizado diz respeito ao roubo de dispositivos móveis, principalmente celulares, para coleta de dados visando

constituir um conjunto de contas “laranjas”. Além disso, as facções passaram a enviar mensagens maliciosas de *phishing*. Os referidos golpes se estendem às empresas, que estão tendo os dados sequestrados.

Ações de inteligência por parte das facções criminosas para monitorar alvos ligados às forças policiais também representam uma tática já identificada. Como foi o caso em que a rotina de um delegado responsável por uma investigação, delatado por advogada ligada ao crime, era acompanhado pelo crime organizado a partir das mídias sociais do alvo.

A tática de venda direta de drogas via aplicativos de mensagens, quando realizadas em grupos ou comunidades, cuja criação e administração estão disponíveis nas principais plataformas, permitem a infiltração de agentes policiais para a identificação de pseudônimos e *modus operandi*.

As táticas ligadas ao comando e controle são caracterizadas pela coordenação de logística e operações, através de comunicações criptografadas e com uso de aplicativos de GPS, que oferecem recursos de mapas e navegação em tempo real. Esses aplicativos possibilitam, inclusive, desviar a rota de postos policiais, por vezes permitem identificar operações policiais aleatórias ou programadas que viriam a impactar na ação criminosa. Esse tipo de coordenação em tempo real favorece também a movimentação de grandes volumes de drogas.

Do ponto de vista das táticas, a lavagem de dinheiro via criptomoedas para financiar operações criminosas merece destaque. O método *follow the money*, muito praticado pelos órgãos policiais de investigação, é fortemente impactado pelo uso de criptomoedas, que dificultam o rastreamento.

Em análise ao UNIDIR *Intrusion Path* podemos caracterizar o *framework* como uma ferramenta simples de avaliação por técnicos e leigos. Para tanto, o modelo organiza o ambiente em análise em três áreas de atenção: fora da rede, na borda e dentro da rede. A zona externa abrange atividades como o reconhecimento e a preparação do ataque, enquanto a zona interna compreende ações como o acesso indevido, as movimentações laterais, a exfiltração de dados e os abusos sobre os sistemas. Por fim, na borda acontecem as ações de execução propriamente ditas, com o acesso inicial e a persistência no ambiente. Essa divisão permite melhor entendimento sobre onde e como o ataque está acontecendo, promovendo uma visão clara e estratégica para a comunicação entre setores técnicos e alta gestão.

Não há indicadores claros do uso de infraestrutura própria pelo crime organizado ligado ao tráfico de drogas. Todavia a inclusão de servidores e “armas” cibernéticas pode ser uma simples questão de tempo, particularmente, pela facilidade de se usar

ambientes em nuvem com sigilo e baixa exposição, ou mesmo, utilizar da *dark web* para acesso a esse servidor, de forma anônima pelos "clientes" e parceiros dessas organizações. Em 2021, uma operação internacional coordenada entre o FBI, agências de aplicação da lei estrangeiras e parceiros do setor privado desmantelou a infraestrutura do Emotet, um dos *malwares* mais destrutivos dos últimos anos, uma verdadeira arma cibernética. A ação global, realizada, derrubou múltiplas camadas da infraestrutura do *malware*, localizadas em todo o mundo. Essa ação paralisou as operações do malware, pois gerou impacto significativo na rede de comando e controle. A exemplo do grupo que atuava com o *malware* Emotet, uma migração das operações das facções criminosas para tecnologias próprias, necessita de ações policiais na "zona interna" das infraestruturas tecnológicas dos criminosos, assim como estes podem utilizar de *botnets* para realizar suas operações e, portanto, estarão atuando na área *insite* de estruturas legítimas.

O uso da *Darknet* pode ser entendido como uma ação na borda. Pelo lado dos meliantes, a anonimização possibilitada pela Rede Tor favorece o comércio ilícito de drogas, assim como a aquisição de informações que favoreçam a lavagem de dinheiro. A Operação *DisrupTor*, desencadeada pela equipe Conjunta de Combate ao Opioide Criminal da Darknet (JCODE) desativou um dos maiores vendedores de drogas na darknet.

No perímetro das estruturas e sistemas das plataformas, as atividades criminosas são em geral pouco efetivas ou impactantes, todavia, para as ações investigativas, o uso dos algoritmos e as coletas de dados das diversas plataformas são importantíssimas. Isso indica a identificação, pelo próprio algoritmo da solução utilizada, como uma ferramenta importante para os agentes da lei, tornando determinante a colaboração entre plataformas e forças policiais. Cabe aos órgãos de investigação buscar colaboração junto aos representantes das plataformas, para que estes verifiquem os requisitos que tornem o tráfego de dados como suspeito. Além disso, deve haver celeridade nas ações estabelecidas pela justiça nos seus atos formais, resguardando as plataformas e os seus usuários, para que apenas o uso indevido seja alvo de quebra de sigilo e usuários legítimos e honestos não sejam prejudicados em seus direitos. A Inteligência Artificial representa um elemento de automação adequado para esse tipo de ação por parte das plataformas que permitem a indicação de rotinas suspeitas, colaborando efetivamente na filtragem dos dados, que serão objeto de análise dos agentes policiais.

Seguindo a proposta dos pesquisadores da UNIDIR, no ambiente *outside* do perímetro da rede, podemos identificar que o autor da ação criminosa

realiza a coleta de informações sobre a vítima ou sobre os alvos, que podem ser utilizadas para planejamento e preparação do crime. Com essa visão e observadas as práticas das facções criminosas, as investigações poderiam tratar os atos criminosos a partir da identificação de "distribuidores", ou seja, traficantes menores e usuários, além de pessoas recrutadas ou assediadas para fazer parte dos atos criminosos. Essa visão simplificada permite aos integrantes do esforço de repressão ao tráfico com a Inteligência de ameaças coletar indicadores de comprometimento e de ataque, considerados dados de inteligência tática, que permitem a detecção das ações praticadas pelo tráfico no ambiente cibernético. O processamento desses dados, particularmente as TTPs, poderia, inclusive, compor a Inteligência no seu nível estratégico. Por intermédio dos IoCs (indicadores de comprometimento) torna-se viável a detecção automatizada das ações praticadas pelo tráfico no ambiente cibernético. Os IoAs (indicadores de ataque), que focam na identificação das táticas e comportamentos do agente delinquente, favorecem o monitoramento dos usuários ativos nas ações criminosas. Com os dados de inteligência tática, IoCs e IoAs devidamente processados, as Forças Legais teriam informações para construir relatórios, os quais permitem estabelecer as Técnicas, Táticas e Procedimentos de cada facção em análise, expandindo o uso para compor a inteligência no seu nível estratégico.

Observa-se que, devido às plataformas usadas pelos meliantes, o uso de técnicas de Inteligência de Fontes Abertas (OSINT) é indicada. A Operação *DisrupTor* também representa um caso em que a investigação fora de perímetro, permitiu a ação na área de fronteira, pois as coletas que permitiram o sucesso da operação foram realizadas no monitoramento dos vendedores, que precisavam transformar o dinheiro em espécie, pegar e transportar as drogas.

Na visão holística apresentada até aqui, um aspecto a ser considerado é a dificuldade em distinguir o uso legítimo de plataformas do uso criminoso, o que requer novas técnicas de monitoramento e, possivelmente, de coleta. Além disso, a velocidade das transações e comunicações supera a capacidade de resposta, particularmente, na ausência de instrumentos jurídicos adequados ao provável ato criminoso que precise ser tratado.

No tocante à ausência de marcos legais ou questões jurisdicionais, ocasionadas pela natureza "sem fronteiras" do cibercrime, podemos destacar a existência de paraísos fiscais e canais não regulamentados, que criam lacunas legais, impedindo a atuação das autoridades policiais, que não conseguem atuar ou rastrear o dinheiro.

Os obstáculos tecnológicos também impactam nas ações policiais, como no caso

da criptografia, que dificulta o acesso a comunicações criminosas, exigindo soluções tecnológicas ou cooperação internacional, inclusive no âmbito judicial.

SANTOS (2021), conclui sobre o uso de ações de "tríplice hélice" como modelo para a inovação de métodos de compra e regramentos diversos na preparação para as ações legais contra o crime organizado.

Infere-se parcialmente que o mapeamento das atividades criminosas, no tocante às táticas, técnicas e estratégias dos criminosos ligados ao tráfico de drogas, permite desenvolver planos de detecção mais precisos, identificando os *adversary behaviors*.

CONCLUSÃO

Embora os casos confirmados de participação do crime organizado no Brasil com uso do domínio cibernético para o tráfico de drogas sejam pouco documentados em fontes abertas, as evidências demonstram uma evolução por parte de facções criminosas. Essas organizações criminosas utilizam extensivamente redes sociais, *dark web*, criptomoedas e, até mesmo, inteligência artificial para recrutamento, logística, vendas, e lavagem de dinheiro. A tecnologia não é utilizada apenas como um processo de apoio. Essa postura, em busca da eficiência nas operações, permite uma maior resiliência dos processos desenvolvidos por essas organizações criminosas e, consequentemente, as apreensões e prisões tendem a ter um percentual menor em relação ao envolvido nas operações como um todo.

O enfrentamento policial e judicial a essa modalidade de crime precisa acompanhar essa evolução. Observa-se que há diversas iniciativas, com a criação de unidades especializadas na Polícia Federal e no Ministério Público. No entanto, essas ações enfrentam barreiras significativas em termos de tecnologia, jurisdição, regramentos legais e cooperação internacional.

