

QUANDO A FARDA ENFRENTA O FEED: ANTIFRAGILIDADE, CONTRAINTELIGÊNCIA E A TÉCNICA DE AVALIAÇÃO DE DADOS NO COMBATE À DESINFORMAÇÃO NA POLÍCIA MILITAR DO AMAZONAS

WHEN THE UNIFORM FACES THE FEED: ANTIFRAGILITY, COUNTERINTELLIGENCE, AND THE DATA EVALUATION TECHNIQUE IN COMBATING DISINFORMATION IN THE AMAZONAS MILITARY POLICE

Flavio Carvalho Cavalcante¹
Agley Pereira Cavalcante²
Hélio dos Santos Júnior³
Linton Sá Botelho⁴
José Rodrigo Barbosa das Neves⁵

RESUMO: A credibilidade institucional é o ativo intangível mais valioso das organizações policiais democráticas. O presente artigo analisa o impacto da desinformação e das *fake news* no âmbito da Polícia Militar do Amazonas (PMAM), evidenciando como a propagação de narrativas falsas no ambiente digital compromete a legitimidade da corporação e a segurança das guarnições. A partir de uma revisão bibliográfica, demonstra-se a vulnerabilidade tática gerada pelo repasse imediato de informações não verificadas pela própria tropa, muitas vezes motivada pela urgência operacional. Como solução para essa assimetria informacional, propõe-se a aplicação rigorosa da Técnica de Avaliação de Dados (TAD) para a filtragem de informações em fontes abertas, aliada à modernização do Sistema de Inteligência através dos princípios da antifragilidade. Conclui-se que a transição de uma cultura organizacional reativa para uma postura antifrágil, amparada pela contrainteligência policial, permite que a instituição não apenas resista às crises midiáticas, mas transforme esses ataques em oportunidades de aprimoramento tático e fortalecimento de sua credibilidade perante a sociedade amazonense.

1

Palavras-chave: Contrainteligência Policial. Antifragilidade. Fake News. Polícia Militar do Amazonas. Técnica de Avaliação de Dados.

¹ Doutorando no Programa de Pós-graduação em Ciências do Ambiente e Sustentabilidade na Amazônia PPGCASA da Universidade Federal do Amazonas. Mestre em Segurança Pública, Cidadania e Direitos Humanos do Programa de Pós-Graduação em Segurança Pública-PPGSP da Universidade do Estado do Amazonas - UEA. Especialista em Gestão Estratégica em Segurança Pública. ORIENTADOR/AUTOR. Atualmente é Oficial da Polícia Militar do Estado do Amazonas com atuação em Inteligência e Investigação Criminal (MPAM).

² Cadete da Polícia Militar do Amazonas. Especialista em Política e Gestão em Segurança Pública pela Faculdade Única (2023). Bacharel em Farmácia pela Universidade Nilton Lins - UNL (2017). Bacharelando em Segurança Pública e do Cidadão pela Universidade do Estado do Amazonas - UEA.

³ Cadete da Polícia Militar do Amazonas. Especialista em Direito Penal e Processo Penal pela Faculdade Venda Nova do Imigrante - FAVENI - (2021). Bacharel em Direito pela Faculdade Brasileira de Vitória - MULTIVIX - (2020). Bacharelando em Segurança Pública e do Cidadão pela Universidade do Estado do Amazonas - UEA - (2025).

⁴ Cadete da Polícia Militar do Amazonas. Especialista em Segurança Pública pela Faculdade Focus (2024). Bacharel em Engenharia Civil pela Universidade do Estado do Amazonas - UEA (2018). Bacharelando em Segurança Pública e do Cidadão pela Universidade do Estado do Amazonas - UEA.

⁵ Cadete da Polícia Militar do Amazonas. Especialista em Segurança Pública e Atividade Policial pela Faculdade de Direito Padre Arnaldo Janssen (2018). Bacharel em Direito pelo Centro Universitário de Ensino Superior do Amazonas - CIESA (2014). Bacharelando em Segurança Pública e do Cidadão pela Universidade do Estado do Amazonas - UEA.

ABSTRACT: Institutional credibility is the most valuable intangible asset of democratic police organizations. This article analyzes the impact of disinformation and fake news within the Amazonas Military Police (PMAM), highlighting how the propagation of false narratives in the digital environment compromises the corporation's legitimacy and the safety of its police units. Based on a literature review, it demonstrates the tactical vulnerability generated by the immediate forwarding of unverified information by the troops themselves, often motivated by operational urgency. As a solution to this informational asymmetry, the rigorous application of the Data Evaluation Technique (TAD) is proposed for filtering information from open sources, combined with the modernization of the Intelligence System through the principles of antifragility. It concludes that the transition from a reactive organizational culture to an antifragile posture, supported by police counterintelligence, allows the institution not only to resist media crises but also to transform these attacks into opportunities for tactical improvement and the strengthening of its credibility before the society of Amazonas.

Keywords: Police Counterintelligence. Antifragility. Fake News. Amazonas Military Police. Data Evaluation Technique.

