JURNAL WACANA SOSIAL NUSANTARA

Jurnal Wacana Sosial Nusantara
2026, Volume 2, No.6
E-ISSN: 3110-6439

Peran Open-Source Intelligence (OSINT) sebagai Early Warning Ukraina Menjelang Invasi Rusia Februari Tahun 2022

Safira[1], Adira May Cantica Sembiring[2], Muhammad Zaydan Firdaus[3], Nafisah Dian Tsabitah[4], Gabriella Aldeheid Conda Longdong[5], Ivandra Solihin[6]

Program Studi Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Pembangunan Nasional Veteran Jakarta

ARTICLE INFO

Article history:
Received June 01, 2026
Revised June 22, 2026
Accepted June 23 , 2026
Available online June 23, 2026

Kata Kunci:
OSINT, early warning, Rusia-Ukraina, intelijen, keamanan internasional.

Keywords :
OSINT, early warning, Russia–Ukraine, intelligence, international security.

This is an open access article under the CC BY-SA license.
Copyright © 2026 by Author. Published by Jurnal Wacana Sosial Nusantara

ABSTRAK

Open Source Intelligence (OSINT) menjadi salah satu pendekatan intelijen modern yang memanfaatkan sumber informasi terbuka untuk mendukung identifikasi ancaman keamanan. Dalam konteks invasi Rusia terhadap Ukraina pada Februari 2022, OSINT berperan penting dalam mengungkap berbagai indikasi persiapan militer sebelum serangan berlangsung. Melalui pemanfaatan citra satelit komersial, media sosial, laporan media, dan data geospasial terbuka, berbagai aktivitas seperti mobilisasi pasukan, penempatan kendaraan tempur, pembangunan fasilitas logistik, dan peningkatan kesiapan operasional Rusia dapat terdeteksi lebih awal. Informasi yang diperoleh dari sumber terbuka kemudian diverifikasi melalui teknik geolokasi dan analisis lintas sumber sehingga menghasilkan gambaran situasi yang lebih akurat. Kehadiran OSINT menunjukkan bahwa data yang tersedia secara publik dapat digunakan sebagai instrumen peringatan dini (early warning) dalam mendukung pemahaman terhadap dinamika keamanan internasional. Meskipun demikian, OSINT masih menghadapi berbagai keterbatasan, seperti risiko misinformasi, bias data, volume informasi yang sangat besar, serta ketergantungan pada proses verifikasi dan respons pengambil kebijakan. Oleh karena itu, OSINT lebih tepat diposisikan sebagai pelengkap intelijen konvensional dalam membangun sistem peringatan dini yang lebih komprehensif dan adaptif terhadap ancaman keamanan modern.

ABSTRACT

Open Source Intelligence (OSINT) has emerged as a modern intelligence approach that utilizes publicly available information to support the identification of security threats. In the context of Russia's invasion of Ukraine in February 2022, OSINT played a significant role in revealing various indicators of military preparations before the attack occurred. Through the use of commercial satellite imagery, social media content, media reports, and open geospatial data, activities such as troop mobilization, deployment of combat vehicles, construction of logistical facilities, and increased operational readiness were detected at an early stage. Information obtained from open sources was subsequently verified through geolocation techniques and cross-source analysis, providing a more accurate understanding of the situation. The emergence of OSINT demonstrates that publicly accessible data can function as an early warning instrument in supporting the understanding of international security dynamics. Nevertheless, OSINT faces several limitations, including the risks of misinformation, data bias, information overload, and dependence on verification processes and policy responses. Therefore, OSINT is better positioned as a complement to conventional intelligence in developing a more comprehensive and adaptive early warning system for modern security threats.

1. PENDAHULUAN

Perkembangan lingkungan keamanan internasional pada abad ke-21 menunjukkan bahwa ancaman terhadap suatu negara tidak lagi hanya berasal dari serangan militer secara langsung, tetapi juga dari berbagai dinamika politik, ekonomi, teknologi, dan informasi yang

E-mail addresses: 2310412051@mahasiswa.upnvj.ac.id[1], 2310412035@mahasiswa.upnvj.ac.id[2], 2310412059@mahasiswa.upnvj.ac.id[3], 2310412061@mahasiswa.upnvj.ac.id[4], 2010412102@mahasiswa.upnvj.ac.id[5], ivandrasolihin@upnvj.ac.id [6]

berkembang dengan sangat cepat. Kemajuan teknologi informasi telah mengubah cara negara, organisasi, maupun individu memperoleh dan menyebarkan informasi. Dalam situasi keamanan yang kompleks, informasi menjadi salah satu sumber daya strategis yang sangat penting karena dapat digunakan untuk memahami potensi ancaman yang sedang berkembang. Negara yang mampu memperoleh informasi lebih cepat umumnya memiliki peluang yang lebih besar untuk mempersiapkan langkah antisipasi dibandingkan pihak yang terlambat menerima informasi (Sitanggang, 2024). Oleh karena itu, kemampuan untuk mengidentifikasi dan menganalisis tanda-tanda awal suatu ancaman menjadi bagian penting dalam sistem keamanan modern. Kebutuhan akan informasi yang cepat, akurat, dan relevan mendorong berkembangnya berbagai metode pengumpulan intelijen yang dapat mendukung proses pengambilan keputusan. Salah satu metode yang saat ini banyak digunakan adalah Open Source Intelligence (OSINT) yang memanfaatkan berbagai sumber informasi terbuka untuk menghasilkan informasi intelijen yang bernilai (Nikhlis & Ghofur, 2025).

