A Importância Crescente da Informação de Fontes Abertas – O Papel dos Colectivos e Analistas Independentes

Auditor
Pedro Pereira Mateus

Introdução

A produção de informação a partir de fontes abertas (no original anglo-saxónico, “Open Source Intelligence”, OSINT) é um termo formalizado pela comunidade de informações militares dos Estados Unidos da América (EUA) entre finais da década de 1980 e início da década de 1990, sendo adoptado pela “North Atlantic Treaty Organization” (NATO) como uma metodologia formal em meados da década de 1990.

A sua produção assenta essencialmente em três etapas: (i) na recolha de dados a partir de fontes disponíveis ao público, e.g., notícias e reportagens de órgãos de comunicação social, comunicados do governo, das forças de defesa e de segurança, das academias ou das indústrias; ou das redes sociais; (ii) na verificação e cruzamento desta informação entre diversas fontes e no contexto em que se inserem; e (iii) no enriquecimento técnico desta informação.

Os produtores de informação a partir de fonte abertas inserem-se em três grandes grupos: (i) de Estado, compreendendo Ministérios, Forças de Defesa, Forças de Segurança e Serviços de Informações Civis e Militares; (ii) Privados, compreendendo

empresas que operam do sector industrial, ao imobiliário ao da distribuição, às de cibersegurança, investigação ou segurança privada; e (iii) Independentes, compreendendo jornalistas de investigação, verificadores de factos, activistas até aos colectivos e analistas com foco na área dos temas contemporâneos de defesa e segurança.

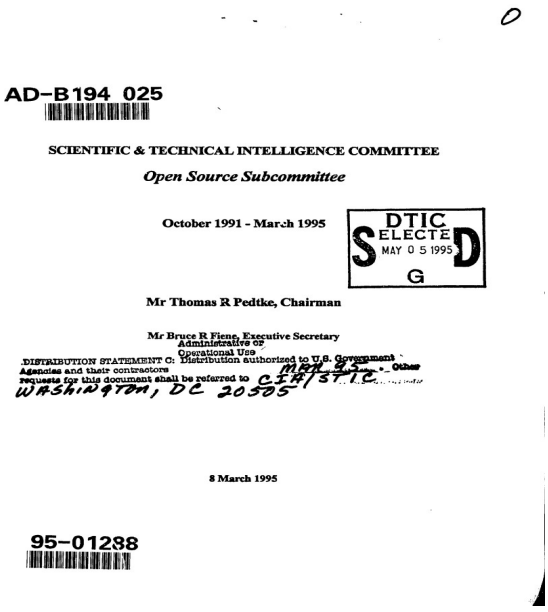
Entre 2014 e 2024, especialmente impulsionada pelos contextos da invasão da Crimeia, da Guerra do Donbas e da Guerra da Ucrânia, e pela disponibilidade e aceitação pública e alargada de ferramentas digitais de pesquisa, cruzamento e publicação de conteúdos e seu comentário (em particular com o crescimento das diferentes redes sociais), a dinâmica de informação a partir de fontes abertas resultado da acção de produtores independentes e, entre estes, especialmente por parte dos colectivos e analistas de defesa, atingiu um crescimento substancial e um patamar sustentando, sendo os mesmos citados e usados regularmente como referência de valor, reconhecidos nos mais variados contextos e canais.

Origens

Estima-se que durante a Guerra Fria (1947-1991), cerca de 20% da informação recolhida sobre a União das Repúblicas Socialistas Soviéticas (URSS), pelos serviços de informações dos Estados Unidos da América (EUA), teria por base fontes abertas (Lowenthal, 2005).

O termo "informação de fontes abertas" usado a par do acrónimo original anglo-saxónico, OSINT, surge pela primeira vez na literatura em 1990 (Steele, 1990), pela mão de Robert David Steele (1952-2021), com os primeiros "papers" e conferências alargadas sobre o tema a surgirem de outros autores norte-americanos, no contexto da comunidade dos serviços de informações dos EUA, ao longo de 1992 e 1993.

Em Outubro de 1991, é formado pelo Governo dos EUA, sob a égide da "Central Intelligence Agency" (CIA), o "Scientific & Technical Intelligence Commitee – Open Source Subcommitte" (STIC-OSS), que levaria a comunidade dos serviços de informações dos EUA, aqui liderada pela CIA, a estabelecer, em Março de 1994, o COSPO, "Community Open-Source Program Office" (COSPO, 1995), com Joseph Markowitz (1938-2019) como seu primeiro director, firmando a metodologia de operação sobre fontes abertas de informação e estabelecendo o programa de desenvolvimento estratégico da mesma, com impacto em organizações que foram desde o "Federal Bureau of Investigation" (FBI) à "National Aeronautics and Space Administration" (NASA).