A criptografia, a existência de paraísos fiscais e a natureza sem fronteiras da internet criam desafios persistentes para a investigação e a coleta de provas, impactando diretamente na capacidade de documentar e processar esses crimes. A aliança entre facções brasileiras e máfias internacionais, facilitada por meios digitais, eleva o tráfico de drogas a um patamar global, exigindo uma resposta coordenada e tecnologicamente compatível.

Conclui-se, a partir do tratado neste trabalho, que a aplicação de inteligência de ameaças representa uma ferramenta adequada para direcionar o processo investigativo.

A coleta necessita ser restritiva de falsos positivos ou "lixo eletrônico", que apenas retarda as ações ou oculta os pontos de interesse e de atenção. Realizar atos de colaboração com as plataformas de mídias sociais, que limitem os dados em tempo, características e alvos dos criminosos é

fundamental para uma coleta e filtragem mais eficiente.

O uso de *frameworks*, com grande automação, baseado em IA e inovação, permite a construção de inteligência acionável, o que favorece a decisão de juízes e a ação futura de promotores, além de permitir identificar com precisão as lacunas legais necessárias.

A estratégia de combate ao crime, tanto na camada investigativa como no âmbito jurídico, tem que ser direcionada para atender os atuais requisitos criados pelo uso intenso da tecnologia com o óbvio cuidado de não atentar contra o direito inalienável dos cidadãos.

A partir dos relatórios de inteligência de ameaças, com o possível e adequado detalhamento, seria viável buscar o apoio necessário junto à indústria nacional, que direta ou indiretamente é vítima do crime organizado. A emissão de relatórios periódicos mais detalhados, com dados anonimizados sobre o *modus operandi* cibernético do crime organizado, representaria a transparência sem comprometer investigações. Essa medida permitiria que a indústria fornecesse recursos financeiros ou desenvolvesse soluções tecnológicas em apoio à área academica e ao Estado para inovar no setor de combate ao crime organizado.

A academia, a partir de relatórios de inteligência consistentes, poderia desenvolver propostas de arcabouços legais e regulatórios, a serem avaliadas pelos Poderes Judiciário e Legislativo, para lidar efetivamente com o uso de criptomoedas, finanças descentralizadas e o ambiente digital em geral, visando fechar as brechas exploradas pelo crime organizado.

A compreensão aprofundada e o combate eficaz ao uso do domínio cibernético pelo crime organizado no tráfico de drogas exigem uma abordagem integrada que combine inteligência, tecnologia, legislação e cooperação, tanto em nível nacional quanto internacional.

O poder público deveria acelerar o processo de Cooperação Internacional, tendo em vista o caráter "sem limites" do domínio cibernético para, em particular, fomentar intercâmbio de inteligência em tempo real. A adesão ou criação de regramentos internacionais que tratem o tema do crime organizado e o uso do ambiente cibernético devem ser priorizados em todos os poderes da federação.

Por fim, a aplicação das ações de "tríplice hélice" com participação efetiva da indústria, governo e Academia representam uma alternativa viável em busca da inovação necessária em todas as áreas do processo investigativo e processual.

Infere-se que o trabalho aqui apresentado contribui para construção de um tutorial, com *frameworks* e técnicas tradicionalmente utilizadas por analistas de

Inteligência de Ameaças em casos de segurança cibernética, assim como pode colaborar com analistas de segurança pública, quando em ações que envolvam o uso de tecnologia em rede pelo crime organizado, em particular as facções ligadas ao tráfico de drogas.

REFERÊNCIAS

NAÇÕES UNIDAS. Tráfico de drogas online cresce e exige ação coordenada, diz Junta Internacional de Fiscalização. ONU News, 5 mar. 2024. Disponível em: https://news.un.org/pt/story/2024/03/1828692. Acesso em: 11 jun. 2025.

UNITED NATIONS OFFICE ON DRUGS AND CRIME (UNODC). World Drug Report 2024 – Annex. Viena: UNODC, 2024. Disponível em: https://www.unodc.org/unodc/en/data-and-analysis/wdr2024-annex.html. Acesso em: 11 jun. 2025.

YANG, Xitong; LUO, Jiebo. Tracking illicit drug dealing and abuse on Instagram using multimodal analysis. ACM Transactions on Intelligent Systems and Technology (TIST), v. 8, n. 4, p. 1-15, 2017.

MITRE ATT&CK Framework
MITRE Corporation. MITRE ATT&CK Framework. Disponível em: https://attack.mitre.org. Acesso em: 6 jun. 2025.

OBRIEN, L.; RODRIGUEZ, A.; CARRARA, W. Semantic models for cyber threat intelligence. In: CONFERENCE ON SEMANTIC TECHNOLOGY FOR INTELLIGENCE, DEFENSE, AND SECURITY (STIDS), 7., 2012, Fairfax, VA. CEUR Workshop Proceedings, 2012. p. 41–48.

MITRE CORPORATION. CAR – Cyber Analytics Repository: glossary. Disponível em:https://car.mitre.org/resources/glossary/. Acesso em: 6 jun. 2025.

NIST SP 800-150 – Guide to Cyber Threat Information Sharing
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Guide to Cyber Threat Information Sharing. NIST SP 800-150, 2016. Disponível em: https://csrc.nist.gov/publications/detail/sp/800-150/final. Acesso em: 6 jun. 2025.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). The NIST Cybersecurity Framework 2.0. Gaithersburg, MD: NIST Cybersecurity White Paper (CSWP) 29, 2024. Disponível em: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf. Acesso em: 5 jun. 2025.

CENTER FOR INTERNET SECURITY (CIS). CIS Critical Security Controls v8.1. [S.l.]: Center for Internet Security, 2024. Disponível em: https://www.cisecurity.org/controls/v8-1/. Acesso em: 5 jun. 2025.

POLÍCIA FEDERAL. Polícia Federal deflagra segunda fase de operação contra grupo hacker. Brasília: Polícia Federal, 11 jun. 2025. Disponível em: https://www.gov.br/pf/pt-br/assuntos/noticias/2025/06/policia-federal-deflagra-segunda-fase-de-operacao-contra-grupo-hacker. Acesso em: 5 jun. 2025.

AGÊNCIA BRASIL. Estudo aponta que crime organizado se adapta a novas tecnologias. Rádioagência Nacional, 29 abr. 2025. Disponível em: https://agenciabrasil.ebc.com.br/radioagencia-nacional/seguranca/audio/2025-04/estudo-aponta-que-crime-organizado-se-adapta-novas-tecnologias. Acesso em: 5 jun. 2025.

UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH (UNIDIR). Introducing a new framework to analyze ICT activities. Genebra: UNIDIR, 2025. Disponível em: https://unidir.org/introducing-a-new-framework-to-analyze-ict-activities/. Acesso em: 8 jun. 2025.

SANTOS, Roberta de Oliveira. A tríplice hélice como modelo de gestão em segurança pública: o papel da inovação tecnológica no enfrentamento ao crime organizado. 2021. 167 f. Dissertação (Mestrado Profissional em Polícia Científica) – Universidade Federal de Santa Catarina, Florianópolis, 2021.

AGÊNCIA PARÁ. Polícia Civil do Pará prende três pessoas em operação contra o tráfico de drogas pela Dark Web. [S. l.]: [s. n.], [s. d.]. Disponível em: https://agenciapara.com.br/noticia/61594/policia-civil-do-para-prende-tres-pessoas-em-operacao-contra-o-trafico-de-drogas-pela-dark-web. Acesso em: 6 jun. 2025.

SÁ, Vinícius Valdir de. Mecanismos de coordenação e wicked problems: estudo de um arranjo interorganizacional voltado ao combate do crime organizado em Santa Catarina. 2021. 184 f. Dissertação, Universidade do Estado de Santa Catarina, Florianópolis 2021.

FERRO, Ana Luiza Almeida. O crime organizado e as organizações criminosas: conceito, características, aspectos criminológicos e sugestões político-criminais. 2006. 365 f. Tese de Doutorado em Direito, Universidade Federal de Minas Gerais, Belo Horizonte, 2006.

VESSONI, Adriana Lourenço Pessoa. A importância das operações interagências no combate ao crime organizado: Força Integrada de Combate ao Crime Organizado e impactos para a segurança e defesa. 2023. Trabalho de Conclusão de Curso para Especialização em Altos Estudos em Defesa, Escola Superior de Defesa, Brasília, 2023.

FEDERAL BUREAU OF INVESTIGATION. FBI, partners disarm Emotet malware: global law enforcement and private sector take down a major cyber crime tool. Washington, D.C.: FBI, 1 fev. 2021. Disponível em: https://www.fbi.gov/news/stories/emotet-malware-disrupted-020121. Acesso em: 10 jul. 2025.

FEDERAL BUREAU OF INVESTIGATION. Operation DisrupTor: JCODE actions in Los Angeles shut down major darknet drug vendor. Washington, D.C.: FBI, 22 set. 2020. Disponível em: https://www.fbi.gov/news/stories/operation-disruptor-jcode-shuts-down-darknet-drug-vendor-092220. Acesso em: 10 jul. 2025.

PINHEIRO, Mirelle; CARONE, Carlos. Inteligência do PCC mapeou rotina de delegado da PCDF que investigou facção. Metrópoles, Brasília, 28 fev. 2023. Disponível em: https://www.metropoles.com/distrito-federal/na-mira/inteligencia-do-pcc-mapeou-rotina-de-delegado-da-pcdf-que-investigou-faccao. Acesso em: 10 jul. 2025.