Dalam studi keamanan internasional, konsep peringatan dini atau *early warning* memiliki peran yang sangat penting dalam mendeteksi kemungkinan terjadinya konflik sebelum konflik tersebut benar-benar terjadi. Sistem peringatan dini bertujuan untuk mengidentifikasi berbagai indikator yang dapat menunjukkan adanya ancaman terhadap stabilitas keamanan suatu negara atau kawasan. Melalui sistem ini, pemerintah dan lembaga terkait dapat melakukan berbagai langkah pencegahan maupun persiapan guna mengurangi dampak yang mungkin timbul apabila ancaman tersebut benar-benar terjadi. Keberhasilan suatu sistem peringatan dini sangat bergantung pada kemampuan memperoleh informasi yang akurat dan tepat waktu. Semakin cepat suatu ancaman dapat dikenali, semakin besar peluang bagi pihak yang terancam untuk menyusun strategi respons yang efektif. Sebaliknya, keterlambatan dalam mendeteksi ancaman dapat menyebabkan berbagai kerugian, baik dalam aspek keamanan, politik, ekonomi, maupun kemanusiaan. Oleh karena itu, sistem *early warning* menjadi salah satu komponen penting dalam manajemen keamanan modern (Samudro et al., 2024).

Salah satu peristiwa yang menunjukkan pentingnya sistem peringatan dini adalah invasi Rusia ke Ukraina yang dimulai pada tanggal 24 Februari 2022. Peristiwa tersebut tidak hanya mengubah situasi keamanan di kawasan Eropa Timur, tetapi juga memberikan dampak yang luas terhadap stabilitas politik dan ekonomi global. Konflik tersebut menjadi perhatian dunia karena melibatkan dua negara yang memiliki posisi strategis dalam percaturan politik internasional. Invasi Rusia ke Ukraina memicu berbagai respons dari negara-negara lain, termasuk pemberian sanksi ekonomi, bantuan militer, serta berbagai upaya diplomasi untuk meredakan konflik (Firdaus et al., 2025). Selain menimbulkan korban jiwa dan kerusakan infrastruktur dalam jumlah besar, perang tersebut juga menyebabkan gangguan terhadap perdagangan internasional, pasokan energi, dan ketahanan pangan dunia. Oleh karena itu, banyak pihak kemudian berupaya memahami bagaimana tanda-tanda invasi tersebut sebenarnya telah muncul jauh sebelum perang dimulai. Upaya tersebut penting untuk mengetahui apakah ancaman tersebut sebenarnya dapat dideteksi lebih awal melalui berbagai sumber informasi yang tersedia (Parawita et al., 2025).

Sebelum invasi terjadi, hubungan antara Rusia dan Ukraina telah mengalami ketegangan yang cukup panjang. Ketegangan tersebut semakin meningkat setelah Rusia melakukan aneksasi terhadap wilayah Krimea pada tahun 2014. Peristiwa tersebut mendapat kecaman dari berbagai negara karena dianggap melanggar kedaulatan Ukraina dan hukum internasional. Setelah aneksasi Krimea, konflik bersenjata juga terjadi di wilayah Donbas yang melibatkan kelompok separatis yang didukung Rusia dan pemerintah Ukraina. Konflik tersebut menyebabkan ribuan korban jiwa dan memperburuk hubungan kedua negara. Meskipun berbagai upaya diplomasi telah dilakukan melalui sejumlah perundingan internasional, konflik di kawasan tersebut tidak pernah benar-benar terselesaikan. Situasi yang tidak stabil tersebut menciptakan kondisi yang memungkinkan terjadinya eskalasi konflik yang lebih besar pada masa berikutnya (Udayana, 2025).

Memasuki tahun 2021, berbagai laporan mulai menunjukkan adanya peningkatan aktivitas militer Rusia di wilayah yang berbatasan dengan Ukraina. Sejumlah negara dan lembaga internasional melaporkan adanya pengerahan pasukan dalam jumlah besar ke berbagai titik strategis di sekitar perbatasan. Aktivitas tersebut mencakup perpindahan personel militer,

kendaraan lapis baja, tank, artileri, sistem rudal, serta berbagai perlengkapan logistik yang mendukung operasi militer. Peningkatan aktivitas militer tersebut berlangsung secara bertahap dan terus berkembang hingga awal tahun 2022. Keberadaan pasukan dalam jumlah besar di sekitar wilayah perbatasan menimbulkan berbagai spekulasi mengenai kemungkinan terjadinya operasi militer terhadap Ukraina. Walaupun Rusia menyatakan bahwa aktivitas tersebut merupakan bagian dari latihan militer rutin, banyak pihak menilai bahwa pengerahan pasukan tersebut memiliki tujuan yang lebih besar. Perbedaan pandangan tersebut menunjukkan bahwa situasi keamanan pada saat itu masih dipenuhi oleh ketidakpastian (Husein & Sudiarto, 2024).

