INTELIGÊNCIA DE FONTES ABERTAS: QUANDO “OSINT” VIRA “OSHIT”

*Por Tristan Lee, Kolina Koltai e Giancarlo Fiorella**

Imagem gerada por IA.

Conduzir pesquisas em fontes abertas de forma adequada não significa ser “verificado” ou ter muitos seguidores em redes sociais, e nem tampouco de esperar que as pessoas acreditem na sua palavra.

Quando as notícias surgem e a Internet está repleta de atividades e especulações, muitos recorrem a especialistas e contas de fontes abertas para entender os acontecimentos. Este é realmente um sinal de que a pesquisa de fontes abertas – usando recursos como imagens de satélite, sites de rastreamento de voos e imagens gravadas no terreno – é vista como confiável e cada vez mais procurada. É gratuita, está disponível publicamente e qualquer pessoa pode fazê-lo.

Mas esse sucesso traz consigo desvantagens. Ao monitorar os acontecimentos no Irã e na Ucrânia, este aumento de credibilidade permite que o termo “OSINT” seja facilmente abusado, consciente ou inconscientemente, por usuários que não seguem realmente as melhores práticas em métodos de pesquisa em fontes abertas. Na verdade, desde o início da guerra em Gaza, em outubro de 2023, tem havido um aumento das contas “OSINT” verificadas no *Twitter*, o que cria ruído e confusão adicionais devido à fraca análise de fontes abertas.

Conduzir pesquisas em fontes abertas de forma adequada não significa ser “verificado” ou ter muitos seguidores. Não se trata de esperar que as pessoas acreditem na sua palavra. Trata-se de colaboração e compartilhamento das habilidades necessárias para verificar de forma independente o que você vê

online. Trata-se de mostrar o seu trabalho e a origem dos seus dados para que qualquer pessoa possa replicar a sua metodologia.

Como Giancarlo Fiorella, do Bellingcat, indicou no *Financial Times* em dezembro, a pesquisa em fontes abertas é crítica a longo prazo, quando poderá vir a desempenhar um papel na acusação de responsáveis por crimes e atrocidades. Isto levanta a barra significativamente – não apenas para o bem da comunidade de pesquisa em fontes abertas como um todo, mas também para o bem da responsabilização das vítimas de conflitos armados.

Aqui estão alguns erros que notamos em pesquisadores de fontes abertas nos últimos anos. Muitos exemplos são relevantes para a monitoração de conflitos armados, mas podem se aplicar amplamente a qualquer coisa em que a pesquisa em fontes abertas se destaque – como catástrofes naturais ou crime organizado.

Trabalhamos em um campo jovem e em rápida evolução, enfrentando um dilúvio de informações. Os erros não devem ser motivo de surpresa ou vergonha. Todo mundo os comete. Mas um bom pesquisador de fontes abertas está aberto a fazer isso –corrigir seus erros rapidamente e se comprometer a fazer melhor da próxima vez.

Se você é um leitor, procurar esses "Sete Pecados" (listados sem nenhuma ordem específica de gravidade) o ajudará a julgar de forma independente a qualidade da pesquisa de fontes abertas que você encontra *online*. Se você também é pesquisador de fontes abertas, levá-los em conta vai ajudar a melhorar a qualidade do seu próprio trabalho.

1. NÃO INFORMAR A FONTE ORIGINAL

O principal princípio da pesquisa em fontes abertas é que ela é "aberta": idealmente, a informação é acessível ao público e utilizada de forma transparente. Isso permite que qualquer pessoa verifique a origem e a veracidade de uma filmagem, sem ter que confiar na pessoa que a postou.

Na sequência da invasão em grande escala da Ucrânia pela Rússia em 2022, muitas contas de "agregadores OSINT" desenvolveram grandes números de seguidores no *Twitter*, na maioria repostando vídeos do *Telegram*, muitas vezes sem ligação à fonte original do vídeo. Quando alguém posta um vídeo sem dizer de onde o tirou, a verificação fica muito mais difícil; os pesquisadores não podem simplesmente seguir uma cadeia de links até sua origem.