NUNES, Vicente; STRICKLAND, Fernanda. Facções criminosas de olho nos celulares. Correio Braziliense, Brasília, 9 maio 2022. Disponível em: https://www.correiobraziliense.com.br/economia/2022/05/5006431-faccoes-criminosas-de-olho-nos-celulares.html. Acesso em: 10 jul. 2025

RISP
REVISTA DE INTELIGÊNCIA DE SEGURANÇA PÚBLICA
ISSN 2675-7168 ; 2966-0254

MODERNIZAÇÃO DAS AGÊNCIAS CENTRAIS DE INTELIGÊNCIA DE SEGURANÇA PÚBLICA: *Business Intelligence* como Instrumento Estratégico para o Assessoramento do Tomador de Decisão

André Galvão[*]

RESUMO

A crescente complexidade das ameaças à segurança pública e o avanço do poder informacional impõem desafios significativos às agências de inteligência. Nesse cenário, o uso de ferramentas de *Business Intelligence* (BI) torna-se um vetor fundamental de modernização, capaz de aprimorar o assessoramento ao tomador de decisão, reduzir o tempo de latência no processo decisório e elevar a eficiência das operações de inteligência. Este artigo analisa o papel do BI na modernização das agências centrais de inteligência dos entes federativos brasileiros, explorando as contribuições teóricas e práticas de sua aplicação destacando o impacto positivo dessas soluções na produção de conhecimento estratégico. A metodologia empregada baseia-se em revisão bibliográfica de literatura especializada e análise documental de estudos de caso na área de Inteligência de Segurança Pública, permitindo uma compreensão abrangente dos desafios e das oportunidades relacionadas à implementação de tecnologias de BI no contexto da segurança pública brasileira. Adicionalmente, incorpora-se a experiência prática do autor na aplicação de ferramentas de *Business Intelligence* em ambientes institucionais de segurança pública, contribuindo para aproximar a análise teórica das práticas adotadas no âmbito profissional.

Palavras-chave: Inteligência de Segurança Pública; *Business Intelligence*; Modernização; Tomada de Decisão; Poder Informacional.

MODERNIZATION OF CENTRAL PUBLIC SECURITY INTELLIGENCE AGENCIES: *Business Intelligence* as a Strategic Instrument for Decision-Maker Support

ABSTRACT

The increasing complexity of threats to public security and the advancement of informational power pose significant challenges to intelligence agencies. In this scenario, the use of *Business Intelligence* (BI) tools becomes a key vector for modernization, capable of improving decision-maker support, reducing latency in the decision-making process, and increasing the efficiency of intelligence operations. This article analyzes the role of BI in modernizing central intelligence agencies of Brazilian federative entities, exploring the theoretical and practical contributions of its application and highlighting the positive impact of these solutions on the production of strategic knowledge. The methodology employed is based on a bibliographic review of specialized literature and documentary analysis of case studies in the area of Public Security Intelligence, allowing for a comprehensive understanding of the challenges and opportunities related to the implementation of BI technologies in the context of Brazilian public security.

Keywords: Public Security Intelligence; Business Intelligence; Modernization; Decision-Making; Informational Power.

[*]Graduado em Administração pela Universidade Tiradentes, pós-graduado em Gestão de Tecnologia, especialista em Inteligência de Segurança Pública pela Academia de Polícia Federal - ANP. Policial Militar do Estado de Alagoas, atua como servidor mobilizado no Ministério da Justiça e Segurança Pública, na Secretaria Nacional de Segurança Pública, Diretoria de Operações Integradas e de Inteligência, Coordenação-Geral de Inteligência.
Endereço eletrônico: andre.galvao@mj.gov.br
ORCID: https://orcid.org/0009-0007-0684-8490/ Currículo Lattes: https://lattes.cnpq.br/4848800600662383

INTRODUÇÃO

A segurança pública brasileira enfrenta um contexto cada vez mais complexo, caracterizado por ameaças transnacionais, criminalidade organizada e intensificação do uso de tecnologias por grupos ilícitos (SILVA, 2025). Nesse ambiente, a Inteligência de Segurança Pública emerge como ferramenta estratégica para antecipação de riscos e assessoramento qualificado ao Estado.

O cenário contemporâneo da segurança pública é marcado por transformações profundas que exigem respostas institucionais inovadoras. A globalização dos mercados ilícitos, a sofisticação dos métodos criminosos e a crescente interconexão entre diferentes modalidades de crime demandam das agências de inteligência uma capacidade de análise e resposta cada vez mais refinada e ágil (CARNEIRO; INHAN, 2025).

Entretanto, conforme destacam Falsarella, Jannuzzi e Sugahara (2017), o volume crescente de dados e informações gera um problema central: como as organizações podem realizar uma observação constante e integrada do ambiente, de modo a reduzir o tempo de resposta e transformar dados dispersos em conhecimento estratégico?

Esta questão torna-se ainda mais relevante quando se considera que as agências de Inteligência de Segurança Pública operam em um ambiente informacional caracterizado pela fragmentação de fontes, pela multiplicidade de sistemas e pela necessidade de integração de dados provenientes de diferentes órgãos e esferas governamentais.

A modernização das agências centrais de inteligência dos entes federativos, por meio da aplicação de *Business Intelligence* (BI), apresenta-se como uma resposta eficaz a esse desafio. Iniciativas recentes, como a consolidação de painéis operacionais no âmbito das operações integradas demonstram como o BI permite a análise preditiva e a visualização rápida dos dados relevantes para o assessoramento do tomador de decisão, qualificando as ações de inteligência e ampliando a capacidade institucional de resposta.

Nesse contexto, o presente artigo tem como objetivo analisar o papel do *Business Intelligence* na modernização das agências centrais de Inteligência de Segurança Pública, explorando suas contribuições para o aprimoramento do assessoramento estratégico e identificando os principais desafios e as oportunidades relacionadas à sua implementação no contexto brasileiro.

1 INTELIGÊNCIA POLICIAL E PODER INFORMACIONAL

1.1 Atividade de Inteligência Policial

A atividade de inteligência policial compreende um conjunto de práticas orientadas à coleta, análise e disseminação de informações estratégicas, fundamentais para o enfrentamento ao crime e à preservação da ordem pública. Segundo Andrade (2012), as distorções no entendimento e na aplicação da inteligência policial comprometem a eficácia das ações de segurança, reforçando a necessidade de capacitação técnica e o uso adequado das ferramentas disponíveis.

A inteligência policial, enquanto atividade especializada, distingue-se das demais funções policiais por seu caráter prospectivo e analítico. Diferentemente das ações reativas tradicionais, a inteligência busca antecipar cenários, identificar padrões e fornecer subsídios para a tomada de decisão estratégica, contribuindo para a prevenção de crimes e a otimização do emprego dos recursos de segurança pública.

No contexto brasileiro, embora a inteligência policial tenha evoluído significativamente nas últimas décadas, incorporando metodologias e tecnologias que ampliam sua capacidade de produção de conhecimento (OLIVEIRA; SANTOS, 2022), persistem desafios relacionados à padronização de procedimentos, à integração entre diferentes órgãos e à capacitação de recursos humanos especializados.

1.2 O Conceito de Poder Informacional no Contexto da Segurança Pública

Nesse cenário de evolução e desafios da inteligência policial, o conceito de poder informacional, associado à capacidade de acessar, manipular e transformar fluxos de informação em vantagem estratégica, torna-se cada vez mais relevante. Reginato e Nascimento (2007) apontam que a informação e sua gestão eficaz interferem diretamente na qualidade das decisões organizacionais, sendo um dos elementos centrais para a efetividade das políticas públicas.

O poder informacional no âmbito da segurança pública manifesta-se através da capacidade de coletar, processar e analisar grandes volumes de dados, de forma sistemática e integrada. Essa capacidade permite às agências de inteligência não apenas reagir a eventos criminosos, mas também antecipar tendências, identificar vulnerabilidades e propor estratégias preventivas.

No contexto da segurança pública, o domínio informacional não apenas fortalece a capacidade de resposta, mas também posiciona o Estado, de modo mais competitivo na arena internacional, em um ambiente onde dados, conhecimento e tecnologia definem os novos contornos do poder.

O que diferencia instituições bem-sucedidas das que acumulam falhas é a

maneira como tratam os dados: quem consegue organizá-los e transformá-los em informação e inteligência estratégica tem a capacidade de se antecipar a cenários futuros. Organizações no âmbito da segurança pública que conseguem transformar dados brutos em inteligência acionável ganham vantagens significativas na prevenção e no combate ao crime, bem como na otimização de recursos e na melhoria da qualidade dos serviços prestados à sociedade.

2 *BUSINESS INTELLIGENCE* COMO FERRAMENTA DE MODERNIZAÇÃO

2.1 Definição e Aplicações do *Business Intelligence*

O *Business Intelligence* reúne um conjunto de processos, tecnologias e ferramentas projetados para transformar grandes volumes de dados em informações úteis e acionáveis. Watson e Wixom (2007) destacam que o BI permite integrar fontes de dados diversas, aplicar análises avançadas e gerar visualizações que subsidiem decisões mais ágeis e precisas.

O conceito de *Business Intelligence* evoluiu, significativamente, desde sua concepção inicial, incorporando tecnologias emergentes como inteligência artificial, *machine learning* e análise preditiva (CASTRO et al., 2014). No contexto atual, o BI não se limita apenas à geração de relatórios, mas engloba capacidades avançadas de análise que permitem identificar padrões complexos, prever tendências e simular cenários futuros.