1. INTRODUÇÃO

Os órgãos de Segurança Pública exercem papel fundamental na manutenção da ordem democrática, operando em uma sociedade que se transforma de forma acelerada e que exige a modernização ininterrupta de suas instituições (LEHMANN, 2008). O cenário operacional contemporâneo da Polícia Militar do Amazonas (PMAM) não se restringe mais ao patrulhamento físico das complexas áreas urbanas e vastas calhas fluviais do Estado; ele expandiu-se de forma irreversível para o ambiente cibernético e para as mídias sociais. É nesse espaço que a farda enfrenta o "feed", termo que designa o fluxo contínuo, dinâmico e algorítmico de publicações, notícias e vídeos que os usuários consomem ininterruptamente nas telas de seus dispositivos móveis. Nessas redes digitais, caracterizadas por um volume massivo de dados, verdades e mentiras se sobrepõem de forma volátil, criando um novo e desafiador teatro de operações (PINHEIRO; BRITO, 2014).

Neste ecossistema digital, a credibilidade institucional consagra-se como o ativo intangível mais crítico das organizações policiais (CEPIK, 2001), sendo determinante tanto para a sua legitimidade perante a sociedade amazonense quanto para a efetividade tática das guarnições nas ruas. Contudo, forças de segurança enfrentam atualmente ataques sistemáticos a esse patrimônio por meio da desinformação e de *fake News*, publicações maliciosas que assumem a aparência de produtos jornalísticos e relatos verídicos para manipular a percepção coletiva (TRASEL, 2018; MENDES; DONEDA; BACHUR, 2018). Estabelece-se, portanto, uma severa assimetria comunicacional: a velocidade de propagação de narrativas falsas excede vertiginosamente o alcance das notas de esclarecimento oficiais, gerando uma vulnerabilidade

que contamina não apenas a opinião pública, mas o próprio efetivo policial imerso no fluxo constante de aplicativos de mensagens (INSTITUTO IGARAPÉ, 2023).

Diante dessa conjuntura, a atividade de Inteligência de Segurança Pública torna-se a primeira linha de defesa. Para que o processo decisório do comando não seja induzido a erros operacionais baseados em boatos, é imperativo o emprego da Técnica de Avaliação de Dados (TAD) para filtrar rigorosamente as informações (BRASIL, 2019). Aliada a essa ferramenta tática, a corporação necessita de uma postura estratégica de contrainteligência embasada no conceito de "antifragilidade" (TALEB, 2012), abandonando o mero reacionismo para prosperar e se fortalecer diante do caos informacional.

Cunhada para descrever sistemas que superam a mera resiliência, a antifragilidade é uma propriedade organizacional que caracteriza instituições capazes não apenas de resistir a choques e crises, mas de aprender, prosperar e se fortalecer a partir da desordem. Adotar essa postura significa abandonar o reacionismo para utilizar os ataques informacionais como força motriz de evolução institucional.

Com base nessa premissa, o presente artigo tem como objetivo geral analisar e demonstrar de que forma a contrainteligência policial, fundamentada nos princípios da antifragilidade e associada metodologicamente à Técnica de Avaliação de Dados (TAD), atua como instrumento estratégico indispensável para a defesa institucional e a preservação da credibilidade da PMAM frente aos ataques de desinformação. Para dar cabo a essa diretriz, o estudo traça objetivos específicos que visam diagnosticar a vulnerabilidade tática gerada pelo repasse de informações falsas pela própria tropa, descrever a aplicação prática da TAD como filtro metodológico e propor estratégias de liderança que permitam transformar crises cibernéticas em oportunidades reais de fortalecimento organizacional.

Para o alcance dos objetivos propostos, a pesquisa estrutura-se metodologicamente como um estudo de revisão bibliográfica e documental, de natureza exploratória e abordagem qualitativa. O referencial teórico foi construído mediante o levantamento sistemático de artigos científicos, legislações, literaturas consagradas em segurança pública e manuais doutrinários (como o Manual Técnico de Produção do Conhecimento de Inteligência). A fundamentação ancorou-se em autores seminais da área de inteligência governamental e gestão da informação, a exemplo de Marco Cepik, Celso Moreira Ferro Júnior e Priscila Brandão, intrinsecamente articulados à teoria da antifragilidade de Nassim Taleb. Adicionalmente, a pesquisa valeu-se da análise secundária de dados empíricos sobre o comportamento informacional de agentes de

segurança, permitindo a triangulação entre a teoria acadêmica e a realidade logística e operacional da segurança pública.

Para propiciar uma compreensão lógica e processual da temática, o presente estudo constrói sua argumentação a partir do diagnóstico inicial da ameaça cibernética contemporânea, evidenciando como a assimetria digital e a própria urgência operacional podem transformar os agentes de segurança em vetores involuntários de desinformação no "feed" das redes sociais. Compreendida essa vulnerabilidade primária, a análise avança para a demonstração das ferramentas táticas de mitigação, com destaque para a aplicação da Técnica de Avaliação de Dados (TAD) e dos métodos de *fact-checking*, recursos de inteligência vitais para a depuração do dado bruto e para a garantia do emprego seguro da tropa no terreno.

Em seguida, a pesquisa eleva a discussão ao nível gerencial ao examinar as limitações estruturais crônicas das corporações policiais para, então, apresentar a Contrainteligência, em suas vertentes Orgânica e Ativa, como o mecanismo definitivo de superação. Esse raciocínio culmina na aplicação prática do modelo antifrágil, detalhando de que maneira a opcionalidade estratégica e a aprendizagem adaptativa são capazes de forjar uma instituição superior diante de sucessivas crises midiáticas. O percurso analítico encerra-se com a consolidação dos achados, reafirmando a gestão estratégica da informação não apenas como uma ferramenta técnica, mas como um requisito inarredável para o exercício da liderança e a efetiva preservação da ordem pública democrática.