Dalam menghadapi situasi yang penuh ketidakpastian tersebut, informasi menjadi faktor yang sangat penting dalam membantu proses pengambilan keputusan. Berbagai negara berusaha mengumpulkan dan menganalisis informasi mengenai aktivitas militer Rusia untuk memahami kemungkinan skenario yang akan terjadi. Informasi tersebut tidak hanya berasal dari lembaga intelijen pemerintah, tetapi juga dari berbagai sumber lain yang tersedia secara terbuka. Dalam era digital, masyarakat dapat memperoleh akses terhadap informasi yang sebelumnya sulit dijangkau, termasuk informasi mengenai aktivitas militer dan perkembangan konflik internasional. Kemajuan teknologi komunikasi memungkinkan berbagai informasi disebarluaskan dalam waktu yang sangat singkat kepada masyarakat global. Akibatnya, proses pengumpulan informasi tidak lagi hanya dilakukan oleh lembaga intelijen resmi, tetapi juga melibatkan akademisi, jurnalis, peneliti, organisasi nonpemerintah, dan masyarakat umum. Fenomena ini menunjukkan adanya perubahan besar dalam cara informasi intelijen diperoleh dan dianalisis (Azzahra et al., 2025).

Intelijen konvensional selama ini menjadi instrumen utama yang digunakan negara untuk memperoleh informasi mengenai ancaman keamanan. Melalui berbagai metode seperti pengintaian, penyadapan, penggunaan agen rahasia, dan operasi khusus lainnya, lembaga intelijen dapat memperoleh informasi yang tidak tersedia bagi publik. Namun demikian, intelijen konvensional juga memiliki sejumlah keterbatasan. Informasi yang diperoleh biasanya bersifat rahasia sehingga tidak dapat diakses atau diverifikasi oleh masyarakat umum (Riyanta & Permatasari, 2025). Selain itu, proses pengumpulan informasi seringkali membutuhkan sumber daya yang besar, baik dari segi biaya, teknologi, maupun personel. Dalam situasi yang berkembang sangat cepat, proses pengolahan informasi yang panjang dapat menjadi hambatan dalam menghasilkan respons yang tepat waktu. Keterbatasan tersebut mendorong berkembangnya pendekatan alternatif yang mampu melengkapi fungsi intelijen tradisional. Salah satu pendekatan yang semakin mendapat perhatian adalah pemanfaatan OSINT (Paluvi & Nasution, 2025).

OSINT merupakan metode pengumpulan dan analisis informasi yang berasal dari sumber-sumber terbuka yang dapat diakses secara legal oleh masyarakat. Sumber informasi tersebut dapat berupa media sosial, situs berita daring, citra satelit komersial, forum internet, data geospasial, rekaman video, blog, dokumen publik, dan berbagai platform digital lainnya. Meskipun berasal dari sumber terbuka, informasi yang terkandung di dalamnya dapat memberikan gambaran yang sangat berharga mengenai suatu peristiwa atau ancaman keamanan. Melalui teknik analisis tertentu, berbagai data yang tersebar dapat diolah menjadi informasi intelijen yang relevan dan dapat digunakan untuk mendukung pengambilan keputusan. Keunggulan utama OSINT terletak pada kemampuannya menyediakan informasi secara cepat dan dalam jumlah yang sangat besar. Selain itu, informasi yang digunakan dapat diverifikasi oleh berbagai pihak sehingga meningkatkan transparansi proses analisis. Oleh karena itu, OSINT semakin banyak digunakan dalam berbagai bidang, termasuk keamanan, pertahanan, penegakan hukum, dan investigasi jurnalistik (Gunawan et al., 2024).

Menjelang invasi Rusia pada Februari 2022, OSINT menunjukkan peran yang sangat signifikan dalam mengungkap berbagai indikasi persiapan serangan militer. Berbagai kelompok analis independen berhasil mengidentifikasi peningkatan aktivitas militer Rusia melalui citra satelit komersial yang tersedia untuk publik. Analisis tersebut menunjukkan adanya pembangunan kamp militer sementara, penambahan kendaraan tempur, peningkatan kapasitas logistik, dan perpindahan pasukan ke lokasi-lokasi strategis di dekat perbatasan Ukraina. Selain citra satelit, berbagai foto dan video yang diunggah oleh masyarakat melalui media sosial juga memberikan informasi tambahan mengenai pergerakan militer Rusia. Informasi tersebut

kemudian diverifikasi menggunakan teknik geolokasi, analisis metadata, dan perbandingan dengan sumber lain untuk memastikan keakuratannya. Hasil analisis yang dilakukan oleh komunitas OSINT menunjukkan bahwa terdapat indikasi kuat mengenai kemungkinan terjadinya invasi jauh sebelum serangan resmi dimulai. Fakta ini menunjukkan bahwa sumber informasi terbuka dapat berfungsi sebagai alat deteksi dini terhadap ancaman keamanan (Sudiq & Yustitianingtyas, 2022).

Keberhasilan berbagai komunitas OSINT dalam mengidentifikasi tanda-tanda awal invasi Rusia menarik perhatian banyak pihak karena menunjukkan perubahan dalam praktik intelijen modern. Jika sebelumnya aktivitas intelijen identik dengan lembaga negara dan informasi rahasia, kini masyarakat sipil juga dapat berkontribusi dalam proses pengumpulan dan analisis informasi strategis. Perkembangan ini memperlihatkan bahwa teknologi digital telah membuka peluang baru dalam produksi informasi intelijen (Sarjito, 2024). Namun demikian, penggunaan OSINT juga menghadapi berbagai tantangan, seperti penyebaran informasi palsu, manipulasi data, propaganda, dan disinformasi yang sengaja dilakukan untuk mempengaruhi opini publik. Oleh karena itu, setiap informasi yang diperoleh dari sumber terbuka harus melalui proses verifikasi yang ketat agar dapat digunakan sebagai dasar analisis yang valid. Tanpa proses verifikasi yang baik, informasi yang beredar justru dapat menimbulkan kesalahan dalam memahami situasi yang sebenarnya. Dengan demikian, efektivitas OSINT sangat bergantung pada kualitas metode analisis yang digunakan (Ramadhani, 2025).