AD-B194 025

SCIENTIFIC & TECHNICAL INTELLIGENCE COMMITTEE

Open Source Subcommittee

October 1991 - March 1995

DTIC ELECTE MAY 0 5 1995 S D G

Mr Thomas R Pedtke, Chairman

Mr Bruce R Fiene, Executive Secretary

Administrative or Operational Use

DISTRIBUTION STATEMENT C: Distribution authorized to U.S. Government Agencies and their contractors. Other requests for this document shall be referred to CIA/STIC WASHINGTON, DC 20505

8 March 1995

95-01288

Figura 1 – "Central Intelligence Agency" (CIA) – “Scientific & Technical Intelligence Commitee – Open Source Subcommitte” (STIC-OSS), 1991-1995,

in "Defense Technical Information Center" (DoD), Fort Belvoir, Virginia, EUA.

A metodologia OSINT acompanharia e beneficiaria do desenvolvimento acelerado dos sistemas e tecnologias de informação e comunicação a partir da década de 2000, em particular com a introdução e acesso alargado a motores de pesquisa, sistemas de georreferenciação sobre cartografia com fotos de satélite e redes sociais, todos com alcance global.

Metodologia

A metodologia dos analistas e colectivos independentes assenta, essencialmente, num processo em cascata, com a recolha inicial de um elemento de informação (e.g., uma foto ou um vídeo, com ou sem legenda, associado ou não a um artigo ou descritivo original; ou num excerto de um artigo ou nota de imprensa); na análise crítica de tal elemento “per se” aferindo da sua autenticidade (com cruzamento ainda com outras fontes e republicações); na identificação e concretização de pontos a merecer enriquecimento de informação (e.g., datação, georreferenciação, identificação e descrição de equipamentos e armas ou procedimentos); e na identificação e descrição de contextos (e.g., se aquele equipamento, unidade ou prática são antes conhecidos e onde).

Com este elemento de informação (ou um conjunto agregado de elementos de um mesmo contexto, e.g., uma manobra táctica num determinado momento e sector), o analista OSINT publicará a informação produzida, tipicamente em contexto digital, com uso

articulado de “website”/”blog” e redes sociais. Pela exposição pública e pela análise cruzada, em particular pelos seus pares da comunidade OSINT, e pelo público em geral, tem lugar de forma literalmente imediata (e universal) um processo alargado de validação da informação (com a dinâmica das redes sociais a permitir que contra evidências ou oportunidades de melhoria do enriquecimento tenham lugar de forma tão rápida quanto aberta).

Validado e suportar o elemento informativo publicado, sucede, organicamente, a dinâmica de republicação e alcance alargado, sendo o mesmo incorporado, não poucas vezes, em artigos de fundo de órgãos de comunicação social, na recolha de informações por parte dos respectivos serviços afectos às forças de segurança e defesa, ou, em dinâmicas de “fact check” (“verificação de factos”) nos mais variados contextos.

Numa perspectiva colaborativa, muitos dos colectivos independentes e analistas da comunidade OSINT, trocam e validam regularmente informação entre si – seja numa perspectiva de (i) complementaridade por especialidade vertical (e.g., um tema envolvendo meios terrestres, aéreos e navais pode envolver especialistas em cada um destes contextos); por (ii) seguimento geográfico (e.g., um meio naval num percurso entre o Mar Báltico e o Mediterrâneo Oriental, envolver os analistas OSINT localizados e especialistas em pontos do percurso – Dinamarca, Reino Unido, Portugal, Gibraltar e Itália); numa perspectiva de (iii) competências técnicas em determinadas ferramentas (acompanhamento de “transponders”, análise de informação multiespectral em contexto de imagens satélite; construção de modelos analíticos e algoritmos); ou ainda por (iv) especificidades locais (expressões idiomáticas, regionalismos e afins).

Ferramentas

No contexto actual da recolha, verificação, enriquecimento e publicação-difusão de informação produzida por colectivos e analistas independentes, são usados sete grandes grupos de ferramentas digitais: (i) os diferentes canais de publicação das fontes públicas; (ii) os motores de pesquisa; (iii) os motores de pesquisa de incidência reversa sobre imagens; (iv) as plataformas de cartografia e fotos de satélite; (v) as plataformas de acompanhamento de tráfego aeronaval; (vi) as plataformas de inteligência artificial e (vii) as redes sociais.

(i) os diferentes canais de publicação das fontes públicas

As fontes públicas de informação compreendem todos os órgãos de comunicação social (rádios, jornais, televisão, canais e meios digitais; locais, regionais, nacionais e internacionais), as comunicações dos órgãos de estado, governo (nacional, local), administração pública, comunicados e notícias das forças armadas e de defesa, da protecção civil, de empresas e associações e, naturalmente, toda a informação pública

que consta das redes sociais e dos canais digitais de publicação.