2. OBJETIVOS

2.1 Objetivo Geral

O objetivo geral deste artigo é analisar e demonstrar de que forma a contrainteligência policial, fundamentada nos princípios da antifragilidade e associada à Técnica de Avaliação de Dados (TAD), atua como instrumento estratégico indispensável para a defesa institucional e a preservação da credibilidade da Polícia Militar do Amazonas (PMAM) frente aos ataques sistemáticos de desinformação.

2.2 Objetivos Específicos

Para alcançar o objetivo geral, a pesquisa desenvolve-se a partir de três eixos fundamentais, que balizam o corpo deste estudo:

- Diagnosticar a vulnerabilidade gerada pelo consumo e repasse imediato de desinformação (*fake news*) por parte do próprio efetivo policial nas redes sociais, evidenciando os impactos dessa prática na segurança tática das guarnições e na credibilidade da corporação.
- Descrever a aplicação prática da Técnica de Avaliação de Dados (TAD) como filtro metodológico essencial na atividade de inteligência policial, demonstrando como o julgamento rigoroso de fontes e conteúdos baliza a tomada de decisão do comando.
- Propor a adoção de estratégias de contrainteligência fundamentadas no conceito de antifragilidade, visando superar a cultura organizacional reativa e capacitar a PMAM a transformar crises reputacionais e cibernéticas em oportunidades de fortalecimento institucional.

3. METODOLOGIA

A presente pesquisa classifica-se metodologicamente como um estudo de revisão bibliográfica e documental, de natureza exploratória e com abordagem qualitativa. Para a construção do referencial teórico-conceitual, realizou-se um levantamento sistemático e criterioso em literaturas acadêmicas nacionais e internacionais, abordando os eixos temáticos centrais de inteligência de segurança pública, contrainteligência, desinformação e antifragilidade.

A coleta de dados abrangeu a análise pormenorizada de artigos científicos, legislações pertinentes, obras literárias consagradas na área de segurança e manuais doutrinários, com destaque para a aplicação da metodologia prevista no Manual Técnico de Produção do Conhecimento de Inteligência. O escopo teórico integrou contribuições de autores seminais na doutrina de inteligência governamental e gestão da informação policial, tais como Marco Cepik, Celso Moreira Ferro Júnior e Priscila Brandão, os quais foram intrinsecamente aliados à aplicação do conceito de antifragilidade desenvolvido por Nassim Taleb, adaptando-o ao contexto da defesa institucional.

Adicionalmente, a pesquisa valeu-se da análise de dados secundários oriundos de levantamentos quantitativos prévios consolidados na literatura acadêmica da área. Destacam-se, nesse escopo, a pesquisa empírica conduzida por Brocanelle e Oliveira (2020) — baseada na aplicação de questionários fechados junto a agentes de inteligência policial militar —, bem como os relatórios estatísticos sobre desinformação e percepção de segurança elaborados pelo Instituto

Igarapé (2023) e pelo Instituto de Referência em Economia e Estatística (IREE, 2025). Embora tais fontes apresentem natureza quantitativa, seus dados foram apropriados e tratados neste estudo sob uma ótica estritamente qualitativa. Os índices percentuais levantados por esses autores não foram empregados para projeções matemáticas, mas interpretados analiticamente para compreender o comportamento cultural da tropa frente ao uso das mídias sociais, diagnosticar a vulnerabilidade no repasse imediato de mensagens e fundamentar a urgência da aplicação de metodologias de checagem de fatos (*fact-checking*) no cotidiano operacional.

A partir do cruzamento dessa base teórica robusta com os dados empíricos de comportamento policial, realizou-se uma triangulação de dados. Esse método analítico permitiu transpor os diagnósticos acadêmicos puramente teóricos para a realidade logística e operacional peculiar da segurança pública, visando fundamentar estratégias gerenciais e doutrinárias robustas, essenciais para o exercício da liderança e da tomada de decisão no teatro de operações contemporâneo.

4. DISCUSSÕES DOS RESULTADOS

4.1 A Ameaça da Desinformação e a Vulnerabilidade no "Feed"

O avanço tecnológico e a ubiquidade dos smartphones transformaram radicalmente o 6
fluxo informacional na sociedade contemporânea, impondo às forças de segurança um desafio que transcende o policiamento ostensivo tradicional. A desinformação direcionada contra as instituições policiais manifesta-se por meio de uma anatomia estruturada, utilizando-se de três vetores primários: a amplificação desproporcional de incidentes isolados, a descontextualização de dados estatísticos e a criação de narrativas falsas que exploram preconceitos sociais latentes (RUEDIEGER, 2019). Na realidade da Polícia Militar do Amazonas (PMAM), cujas dimensões continentais e localidades ribeirinhas impõem desafios logísticos ímpares, esse fenômeno ganha contornos do que a literatura define como "guerrilha reputacional", caracterizada por ataques rápidos que exploram pontos fracos específicos e se retraem antes que a resposta institucional chegue às comunidades isoladas ou à capital (SILVA, 2009).