Meskipun OSINT terbukti banyak digunakan dalam memantau perkembangan konflik Rusia-Ukraina, masih terdapat perdebatan mengenai sejauh mana metode tersebut efektif sebagai instrumen *early warning*. Sebagian pihak berpendapat bahwa OSINT berhasil memberikan gambaran yang cukup akurat mengenai kemungkinan invasi Rusia sebelum perang dimulai. Namun, sebagian lainnya menilai bahwa keberhasilan tersebut tidak dapat dilepaskan dari dukungan berbagai sumber informasi lain yang digunakan dalam proses analisis. Perbedaan pandangan tersebut menunjukkan bahwa peran OSINT dalam sistem peringatan dini masih memerlukan kajian yang lebih mendalam. Penelitian mengenai efektivitas OSINT menjadi penting untuk memahami kontribusinya dalam mendukung deteksi ancaman dan pengambilan keputusan di bidang keamanan. Selain itu, penelitian ini juga dapat memberikan gambaran mengenai kelebihan dan keterbatasan penggunaan sumber informasi terbuka dalam menghadapi konflik internasional. Berdasarkan uraian tersebut, penelitian yang berjudul "Peran Open Source Intelligence (OSINT) Sebagai *early warning* Ukraina Menjelang Invasi Rusia Februari Tahun 2022" penting dilakukan untuk menganalisis bagaimana OSINT dimanfaatkan dalam mendeteksi tanda-tanda awal invasi Rusia serta menilai efektivitasnya sebagai instrumen peringatan dini dalam konteks keamanan internasional.

2. METODE PENELITIAN

Penelitian ini melakukan pendekatan kualitatif yang menggunakan desain deskriptif-analitis sebagai dasar. Metode pengumpulan data dilakukan dengan meninjau literatur tentang: (1) artikel jurnal terkemuka yang membahas OSINT, *warning intelligence*, dan perang Rusia-Ukraina; (2) buku dan laporan lembaga kajian strategis tentang perang hibrida Rusia dan transformasi intelijen; dan (3) analisis konseptual studi kasus OSINT terkait ukraina.

Data dikumpulkan melalui studi literatur, yang berarti mengumpulkan berbagai sumber sekunder yang relevan dengan topik penelitian. Beberapa sumber data yang digunakan termasuk artikel jurnal ilmiah, buku dan buku elektronik, laporan organisasi atau lembaga yang bergerak di bidang keamanan dan intelijen, artikel berita dari media kredibel, serta berbagai publikasi yang membahas OSINT, studi intelijen, dan konflik Rusia. Karya teoritis tentang de-monopolisasi intelijen dan kebangkitan OSINT (Van Puyvelde & Tabárez Rienzi, 2025; Dokman & Ivanjko, 2020; Rønn & Ördén, 2025) dan studi empiris tentang peringatan intelijen dalam perang Ukraina (Gustafson et al., 2024; Stone et al., 2024; Belghith et al., 2022) adalah sumber utama yang kami gunakan. Struktur situasional dibangun dari literatur tentang konteks strategis perang hibrida Rusia (Lanoszka, 2016; Galeotti, 2016; Fox, 2021; Fábián, 2019).

Ada tiga tahap yang kami analisis dari data tersebut. Pertama, kami mengumpulkan dan memilih literatur yang relevan dengan OSINT, *early warning*, dan konflik Rusia-Ukraina.

Kemudian kami membagi tema menjadi beberapa kelompok: (a) konsep dasar OSINT dan *early warning*; (b) hubungan OSINT dengan sistem peringatan dini; (c) indikasi persiapan invasi Rusia yang terdeteksi melalui OSINT; (d) peran OSINT sebagai *early warning* bagi Ukraina dalam konflik; serta (e) keterbatasan OSINT sebagai instrumen peringatan dini. Ketiga, dilakukan analisis deskriptif untuk mengidentifikasi pola, keterkaitan, serta potensi kontradiksi dalam temuan literatur. Tahap ini bertujuan untuk merumuskan argumentasi mengenai peran OSINT sebagai sistem peringatan dini dalam konflik Rusia-Ukraina secara lebih komprehensif.

Metode ini tidak melakukan klaim kausal yang melampaui kapasitas data, melainkan memungkinkan integrasi antara kerangka teoritis studi intelijen dan hubungan internasional dengan hasil empiris dari berbagai sumber tentang konflik Rusia-Ukraina.