Sem quaisquer pistas sobre quem originalmente carregou o vídeo, perdemos informações potencialmente cruciais sobre o conteúdo. Embora a maioria das plataformas de mídia social retire os metadados, algumas plataformas como *Telegram* e *Parler* os mantêm. Esses metadados de imagem desempenharam papéis importantes nas pesquisas do *Bellingcat* sobre assuntos desde as origens do QAnon até a desinformação russa sobre a Ucrânia. Isso significa que a primeira instância de uma foto ou vídeo também pode conter metadados que são perdidos quando o conteúdo é recarregado, compartilhado ou compactado.

Tenha em mente que há circunstâncias em que pode ser eticamente complicado fornecer um *link*, como quando isso amplifica contas de ódio ou direciona tráfego

para conteúdo gráfico. No entanto, uma regra prática é compartilhar quando puder.

Isso porque compartilhar a origem de um conteúdo é uma contribuição maior do que guardá-lo para si – para melhor acumular futuras "descobertas".

2. DEIXAR QUE A TORCIDA PREJUDIQUE SEU TRABALHO

Embora todos tenham preconceitos, é importante que os pesquisadores de fontes abertas tentem separar esses preconceitos das evidências que examinam. Embora muitos pesquisadores ou comunidades de fontes abertas utilizem claramente estas técnicas em prol de uma determinada causa, devem ainda assim reconhecer quando suas fontes ou pesquisa não apoiam essa causa e ser sempre transparentes sobre o nível de incerteza.

O viés de confirmação é nossa tendência de aceitar como verdadeira qualquer nova informação que confirme o que já "sabemos" ser verdade e de rejeitar novas informações que contradizem nossas crenças. Assim como todos têm preconceitos, todos estão sujeitos a ser vítimas de preconceitos de confirmação.

No entanto, a qualidade da pesquisa em fontes abertas pode ser avaliada independentemente da posição política ou social. É por isso que as advertências são tão importantes. As informações de fontes abertas não mostram tudo e podem não provar o ponto mais amplo que você gostaria.

Reconhecer o que você não sabe e o que não pode saber é crucial para construir confiança – mesmo que você tenha posições muito claras e públicas. Não fazer isso pode resultar em pesquisas errôneas e egoístas.

3. NÃO ARQUIVAR MATERIAL

O conteúdo *online* é muitas vezes efêmero: a Internet está repleta de *links* para páginas que já não existem. Isso pode ocorrer porque o proprietário do domínio da *web* parou de pagar suas contas. Pode ser porque o site mudou a forma como organizava as páginas. Uma plataforma de hospedagem de conteúdo poderia ter decidido excluir grandes quantidades de seus arquivos, seja propositalmente ou por acidente. As postagens nas redes sociais são frequentemente excluídas, seja pela conta que a criou ou pela equipe de moderação da plataforma de mídia social.