Nesse cenário de conflito informacional, o ambiente digital atua com uma assimetria temporal devastadora contra o policiamento. Estudos demonstram que a velocidade de propagação de informações falsas na internet excede em até seis vezes a velocidade de alcance das correções factuais emitidas pelos órgãos oficiais (INSTITUTO IGARAPÉ, 2023). Durante ocorrências de grande repercussão, é comum que recortes de vídeos descontextualizados gerem

milhões de visualizações em poucas horas, ao passo que o esclarecimento oficial da corporação atinge um público irrisório no mesmo período (SILVA JUNIOR, 2024). Essa disparidade favorece sistematicamente as narrativas criminosas, evidenciando que a confiança pública nas polícias não deriva exclusivamente de sua eficiência objetiva nas ruas, mas, de maneira crítica, da percepção social que é manipulada no ciberespaço (OLIVEIRA JUNIOR, 2011).

A ameaça da desinformação, contudo, não se restringe aos ataques externos, encontrando também um terreno fértil de propagação no interior das próprias guarnições e seções administrativas. O uso sistemático das redes sociais pelos agentes de segurança possibilita uma comunicação rápida e o compartilhamento dinâmico de informações de serviço (HAMADA, 2011). Todavia, imersos nesse "feed" ininterrupto, os policiais deparam-se com uma vulnerabilidade severa: frequentemente, informações inverídicas chegam até os militares por meio de fontes que eles consideram idôneas, como grupos institucionais ou colegas de farda (BROCANELLE; OLIVEIRA, 2020). Isso comprova que a manipulação orquestrada por atores maliciosos eleva a vulnerabilidade não apenas da sociedade, mas dos próprios indivíduos que compõem a instituição policial (DELMAZO; VALENTE, 2018).

O comportamento do policial frente a esse conteúdo agrava exponencialmente o risco tático. Movidos pelo senso de urgência inerente à profissão e pela busca da oportunidade operacional, muitos militares repassam informações imediatamente aos seus pares ou superiores sem realizar a devida checagem (BROCANELLE; OLIVEIRA, 2020). Tal prática reflete a dificuldade rotineira de processar o grande volume de dados de fontes abertas para extrair o que é legitimamente relevante para a Inteligência (GONÇALVES, 2018). Ao compartilhar material sem avaliação, baseando-se na premissa equivocada de que a informação já fora verificada por quem a enviou, o próprio policial torna-se um vetor de desinformação, alimentando engrenagens de reprodução de conteúdo cujo escopo é influenciar vontades coletivas e gerar desordem (MENDES; DONEDA; BACHUR, 2018).

Por fim, a contaminação informacional no meio policial possui ramificações que atingem o moral da tropa e a própria segurança pública do Amazonas. A literatura aponta que a erosão da credibilidade gera um ciclo vicioso: a diminuição da confiança diminui a cooperação do cidadão comum, essencial para o fornecimento de denúncias, o que reduz a efetividade policial nas ruas e, conseqüentemente, justifica a desconfiança inicial da sociedade (SILVA, 2009). Pesquisas reforçam o efeito multiplicador dessa erosão, demonstrando que pequenas quedas na confiança policial resultam em aumentos expressivos na sensação de insegurança (IREE, 2025). Evidencia-se, portanto, a necessidade de preparar o efetivo para neutralizar a

amplificação midiática e o viés de confirmação (OLIVEIRA JUNIOR, 2011), exigindo metodologias formais de filtragem de dados para balizar a atuação da tropa.

4.2 A INTELIGÊNCIA POLICIAL E A TÉCNICA DE AVALIAÇÃO DE DADOS (TAD)

A transição do dado bruto para o conhecimento de inteligência é um dos pilares para o sucesso e a segurança das operações da Polícia Militar do Amazonas (PMAM). Em um cenário onde guarnições de recobrimento e unidades de patrulhamento tático operam sob alta tensão, a informação não lapidada oriunda de mídias sociais pode induzir a falhas críticas.

Para a ciência da informação, a inteligência constitui uma camada analítica que converte dados fragmentados na base em conhecimentos reflexivos no vértice, essenciais para o tomador de decisões (CEPIK, 2003). Logo, a atividade de inteligência policial necessita processar essa matéria bruta, lidando com incertezas e intenções ocultas, para entregar um produto preciso e confiável que embase o emprego seguro da tropa (KRAEMER, 2015; GONÇALVES, 2018).

Para mitigar os riscos inerentes à desinformação disseminada no ciberespaço, a Doutrina Nacional de Inteligência de Segurança Pública (DNISP) estabelece, como diretriz basilar, o uso rigoroso da Técnica de Avaliação de Dados (TAD). Como documento guarda-chuva da atividade no Brasil, a DNISP determina que o serviço de inteligência empregue essa metodologia para atribuir credibilidade a qualquer reprodução de acontecimentos captada por documentos, fotografias, vídeos ou relatos antes de integrá-la à produção do conhecimento (BRASIL, 2016).