(ii) os motores de pesquisa

Com origens a remontar aos inícios da "World Wide Web", os primeiros motores de pesquisa foram o WebCrawler (1994), o Lycos (1994), o Altavista (1995), o Excite (1995), o Yahoo (1995) e o Infoseek (1995), permitindo, de forma gratuita, universal e de uso simples, que os utilizadores fizessem pesquisas de texto livre sobre os conteúdos existentes na Internet. Com a introdução do motor de pesquisa Google, em 1998 assiste-se a um salto tecnológico de grande escala, quer em termos de indexação de conteúdos, de algoritmos da sua selecção e classificação, e do desenvolvimento dos mais variados subcomponentes e derivados da pesquisa.

A comunidade OSINT usa frequentemente o Yandex (2000), dado o seu enquadramento e popularidade de uso na Federação Russa, bem como o Baidu (2000) no mesmo contexto da República Popular da China.

(iii) os motores de pesquisa de incidência reversa sobre imagens

Com o lançamento, em 2008, do serviço TinEye, da canadiana Idée Inc., iniciou-se a possibilidade de pesquisar usando como "input" imagens e não apenas texto livre. Conseguia-se assim usar uma imagem como fonte de informação "per se" pesquisando sobre diversos contextos da mesma, como sejam a data e contexto de publicação original, bem com o número e dispersão das publicações ou ainda encontrar imagens de maior resolução. Em 2011 o Google lançaria esta componente de serviço de incidência reversa sobre o seu "Image Search" (que permitia desde 2001 obter imagens a partir de pesquisa por texto), tornando-se o mais popular recurso de investigação neste âmbito.

Trata-se da principal funcionalidade usada para aferir o contexto original de publicação de uma determinada foto e que permite rapidamente identificar, em contextos de desinformação, o uso de uma foto antiga a ser publicada como referente a um facto actual, ou de diferentes geografias e âmbitos.

(iv) as plataformas de cartografia e fotos de satélite

A partir do lançamento, em 1999, da primeira operação privada de captura e disponibilização de imagens de alta-resolução (80 centímetros), através do satélite IKONOS (com sistema óptico da norte-americana Kodak), desenvolvido e operado pela Space Imaging Inc., inicia-se, a par da sua incorporação como ortofotomapas na plataforma Google Earth, em 2005, e cruzando com os mapas e cartografia do Google Maps, do mesmo ano, a entrega, de forma gratuita e universal, de ferramentas que

permitem a todos pesquisar e georreferenciar (de uma forma antes apenas disponível no contexto de meios militares).

Operando actualmente os satélites privados da WorldView e da GeoEye, e com todo o arquivo da Space Imaging, a Maxar Technologies é hoje o líder de fornecimento de fotos de satélite aos serviços da Google, do Governo dos EUA, e a inúmeras empresas e, claro, a colectivos e analistas independentes de fontes abertas de informação. Conseguindo entregar fotos de 31 centímetros de resolução, conta actualmente com dez satélites em operação, os dois mais recentes dos quais (WorldView Legion 5 e 6) colocados em órbita a 4 de Fevereiro de 2025.

As plataformas digitais Google Maps e Google Earth vieram permitir, ao longo das 2 últimas décadas, pela sua arquitectura aberta, não só a pesquisa por texto livre, por coordenadas ou pontos de interesse, mas também suportar camadas de informação autónomas (por parte dos utilizadores), como sejam uso em contexto de planeamento urbanístico e agrícola ou em termos de informação sobre defesa.

> Destacando um caso prático de uso, o "UA Control Maps" (desenvolvido pelo colectivo independente "Project Owl OSINT"), dedicado a publicar informação georreferenciada, confirmada com evidência publicada a par da própria informação, de acções de combate dos dois beligerantes no Teatro de Operações sobre a Ucrânia como um "layer" autónomo sobre o Google Maps – cujo conteúdo foi possível observar em uso nos ecrãs de umas das salas de acompanhamento de operações do quartel general do Departamento de Defesa dos Estados Unidos, durante a reportagem de David Martin (CBS News), acompanhado pelo General Mark Milley ("chairman" da Chefia Conjunta de Chefes de Estado Maior das Forças Armadas dos Estados Unidos), em Setembro de 2023.

Figura 2 – Uso da plataforma independente "UA Control Maps" pelo Departamento de Defesa dos Estados Unidos em análise sobre o Teatro de Operações da Ucrânia.

A informação do UA Control Maps resulta da agregação e filtragem feita por tal colectivo

a partir das georreferenciações produzidas e submetidas, de forma aberta, pelos mais diversos analistas independentes, – em que se inclui, entre largas dezenas de outros, o colectivo OSINT português “Espada & Escudo” (UAControlMap, 2024).