3. HASIL DAN PEMBAHASAN

Konsep OSINT dan *early warning*

Open-Source Intelligence (OSINT) merupakan disiplin intelijen yang mengandalkan pengumpulan dan analisis informasi dari sumber-sumber yang tersedia secara terbuka untuk umum, bukan dari teknik pengumpulan rahasia. Secara legal-formal, definisi OSINT yang banyak dirujuk dalam undang-undang dan literatur intelijen Amerika Serikat menyebutnya sebagai intelijen yang dihasilkan dari informasi yang tersedia secara publik, lalu dikumpulkan, diolah, dan disebarkan secara tepat waktu kepada audiens yang sesuai untuk memenuhi kebutuhan intelijen tertentu (Public Law 109-163, dikutip dalam PMC, 2023). Definisi ini kemudian disempurnakan oleh Coulthart dan Nussbaum melalui kajian literatur sistematis, yang merumuskan OSINT sebagai informasi publik atau komersial yang diperoleh secara legal, telah divalidasi, dianalisis, dan disebarluaskan untuk memenuhi kebutuhan intelijen (Springer, 2025). Uni Eropa pun mengonstruksikan OSINT secara serupa sebagai praktik pengumpulan dan analisis informasi dari sumber terbuka untuk menghasilkan intelijen yang dapat ditindaklanjuti, dengan catatan penting bahwa OSINT berbeda dari sekadar informasi sumber terbuka (open-source information/OSINF) karena melalui proses sistematis berupa pengumpulan, pengolahan, dan distribusi (Cambridge Core, 2025). Di Indonesia, pemahaman serupa juga berkembang, di mana OSINT dipahami sebagai praktik pengumpulan, analisis, dan pemanfaatan informasi dari sumber terbuka untuk mendukung pengambilan keputusan dalam berbagai bidang, baik keamanan nasional, penegakan hukum, maupun kecerdasan bisnis (Indonesiana, 2023).

Sumber OSINT bersifat sangat luas dan beragam, mencakup publikasi akademik, jurnal ilmiah, media sosial, komunitas daring, surat kabar, dokumen pemerintah, hingga peta dan citra geospasial (ResearchGate, 2021). OSINT sendiri pada awalnya muncul dari kebutuhan militer untuk mengumpulkan informasi publik yang relevan, sebagaimana terlihat dari sejarah panjangnya sejak Perang Dunia II ketika Foreign Broadcast Information Service Amerika Serikat ditugaskan menyadap, menerjemahkan, dan menganalisis siaran radio negara musuh demi memperoleh informasi strategis (PMC, 2023). Dalam konteks pengamatan militer kontemporer, salah satu sumber OSINT yang paling berpengaruh adalah imagery intelligence (IMINT) komersial, di mana perusahaan swasta seperti Maxar Technologies menyediakan citra satelit yang dapat diakses publik dan media massa untuk memantau aktivitas pergerakan militer di suatu wilayah (RFE/RL, 2022; Military Times, 2021). Selain citra satelit, unggahan masyarakat sipil di platform media sosial seperti Twitter dan Telegram juga menjadi sumber penting yang memungkinkan verifikasi silang atas klaim resmi pemerintah maupun media, sebagaimana dilakukan oleh kelompok investigasi sipil seperti Bellingcat yang kini lebih memilih istilah *open-source investigation* (OSINV) untuk membedakan praktik mereka dari intelijen pemerintah maupun korporasi (Cambridge Core, 2025; Centre for Information Resilience, 2025).

Sebagai sebuah disiplin intelijen, OSINT memiliki karakteristik khas, yaitu sifatnya yang legal dan dapat diakses tanpa otorisasi khusus, transparan karena dapat diverifikasi ulang oleh pihak lain, serta bersumber dari data yang terus diperbarui secara masif oleh aktor non-negara seperti jurnalis, peneliti independen, dan masyarakat sipil. Literatur kajian intelijen bahkan menyebutkan bahwa OSINT kini menyumbang sekitar 70 hingga 90 persen dari seluruh material intelijen kontemporer yang digunakan oleh lembaga penegak hukum dan badan intelijen di negara-negara Barat, sebuah proporsi yang terus meningkat seiring berkembangnya teknik

penambangan data, pembelajaran mesin, dan forensik visual (PMC, 2023). Namun demikian, OSINT juga memiliki keterbatasan, antara lain risiko bias informasi, potensi disinformasi, serta ketergantungan pada interpretasi analis dalam menyaring data yang relevan dari volume informasi yang sangat besar, sehingga keandalannya sangat bergantung pada proses verifikasi multisumber sebelum dijadikan dasar pengambilan kebijakan strategis (Putra, Kusumastuti, & Ma'arif, 2023).

Berbeda dengan OSINT, *early warning* atau peringatan dini adalah suatu sistem yang dirancang untuk mendeteksi, menganalisis, dan menyebarkan informasi terkait potensi ancaman sebelum ancaman tersebut terjadi atau berkembang menjadi krisis, dengan tujuan memberi waktu yang cukup bagi pihak berwenang maupun masyarakat untuk mengambil langkah antisipatif (ScienceDirect, 2024). Secara konseptual, sistem peringatan dini yang efektif terdiri atas empat elemen utama, yaitu pengetahuan risiko (*risk knowledge*), pemantauan (*monitoring*), kemampuan response (*response capability*), dan komunikasi peringatan (*warning communication*) (PMC, 2025). Dalam konteks keamanan dan pertahanan, konsep peringatan dini konflik telah berevolusi melalui beberapa generasi, dari pendekatan kualitatif dan terdesentralisasi pada awal tahun 2000-an, menuju pendekatan generasi keempat sejak 2015 yang bersifat kuantitatif dan memanfaatkan multilapisan data spasial, mulai dari penginderaan jauh berbasis satelit hingga media sosial, untuk menghasilkan indikasi dini atas potensi konflik (Stability Journal, 2022).

