OBSERVATÓRIO MILITAR da Praia Vermelha
http://ompv.eceme.eb.mil.br/

O Escudo Forense: visão computacional e autenticação de imagem como capacidade dual de defesa cognitiva

Rogério Rodrigues de Oliveira
Executivo e mentor em transformação digital, IA e dados.
Aluno da VIII Turma do Curso de Liderança Estratégica
da Escola de Comando e Estado-Maior do Exército.

1. Introdução

Durante séculos, uma imagem foi sinônimo de prova. Ver era crer. Essa equação ruiu. A inteligência artificial generativa tornou trivial fabricar fotos, vídeos e documentos indistinguíveis dos verdadeiros. O que era garantia de verdade virou vetor de vulnerabilidade. Na guerra cognitiva, quem controla o que parece verdadeiro controla a decisão.

O cenário aponta para Estados soterrados por mídias não verificáveis. Documentos forjados, provas adulteradas, vídeos sintéticos. Cada um corrói uma engrenagem diferente: a decisão de comando ou a confiança pública. O adversário sequer precisa vencer o argumento. Basta envenenar o ambiente probatório, semeando a dúvida sobre o que é real.

Essa é a face material da guerra cognitiva. Se a mente é o campo de batalha, a evidência é o terreno. Uma força que não consegue distinguir o autêntico do fabricado, com rapidez, perde a iniciativa antes do primeiro tiro. E a defesa por narrativa chega sempre tarde, correndo atrás de uma mentira que já circulou.

A dissimulação sempre existiu na guerra, e o ardil é tão antigo quanto o combate, entretanto, a escalabilidade desse fenômeno da produção fraudulenta de dados aumenta exponencialmente os danos. O que a inteligência artificial generativa introduziu não foi a mentira, mas a sua industrialização: qualquer pessoa com um *smartphone* produz e difunde uma falsificação que antes exigia um estúdio com muitos recursos. Quando o engano deixa de ser obra artesanal e se torna industrial, a defesa também precisa se industrializar.

Imagine uma fotografia adulterada acusando uma tropa de um ato que jamais cometeu, ou um vídeo sintético de um comandante emitindo uma ordem falsa, disparado nas primeiras horas de uma crise. O risco deixa de ser abstrato e o dano se consuma no intervalo entre a publicação e o desmentido. Reduzir esse tempo a quase zero é, hoje, um desafio para a Defesa.

O problema transborda o campo de batalha. A mesma falsificação que engana um comando pode contaminar um inquérito, incriminar um inocente ou inocentar um culpado. Em operações de garantia da lei e da ordem, uma imagem forjada de abuso pode incendiar uma cidade antes que qualquer apuração comece. Na defesa civil, um vídeo falso de rompimento de barragem pode disparar um pânico com vítimas reais. Autenticar mídia, portanto, não é um luxo técnico: é infraestrutura de confiança pública.

Portanto, o desafio deixou de ser produzir imagens e passou a ser autenticá-las, em escala e em velocidade, e aqui reside uma capacidade de Defesa que o Brasil ainda não constituiu de forma soberana, e proponho chamá-la de Escudo Forense. Este trabalho pretende contextualizar o ambiente de fabricação de fraudes em imagens e apontar caminhos para a sua solução pelo Estado, no contexto da defesa cognitiva.

2. Uma oportunidade para a Defesa

No setor de seguros, a visão computacional forense já é usada para flagrar fraudes: detectar fotos adulteradas, geometrias inconsistentes, metadados violados, cenas remontadas. No fundo, esse motor não caça a fraude — ele autentica a verdade de uma imagem.

O que esse motor examina é a coerência interna da imagem. Sombras que não batem com a fonte de luz. Bordas com marcas de recorte. Ruído de sensor ausente ou artificial. Metadados que contam uma história diferente da dos *pixels*. Nenhuma dessas pistas, isoladas, prova a fraude; juntas, formam um veredito probabilístico que um perito humano então referenda. É o mesmo método que, no seguro, separa o sinistro legítimo do encenado.