O programa “Copernicus” da União Europeia, que iniciou a sua operação em 2014, e que opera actualmente com uma constelação de oito satélites Sentinel, de acesso aberto e público, fornece ainda um importante recurso aos analistas, com uma resolução de 10 metros, com componente multiespectral e de radar de abertura sintética.

> Um caso prático de uso, pelo analista independente português André Carvalho que, a 27 de Novembro de 2024, recorreu à informação do satélite Sentinel 2, de 22 de Novembro de 2024, para georreferenciar a passagem do porta-aviões USS Harry S. Truman (CNV) 75 ao largo de Aljezur, na costa continental Portuguesa (Carvalho, 2024).

O sistema NASA FIRMS (“Fire Information for Resource Management System”), assente nos satélites da constelação MODIS (“Moderate Resolution Imaging Spectroradiometer “, Terra e Aqua) e VIIRS (“Visible Infrared Imaging Radiometer Suite“, Suomi NPP e NOAA-20 e 21), disponibiliza, praticamente em tempo real (com um “delay” de 3 horas), informação sobre incêndios activos.

Um caso prático de uso, pelo colectivo independente português “Espada & Escudo”, a 7 de Dezembro de 2024, que recorreu ao sistema NASA FIRMS para identificar o ataque, pelas forças da Marinha da Ucrânia, a plataformas “offshore” de exploração de gás natural no Mar Negro, anexadas e nacionalizadas pela Federação Russa, ao largo da costa ocidental da Crimeia (E&E, 2024b).

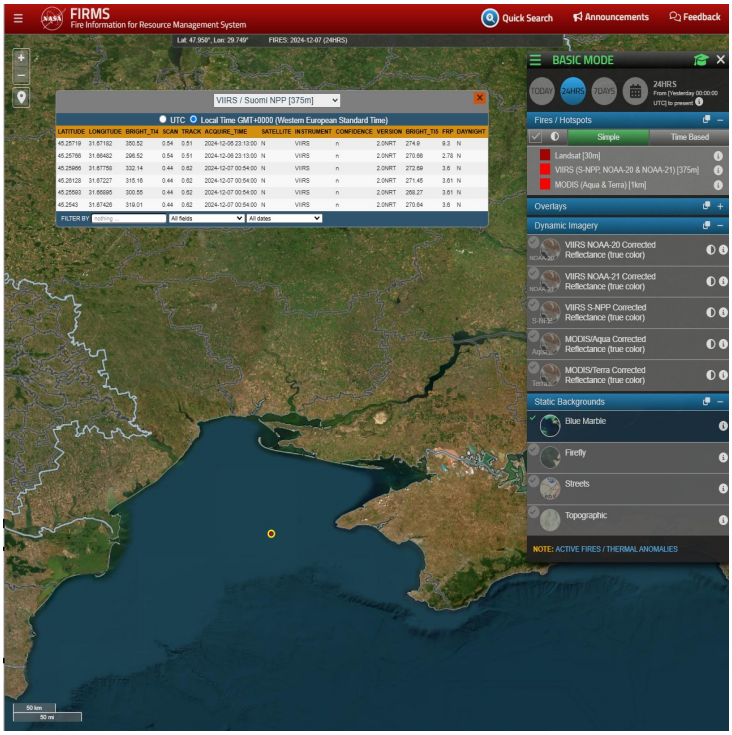


Figura 3 – Uso da plataforma aberta "NASA FIRMS" pela colectivo independente português "Espada & Escudo" em análise sobre o Teatro de Operações da Ucrânia.

(v) as plataformas de acompanhamento de tráfego aeronaval

Um elemento de elevado valor acrescentado no acompanhamento e verificação de informação são as plataformas abertas de acompanhamento ("online" e histórico) da actividade aeronaval assente na recolha e processamento georreferenciado dos sinais dos "transponders".

Em termos de meios navais temos o Marine Traffic (2007), o FleetMon (2007), o AIS Hub (2007), o ShipFinder (2010) VesselFinder (2011) e o MyShipTracking (2014). Estas plataformas apresentam informação sobre a identificação do navio, sua velocidade, rumo e posição, bem como paragens em portos.

Em termos de meios aéreos temos o FlightAware (2005), o FlightRadar (2006), o RadarBox (2007), o PlaneFinder (2009), o OpenSky Network (2012) e o ADS-B Exchange (2016). Estas plataformas apresentam informação sobre a identificação da aeronave, sua velocidade, sua altitude rumo e posição, bem como paragens em aeroportos e horas previstas / realizadas de operação.

Com a recolha continuada de informação permitem apresentar, em formato visual sobre mapa, o "tracking" da operação e viagem de um navio ou de uma aeronave. São particularmente referenciados pela comunidade OSINT o ADS-B Exchange e FlightRadar, em termos aéreos, e o Marine Traffic e Vessel Finder, em termos navais.