Nesse processo, o BI se apoia fortemente em rotinas de ETL (*Extract, Transform, Load*), responsáveis por extrair os dados de diferentes fontes, transformá-los de maneira sistemática, padronizada e confiável, e carregá-los em estruturas analíticas. Essa etapa garante que o dado seja tratado e validado antes de ser disponibilizado ao tomador de decisão, assegurando maior consistência, precisão e valor estratégico às informações produzidas.

Para as organizações de segurança pública, o BI representa uma oportunidade de modernização que vai além da simples automação de processos. Trata-se de uma transformação na dinâmica segundo a qual a informação é coletada, processada e utilizada para apoiar a tomada de decisão em todos os níveis organizacionais.

2.2 Contribuições do BI para Agências de Inteligência

No âmbito das agências centrais de inteligência, a aplicação do BI contribui para: acelerar o processo de coleta, organização e análise de dados estratégicos; integrar dados de diferentes fontes e sistemas, superando a fragmentação informacional; reduzir o tempo de latência na produção de conhecimento para o tomador de decisão; ampliar a capacidade preditiva por meio de análises espaciais, temporais e estatísticas; e fortalecer o

assessoramento estratégico, elevando a eficiência e eficácia das ações de inteligência.

A integração de dados provenientes de múltiplas fontes representa um dos principais benefícios do BI para as agências de inteligência. Essa capacidade permite a criação de uma visão holística dos fenômenos criminais, superando as limitações impostas pela fragmentação informacional que, tradicionalmente, caracteriza a segurança pública.

Além disso, as ferramentas de BI possibilitam a implementação de análises sofisticadas que vão desde a identificação de padrões criminais até a predição de eventos. Essas capacidades analíticas avançadas permitem às agências de inteligência não apenas compreender o que aconteceu, mas também antecipar o que pode acontecer, fornecendo subsídios valiosos para o planejamento estratégico e a alocação de recursos.

2.3. A Importância do *Big Data* e Desafios Culturais na Implementação do BI

Wixom et al. (2014) ressaltam, ainda, a importância do *Big Data* no contexto do BI, evidenciando que a capacidade de lidar com grandes volumes de dados em tempo real é um diferencial competitivo, especialmente em ambientes complexos como a segurança pública.

O fenômeno do *Big Data* na segurança pública é caracterizado não apenas pelo volume de dados disponíveis, mas também pela velocidade com que esses dados são gerados e pela variedade de fontes e formatos envolvidos (NEIVA, 2020). Essa realidade exige das agências de inteligência uma capacidade tecnológica e analítica cada vez mais sofisticada.

Freitas Neto (2014) corrobora essa perspectiva ao demonstrar que, em cenários de segurança pública, a aplicação de BI reduz gargalos informacionais, amplia a capacidade analítica e fortalece o planejamento e a tomada de decisão. Contudo, a adoção dessas tecnologias requer mudanças significativas na cultura e nos processos organizacionais, além da gestão eficaz da resistência à mudança (Amélia et al., 2011).

A transformação cultural necessária para a implementação bem-sucedida do BI envolve não apenas a capacitação técnica dos profissionais, mas também uma mudança de mentalidade em relação ao uso da informação como recurso estratégico. Essa transformação requer comprometimento, investimento em capacitação e a criação de uma cultura organizacional que valorize a análise baseada em evidências (SAISSE, 2017).

3 MODERNIZAÇÃO E DESAFIOS NAS AGÊNCIAS DE INTELIGÊNCIA

3.1. Experiências e Aplicações Práticas do BI na Segurança Pública

O uso de ferramentas de *Business Intelligence* na segurança pública já apresenta resultados concretos em diferentes níveis

governamentais. Experiências em secretarias estaduais e projetos nacionais demonstram que a consolidação de dados operacionais em painéis interativos possibilita ganhos expressivos em tempo e qualidade de resposta (DINIZ *et al*., 2023).

Essas soluções têm permitido:

- Monitoramento em tempo real de operações integradas, abrangendo diferentes temáticas e áreas de interesse operacional, o que possibilita ajustes imediatos na alocação de recursos, como ocorre nas operações integradas coordenadas pela Secretaria Nacional de Segurança Pública (Agência Gov, 2025).
- Cruzamento automatizado de dados criminais com bases administrativas e financeiras, facilitando a identificação de padrões e vínculos entre organizações criminosas.
- Mapeamento georreferenciado de ocorrências e apreensões, fundamental para o planejamento do policiamento e para o emprego tático dos recursos operacionais. Como demonstrado pelo Sinesp Análise, permitindo a visualização espacial dos dados e apoiando decisões estratégicas em diferentes níveis de gestão (MJSP, 2025).
- Acompanhamento de indicadores estratégicos na esfera federal, estadual e municipal, permitindo maior transparência e controle social sobre os resultados das políticas de segurança. Na esfera federal, essas informações são consolidadas e disponibilizadas por meio do Sinesp Integração e do Sinesp VDE (Visualização Dinâmica de Estatísticas), soluções que integram dados de segurança pública e os apresentam em painéis de *Business Intelligence.* Esses painéis permitem a visualização dinâmica dos dados, sua correlação em diferentes contextos e a análise estratégica voltada ao apoio à tomada de decisão (MJSP, 2025).

Ainda em âmbito federal, a Plataforma PF-SCCON, vinculada ao Programa Meio Ambiente Integrado e Seguro – Programa Brasil MAIS e à RedeMAIS, constitui um exemplo exitoso de aplicação do *Business Intelligence* na gestão integrada da segurança pública e da proteção do meio ambiente. O sistema permite o acesso e o compartilhamento de imagens diárias de satélite, otimizando o monitoramento territorial.

Entre suas ferramentas, destacam-se os painéis "Dinâmica da Detecção de Mudança na Amazônia Legal – Analytic Desmatamento" e "Transparência", que apresentam dados e indicadores institucionais em ambiente de transparência ativa. As visualizações do painel "Transparência" abrangem seções com o quantitativo de instituições e usuários cadastrados, além de informações sobre *download* de imagens, acessos à plataforma, monitoramento de alertas, cobertura de monitoramento por alertas, investimento e retorno, suporte e

treinamentos, premiações e notícias de impacto. Esse conjunto de informações possibilita ao setor público e à sociedade o acesso aos resultados do programa, configurando-se como um case de sucesso em transparência ativa por meio do *Business Intelligence*.

A plataforma promove a abertura e a democratização das informações, consolidando dados estratégicos e contribuindo diretamente para o monitoramento e a avaliação da política pública. Entre suas funcionalidades, destaca-se o *Dashboard* de Alertas de Mudança, que permite a visualização interativa de detecções automáticas, comparação de camadas e aplicação de filtros por área e período, conferindo objetividade e precisão analítica às ações de fiscalização.

O êxito da iniciativa é evidenciado pelas premiações recebidas, como o Prêmio Força Policial Inovadora da Cúpula Mundial da Polícia (*World Police Summit*), o 1º lugar em Inovação para Organizações Públicas, entre outros reconhecimentos. Atualmente, o sistema conta com mais de 100 mil usuários cadastrados e cerca de 650 órgãos públicos integrados, abrangendo todas as esferas administrativas, o que demonstra sua ampla capilaridade e relevância institucional.

De acordo com Mendes (2015), a adoção de ferramentas de BI no planejamento policial contribuiu significativamente para a redução da criminalidade, com quedas expressivas nos índices de violência, mesmo diante do aumento populacional, evidenciando a eficácia da tecnologia na otimização do policiamento e no uso inteligente dos recursos. Esses exemplos evidenciam que a aplicação prática do BI não apenas moderniza a gestão da informação, mas também fortalece o caráter proativo da inteligência, contribuindo diretamente para a redução do tempo de resposta, a prevenção de ilícitos e a elevação da capacidade de assessoramento ao tomador de decisão.

As experiências práticas também demonstram que a implementação de soluções de BI na segurança pública pode gerar benefícios que vão além da melhoria operacional, incluindo o fortalecimento da transparência, do *compliance* e da *accountability* das instituições de segurança pública perante a sociedade.

3.2 Transformações Estruturais e Culturais Necessárias

A modernização das agências centrais de inteligência, especialmente aquelas inseridas nas Secretarias de Segurança Pública dos estados brasileiros, não se resume à aquisição de tecnologias, mas demanda transformações estruturais e culturais profundas

As transformações estruturais envolvem a reorganização de processos, a redefinição de fluxos de trabalho e a criação de novas competências organizacionais. Tais mudanças requerem um planejamento

cuidadoso e uma implementação gradual que considere as especificidades de cada organização e as limitações existentes.

Do ponto de vista cultural, a inovação tecnológica exige uma mudança de paradigma em relação ao papel da informação e da tecnologia na atividade de inteligência. Essa transformação cultural é frequentemente o aspecto mais desafiador da modernização, pois envolve mudanças em práticas consolidadas e no modo como os profissionais percebem e executam suas atividades.

3.3 Principais Desafios na Implementação do BI

A implementação de soluções de *Business Intelligence* em agências de inteligência não ocorre sem desafios. A seguir são apresentados os principais desafios à implementação de soluções de *Business Intelligence* em agências de inteligência.