Vale, aqui, um princípio central: a tecnologia não deve definir o problema; é o problema que deve convocar a tecnologia. No Escudo Forense, o problema real é a verdade — a visão computacional é apenas o instrumento adequado para protegê-la.

Produzir uma falsificação convincente custa hoje centavos e minutos; verificá-la à mão custa horas de um profissional especialista de difícil formação. A assimetria é cruel. Enquanto a detecção depender de trabalho artesanal, o falsário vencerá pela quantidade. Só uma capacidade automatizada, soberana e em escala reequilibrará essa conta.

Não é coincidência que a linha de frente dessa tecnologia esteja no setor de seguro, e não no quartel. É ali que o incentivo para fraudar encontra, todos os dias, o incentivo para detectar. Cada apólice é um pequeno campo de provas onde o motor forense é testado, corrigido e endurecido contra adversários reais. Essa maturidade operacional, adquirida na prática, é precisamente o que costuma faltar a uma solução nascida apenas em laboratório.

Essa mesma tecnologia que protege o patrimônio privado pode proteger a decisão pública. E o talento que a desenvolve já existe, disperso na indústria, nas seguradoras, nas *fintechs.* Um ecossistema de Defesa inteligente não o ignora: o mobiliza.

É o uso dual em estado puro. Se a falsificação foi democratizada, a detecção precisa ser democratizada na mesma medida — e soberana. Depender de ferramentas estrangeiras para autenticar a nossa própria verdade é abrir mão de uma prerrogativa do Estado. Quem controla o veredito sobre o que é real controla um ponto de apoio decisivo do poder.

O Brasil tem, nesse ponto, uma vantagem pouco explorada. Seu setor financeiro e securitário está entre os mais sofisticados do mundo em análise de fraude, justamente porque a fraude aqui é abundante e criativa. Essa competência, forjada na necessidade privada, é um ativo estratégico latente. Um ecossistema de Defesa que a reconheça e a convoque converte um problema nacional em uma capacidade nacional, pois essa é a proposta do Escudo Forense.

3. Linhas de esforço para o ecossistema do Escudo Forense

Constituir esse ambiente exige quatro linhas de esforço do Estado brasileiro, envolvendo diversas políticas públicas integradas. A primeira é a capacidade soberana de perícia de imagem por inteligência artificial — modelos, dados e infraestrutura, de tecnologias nacionais, capazes de operar em escala e em tempo útil.

A segunda são os padrões de autenticação e cadeia de custódia. Toda imagem de interesse operacional ou judicial deveria carregar a sua procedência assinada, do sensor à decisão. A autenticidade deixa de ser presumida e passa a ser demonstrável. Vale detalhar essa linha, porque nela está a visão estratégica. Assinar a procedência na origem — vinculando a imagem ao dispositivo, ao instante e ao local de captura, por meio de credenciais de conteúdo — inverte o ônus da prova. Em vez de tentar demonstrar que algo é falso, passa-se a exigir a prova de que é verdadeiro. O que não traz procedência assinada torna-se, por padrão, suspeito. É a diferença entre correr atrás da mentira e blindar a verdade — e é a resposta durável à corrida sem fim entre falsificar e detectar.

A terceira é a integração com a comunicação estratégica. A autenticação técnica é a espinha dorsal da resiliência cognitiva. Ela habilita o *prebunking*, ou seja, inocular a verdade antes que a mentira se espalhe, em vez do desmentido tardio. Verificar de forma rápida é mais eficaz do que corrigir depois.

A quarta é o uso dual pela tríplice hélice. Estado, academia e o inesperado reservatório de talento forense do setor privado, todos articulados. É a lógica de *whole-of-society*[1]*:* a Defesa como empreendimento de toda a sociedade, e não apenas das Forças Armadas. A mesma capacidade serve à defesa civil, ao Judiciário e às operações de garantia da lei e da ordem, ampliando o retorno de cada real investido pela população.