Complementam esta informação ainda os serviços independentes que referenciam situações de emergência, ataque ou acidente, como sejam, na aviação, a "Aviation Safety Network" (da "Flight Safety Foundation") ou em termos navais e para os Teatros de Operações do Mar Vermelho, Golfo de Áden e Oceano Índico, o "UK Maritime Trade Operations" (UKMTO).

> Destacando um caso prático de uso, a 21 de Agosto de 2024, surgindo referências (alarmistas) nas redes sociais que estaria uma frota de pesqueiros, com cerca de 2 dezenas de navios de pavilhão chinês, a operar a cerca de 20 a 30 milhas náuticas ao largo da Ilha das Flores, na Região Autónoma dos Açores dentro da ZEE da República Portuguesa, o colectivo OSINT português "Espada & Escudo" recorreu a uma análise, suportada na plataforma VesselFinder, de rumos, velocidades e intermitências de sinal, apresentando contexto e evidências de que se trataria de um caso de manipulação de dados de identificação marítima automática ("AIS Spoffing"), complementando a produção de informação com o detalhe e resultado das acções conduzidas no local pelos meios da Marinha (via Comando Local da Polícia Marítima) e da Força Aérea Portuguesas, e publicando esta informação em "blog" e redes sociais (E&E, 2024a).

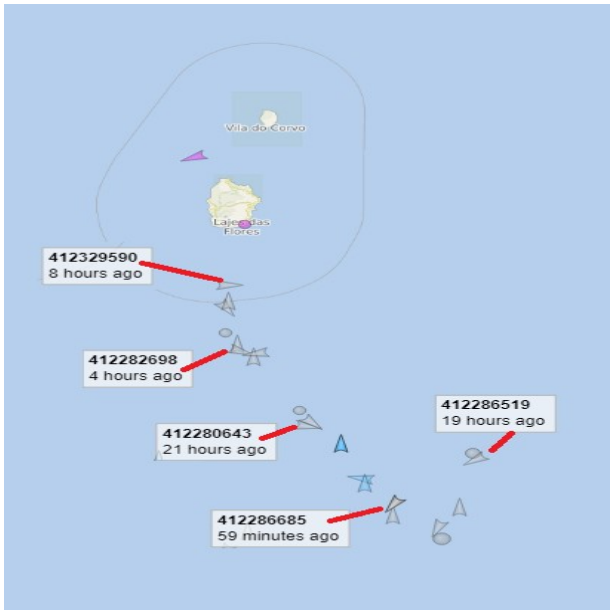


Figura 4 – Uso da plataforma aberta "Vessel Finder" pela colectivo independente português "Espada & Escudo" em análise sobre o Teatro de Operações da Região Autónoma dos Açores, Ilha das Flores.

(vi) as plataformas de inteligência artificial

Com especial incidência na ferramenta ChatGPT da plataforma Open AI, disponível desde 30 de Novembro de 2022, a inteligência artificial tem um papel da maior importância na pesquisa e verificação de informação a partir de fontes abertas.

Veio permitir: (i) desencadear pesquisas usando linguagem natural (direccionando, restringindo critérios, dando exemplos, etc.), como texto livre e/ou imagens; (ii) permitir fazê-lo em 95 línguas (com suporte alargado e cruzado de tradução e retroversão, transcrição, reconhecimento óptico e de voz); (iii) apresenta e permitir seguir fontes; e, (iv) por permitir efectuar cálculos e extrapolar modelos de análise operacional a partir de linguagem natural.

> Tomemos o exemplo genérico de um analista de fontes abertas de informação que quer determinar (ou confirmar) o ponto máximo onde poderia ter tido lugar uma acção de evacuação sobre o oceano. Sabendo, a partir de um órgão de comunicação social local, a partida e chegada de uma determinada aeronave, de uma determinada base num determinada data hora, bastará indicar o modelo da aeronave (ou sugerir várias), o ponto de origem e chegada e as datas-horas respectivas, e poderá ter, em poucos segundos, uma tabela (com pré-explicitação dos cálculos pela ferramenta) indicando a distância ao ponto máximo, enriquecida com variantes como o tempo decorrido sobre o objectivo, e o impacto estimado da intensidade e direcção do histórico ventos médios no curso da missão em diferentes pontos cardeais. Tarefa que demoraria muitíssimo mais tempo em cálculo manual (mesmo em folha de cálculo) a um analista.

Num exemplo mais complexo, envolvendo a análise de uma acção conjunta de uma aeronave e de um meio naval, pode o analista usar a ferramenta de inteligência artificial para, com pedido em linguagem natural, construir um modelo com diferentes cenários

(intervalos de data-hora, variantes de rumo e velocidade) e apurar onde os mesmos se poderão ter cruzado sobre um mesmo objectivo ou em etapas referenciadas (ou conhecendo o cruzamento, projectar a sua origem).