Keterkaitan antara OSINT dan sistem peringatan dini terletak pada fungsi keduanya yang sama-sama berorientasi pada deteksi indikasi ancaman sebelum eskalasi penuh terjadi. Sistem peringatan dini berbasis OSINT dapat melengkapi dan bahkan memperbaiki performa sistem pengawasan formal dengan memungkinkan deteksi dini atas peristiwa serius, terutama ketika sistem pelaporan resmi mengalami keterlambatan atau ketidaktersediaan data (PMC, 2023). Dalam kasus krisis Rusia–Ukraina, kombinasi antara citra satelit komersial dan unggahan masyarakat sipil di media sosial memungkinkan publik, jurnalis, maupun lembaga think tank untuk memantau secara langsung pergerakan pasukan Rusia, sehingga OSINT secara efektif berfungsi sebagai instrumen peringatan dini yang melengkapi bahkan dalam beberapa aspek menyamai kecepatan intelijen rahasia negara (Tandfonline, 2024).

Indikasi Persiapan Invasi Rusia yang Terdeteksi Melalui OSINT

Sejak akhir tahun 2021, OSINT berbasis citra satelit komersial mulai mendeteksi peningkatan aktivitas militer Rusia yang signifikan di wilayah-wilayah yang berdekatan dengan perbatasan Ukraina. Citra satelit yang dirilis oleh Maxar Technologies pada November 2021 memperlihatkan elemen-elemen dari Tentara Gabungan ke-41 Rusia, termasuk ratusan tank dan *self-propelled artillery*, yang terkonsentrasi di area pelatihan Yelnya, sekitar 160 mil dari perbatasan Rusia-Ukraina (Military Times, 2021). Maxar diketahui menyediakan sekitar 90 persen kebutuhan citra geospasial dasar yang digunakan oleh pemerintah Amerika Serikat, sehingga data ini menjadi rujukan penting bagi analis maupun media internasional dalam memantau eskalasi (RFE/RL, 2022). Memasuki Desember 2021, indikasi tersebut berkembang menjadi mobilisasi pasukan yang lebih nyata: pejabat Ukraina memperkirakan lebih dari 90.000 personel militer Rusia telah dikerahkan di sepanjang perbatasan, termasuk di Semenanjung Krimea, sementara estimasi intelijen Amerika Serikat memprediksi jumlah tersebut dapat mencapai 175.000 personel, menjadikannya salah satu mobilisasi pasukan Rusia terbesar dalam beberapa tahun terakhir di luar latihan militer terjadwal yang biasa diumumkan secara resmi (RFE/RL, 2022). Citra satelit lanjutan yang dirilis pada akhir Desember 2021 dan Januari 2022 memperkuat temuan ini dengan memperlihatkan unit-unit baru bertaraf kekuatan batalion di area pelatihan dekat Valuyki, Rusia, hanya berjarak sekitar 15 kilometer dari perbatasan, serta penempatan pasukan dan perlengkapan tambahan di area pelatihan Opuk, Krimea (Military Times, 2021, 2022).

Indikasi yang lebih konkret atas persiapan operasi militer kemudian terlihat dari kemunculan infrastruktur pendukung pasukan, bukan sekadar kendaraan tempur semata. Pada awal Februari 2022, Maxar Technologies melaporkan bahwa tenda dan tempat penampungan personel telah teramati di hampir setiap lokasi penempatan di Belarus, Krimea, dan wilayah barat

Rusia, yang mengindikasikan bahwa unit-unit tersebut kini disertai oleh personel sungguhan dan telah meningkatkan tingkat kesiapan operasionalnya (Deccan Herald, 2022). Selain itu, citra satelit pada awal Februari 2022 juga mengonfirmasi penempatan pasukan dan persenjataan di Belarus, termasuk pesawat tempur Su-25 dan sistem pertahanan udara S-400 di lapangan udara Luninets yang berlokasi sekitar 50 kilometer dari perbatasan Ukraina, bersamaan dengan pengumuman latihan militer gabungan Rusia–Belarus bertajuk "Union Resolve 2022" (Reuters via Inquirer, 2022). Akumulasi data OSINT ini berjalan paralel dengan eskalasi tensi diplomatik antara Rusia dan negara-negara Barat: pembangunan kekuatan militer yang terungkap melalui citra satelit mendorong terjadinya komunikasi tingkat tinggi, termasuk panggilan video antara Presiden Joe Biden dan Presiden Vladimir Putin pada awal Desember 2021 untuk membahas kekhawatiran atas pergerakan pasukan Rusia (RFE/RL, 2022; Fox News, 2021). Laporan intelijen resmi Amerika Serikat pun menguatkan temuan OSINT tersebut, di mana sejak Oktober 2021 badan-badan intelijen AS telah mengindikasikan kemungkinan adanya "serangan strategis signifikan", yang memicu serangkaian pertemuan tingkat tinggi di Gedung Putih (Tandfonline, 2024). Kombinasi antara temuan OSINT yang dapat diverifikasi secara publik dan intelijen rahasia negara inilah yang pada akhirnya membentuk pemahaman kolektif komunitas internasional bahwa Rusia secara serius mempersiapkan invasi skala penuh terhadap Ukraina, yang pada akhirnya benar-benar terjadi pada 24 Februari 2022.