No âmbito prático e metodológico, as corporações militares aprofundam e padronizam a aplicação desse conceito valendo-se dos parâmetros técnicos estabelecidos em legislações complementares, como o Manual Técnico de Produção do Conhecimento de Inteligência do Exército Brasileiro (BRASIL, 2019). O uso contínuo dessa técnica combinada pelo oficialato e pelas seções de inteligência atua como um escudo profilático, impedindo que o fluxo ininterrupto e muitas vezes caótico de mensagens de aplicativos dite o ritmo das ações de segurança pública de forma precipitada e desestruturada (BROCANELLE; OLIVEIRA, 2020).

A operacionalização da TAD, em estrita obediência à hierarquia doutrinária, exige que o analista de inteligência realize um julgamento sistemático dividido em duas vertentes complementares: a fonte e o conteúdo (BRASIL, 2016; BRASIL, 2019). O julgamento da fonte busca estabelecer o seu grau de idoneidade, avaliando critérios de autenticidade, confiança e competência do emissor original ou do canal de transmissão intermediário, exigindo cautela extra quando o dado chega por terceiros. Simultaneamente, o julgamento do conteúdo visa

determinar a sua veracidade, confrontando a informação com parâmetros de semelhança, coerência e compatibilidade com fatos já conhecidos pela corporação. O cruzamento dessas duas matrizes fornece uma classificação padronizada que baliza o nível de confiança operacional daquele dado (BRASIL, 2019; BROCANELLE; OLIVEIRA, 2020).

Simultaneamente, o julgamento do conteúdo visa determinar a sua veracidade, confrontando a informação com parâmetros de semelhança, coerência e compatibilidade com fatos já conhecidos pela corporação. O cruzamento dessas duas matrizes fornece uma classificação padronizada que baliza o nível de confiança operacional daquele dado (BRASIL, 2019; BROCANELLE; OLIVEIRA, 2020).

No entanto, a complexidade da "guerrilha informacional" contemporânea exige que a TAD tradicional seja aliada a técnicas modernas de verificação, especialmente no manuseio de fontes abertas. O maior obstáculo do analista ao lidar com o ambiente cibernético é justamente filtrar o volume massivo de dados para extrair o que é verdadeiramente relevante para a missão (GONÇALVES, 2018).

Nesse contexto, incorpora-se a prática do *fact-checking* (checagem de fatos), uma ferramenta indispensável para verificar a autenticidade de mídias audiovisuais e textos virais que circulam nas redes, garantindo que a corporação não seja manipulada por campanhas difamatórias ou evidências forjadas (TRASEL, 2018).

9

A consolidação dessas práticas analíticas reflete diretamente na liderança e na gestão do policiamento diário. O comandante que compreende a diferença entre o imediatismo das redes sociais e a precisão do conhecimento de inteligência protege seu efetivo de exposições desnecessárias, desgastes físicos e emboscadas (FERREIRA, 2018). A busca constante por elementos e fatos analisados criteriosamente é o que garante um assessoramento de qualidade aos escalões superiores, adaptando as estratégias às novas demandas da sociedade da informação (LEHMANN, 2008).

Dessa forma, a aplicação metódica da TAD deixa de ser apenas uma rotina burocrática de gabinete e consagra-se como uma manobra tática essencial para a preservação da ordem pública e da integridade das operações no vasto território amazonense (BROCANELLE; OLIVEIRA, 2020).

4.3 Contrainteligência e a Superação de Limitações Institucionais

O enfrentamento da desinformação no cenário da segurança pública contemporânea esbarra, frequentemente, em limitações estruturais crônicas das corporações. A análise empírica

do comportamento das instituições policiais frente a ataques reputacionais e operacionais revela que as respostas tendem a se concentrar em dois extremos ineficientes: a "paralisia institucional" ou a "ação precipitada".

No primeiro caso, observa-se a negação do problema e uma burocracia excessiva que atrasa o esclarecimento dos fatos; no segundo, as corporações emitem comunicados contraditórios ou respostas emocionais (FERRO JÚNIOR, 2020). Essa matriz de falhas decorre da defasagem tecnológica das instituições em relação à velocidade das mídias digitais, o que compromete não apenas a resposta da assessoria de comunicação, mas a própria segurança das tropas no terreno, criando uma assimetria fundamental que favorece agressores sistêmicos (CEPIK, 2001; INSTITUTO IGARAPÉ, 2023).

A superação dessas vulnerabilidades e a defesa intransigente da credibilidade da Polícia Militar do Amazonas (PMAM) encontram respaldo direto e obrigatório na Doutrina Nacional de Inteligência de Segurança Pública (DNISP). No que tange às suas finalidades, a DNISP preconiza que a atividade de inteligência deve atuar na antecipação de cenários e na neutralização de ameaças ou ações adversas, o que, no ecossistema cibernético, traduz-se no combate proativo a campanhas de desinformação. Ademais, ancorando-se em Valores fundamentais como a busca pela verdade real, a ética e a legalidade (BRASIL, 2016), a doutrina exige que a instituição não admita que narrativas falsas manipulem a ordem pública. A proteção da imagem policial deixa de ser, portanto, uma mera questão de marketing institucional e consolida-se como uma missão doutrinária de inteligência.