(vii) as redes sociais

Desenvolvidas a partir da década de 2000, e com crescimento acelerado a partir da década de 2010, as redes sociais desempenham, pela sua acessibilidade gratuita e universal, e pela facilidade de uso (na produção e na consulta de conteúdo), um papel de elevado relevo no desenvolvimento da informação a partir de fontes abertas – seja (i) como fonte de informação, seja (ii) como canal de publicação da informação produzida, seja ainda (iii) como meio de validação da mesma.

> Destacam-se, cronologicamente, o LinkedIn (2002), o Facebook (2004), o YouTube (2005), o Twitter (2006), o Instagram (2010), o TikTok (2017) e o Bluesky (2021). Ainda que sejam, em termos de conceito e arquitectura base, ferramentas de troca de mensagens, o WhatsApp (2009), o Telegram (2013) e o Discord (2015), com as suas componentes de grupos e canais, qualificam ainda nesta mesma categoria.

Os colectivos e analistas independentes de fontes abertas de informação assentam actualmente a sua acção especialmente nas redes Twitter, Bluesky, Telegram e Discord.

Do “Hobby”, da “gamificação” e da Neutralidade

Os colectivos e analistas independentes distinguem-se dos demais enquadrados na produção independente do contexto OSINT (como são os jornalistas de investigação, os verificadores de factos e os activistas) por desenvolveram esta actividade, não só “pro bono”, como por o fazerem numa dinâmica de “hobby” e num contexto, dinâmico e auto-estimulante, de “gamificação” (i.e., a aplicação de elementos típicos dos jogos, como sejam pontos, níveis, desafios, recompensas e rankings, em contextos não lúdicos, com o objectivo ou resultado de reforço de motivação e resultados).

A dinâmica de “hobby”, ou daquilo que em maior rigor se designa por “hobby profissional”, leva estes especialistas a desenvolveram muitas vezes uma produção de informação especializada em segmentos verticais, como sejam, em concreto, apenas a aeronáutica ou a marinha, apenas os meios de um determinado País ou os meios militares que transitam em determinadas geografias (e.g. Mediterrâneo, Gibraltar, Canal da Mancha, Báltico, etc.). Cooperando, de forma não necessariamente orgânica, mas através de publicação desta informação numa mesma rede, a produção alcançada atinge uma proporção global e universal nunca antes conhecida (em quantidade, qualidade e actualidade).

O elemento de “gamificação” é aquele que colectivos e analistas independentes

incorporam ao quererem não só publicar primeiro uma determinada informação, como em ver a mesma rápida e alargadamente reconhecida (como correcta) e reproduzida com alcance, acrescentando valor, por exemplo, com a identificação técnica do detalhe de um determinado equipamento presente numa foto e/ou a sua georreferenciação ao ponto. Mais: é todo uma dinâmica que estimula a aprendizagem e aperfeiçoamento da metodologia.

Acresce ainda à maioria destes colectivos e analistas independentes um nível de abstracção e neutralidade, encarando a produção desta informação e a melhoria e enriquecimento contínuo da mesma, numa perspectiva sem contextos políticos, partidários, políticos ou activistas, procurando apenas que a sua entrega corresponda a um elemento de qualidade reconhecida por todo o público e pelos seus pares – cruzando, também aqui, com a perspectiva de "rank" em termos de "gamificação".

Não são OSINT

É frequente que projectos ou acções ligadas ao activismo, às acções privadas de investigação ou mesmo do comentário geopolítico sejam confundidos com as metodologias e práticas de produção de informação a partir de fontes abertas. Importa separar aqueles que, "tout court", seguem outros critérios e metodologias.

> Projectos e acções de denunciantes de infracções ("Whistleblowers"), como, e.g., o WikiLeaks, fundado em 2006 pelo australiano Julian Assange, não são, de todo, projectos de informação sobre fontes abertas de informação – sendo precisamente resultado da captura e divulgação de fontes fechadas de informação (privada, secreta, classificada, etc.).
>
> Tal como, em outro exemplo, acções conduzidas pelo colectivo independente de produção de informações Bellingcat, que se define como partilhando uma "paixão por pesquisa sobre fontes abertas de informação" (Bellingcat, 2025), fundado em 2014 pelo britânico Eliot Ward Higgins, em que optaram, no decurso de uma investigação em torno do envenenamento em 2020 do activista russo Alexei Navalny, por comprar informação (i.e., meta dados sobre uso telefónico, registos pessoais de viagem e afins) junto do "probiv" ("пробив"), o mercado negro russo de informação (Yaffa, 2021). Comprar informação privada, com a agravante de se tratar de uma acção de natureza ilegal, não corresponde, de todo, a uma prática de produção de informação a partir de fontes abertas.
>
> Mais comumente quando alguns comentadores de defesa, segurança e geopolítica, nas redes sociais ou em rubricas televisivas, exibem uma foto ou vídeo de uma determina acção, denotando estarem, genericamente, a usar informações recolhidas por fontes no terreno, não estão também a praticar metodologias OSINT, mas simplesmente a reproduzir algo (i.e., reproduzir informação e produzir informação são conceitos distintos). Reproduzir um determinado elemento multimédia sem o verificar e sem enriquecimento de informação é apenas uma reprodução e não a produção de informação. Tanto mais quanto, em Portugal, é comum que alguns destes comentadores, além do não reconhecimento das fontes (públicas) usadas, cometerem os mais variados erros de interpretação ou validação, resultando em actos de desinformação (Galrão, 2025).