Peran OSINT sebagai *Early Warning* bagi Ukraina

Dalam konflik Rusia-Ukraina, kemampuan untuk mendeteksi ancaman sejak dini menjadi faktor penting dalam menentukan kesiapan Ukraina dalam menghadapi eskalasi konflik yang dilakukan oleh Rusia. Dalam hal ini, OSINT hadir sebagai salah satu sumber informasi yang dapat memberikan *early warning* terhadap perkembangan situasi keamanan dengan waktu yang cukup singkat. Kalau biasanya intelijen tradisional yang umumnya bersifat tertutup, OSINT memanfaatkan berbagai sumber informasi yang dapat diakses publik, seperti citra satelit komersial, media sosial, laporan media, hingga data geospasial yang tersedia secara terbuka. Sejak April 2021, mobilisasi pasukan Rusia di perbatasan Ukraina telah terdeteksi melalui berbagai sumber informasi terbuka, termasuk unggahan media sosial warga sipil dan citra satelit komersial (Van Beek & Rietjens, 2024). Artinya, pemanfaat sumber-sumber tersebut membantu Ukraina dalam menganalisis dan menemukan indikasi peningkatan aktivitas militer Rusia sebelum invasi dimulai pada Februari 2022.

Salah satu bentuk penggunaan OSINT sebagai *early warning* terlihat dari penggunaan citra satelit komersial yang berhasil menunjukan adanya peningkatan konsentrasi pasukan Rusia di wilayah dekat perbatasan Ukraina. Sejumlah perusahaan satelit berkala merilis gambar kondisi kerusakan infrastruktur, keberadaan kendaraan tempur, pembangunan *camp*, hingga pergerakan logistik yang cukup masif. Salah satunya dari gambar citra satelit Planet Labs PBC yang menunjukan adanya penumpukan pasukan militer di Yelnya, Rusia pada 2 Februari 2022. Hal ini memungkinkan para peneliti tidak hanya mengidentifikasi kerusakan infrastruktur, tetapi juga melacak dan mengidentifikasi pergerakan pasukan melalui citra satelit (*How OSINT Shaped Reporting on the War in Ukraine - Centre for Information Resilience*, 2025). Keberadaan data satelit yang dapat diakses oleh berbagai pihak juga membuat informasi mengenai perkembangan situasi bisa dianalisis oleh berbagai pihak tidak hanya negara dan intelijen.

Selain citra satelit, media sosial menjadi sumber informasi yang banyak dimanfaatkan dalam proses pemantauan. Melalui unggahan foto atau video dari warga sipil yang kerap memperlihatkan tempat atau pergerakan dari pasukan militer Rusia. Seperti yang dilakukan oleh seorang *pro* Rusia yang membagikan gambar melalui telegram yang menunjukan lokasi paramiliter Rusia. Beberapa hari setelah foto tersebut diunggah ke internet, pasukan Ukraina kemudian menghancurkan markas itu hingga berubah menjadi reruntuhan (Van Beek & Rietjens, 2024). Media sosial dipenuhi oleh konten yang menunjukkan pergerakan militer Rusia dan dampak perang, di mana warga dengan ponsel berperan sebagai sensor yang merekam aktivitas militer secara *real-time* (Aldhous & Miller, 2022). Informasi yang berasal dari warga sipil pada akhirnya mampu memberikan gambaran yang lebih luas mengenai situasi di lapangan.

Namun demikian, informasi dari sumber terbuka tidak selalu dapat langsung digunakan tanpa proses verifikasi. Oleh karena itu, komunitas OSINT berperan penting dalam melakukan pengecekan terhadap keaslian informasi yang beredar. Organisasi seperti Bellingcat dan Conflict Intelligence Team (CIT) telah lama memanfaatkan teknik geolokasi dan verifikasi waktu untuk memastikan keakuratan foto maupun video yang beredar di internet. Setiap informasi yang ditemukan tidak langsung diterima begitu saja, melainkan diperiksa kembali dengan mencocokkan lokasi, waktu, serta konteks kejadian sebelum digunakan sebagai dasar analisis. Hal ini terlihat saat menjelang invasi Februari 2022, para analis berhasil mengidentifikasi persiapan militer Rusia, termasuk perpindahan personel militer menggunakan jalur kereta api sipil, hanya melalui pengamatan unggahan di media sosial (Kivimäki, 2026). Niu et al. (2024) mencatat bahwa percakapan dan distribusi informasi oleh akun-akun OSINT di Twitter mencapai puncaknya pada 24 Februari 2022. Kondisi ini menunjukkan bahwa komunitas OSINT tidak hanya berfungsi sebagai pengumpul informasi, tetapi juga sebagai mekanisme verifikasi yang membantu menyaring informasi yang kredibel di tengah derasnya arus informasi digital selama konflik berlangsung.