Segundo Amélia (2011), a resistência institucional à mudança é considerada um dos entraves mais recorrentes. Essa resistência pode manifestar-se em diferentes níveis organizacionais, motivada por receio de obsolescência profissional, desconfiança em relação às novas tecnologias ou apego a métodos tradicionais de trabalho. Na prática, observa-se que a resistência institucional também pode estar ligada ao temor de perda de protagonismo por determinadas áreas, dificultando a adoção de processos mais integrados, analíticos e automatizados.

Fragmentação dos sistemas e dificuldade de integração informacional - a dispersão de dados em diferentes plataformas e formatos compromete a visão unificada necessária à análise estratégica, reduzindo a agilidade no assessoramento e enfraquecendo a capacidade de antecipação dos órgãos de inteligência.

Escassez de profissionais capacitados em análise de dados e BI - a ausência de equipes devidamente preparadas resulta no subaproveitamento das ferramentas disponíveis e limita a transformação de dados brutos em conhecimento acionável.

Por fim, a segurança da informação assume relevância central no contexto da inteligência, onde a proteção de dados sensíveis é indispensável. A adoção de soluções de BI deve estar acompanhada de padrões rigorosos de segurança e privacidade, de modo a assegurar que a modernização dos processos não comprometa a confidencialidade das informações (PINHEIRO, 2023).

3.4 Estratégias para Superar os Desafios da Modernização

Superar esses desafios implica em promover uma gestão de mudança eficaz, investimentos em capacitação e treinamento, fortalecimento da cultura organizacional voltada à inteligência analítica e ampliação do uso de ferramentas modernas como o BI para

potencializar o assessoramento ao tomador de decisão.

A gestão da mudança deve ser conduzida de forma sistemática e participativa, envolvendo todos os níveis organizacionais e considerando as especificidades de cada contexto. Essa abordagem requer liderança comprometida, comunicação eficaz e o estabelecimento de metas claras e mensuráveis.

O investimento em capacitação representa outro elemento fundamental para o sucesso da modernização. Essa capacitação deve abranger não apenas aspectos técnicos relacionados ao uso de ferramentas de BI, mas também competências analíticas e metodológicas que permitam aos profissionais extraírem o máximo valor dos dados disponíveis.

A valorização da qualidade dos dados deve ser compreendida como um pilar da modernização. Isso implica estabelecer práticas sólidas de governança da informação, que envolvam processos contínuos de padronização, validação e monitoramento dos fluxos informacionais. Além da dimensão técnica, é igualmente necessário consolidar uma cultura organizacional orientada ao valor estratégico dos dados, de forma que sejam reconhecidos e tratados como ativos fundamentais. Essa mudança garante que os processos analíticos e de assessoramento se apoiem em informações consistentes, fortalecendo a agilidade, a precisão e a credibilidade na tomada de decisão.

No entanto, um dos principais desafios enfrentados nesse processo está relacionado à qualidade dos dados *(data quality).* Em ambientes de inteligência, a utilização de informações inconsistentes, incompletas ou desatualizadas compromete diretamente a efetividade das análises e reduz a confiabilidade do assessoramento estratégico. Como enfatiza Redman (2018), publicado na *Harvard Business Review*, "se os dados são ruins, o conhecimento gerado também será ruim". Isso evidencia que, ainda que se disponha de ferramentas modernas de BI ou de algoritmos avançados, sua utilidade será limitada se a base de dados não apresentar padrões adequados de confiabilidade.

CONSIDERAÇÕES FINAIS

A aplicação de *Business Intelligence* nas agências centrais de Inteligência de Segurança Pública representa um vetor essencial para a modernização institucional e o fortalecimento da capacidade de assessoramento estratégico. Em um cenário onde o poder informacional e o domínio sobre dados definem as vantagens competitivas, o BI emerge como instrumento técnico e estratégico para transformar dados em conhecimento acionável.

A análise realizada neste artigo evidencia que a modernização das agências de inteligência por meio do BI não é apenas uma

questão tecnológica, mas um processo complexo que envolve transformações organizacionais, culturais e estruturais *(data quality).* Os benefícios potenciais são significativos, incluindo a melhoria da qualidade do assessoramento, a redução do tempo de resposta e o fortalecimento da capacidade preditiva.

Contudo, para que sua implementação seja bem-sucedida, é necessário ir além da tecnologia, promovendo mudanças culturais, organizacionais e estruturais nas agências de inteligência, capacitando os profissionais e garantindo que a informação chegue ao tomador de decisão com agilidade, precisão e confiabilidade. Da mesma forma, torna-se imprescindível que o gestor e o próprio tomador de decisão também sejam capacitados para compreender o funcionamento do *Business Intelligence*, assegurando que possam interpretar corretamente os indicadores e utilizar o conhecimento produzido de maneira estratégica.

As experiências práticas evidenciadas demonstram que a implementação de soluções de BI na segurança pública pode gerar resultados concretos e mensuráveis, contribuindo para a melhoria da eficiência operacional e para o fortalecimento da capacidade de resposta às ameaças à segurança pública (MENDES, 2023).

Modernizar as agências centrais de inteligência é, portanto, mais do que um objetivo operacional: trata-se de um compromisso com a eficiência estatal, a segurança da sociedade e a valorização da inteligência como pilar estratégico da governança pública. Este processo de transformação organizacional requer visão estratégica, investimento sustentado e comprometimento de todos os atores envolvidos. A experiência acumulada em projetos como o de desenvolvimento de painéis estratégicos no âmbito da segurança pública nacional, confirma que a inovação tecnológica aplicada à inteligência não é apenas viável, mas necessária. O BI, quando alinhado à inteligência policial e à gestão integrada, transforma-se em instrumento efetivo de assessoramento do tomador de decisão no dia a dia operacional.

Para pesquisas futuras, sugere-se o aprofundamento da análise sobre os impactos específicos da implementação de BI em diferentes contextos organizacionais, bem como o desenvolvimento de metodologias para avaliação da efetividade dessas soluções no contexto da segurança pública brasileira.

REFERÊNCIAS

AMÉLIA, M.; FETZNER, M.; FREITAS, H. *Business Intelligence* (BI) implementation from the perspective of individual change. JISTEM - Journal of Information Systems and Technology Management, v. 8, n. 1, p. 25-50, 2011.

ANDRADE, F. S. Inteligência policial: efeitos das distorções no entendimento e na aplicação. Revista Brasileira de Ciências Policiais, v. 3, n. 2, p. 37-54, 2012.

CARNEIRO, G. B.; INHAN, G. C. A atuação da inteligência policial militar na construção da confiança pública e da imagem da PMPR. Revista Ibero-Americana de Humanidades, Ciências e Educação, v. 11, n. 1, p. 1-15, 2025.

CASTRO, A. et al. *Business Intelligence* aplicada na tomada de decisões em Segurança Pública. In: CONGRESSO BRASILEIRO DE INFORMÁTICA, 2014, Brasília. Anais... Brasília: SBC, 2014. p. 45-58.

DINIZ, B. P. et al. Desenvolvimento de um dashboard a partir do software Power BI para gerenciamento de dados de segurança pública em estados do nordeste entre os anos de 2016 a 2020. Revista Brasileira de Tecnologia, v. 8, n. 3, p. 112-128, 2023.

FALSARELLA, O. M.; JANNUZZI, C. A. S. C.; SUGAHARA, C. R. Gestão estratégica empresarial: proposição de um modelo de monitoramento informacional na era do big data. Revista Digital de Biblioteconomia e Ciência da Informação, v. 15, n. 2, p. 420-441, 2017.

FREITAS NETO, Francisco Paulo de. *Business Intelligence* aplicada no apoio à tomada de decisões em segurança pública. Mossoró: Universidade Federal Rural do Semi-Árido, 2014.

MENDES, R. et al. Planejamento policial a partir do uso de *Business Intelligence* (BI): a experiência da Polícia Militar de Goiás. Revista Brasileira de Estudos de Segurança Pública, v. 15, n. 2, p. 89-105, 2023.

NEIVA, L. Big Data na investigação criminal: desafios e expectativas na União Europeia. 2020. Dissertação (Mestrado) - Universidade do Minho, Braga, 2020.

OLIVEIRA, I. O.; SANTOS, F. C. C. Inteligência artificial e policiamento preditivo: possibilidades de inovação tecnológica para a Polícia Militar do Paraná no enfrentamento aos crimes violentos. *Brazilian Journal of Technology*, v. 5, n. 2, p. 1234-1250, 2022.

PINHEIRO, F. M. L. O papel da tecnologia e da inteligência artificial na segurança pública. Rio de Janeiro: Ministério Público do Estado do Rio de Janeiro, 2023. 45 p.

SILVA, C. V. M. Inteligência policial e os desafios da segurança pública nas cidades 4.0. 2025. Dissertação (Mestrado) - Universidade Federal do Rio Grande do Norte, Natal, 2025.

SAISSE, R. Big data contra o crime: efeito *Minority Report*. Direito & TI, v. 1, n. 1, p. 79-95, 2017.

REGINATO, L.; NASCIMENTO, A. Um estudo de caso envolvendo *Business Intelligence* como instrumento de apoio à controladoria. Revista Contabilidade & Finanças, v. 18, n. spe, p. 69-83, 2007.

WATSON, H. J.; WIXOM, B. H. The current state of *Business Intelligence*. Computer, v. 40, n. 9, p. 96-99, 2007.

WIXOM, B. et al. The current state of *Business Intelligence* in academia: The arrival of big data. Communications of the Association for Information Systems, v. 34, n. 1, p. 1, 2014.