Ética e Segurança Operacional

O desenvolvimento da acção de produção de informação em contexto OSINT deve ser sustentada por critérios éticos especialmente exigentes e rigorosos e pelo garante sustentado de segurança operacional.

Em particular, a componente ética deve garantir que nunca seja confundida (ou tolerada) uma informação privada (ou classificada), disseminada ao público, como passando a ser informação pública de facto. Muito menos uma informação entregue em surdina ao analista.

Deve ser sempre entendida como pública (apenas) aquela informação que o seu agente de publicação tem a autorização e a intenção efectivas de a poder tornar pública e, desejavelmente, que essa agente seja uma fonte primária, ou o mais próximo possível da mesma. Em casa de dúvida sobre a autorização, a decisão deverá ser sempre de não a considerar e, em paralelo, de informar e consultar, de forma documentada, a entidade responsável.

> Imagine-se um caso, hipotético, em que surge publicada numa área (pública) de uma rede social, de forma acidental ou intencional, um plano de operação detalhado para uma acção de uma força de segurança, em que, sob mandado judicial, irão, dentro de poucos dias, conduzir uma acção de abordagem em alto-mar, com a participação de forças de defesa e outras agências, a uma embarcação suspeita de envolvimento numa rede de crime organizado internacional de narcotráfico. Além de comprometer o sucesso e a segurança operacional da acção, a produção e publicação de informação a partir de tal recurso seria, "per se", um acto criminoso (Artigo 195.º e 316.º do Código Penal).

Mesmo no contexto de uma informação pública de uma fonte primária e validada (i.e., publicação intencional legítima), se o analista determinar que possa existir risco de compromisso de segurança operacional deve, mais uma vez, abster-se de considerar tal componente da informação e questionar a fonte, indicando, explicitamente que pretende ver validado o enquadramento de segurança operacional (OPSEC).

Referências Activas em Portugal

Com conteúdo publicado de forma regular e contínua, existem relativamente poucas referências activas de produção de informação a partir de fontes abertas em Portugal por parte de analistas ou colectivos independentes.

A título de referência, temos:

Pássaro de Ferro

Fundado em 2006, na plataforma Blogspot (e presente actualmente também na rede social Facebook), o colectivo Pássaro de Ferro, dedica-se essencialmente à produção de informação sobre o contexto aeronáutico militar português. Além da produção de

informação, editam e publicam também artigos de opinião. Tem actualmente 79 mil seguidores na rede social Facebook.

Luís Galrão

Com presença na rede social Twitter desde 2009, @Lgalrao, é um analista independente, "fact checker" e que desenvolve actividade desde os contextos político-sociais ao militar. É o mais antigo praticante de metodologia OSINT em Portugal com abrangência multitemática e conteúdo publicado. Tem actualmente 6 mil seguidores na rede social Twitter.

André Carvalho

Com presença activa na rede social Facebook desde 2009 (e entretanto também na rede social Instagram), "plane spotter", produz informação com especial incidência na componente de aviação militar com maior relevo ao contexto português.

LP-ADSB

Com presença na rede social Twitter desde 2018, @Lp_adsb, produz informação diária a partir da informação pública dos "transponders" de aviação, via ADS-B Exchange, no contexto estrito da geografia de Portugal cobrindo meios de aviação militar (nacionais e internacionais sobre a mesma). Tem actualmente cerca de 2 mil seguidores na rede Twitter.

Portugal Intel Radar

Com presença na rede social Twitter desde 2019, @IntelPortugal, produz informação sobre actividade de aeronáutica militar portuguesa (nacional e internacional) e sobre meios aéreos militares internacionais sobre a geografia de Portugal. Tem actualmente cerca de 1 milhar de seguidores na rede Twitter.