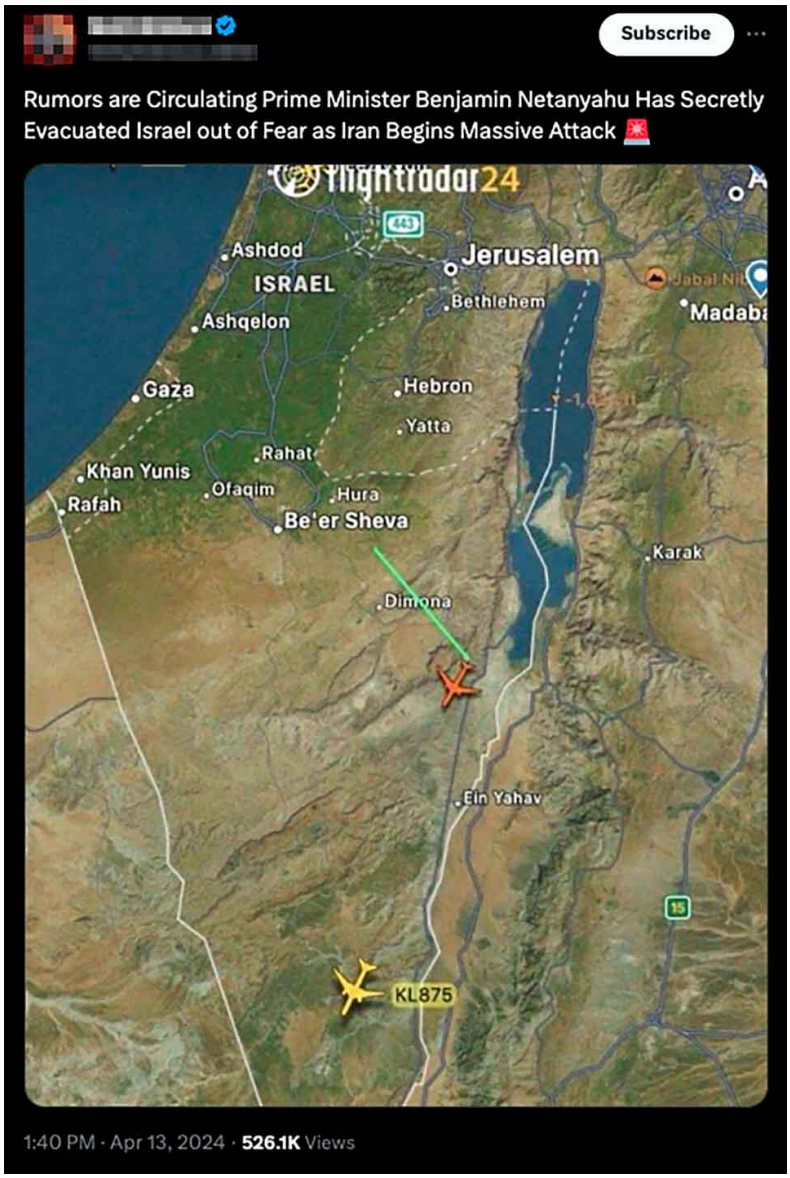
Isso torna o trabalho dos pesquisadores de fontes abertas muito mais difícil. É por isso que a *Bellingcat* enfatiza frequentemente a importância do arquivamento de conteúdo *online* e desenvolveu ferramentas para tornar isso mais fácil.

A maneira mais confiável de arquivar conteúdo é com plataformas de arquivamento de terceiros, como a *Wayback Machine* do *Internet Archive* ou *archive.today*, embora muitas vezes não consigam arquivar corretamente o conteúdo de várias plataformas de mídia social, bem como vídeos em geral. Se tudo o mais falhar, uma captura de tela é melhor do que nada.

4. FALTA DE CONTEXTO PARA OCORRÊNCIAS, COMUNS OU NÃO

Particularmente no contexto da monitoração de conflitos, os acontecimentos que ocorrem regularmente são muitas vezes retirados do contexto original e

exagerados. Por exemplo, pesquisadores não familiarizados com a leitura de imagens e dados do NASA FIRMS podem interpretar incêndios regulares, planejados e controlados ou outras mudanças térmicas como algo mais malicioso. Mas em momentos de tensão, pessoas não familiarizadas com acontecimentos comuns podem dar-lhes um significado indevido.



Captura de tela de uma postagem do Twitter/X alimentando um boato infundado sobre a localização do primeiro-ministro israelense Netanyahu antes do recente ataque com mísseis do Irã contra Israel, com base em dados de voo de um avião do governo. O nome de usuário original foi desfocado pela Bellingcat.