REFERÊNCIAS COMPLEMENTARES

CHEN, H.; CHUNG, W.; XU, J. J. *Crime data mining: a general framework and some examples*. Computer, v. 37, n. 4, p. 50-56, 2004.

MCCUE, C. *Data Mining and Predictive Analysis: Intelligence Gathering and Crime Analysis*. 2. ed. Oxford: Butterworth-Heinemann, 2015.

KUMAR, S.; SINGH, M. *Crime Analysis and Intelligence System Model Design using Big Data. International Journal of Computer Applications*, v. 177, n. 15, p. 1-8, 2020.

REDMAN, Thomas C. *If your data is bad, your machine learning tools are useless*. Harvard Business Review, 02 abr. 2018. Disponível em: https://hbr.org/2018/04/if-your-data-is-bad-your-machine-learning-tools-are-useless. Acesso em: 13 set. 2025.

RISP
REVISTA DE INTELIGÊNCIA DE SEGURANÇA PÚBLICA
ISSN 2675-7168 ; 2966-0254

PERSPECTIVAS DE RETORNO PARA BRASILEIROS VOLUNTÁRIOS NA GUERRA DA UCRÂNIA: Motivação Tática e Formação em Operações com Drones

Marcelo Luiz Santos Martins[*]

RESUMO

Este artigo analisa o fenômeno dos brasileiros voluntários na guerra da Ucrânia, destacando o impacto de seu retorno ao Brasil, especialmente no contexto da segurança pública. Esses indivíduos, capacitados em táticas de guerrilha e operações com drones, representam uma nova ameaça ao transferirem expertise militar para facções criminosas, notadamente no Rio de Janeiro. Informações de inteligência revelam que o crime organizado utiliza esses combatentes para aprimorar sua capacidade operacional, promovendo um salto qualitativo na guerra urbana por meio de "transferência reversa de tecnologia bélica". O texto explora os mecanismos de recrutamento, como plataformas digitais e financiamento por facções, e a formação em guerra eletrônica e drones, adaptada às favelas. Casos concretos, como o uso de drones com explosivos em conflitos locais, ilustram essa evolução. O estudo aponta riscos de difusão nacional e transnacional dessa expertise e propõe estratégias como monitoramento ativo, inteligência ofensiva e reintegração controlada de ex-combatentes. A urgência de modernizar o aparato estatal é enfatizada, sob pena de o crime consolidar um modelo paramilitarizado, agravado pelo excedente de equipamentos pós-conflito.

Palavras-chave: Guerra; Ucrânia; voluntários; brasileiros; drones; inteligência; tática; facções; segurança.

PROSPECTS FOR RETURN FOR BRAZILIAN VOLUNTEERS IN THE WAR IN UKRAINE: Tactical Motivation and Training in Drone Operations

ABSTRACT

This article analyzes the phenomenon of Brazilian volunteers in the Ukrainian war, highlighting the impact of their return to Brazil, especially in the context of public security. These individuals, trained in guerrilla tactics and drone operations, pose a new threat by transferring military expertise to criminal factions, notably in Rio de Janeiro. Intelligence reports reveal that organized crime uses these fighters to enhance their operational capabilities, promoting a qualitative leap in urban warfare through "reverse transfer of weapons technology." The text explores recruitment mechanisms, such as digital platforms and faction financing, and training in electronic warfare and drones, adapted to favelas. Concrete cases, such as the use of explosive-laden drones in local conflicts, illustrate this evolution. The study highlights the risks of national and transnational diffusion of this expertise and proposes strategies such as active monitoring, offensive intelligence, and the controlled reintegration of former combatants. The urgency of modernizing the state apparatus is emphasized, lest crime consolidate a paramilitarized model, exacerbated by the surplus of post-conflict equipment.

Keywords: War; Ukraine; volunteers; Brazilians; drones; intelligence; tactics; factions; security

[*] Delegado de Polícia Civil no Estado do Rio de Janeiro há 24 anos, graduado em Direito pela UFRJ e Especialista em Gestão de Segurança Pública por meio do Curso Superior de Polícia Intregrada, pela UFRJ. Foi Diretor Geral do Departamento de Integração Operacional em Ações de Inteligência, o DGIOAI, na SSINTE, no período de 2022 a julho de 2025. Endereço eletrônico: mlsmartins@pcivil.rj.bv.br.

INTRODUÇÃO: A GUERRA IMPORTADA COMO NOVA FRONTEIRA DO CRIME BRASILEIRO

O século XXI trouxe a globalização para o crime: o que antes era tráfico estático, agora se tornou inteligência móvel, com conhecimento além das fronteiras. O atual ciclo de brasileiros na guerra da Ucrânia — com apoio logístico e estratégico das facções — representa a ponta do iceberg de uma reorganização do crime, que busca vantagem competitiva não apenas em armas, mas em conhecimento tático-operacional.

Ao patrocinar a logística de envio e regresso de combatentes, o crime organizado do Rio de Janeiro inaugura o conceito de "transferência reversa de tecnologia bélica". Não é apenas acesso a armas, mas absorção de doutrina, disciplina, engenharia de guerra eletrônica e metodologias de comando e controle. O Estado precisa entender que, no século XXI, a guerra é uma *commodity* e a expertise, um produto de alto valor.

Historicamente, a maioria dos países que participou de eventos bélicos enfrentou problemas com a reintegração social de seus ex-combatentes. A falta de políticas assistenciais torna a vida no pós-guerra marcada, principalmente, por problemas financeiros e de saúde.

> O primeiro grande obstáculo dos ex-combatentes que voltaram para a vida civil foi retomar as relações sociais e profissionais. Os soldados deixaram suas vidas e foram treinados para o combate, voltar para a vida pacífica não seria nada fácil, assim como não seria fácil para a família receber este combatente novamente em casa. (PRANDI, p.36, 2013)

O envolvimento de veteranos de guerra com o crime organizado não é um fenômeno novo — é uma dinâmica global que se intensifica a cada grande conflito, das trincheiras da Segunda Guerra Mundial às ruas da Europa, passando pelos Estados Unidos, México e Colômbia.

Esses países já enfrentaram o desafio de absorver combatentes treinados, muitos dos quais, sem perspectivas ou apoio, foram cooptados por facções e cartéis, transformando-se em multiplicadores de violência, táticas militares e inovação bélica.

Hoje, esse ciclo atinge uma nova potência. A guerra da Ucrânia, alimentada por ondas de voluntários estrangeiros — inclusive brasileiros —, promove a próxima geração de especialistas em combate, tecnologia militar e operações com drones. O mundo criminal percebe rapidamente o valor desse capital humano: facções internacionais e brasileiras já articulam a importação desse *know-how*, conectando-se em redes digitais, financeiras e logísticas que atravessam fronteiras sem esforço.

Essa transição é consequência direta da globalização. O que antes era problema distante, agora bate à porta do Brasil. As rotas do crime, o tráfico de armas e a circulação de

ex-combatentes são aceleradas por tecnologias de comunicação, sistemas de pagamento globais e um submundo onde a experiência de guerra é moeda valiosa. O Brasil, historicamente espectador desse fenômeno, agora vira protagonista: facções nacionais enxergam nos veteranos da Ucrânia uma elite de choque pronta para elevar o padrão do confronto urbano.

Ignorar esse movimento é condenar o país a um salto qualitativo na criminalidade: mais inteligência tática, mais letalidade, mais dificuldade de resposta estatal. O combate ao "novo crime" começa pelo reconhecimento de que o campo de batalha global se funde com as periferias brasileiras, exigindo ação estratégica, integrada e urgente.

1 MECANISMOS DE RECRUTAMENTO E CAPACITAÇÃO: O NOVO MERCADO DE GUERRA

1.1 Arquitetura digital e logística clandestina

Para combater a crescente sofisticação do recrutamento de brasileiros para a guerra da Ucrânia e sua subsequente integração ao crime organizado é fundamental desmantelar a arquitetura digital e a logística clandestina que sustentam esse processo.

Informações de inteligência revelam a cadeia de recrutamento que grupos em plataformas como "WhatsApp", "Telegram" e "Signal", protegidos por anonimato, operam como verdadeiras agências de emprego militar, conectando candidatos a oportunidades no conflito.

Sites como www.ildu.com.ua/pt/pagina-inicial/, com interfaces em português, facilitam o acesso de indivíduos com pouco domínio de idiomas estrangeiros, simplificando o processo de alistamento. O recrutamento envolve etapas estruturadas, como o envio de vídeos demonstrando aptidão física, preenchimento de formulários digitais, entrevistas em tempo real com recrutadores estrangeiros e o fornecimento de documentação sensível, como passaportes.

Essa rede digital e logística, altamente organizada, exige do Estado ações coordenadas de inteligência cibernética, monitoramento de plataformas e cooperação internacional para rastrear e neutralizar esses canais, impedindo o fluxo de combatentes e a transferência de expertise bélica para as facções criminosas.

1.2 O papel das facções: investimento, proteção e retorno

As facções financiam passagens, garantem logística no exterior e monitoram a trajetória dos enviados. O objetivo é simples e certeiro: treinar especialistas em drones, em guerra eletrônica e em táticas de guerrilha, além de formar instrutores internos que possam multiplicar o conhecimento e assegurar sua permanência sob controle do grupo patrocinador.

Esse ciclo de investimento e retorno configura uma estratégia de "capital tático", através da qual o risco de envio é compensado pelo ganho de vantagem bélica e operacional.