10

A raiz dessa ineficiência reside em cinco vulnerabilidades organizacionais profundas que afligem as polícias militares. A primeira é a centralização decisória, que cria gargalos incompatíveis com a velocidade das redes sociais; enquanto um boato se espalha em horas, a cadeia hierárquica consome dias para autorizar uma resposta. A segunda é a compartimentalização funcional, caracterizada pela separação artificial entre os setores de Inteligência, Operações e Comunicação Social, impedindo uma reação sinérgica. A terceira e a quarta referem-se, respectivamente, ao déficit de capacitação, currículos de formação que negligenciam a gestão de crises informacionais, e à inadequação tecnológica para monitoramento de fontes abertas. Por fim, a cultura organizacional reativa, que historicamente valoriza o enfrentamento do incidente já consumado em detrimento da neutralização prévia da ameaça (CEPIK, 2001; BRANDÃO, 2013; FERRO JÚNIOR, 2020).

Para blindar a corporação e garantir a efetividade, sobretudo das unidades de recobrimento e patrulhamento tático que atuam na linha de frente e são os alvos primários de

narrativas descontextualizadas, a Contrainteligência Policial desponta como a ferramenta gerencial por excelência.

A contrainteligência atua na salvaguarda da instituição valendo-se de duas frentes: a Segurança Orgânica (SEGOR) e a Segurança Ativa (SEGAT). A SEGOR possui caráter eminentemente defensivo, buscando criar barreiras, protocolos e normas para impedir que agentes adversos ou a própria desatenção da tropa exponham dados sensíveis. Já a SEGAT possui natureza proativa (ofensiva), atuando na detecção, identificação e neutralização contínua das campanhas de difamação ou vazamentos, antes que estas alcancem massa crítica e afetem o andamento do serviço ostensivo (GONÇALVES, 2018; BRASIL, 2019).

A operacionalização dessas medidas exige que os comandantes adotem posturas complexas na gestão da informação, como a "Estratégia *Barbell*" (ou estratégia em haltere), oriunda dos conceitos de antifragilidade.

No contexto da inteligência policial, essa abordagem materializa de forma precisa o princípio doutrinário da "Economia de Meios", previsto na DNISP, que preconiza o emprego estritamente racional, seguro e eficiente dos recursos disponíveis para o alcance do objetivo.

Conforme a DNISP:

Economia de meios: característica da IPEN proporcionada pela produção de conhecimentos objetivos, precisos e oportunos. O conhecimento objetivo, preciso e oportuno possibilita otimizar os meios, a proporcionar a economia de pessoal e material (BRASIL, 2016, item 1.3.6).

11

Aplicada à contrainteligência na Polícia Militar do Amazonas (PMAM), a economia de meios traduz-se em alocar a esmagadora maioria dos esforços operacionais (80% a 90%) na proteção rigorosa e ortodoxa de informações táticas, planos de operações e identidades do efetivo. No entanto, otimizando os recursos institucionais, o lado especulativo da estratégia (10% a 20%) deve ser dedicado à inovação agressiva na comunicação pública, testando novas formas de engajamento social rápido e transparente, combatendo as *fake news* no mesmo terreno dinâmico em que elas nascem (TALEB, 2012; FEITOZA, 2012; BRASIL, 2016).

Em suma, a superação das vulnerabilidades institucionais requer uma quebra de paradigmas na liderança. A transição da execução tática ininterrupta para o comando estratégico exige que o futuro oficial enxergue a proteção da imagem da corporação com a mesma prioridade dedicada ao treinamento bélico. Organizações policiais que operam sob essa nova ótica abandonam o quadrante da paralisia reativa e estabelecem uma rede descentralizada, capaz de aplicar a Técnica de Avaliação de Dados de forma fluida (BROCANELLE; OLIVEIRA, 2020).

Ao integrar a inteligência cibernética à doutrina de patrulha e comunicação, a PMAM pavimenta o caminho não apenas para sobreviver aos ataques difamatórios, mas para transformar essas adversidades em mecanismos contínuos de aperfeiçoamento institucional (FERRO JÚNIOR, 2020; SILVA JUNIOR, 2024).

4.4 Construindo uma Polícia Militar Antifrágil

A compreensão da antifragilidade organizacional fundamenta-se em uma taxonomia tripartite que distingue os sistemas entre frágeis, robustos e antifrágeis (TALEB, 2012). Enquanto o sistema frágil quebra sob pressão e o sistema resiliente (ou robusto) apenas resiste aos choques para permanecer o mesmo, o sistema antifrágil melhora, prospera e cresce quando exposto à volatilidade, à aleatoriedade e aos estressores do ambiente (TALEB, 2012).

Para a Polícia Militar do Amazonas (PMAM), adotar uma postura meramente defensiva ou resiliente significa manter a corporação vulnerável a ataques sistemáticos e coordenados nas redes sociais, pois foca-se exclusivamente na recuperação pós-crise (DIAS; SANTOS, 2025). Em contrapartida, a antifragilidade implica em uma assimetria favorável, na qual a instituição tem mais a ganhar do que a perder com as adversidades (TALEB, 2012).

A aplicação desses princípios inovadores à contrainteligência desenvolve-se através de conceitos como a "via negativa", que consiste na identificação sistemática de vulnerabilidades reputacionais e na eliminação de processos falhos que amplificam os danos à credibilidade policial, neutralizando os riscos antes mesmo que sejam explorados pelo crime organizado (TALEB, 2012; CEPIK, 2001).