Um exemplo recente dessa tendência foi quando o famoso jogador de beisebol Shohei Ohtani foi para um novo time, deixando o Los Angeles Angels. Em dezembro de 2023, um voo privado saindo de Anaheim, no estado americano da Califórnia, com destino a Toronto, Canadá, estimulou detetives *online* a acreditar que isso era uma evidência do encontro de Ohtani e potencialmente da assinatura com o Toronto Blue Jays, quando na verdade, o voo transportava um empresário canadense e não tinha ligação com Ohtani ou com o beisebol em geral.

Distinguir entre eventos comuns e incomuns pode exigir muita experiência em domínios específicos, seja esse campo o monitoramento de conflitos, desastres naturais ou qualquer outra área de pesquisa. Muitos pesquisadores não possuem esse conhecimento específico, independentemente de quão bem dominam uma ferramenta ou método.

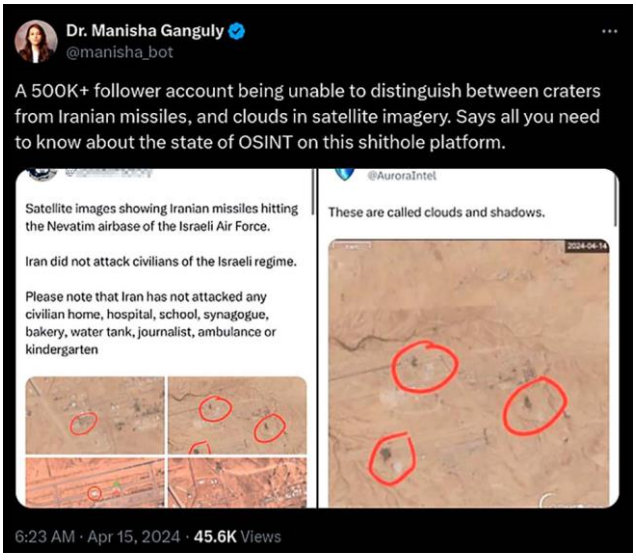
5. USO INCORRETO DE FERRAMENTAS E INTERPRETAÇÃO DE DADOS

Existem muitas ferramentas de fontes abertas diferentes, e até tentamos manter uma lista de recursos úteis no *kit* de ferramentas de pesquisa *online* do Bellingcat. No entanto, como acontece com qualquer nova ferramenta, os usuários muitas vezes precisam de alguma orientação, experiência e treinamento para dominá-la.

Muitas vezes vemos novos usuários não estarem cientes das limitações dessas ferramentas. Novas ferramentas não são soluções mágicas e muitas vezes vêm com muitas ressalvas. Por exemplo, no caso do software de reconhecimento facial, existem pontos fortes e fracos para diferentes serviços e os resultados fornecidos por essas ferramentas não devem ser tratados com total certeza. Normalmente, outros pontos de dados e contexto são necessários para mostrar por que a correspondência é confiável. Dependendo da foto e do caso específico, é possível buscar pistas falsas e chegar a conclusões incorretas com base nas limitações daquele software.

Ferramentas que detectam manipulação de fotos são outro exemplo. Em maio passado, o presidente da Colômbia retuitou uma conta que tinha utilizado indevidamente uma dessas ferramentas, tirando conclusões excessivamente confiantes e incorretas.

Mesmo quando essas ferramentas são dominadas, leva tempo para aprender a interpretar os dados ou resultados que elas geram. Em um exemplo, imagens de drones de um objeto em movimento rápido foram interpretadas como um OVNI, quando na realidade poderia ter sido apenas um balão. Em outro caso, um usuário confundiu nuvens em imagens de satélite com crateras.



Captura de tela da postagem da jornalista investigativa Manisha Ganguly no X/Twitter mostrando a postagem de outra conta com identificação incorreta de nuvens como se fossem danos resultantes do ataque de um míssil iraniano. O nome de usuário original foi desfocado pela Bellingcat.