O recrutamento privilegia jovens sem antecedentes criminais, mas também abre espaço para indivíduos que buscam ascensão social rápida ou possuem histórico de atuação em áreas de risco. O incentivo financeiro é alto (salários até cinco vezes superiores ao tráfico tradicional) e o status simbólico de "combatente internacional" é utilizado como ferramenta de arregimentação e influência nas bases criminosas.

2 FORMAÇÃO EM OPERAÇÕES COM DRONES: DA EUROPA ORIENTAL AO CORAÇÃO DAS FAVELAS

2.1 A capacitação dos voluntários

Na Ucrânia, o brasileiro não é apenas soldado, é aluno de uma escola de guerra em tempo real. O treinamento envolve: pilotagem de drones para reconhecimento, ataque e sabotagem; aprendizado de guerra eletrônica, com identificação e evasão de bloqueadores, adaptação de frequência, uso de contramedidas; customização de drones comerciais para fins militares, com adaptação para transporte de explosivos, monitoramento de patrulhas inimigas e sabotagem de infraestrutura e; doutrina de guerrilha urbana, composta por emboscadas, mobilidade rápida, uso de rotas alternativas e camuflagem em ambientes hostis.

Ao regressar, o ex-voluntário se torna multiplicador. Oficinas informais e células de treinamento são criadas em áreas de difícil acesso, sobretudo em comunidades sob influência do tráfico de drogas no Rio de Janeiro, como os Complexos da Penha, do Alemão, do Salgueiro, de Israel, da Mangueirinha e a Rocinha. O conhecimento é disseminado para grupos de ataque, defesa e logística.

Drones passam a ser utilizados para mapeamento de território, monitoramento de operações policiais e ataques cirúrgicos contra rivais e forças estatais. O treinamento é adaptado para o contexto brasileiro, com foco em resiliência a bloqueadores e adaptação ao ambiente urbano denso.

2.2 Casos concretos

Segundo informações recentes, jovens de baixa escolaridade, oriundos de comunidades da zona norte da cidade do Rio de Janeiro e da região de São Gonçalo retornaram da Ucrânia com placas de colete balístico, fardas militares e *know-how* para disseminar em diversas comunidades, inclusive em uma organização criminosa de projeção transnacional, autodenominada Comando Vermelho.

Informações de inteligência revelam ainda que um indivíduo com expertise em explosivos assumiu o papel de consultor estratégico, ajudando a planejar ataques precisos contra grupos rivais e forças estatais.

Essa atuação destaca o alto valor atribuído à experiência técnica especializada em operações desse tipo, adquirida diretamente na Ucrânia, o que eleva o nível de sofisticação do crime organizado.

Nessa linha, observou-se recentemente o emprego de drones equipados com artefatos explosivos durante o confronto entre integrantes do Comando Vermelho e milicianos atuantes na comunidade do Catiri, no Rio de Janeiro, o que evidencia a incorporação de tecnologia de uso militar em um cenário de guerrilha urbana.

3 BLOQUEADORES DE SINAL: A EVOLUÇÃO DA GUERRA ELETRÔNICA URBANA

3.1 Do enfrentamento aberto à blindagem eletrônica

O uso de drones pelas forças policiais foi rapidamente reprimido pelo crime. As informações de inteligência levantadas documentam a instalação sistemática de bloqueadores de sinal em regiões estratégicas: Parada de Lucas, Vigário Geral e Complexo da Penha passam a ser zonas de exclusão aérea, dificultando tanto operações de inteligência quanto incursões táticas.

Normalmente são utilizados dispositivos inibidores de drones, conhecidos como *jammer*, que se tratam de equipamentos especializados concebidos para interferir e neutralizar os sinais de comunicação que governam as operações de aeronaves remotamente pilotadas. Ao emitir sinais de radiofrequência disruptivos, esse mecanismo compromete os sistemas de controle do drone, resultando na interrupção de sua funcionalidade e na limitação de sua capacidade de voo. A tecnologia é importada, adaptada e constantemente atualizada para evitar detecção e neutralização pelas forças estatais.

3.2 Impactos operacionais: o Estado cego e a favela blindada

O bloqueio de sinal impede a ação de drones policiais, compromete a segurança de aeronaves tripuladas e cria um ambiente de incerteza tática para as forças de segurança. O Estado perde o monopólio da vigilância aérea, sendo forçado a adaptar protocolos, investir em novas tecnologias e treinar equipes para guerra eletrônica.

Enquanto isso, o Estado se acotovela no berço da burocracia e das formalidades da Lei nº 14.133/21 (Lei de Licitações e Contratos), enfrentando processos lentos e entraves administrativos para modernizar seus meios. As facções, por outro lado, simplesmente avançam na proteção de seus territórios, adquirindo, com agilidade, equipamentos de ponta, em um ritmo quase instantâneo, incompatível com a morosidade institucional.

A simbiose entre o conhecimento importado da Ucrânia e a realidade das

favelas cariocas gera um ciclo de inovação criminal. O crime investe em atualização contínua, simulando cenários de guerra híbrida, bloqueando investidas do Estado e sabotando sistemas de vigilância de rivais.

4 ARTICULAÇÃO ENTRE GUERRA EXTERNA E CRIME INTERNO: ESTRATÉGIAS, NOMES E DINÂMICAS

Para enfrentar a articulação entre a guerra externa e o crime interno, o Estado deve adotar estratégias robustas que desarticulem as dinâmicas de liderança e a multiplicação do capital bélico promovidas por facções criminosas. Lideranças da organização criminosa Comando Vermelho têm investido na formação de núcleos autônomos de guerra, articulando logística, proteção e disseminação de conhecimento tático adquirido por ex-combatentes da Ucrânia. Essas lideranças utilizam a expertise dos retornados para blindar operações, dificultar infiltrações estatais e consolidar o domínio territorial, criando estruturas criminosas mais resilientes e sofisticadas.

A lógica de multiplicação do capital bélico resulta na ampliação da capacidade de enfrentamento armado e tecnológico, permitindo que as facções sustentem operações policiais prolongadas e exportem seu modelo paramilitarizado para outras regiões e estados. Essa expansão fortalece uma rede de crime com padrão militar, aumentando a resiliência das facções e dificultando a retomada de controle pelo Estado, o que exige ações coordenadas de inteligência e intervenção para neutralizar essas lideranças e desmantelar suas redes operacionais.

5. AMEAÇAS, CENÁRIOS E RISCOS: O FUTURO DA SEGURANÇA NO BRASIL

Com os desafios impostos pelo retorno de brasileiros voluntários da guerra da Ucrânia e sua integração ao crime organizado, o Estado deve abordar os riscos de difusão nacional e internacional da expertise bélica adquirida. A disseminação dessas habilidades para outros estados brasileiros e até para países vizinhos pode criar um ecossistema de crime transnacional com padrão militar, ampliando a capacidade das facções de operar com táticas sofisticadas e tecnologias avançadas, como o uso de drones e a guerra eletrônica.

A sofisticação do comportamento dos ex-combatentes, que utilizam identidades camufladas, simulação de vínculos legais e técnicas de evasão digital, dificulta a infiltração e o monitoramento pelas forças de segurança, exigindo o desenvolvimento de inteligência humana e cibernética de alto nível, além de protocolos ágeis de cooperação internacional.

Comunidades sob controle de facções estão se transformando em redutos cada vez mais fortalecidos, com o uso de

bloqueadores de sinal, treinamento interno e militarização crescente, o que torna essas áreas em zonas de exclusão para o Estado. Esse cenário eleva o desafio de retomada e controle territorial, demandando do Estado estratégias integradas que combinem inteligência avançada, tecnologia de ponta e ações táticas coordenadas para neutralizar a ameaça de um crime paramilitarizado e impedir sua consolidação em escala regional e nacional.

6. OPORTUNIDADES E RECOMENDAÇÕES ESTRATÉGICAS: VIRANDO O JOGO

Para enfrentar a ameaça do retorno de brasileiros voluntários da guerra da Ucrânia e sua integração ao crime organizado, é crucial implementar um sistema consistente de mapeamento e monitoramento ativo. A criação de um banco de dados nacional dedicado a rastrear ex-combatentes, com detalhes sobre seus movimentos e atividades, é um passo fundamental para identificar potenciais riscos.

Esse esforço deve ser complementado por uma intensificação da cooperação internacional com agências globais, facilitando o rastreamento da circulação desses indivíduos. Além disso, a adoção de protocolos de alerta para autoridades migratórias e aeroportuárias é essencial para garantir a detecção precoce de possíveis ameaças, permitindo uma resposta ágil e coordenada do Estado.

Uma estratégia de inteligência ofensiva deve ser priorizada para desarticular as estruturas criminosas que absorvem o conhecimento bélico desses retornados. A infiltração de agentes em núcleos de treinamento que fazem multiplicação de expertise nas comunidades é uma medida crítica para desmantelar essas redes por dentro, assim como oferecer incentivos a ex-combatentes “arrependidos” para que colaborem com o Estado fornecendo informações estratégicas e enfraquecendo as facções.

Os investimentos em guerra eletrônica urbana, aliados à constante atualização doutrinária das forças de segurança, são indispensáveis para que o Estado "reverta" o conhecimento adquirido pelo crime organizado contra ele próprio, neutralizando tecnologias criminosas como drones e bloqueadores de sinal, garantindo que o Estado recupere a vantagem tática e operacional.