Complementarmente, a "hormese institucional" sugere que a exposição controlada a pequenos estressores fortalece o sistema corporativo (TALEB, 2012). Na rotina de comando, isso se traduz na aplicação de exercícios regulares de gestão de crises reputacionais e na simulação de ataques à imagem da tropa, transformando a exposição controlada ao escrutínio público em uma oportunidade prática de melhoria tática e comportamental (BRANDÃO, 2013).

Para que essa engrenagem funcione na complexa geografia amazonense, o Sistema de Inteligência deve atuar como uma plataforma antifrágil, estruturada em uma rede descentralizada com nós autônomos, porém fortemente interconectados (DIAS; SANTOS, 2025). Essa arquitetura multinível, englobando as esferas estratégica, tática e operacional, permite uma resposta coordenada a ameaças institucionais e viabiliza redundâncias adaptativas essenciais para a sobrevivência do sistema (FERRO JÚNIOR, 2020).

Dessa forma, um boato ou um vídeo manipulado que atinja uma guarnição no interior do Estado pode ter uma resposta local ágil mediante a autonomia regional, mantendo simultaneamente a comunicação contínua com a coordenação central em Manaus para o balizamento de ações estratégicas (FEITOZA, 2012; DIAS; SANTOS, 2025).

A operacionalização final dessa doutrina materializa-se por mecanismos práticos que convertem ataques digitais em fortalecimento, destacando-se a aprendizagem adaptativa e a opcionalidade estratégica (DIAS; SANTOS, 2025). A opcionalidade permite que a corporação mantenha múltiplas linhas de ação disponíveis frente a uma crise, beneficiando-se de resultados positivos enquanto limita a exposição a narrativas prejudiciais (TALEB, 2012; FEITOZA, 2012).

Sob essa ótica, cada crise enfrentada no "feed" passa a representar uma oportunidade valiosa de aprendizagem organizacional, permitindo que a inteligência da corporação capture, analise e integre lições que refinam o policiamento, transformando a adversidade cibernética em um acervo de conhecimento institucional (FERRO JÚNIOR, 2020).

5. CONCLUSÃO

A complexidade do cenário criminal contemporâneo exige que a farda transcenda o confronto físico, enfrentando de forma incisiva as ameaças propagadas no ambiente digital. A transição da execução tática ininterrupta para o exercício do comando e do oficialato demanda do policial militar uma visão sistêmica inabalável: a gestão de unidades não se restringe à manobra de tropas e à logística, mas engloba obrigatoriamente a gestão cirúrgica do fluxo de informações.

A contrainteligência policial revela-se, assim, como um instrumento estratégico indispensável para a preservação estrutural da legitimidade democrática e da credibilidade da corporação. A aplicação implacável da Técnica de Avaliação de Dados (TAD) evita a perigosa propagação de desinformação interna e assegura que o emprego do policiamento seja lastreado em conhecimento verificado, e jamais em ruídos gerados por redes sociais (BROCANELLE; OLIVEIRA, 2020).

Essa evolução institucional encontra seu alicerce normativo irrevogável nas diretrizes da Doutrina Nacional de Inteligência de Segurança Pública (DNISP). A transição de uma cultura reativa para uma Polícia Militar do Amazonas (PMAM) verdadeiramente antifrágil materializa-se, na prática, pela aplicação rigorosa do princípio da economia de meios. Ao otimizar recursos operacionais escassos por meio da Estratégia *Barbell*, garantindo a proteção maciça de dados sensíveis (Segurança Orgânica) e empregando frações cirúrgicas de esforço na

inovação comunicacional (Segurança Ativa), a corporação atinge máxima eficiência defensiva. Ademais, ao balizar suas ações nas finalidades de antecipação de cenários e na salvaguarda de valores éticos focados na busca pela verdade real (BRASIL, 2016), a agência de inteligência transcende a mera autopreservação de imagem, cumprindo sua missão de Estado.

Portanto, a integração da inteligência cibernética à doutrina ostensiva constitui o alicerce absoluto de uma força de segurança moderna. Ao incorporar permanentemente os princípios da antifrágilidade e os ditames da DNISP, a Polícia Militar do Amazonas superará a limitação de apenas resistir a campanhas difamatórias. A corporação consolida-se, assim, como uma instituição superior, capaz de otimizar seus meios, emergir fortalecida de cada confronto informacional e honrar o seu compromisso inarredável com a sociedade amazonense.

REFERÊNCIAS

BRANDÃO, Priscila Carlos; CEPIK, Marco Aurélio Chaves (Org.). **Inteligência de Segurança Pública: teoria e prática no controle da criminalidade**. Rio de Janeiro: Impetus, 2013.

BRASIL. Ministério da Justiça e Cidadania. Secretaria Nacional de Segurança Pública. **Doutrina Nacional de Inteligência de Segurança Pública**. 3. ed. rev. e atual. Brasília, DF: SENASP, 2016.

BRASIL. Ministério da Defesa. Exército Brasileiro. Comando de Operações Terrestres. **Manual Técnico: Produção do Conhecimento de Inteligência**. 1. ed. Brasília, DF: COTER, 2019.

BROCANELLE, David Lopes; OLIVEIRA, Paulo Tiego Gomes de. Inteligência de Segurança Pública, Desinformação e Fake News: como identificar esse problema? **O Alferes**, Belo Horizonte, v. 76, n. 30, p. 110-142, jan./jun. 2020.