6. EDIÇÃO DE FILMAGENS

Embora geralmente não sejam feitas de forma maliciosa, as contas OSINT às vezes editam as filmagens de maneira inútil, como colocar uma trilha de áudio sobre o vídeo, fazer uma compilação de clipes ou cortar a filmagem original.

Por exemplo, um hábito das contas "agregadoras" é sobrepor a marca d'água do canal em vídeos e imagens. Se não conseguirmos encontrar a origem de um vídeo, geralmente realizamos uma pesquisa reversa de imagens de quadros da filmagem. Mas graças às marcas d'água, essa técnica útil torna-se mais propensa a erros.

Exemplo de uma imagem com marca d'água gratuita, baseada em uma foto de uma pesquisa recente do Bellingcat sobre o chefe do narcotráfico Christy Kinahan. Esta edição é apenas um pouco exagerada quando comparada às práticas de marca d'água das contas de alguns usuários. Tais práticas muitas vezes dificultam a verificação e a análise de imagens.

Ao interpretar e compartilhar conteúdo de fontes abertas, é fundamental não editar a filmagem de forma que diminua, remova ou oculte informações úteis contidas nesse conteúdo. Mesmo que você pense que não está ocultando informações críticas, não há como saber se as informações alteradas seriam úteis posteriormente.

Por exemplo, o áudio contido nas imagens do assassinato do jornalista colombiano Abelardo Liz continha pistas vitais que nos permitiram localizar geograficamente a origem dos tiros. Se esta filmagem fosse editada com uma faixa de áudio dramática, teria ocultado um componente vital desta pesquisa.

7. CORRER PARA SER O PRIMEIRO A QUALQUER CUSTO

É fácil se deixar envolver pelo turbilhão de notícias de última hora, especialmente em torno de ataques terroristas e conflitos militares. Os incentivos das

plataformas de redes sociais, onde é realizada a maior parte da pesquisa pública de fontes abertas, encorajam este comportamento. Existe uma grande tentação de ser a primeira pessoa a fazer um "avanço" em uma história em desenvolvimento, ou a gerar rapidamente uma análise sobre um evento.

No entanto, a validação do conteúdo deve sempre ter prioridade sobre a velocidade.

Alguns dos exemplos mais notórios e prejudiciais disto são as muitas vezes em que pesquisadores amadores identificaram erroneamente pessoas inocentes como perpetradoras de ataques terroristas. Isso ocorreu recentemente com o esfaqueamento de Bondi Junction, bem como os atentados à bomba na Maratona de Boston em 2013 e o tiroteio no *shopping* Allen, no Texas, em 2023. Esse tipo de resultado errado se baseia no fato de a pessoa inocente ter o mesmo nome ou um rosto de aparência semelhante ao do perpetrador – nenhum dos quais é prova suficiente por si só, dada a gravidade de tais identificações.

Muitas vezes, a verificação é ignorada quando o desejo de rapidez é priorizado, o que pode criar mais danos e confusão sobre o desenrolar de uma situação, ao invés de trazer os fatos e a clareza necessários.

Publicado no Bellingcat.

***Tristan Lee** é cientista de dados da Bellingcat cujo trabalho se concentra em redes online de extrema direita e de teorias da conspiração.*

***Kolina Koltai** é pesquisadora sênior da Bellingcat. Especialista em como os sistemas sociotécnicos influenciam a tomada de decisões de grupos sociais, ela tem um doutorado pela Escola de Informação da Universidade do Texas, tendo trabalhado anteriormente no Centro para um Público Informado da Universidade de Washington.*

***Giancarlo Fiorella** é Diretor de Pesquisa e Treinamento da Bellingcat. Ele tem doutorado pelo Centro de Criminologia e Estudos Sociolegais da Universidade de Toronto, onde sua pesquisa se concentrou em atores não-estatais e protestos antigovernamentais na Venezuela. Ele é professor assistente do Laboratório de Investigações de Justiça Global da Universidade de Utrecht.*