Espada & Escudo

Um colectivo fundado a 4 de Janeiro de 2022, na rede social Facebook e na plataforma Blogspot (e presente actualmente também na rede social Twitter e Bluesky), produz informação diária sobre forças de defesa e segurança nacionais e internacionais em todas as geografias e contextos. Produz periodicamente informação sobre temas históricos e publica, no seu "website" em formato digital, um magazine trimestral com uma selecção de artigos antes publicados. Tem actualmente 27 mil seguidores na rede social Facebook e publicou 13 magazines.

Conclusão

A metodologia de produção de informação a partir de fontes abertas, com origens em finais da década de 1980 e inícios da década de 1990, conhece um desenvolvimento muitíssimo alargado com o acesso universal e gratuito a tecnologias e plataformas digitais de elevada sofisticação e aceitação, nas décadas de 2000 e 2010.

Os serviços e ferramentas entregues por estas plataformas, permitem, por um lado, uma maior produção e disseminação de elementos informativos (seja pelos agentes tradicionais, seja pelo público em geral) e, por outro, que a sua selecção, validação e enriquecimento por analistas e colectivos independentes sejam feita numa escala e com um rigor metodológico nunca antes conhecido.

A análise crítica, o cruzamento de fontes, a produção de evidências e a validação por pares (altamente especializados e em grande número e distribuição geográfica), de forma quase imediata e universal, sustentam uma qualidade e actualidade desta informação que a permite ver-se incorporada nas dinâmicas dos próprios serviços de informações de segurança e defesa bem como nos mais diversos contextos de "fact check" e de artigos de fundo dos "media" tradicionais.

Bibliografia

Bellingcat (2025), 'Who We Are', URL: https://www.bellingcat.com/about/who-we-are/ (acedido a 14 de Abril de 2025).

Carvalho, A. (2024). 'Há poucos dias o porta-aviões USS Harry S. Truman (CVN 75) realizou o transito junto à nossa costa a caminho do Mediterrâneo', 27 de Novembro de 2024. URL: https://www.facebook.com/photo?fbid=10169507931945007&set=a.10150237881345007 (acedido a 14 de Abril de 2025).

Carvalho, C.V. (2015) 'Aprendizagem baseada em jogos', II World Congress on Systems Engineering and Information Technology.

Central Intelligence Agency (CIA), STIC-OSS (1995) Scientific & Technical Intelligence Committee – Open Source Subcommittee, CIA/STIC 012-97 ltr., 3 April 1997, ADB194025, Washington, D.C.

Community Open Source Program Office (COSPO) (1995) Community open source strategic plan. UB 215 U58 H06762 C.2., DIA Library RST-2A, 00000442 J.

E&E (2024a), 'Acção de manipulação de dados de identificação marítima automática detectada ao largo das Flores', 22 de Agosto de 2024. URL: https://espada-e-escudo.blogspot.com/2024/08/accao-de-manipulacao-de-dados-de.html

(acedido a 14 de Abril de 2025).

E&E (2024b), 'Marinha da Ucrânia ataca plataforma "offshore" da Federação Russa no Mar Negro com drones navais projectando drones aéreos de ataque', 7 de Dezembro de 2024. URL: https://espada-e-escudo.blogspot.com/2024/12/marinha-da-ucrania-ataca-plataforma.html (acedido a 14 de Abril de 2025).

Galrão, L. (2025), 'Guerra Fria aos Factos' | 'Factos Alternativos'. URL: https://x.com/hashtag/guerrafriaaosfactos?src=hashtag_click e https://x.com/hashtag/factosalternativos?src=hashtag_click (acedido a 14 de Abril de 2025).

Lowenthal, M.M. (2005) 'Open-source intelligence: new myths, new realities', in George, R.Z. and Kline, R.D. (eds.) Intelligence and the national security strategist: enduring issues and challenges. Washington, D.C.: National Defense University Press.

Manley, C. (2005) 'Managing Army open source activities', Military Intelligence Professional Bulletin, 31(4).

Martin, D. (2023) 'Gen. Mark Milley on seeing through the fog of war in Ukraine', CBS News, Sunday Morning, 10 September. URL: https://www.cbsnews.com/news/gen-mark-milley-fog-of-war-ukraine-sunday-morning-2023-09-10 (acedido a 14 de Abril de 2025).

Steele, R. (1990) 'Intelligence in the 1990s: recasting national security in a changing world', American Intelligence Journal, Summer/Fall.

UAControlMap (2024), 'Russian T-80BVM tank detonates with enthusiasm after SBU drone hits critical weak spot on rear of turret' URL: https://x.com/UAControlMap/status/1747059806081351946 (acedido a 14 de Abril de 2025).

Yaffa, J. (2021) 'How Bellingcat unmasked Putin's assassins', The New Yorker, 31 March. URL: https://www.newyorker.com/magazine/2021/03/31/how-bellingcat-unmasked-putins-assassins (acedido a 14 de Abril de 2025).