CEPIK, Marco Aurélio Chaves. **Espionagem e Democracia: agilidade e transparência como dilemas na institucionalização de serviços de inteligência**. Rio de Janeiro: Editora FGV, 2001.

DAMBROS, Rafael Mendes. Quando a farda enfrenta o feed: a imagem da PMPR sob o impacto das redes sociais e da desinformação. **Revista Científica RECIMA21**, v. 6, n. 6, e666561, 2025.

DELMAZO, Caroline; VALENTE, Jonas C. L. Fake news nas redes sociais online: propagação e reações à desinformação em busca de cliques. **Media & Jornalismo**, Lisboa, v. 18, n. 32, p. 155-169, abr. 2018.

DIAS, Alexandre Lopes; SANTOS, Lucas Correa dos. A Antifrágilidade Institucional e Contrainteligência Policial: Estratégias de defesa da credibilidade da PMPR. **Revista Científica RECIMA21**, v. 6, n. 10, e6106904, 2025.

FEITOZA, Denilson. **Inteligência, Segurança e Direito: políticas e operações de inteligência**. Belo Horizonte: Del Rey, 2012.

FERREIRA, Gustavo de Castro. **Inteligência na Polícia Militar de Minas Gerais: Desvio de Conduta como objeto da Inteligência de Segurança Pública**. Belo Horizonte: Editora Vorto, 2018.

FERRO JÚNIOR, Celso Moreira. **A Inteligência e a Gestão da Informação Policial**. Brasília, DF: Fortium, 2008.

FERRO JÚNIOR, Celso Moreira. **Inteligência Organizacional e Competitiva no Contexto da Segurança Pública**. Brasília, DF: Fortium, 2020.

GONÇALVES, Joanisval Brito. **Atividade de inteligência e legislação correlata**. 6. ed. Niterói: Impetus, 2018.

HAMADA, Hélio Hiroshi. Utilização das Redes Sociais na produção de conhecimento de inteligência de Segurança Pública. **O Alferes**, Belo Horizonte, v. 66, n. 25, p. 11-46, jul./dez. 2011.

INSTITUTO DE REFERÊNCIA EM ECONOMIA E ESTATÍSTICA (IREE). **Pesquisa Nacional sobre Percepção de Segurança Pública 2025**. São Paulo: IREE, 2025.

INSTITUTO IGARAPÉ. **Desinformação e Segurança Pública**: relatório sobre ataques digitais às forças de segurança. Rio de Janeiro: Instituto Igarapé, 2023.

KRAEMER, Rodrigo. Incompreensão do conceito de inteligência na segurança pública. **Revista Brasileira de Inteligência**, Brasília, DF, n. 10, p. 65-75, dez. 2015.

LEHMANN, B. T. Os impactos da chamada sociedade do conhecimento nas ações de segurança pública. In: MIRANDA, Ana Paula Mendes de; LIMA, Lana Lage da Gama (Org.). **Políticas Públicas de Segurança, Informação e análise criminal**. Niterói: Ed. UFF, 2008.

15

MASCARENHAS, Janaina do Couto; OLIVEIRA, Gislene Lisboa de. Percepção social e desinformação: os efeitos das fake news nos serviços policiais e o papel da educação crítica. **Revista Sapiência: sociedade, saberes e práticas educacionais**, [S. l.], 2025.

MENDES, Laura Schertel; DONEDA, Danilo; BACHUR, Paulo João. Manipulação de informação, fake news e os novos desafios para a democracia. **Cadernos Adenauer XIX**, Rio de Janeiro, n. 4, p. 11-25, 2018.

OLIVEIRA JUNIOR, Almir de. Dá para confiar nas polícias? Confiança e percepção social da polícia no Brasil. **Revista Brasileira de Segurança Pública**, São Paulo, v. 5, n. 2, p. 6-22, ago./set. 2011.

PEREIRA, Mário Rui Gonçalves. **O impacto das Fake News na segurança e ordem pública**. 2022. Dissertação (Mestrado Integrado em Ciências Policiais) - Instituto Superior de Ciências Policiais e Segurança Interna, Lisboa, 2022.

PINHEIRO, Marta Macedo Kerr; BRITO, Vladimir de Paula. Em busca do significado da desinformação. **DataGramZero**, Rio de Janeiro, v. 15, n. 6, p. A05, dez. 2014.

RUEDIEGER, Marco Aurélio. **Desinformação e Confiança nas Instituições: O Papel das Fake News na Erosão da Credibilidade Pública**. Rio de Janeiro: FGV DAPP, 2019.

SILVA, Jorge da. **Controle da Criminalidade e Segurança Pública na Nova Ordem Constitucional**. 2. ed. Rio de Janeiro: Forense, 2009.

SILVA JUNIOR, José Mauricio Cavalcanti da. A Polícia Militar e a Sociedade Midiática: Desafios e Implicações. **Revista FT**, v. 27, n. 3, p. 223-245, 2024.

TALEB, Nassim Nicholas. **Antifragile**: Things That Gain from Disorder. New York: Random House, 2012.

TRASEL, Marcelo. A Eficácia da checagem de fatos no combate à desinformação. **Cadernos Adenauer XIX**, Rio de Janeiro, n. 4, p. 57-75, 2018.