[1] Traduzido livremente como "abordagem de toda a sociedade", o conceito designa a mobilização conjunta do governo, do setor privado e da sociedade civil organizada para enfrentar desafios complexos.

O caminho para essa proposta é incremental, e merece ser testado antes de qualquer ambição de produção em escala. Um projeto piloto atendendo a um fluxo real: a triagem de imagens que chegam a um centro de operações, por exemplo, medindo acurácia, tempo de veredito e taxa de falso alarme. A credibilidade do Escudo Forense depende de números honestos, não de promessas.

4. A liderança estratégica no centro do processo

Como toda ferramenta poderosa, o Escudo Forense só faz sentido a serviço do julgamento humano. Clausewitz (2017) descreveu a névoa e a fricção da guerra. A era sintética acrescentou uma névoa nova, fabricada de propósito. O líder estratégico precisa de instrumentos para dissipá-la — mas a decisão sobre o que fazer com a verdade autenticada continua sendo dele.

Kissinger (2023) mostra que a grande liderança governa a percepção e a realidade ao mesmo tempo. Num ambiente saturado de falsificações, defender a realidade compartilhada é função de comando. Zanini (2014) recorda que a confiança é o ativo mais frágil e mais valioso de uma organização. Uma força capaz de provar o que é real preserva a confiança interna e a confiança pública — o capital sobre o qual repousa toda autoridade legítima.

Aqui também vale nomear a virtude. Liderar estrategicamente, num ambiente saturado de falsificações, é recusar tanto a ingenuidade quanto a paranoia. Não crer em tudo; não duvidar de tudo. O Escudo oferece ao líder o terceiro caminho: um critério verificável para separar o real do fabricado, devolvendo à decisão a base factual que a guerra cognitiva tenta destruir. Sem esse alicerce, a melhor das lideranças decide no escuro.

Esse poder, porém, precisa ser ele próprio auditável. Autenticar imagens toca em dados sensíveis e em direitos individuais. O sistema deve operar sob controle, com transparência e respeito à legislação de proteção de dados. A capacidade de dizer o que é verdadeiro não pode se tornar a capacidade de decretar a verdade. A governança é parte do instrumento, não um apêndice.

5. Impactos na Defesa Nacional

A Política Nacional de Defesa e a Estratégia Nacional de Defesa (BRASIL, 2020) colocam a ciência e a tecnologia no coração do Poder Nacional. Autenticar a realidade é, hoje, uma dessas tecnologias críticas. Um país que não consegue distinguir o verdadeiro do falso, em escala, é vulnerável na dimensão informacional, onde as guerras contemporâneas começam.

A recomendação é constituir o Escudo Forense como capacidade nacional, aliando a necessidade militar com o talento civil já existente. Ao lado de uma inteligência artificial doutrinária, ele compõe o par que protege a dimensão cognitiva da Defesa: um amplia o discernimento de quem decide; o outro garante que a realidade sobre a qual se decide seja, de fato, real.

Rio de Janeiro - RJ, 02 de setembro de 2026.

Como citar este documento:

ESCOLA DE COMANDO E ESTADO-MAIOR DO EXÉRCITO (ECEME). OBSERVATÓRIO MILITAR DA PRAIA VERMELHA (OMPV). **O Escudo Forense: visão computacional e autenticação de imagem como capacidade dual de defesa cognitiva.** Rio de Janeiro, 2026.

Referências bibliográficas

BRASIL. Ministério da Defesa. **Política Nacional de Defesa e Estratégia Nacional de Defesa.** Brasília: Ministério da Defesa, 2020. Disponível em: www.gov.br/defesa. Acesso em: 22 ago. 2026.

CLAUSEWITZ, Carl von. **Da guerra**. São Paulo: WMF Martins Fontes, 2017.

KISSINGER, Henry. **Liderança:** seis estudos sobre estratégia. Rio de Janeiro: Objetiva, 2023.

ZANINI, Marco Tulio. **A ponta da lança:** o papel da confiança na gestão de equipes de alto desempenho. Rio de Janeiro: Elsevier, 2014.