Para mitigar os riscos associados ao retorno de brasileiros voluntários da guerra da Ucrânia, é essencial implementar programas de reintegração sob vigilância e controle social. Esses programas devem oferecer acompanhamento e apoio aos ex-combatentes, proporcionando orientação profissional e oportunidades de reinserção social, enquanto se mantém um

monitoramento rigoroso para prevenir sua cooptação por organizações criminosas.

A criação de mecanismos que incentivem denúncias anônimas, aliados ao fortalecimento de redes comunitárias de proteção, é igualmente crucial. Essas redes podem capacitar moradores a resistir à influência do crime, promovendo um ambiente de segurança e cooperação que dificulte a atuação de facções em comunidades vulneráveis.

A modernização das forças de segurança por meio de atualização tecnológica e doutrinária é imprescindível para enfrentar a sofisticação do crime paramilitarizado. As equipes devem estar preparadas para os desafios do combate urbano moderno, utilizando-se da formação continuada em guerra híbrida, combinando elementos convencionais e não convencionais, e de operações com drones. Investimentos massivos em tecnologias capazes de bloquear, rastrear e neutralizar equipamentos eletrônicos usados pelo crime, como os próprios drones e os sistemas de comunicação clandestinos, são necessários para recuperar a vantagem tática.

CONCLUSÃO: O FUTURO PEDE AUDÁCIA E INTELIGÊNCIA

A guerra da Ucrânia deixou de ser distante para se tornar local. O crime brasileiro opera hoje com padrão paramilitar, importando doutrinas, tecnologias e disciplina militar. O retorno dos voluntários é o divisor de águas: ou o Estado aprende a responder com inovação, proatividade e integração, ou continuará refém de organizações criminosas que já pensam, treinam e operam como exércitos privados. O futuro da segurança pública não pertence a quem reage, mas a quem antecipa, infiltra e neutraliza. O tempo do improviso acabou.

Além disso, o fim iminente do conflito europeu deve resultar em um excedente de equipamentos sendo comercializados a preços acessíveis, o que tende a abastecer facções criminosas no Brasil, em especial no estado do Rio de Janeiro, com tecnologia de ponta e grande poder destrutivo. A história já mostrou esse efeito: após o colapso da União Soviética, fuzis AK-47 eram frequentemente vistos em conflitos ao redor do mundo, sobretudo na África, onde até crianças-soldado portavam tal armamento.

Esse paralelo reforça o alerta de que não se trata de mera possibilidade, mas de um risco concreto e imediato a ser mitigado o quanto antes pelo Estado. A convergência entre a militarização do crime organizado e o fluxo iminente de conhecimentos táticos-operacionais, advindos do conflito russo-ucraniano, estabelece uma grave ameaça à ordem social brasileira e, consequentemente, à segurança pública nacional.

REFERÊNCIAS

BRANCO, Zoraia Saint'Clair. Análise de riscos: técnica acessória à produção do conhecimento em Inteligência de Segurança Pública (ISP) em construção – Normas ABNT NBR ISO 31.000:2009, NBR ISO/IEC 31.010:2012 e ABNT ISO GUIA 73:2009. 2017. 94 f. Monografia (Curso de Pós-Graduação Lato Sensu de Especialização em Inteligência de Estado e Inteligência de Segurança Pública) – Faculdade de Direito Milton Campos (FDMC) / Associação Internacional para Estudos de Segurança e Inteligência (INASIS), 2017.

PRANDI, Danilo de Mauro. A Reintegração Social dos Ex-Combatentes Brasileiros: as Condições de Vida dos Veteranos. Monografia apresentada à disciplina de Estágio Supervisionado em Pesquisa Histórica como requisito para a conclusão do Curso de História, Setor de Ciências Humanas, Letras e Artes, Universidade Federal do Paraná, 2013.

BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil. Organizado por Cláudio Brandão de Oliveira. Rio de Janeiro: Roma Victor, 2002. 320 p.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. Diário Oficial da União: seção 1, Brasília, DF, ano 139, n. 8, p. 1-74, 11 jan. 2002. PL 634/1975.

CURITIBA. Lei nº 12.092, de 21 de dezembro de 2006. Estima a receita e fixa a despesa do município de Curitiba para o exercício financeiro de 2007. Curitiba: Câmara Municipal, [2007]. Disponível em: http://domino.cmc.pr.gov.br/contlei.nsf/98454e416897038b052568fc004fc180/e5df879ac6353e7f032572800061df72. Acesso em: 22 mar. 2007.

GLOBAL INITIATIVE AGAINST TRANSNATIONAL ORGANIZED CRIME. The hard return: mitigating organized crime risks among veterans in Ukraine. Genebra, 2024. 48 p. Disponível em: https://globalinitiative.net/analysis/mitigating-organized-crime-risks-among-veterans-in-ukraine/. Acesso em: 28 set. 2025.

LOEVINSOHN, Benjamin. Performance-Based Contracting for Health Services in Developing Countries: a toolkit. Washington, DC: The World Bank, 2008. 202 p. (Health, Nutrition, and Population Series, 44821). ISBN 978-0-8213-7536-5. DOI 10.1596/978-0-8213-7536-5. Disponível em: http://www.who.int/management/resources/finances/CoverSection1.pdf. Acesso em: 7 maio 2010.

ISSN 2675-7168 ; 2966-0254

A ESISPERJ

Criada oficialmente pelo Decreto Estadual nº 40.254/2006, renomeada pelo Decreto Estadual nº 44.528/2013, posteriormente reorganizada e vinculada à Subsecretaria de Inteligência através da Resolução SESEG nº 737/2013 (DOERJ nº 002/2013), a Escola de Inteligência de Segurança Pública do Estado do Rio de Janeiro (ESISPERJ) busca, através de seus cursos, seminários, ações, *workshops* etc. a uniformização da atuação das Agências de Inteligência de Segurança Pública (AISP) formando, especializando e treinando os servidores nelas lotados, com ênfase nos seguintes pilares:

MISSÃO: qualificar os profissionais da Comunidade de Inteligência e manter atualizada a Doutrina de ISP, por meio da pesquisa e produção de conhecimento, visando potencializar a capacidade de atuação estatal na área finalística da Segurança Pública.

VISÃO: ser referência em ensino, doutrina, pesquisa e extensão em Inteligência de Segurança Pública (ISP) para a Comunidade de Inteligência.

VALORES: produção de conhecimento em ISP; valorização do ambiente democrático; fortalecimento de rede; integração; profissionalização técnica; respeito à diversidade; interoperabilidade; e excelência científica e tecnológica.

A RISP

A Revista de Inteligência de Segurança Pública (RISP) é uma publicação continuada, da Escola de Inteligência de Segurança Pública do Estado do Rio de Janeiro (ESISPERJ). Idealizada como um canal de acesso ao conhecimento de forma oficial, objetiva e transparente, a revista visa divulgar manuais e estudos científicos, resenhas, pesquisas atuais, além das melhores e mais apuradas práticas, contribuindo assim para a desmistificação do tema. A RISP é, portanto, voltada para a comunidade acadêmico-científica, profissionais do setor e demais interessados em aprofundar seus conhecimentos na área de Inteligência, notadamente vinculados às questões da segurança pública.

CONDIÇÕES GERAIS PARA SUBMISSÃO

O envio dos textos, em recebimento de fluxo contínuo, deve ser realizado para o e-mail: risp.esisperj@pcivil.rj.gov.br, em formato <.doc/.docx> (*Microsoft Office Word*). No

mesmo e-mail, deve ser encaminhado o Termo de Cessão de Direitos Autorais, assinado e salvo em formato <.pdf>, além do arquivo contendo elementos pré-textuais. Visando facilitar esse processo, todos os modelos destes e outros documentos, além das Diretrizes para Autores, podem ser obtidos na página da ESISPERJ (https://esisperj-ead.pcivil.rj.gov.br/).

Como parte do processo de submissão, os autores são obrigados a verificar a sua conformidade em relação a todos os itens listados nas diretrizes. As submissões em desacordo com as normas serão recusadas e/ou devolvidas aos autores para adequação. Os textos devem seguir os padrões de estilo e requisitos bibliográficos descritos e adotados pelo padrão vigente da ABNT, apresentados nas Diretrizes para Autores.

Os textos devem ter como escopo a atividade de inteligência, com foco na atividade de Inteligência de Segurança Pública, podendo tomar como objeto todas as dimensões e aspectos inerentes à ISP. É necessário que sejam produções intelectuais inéditas dos respectivos autores, atentando-se para que não haja inserção de conteúdo publicado sem menção da fonte, de modo a não ferir a política editorial adotada pela ESISPERJ e a ética científica.

DECLARAÇÃO DE DIREITO AUTORAL

Autores que publicam nesta revista concordam com os seguintes termos:

1) Autores mantêm os direitos autorais e concedem à revista o direito de primeira publicação, sob a Licença *Creative Commons Attribution,* que permite o compartilhamento do trabalho com reconhecimento da autoria e publicação inicial nesta revista.

2) Autores têm autorização para assumir contratos adicionais separadamente, para distribuição não exclusiva da versão do trabalho publicada nesta revista (ex.: publicar em repositório institucional ou como capítulo de livro), com reconhecimento de autoria e publicação inicial nesta revista.

3) Autores têm permissão e são estimulados a publicar e distribuir seu trabalho *online* (ex.: em repositórios institucionais ou na sua página pessoal) a qualquer ponto antes ou durante o processo editorial, já que isso pode gerar alterações produtivas, bem como aumentar o impacto e a citação do trabalho publicado.