Secara keseluruhan, OSINT memiliki peran signifikan dalam mendukung *early warning* pada invasi Rusia terhadap Ukraina pada Februari 2022. Berbagai informasi terbuka seperti citra satelit komersial, media sosial, hingga laporan media memungkin indikasi invasi lebih awal teridentifikasi. Pemanfaatan sumber-sumber terbuka ini memperlihatkan bahwa informasi yang tersedia secara publik dapat diolah menjadi bahan analisis strategis dalam membaca dinamika keamanan. Meskipun demikian, penggunaan OSINT tetap memerlukan proses verifikasi untuk memastikan keakuratan informasi. Dengan demikian, OSINT dapat dipahami sebagai instrumen pendukung intelijen modern untuk melengkapi pendekatan intelijen tradisional dalam kasus konflik kontemporer yang terbuka dan berbasi digital.

Keterbatasan OSINT sebagai *Early warning*

Meskipun OSINT terbukti mampu membantu mendeteksi berbagai indikasi awal invasi Rusia ke Ukraina, penggunaan OSINT sebagai instrumen *early warning* masih memiliki sejumlah keterbatasan. Salah satu keterbatasan utama adalah bahwa informasi yang berhasil diperoleh melalui OSINT tidak selalu mampu mencegah terjadinya ancaman yang telah terdeteksi. Berbagai informasi mengenai pengerahan pasukan Rusia dan peningkatan aktivitas militer di sekitar perbatasan Ukraina memang telah diketahui sebelum invasi dimulai. Namun, informasi tersebut tidak mampu menghentikan Rusia untuk tetap melancarkan invasi pada Februari 2022. Kondisi ini menunjukkan bahwa OSINT lebih berperan dalam memberikan gambaran situasi dan meningkatkan kesiapsiagaan dibandingkan sebagai alat untuk mencegah terjadinya konflik secara langsung (Marleku, 2025).

Selain itu, efektivitas OSINT juga sangat bergantung pada bagaimana informasi yang dihasilkan diterima oleh para pengambil keputusan. Informasi yang akurat tidak selalu langsung dipercaya atau dijadikan dasar tindakan. Dalam kasus Rusia-Ukraina, beberapa negara pada awalnya masih meragukan berbagai peringatan yang disampaikan mengenai kemungkinan invasi Rusia (Marleku, 2025). Akibatnya, informasi yang sebenarnya dapat digunakan untuk mempersiapkan respons lebih awal tidak selalu dimanfaatkan secara optimal. Hal ini menunjukkan bahwa keberhasilan sistem peringatan dini tidak hanya ditentukan oleh kualitas informasi, tetapi juga oleh tingkat kepercayaan terhadap informasi tersebut.

Keterbatasan lainnya adalah adanya risiko misinformasi dan bias data. Sebagian besar informasi OSINT berasal dari sumber terbuka seperti media sosial, situs berita, forum internet, dan berbagai platform digital lainnya. Informasi yang beredar melalui sumber-sumber tersebut tidak selalu benar dan terkadang sengaja dimanipulasi oleh pihak tertentu untuk mempengaruhi opini publik maupun menyesatkan analisis lawan (Karakikes & Kotis, 2025). Oleh karena itu, setiap informasi yang diperoleh melalui OSINT harus melalui proses verifikasi yang ketat sebelum digunakan sebagai dasar analisis.

Selain risiko misinformasi, OSINT juga menghadapi tantangan berupa jumlah informasi yang sangat besar. Perkembangan teknologi digital menyebabkan data dari berbagai sumber terbuka terus bertambah setiap saat. Banyaknya informasi yang tersedia sering kali menyulitkan

proses analisis karena tidak semua data memiliki tingkat relevansi yang sama. Permasalahan terkait kualitas data, verifikasi informasi, dan besarnya volume data yang harus dianalisis dapat mengurangi efektivitas OSINT dalam menghasilkan peringatan dini secara cepat dan akurat (Karakikes & Kotis, 2025).

Di samping itu, semakin berkembangnya penggunaan OSINT juga memunculkan berbagai upaya untuk melemahkan kredibilitasnya. Beberapa pihak berusaha menyebarkan propaganda, disinformation, maupun narasi tertentu untuk mengaburkan fakta yang sebenarnya. Bahkan terdapat upaya untuk mendiskreditkan organisasi maupun komunitas yang melakukan investigasi berbasis OSINT (Colley & Dylan, 2025). Kondisi ini dapat mempersulit proses pengumpulan dan verifikasi informasi sehingga mempengaruhi kualitas hasil analisis yang dihasilkan.

Berdasarkan berbagai keterbatasan tersebut, OSINT tidak dapat digunakan sebagai satu-satunya sumber dalam sistem peringatan dini. OSINT lebih tepat digunakan sebagai pelengkap intelijen tradisional karena mampu menyediakan informasi secara cepat dan terbuka. Dengan mengkombinasikan OSINT dan sumber intelijen lainnya, proses identifikasi ancaman dapat dilakukan secara lebih komprehensif sehingga mendukung pengambilan keputusan yang lebih tepat

4. SIMPULAN

Penelitian ini menemukan bahwa OSINT sangat penting sebagai mekanisme peringatan dini sebelum dan selama invasi Rusia ke Ukraina pada Februari 2022. Berbagai indikator awal, seperti mobilisasi pasukan Rusia, peningkatan eskalasi konflik, dan potensi ancaman keamanan lainnya, dapat diidentifikasi dengan menggunakan berbagai sumber informasi terbuka, seperti gambar satelit komersial, media sosial, berita online, dan intersepsi radio berbasis web. Kehadiran OSINT menunjukkan bahwa kemampuan mendeteksi ancaman dapat diperkuat dengan menggunakan data terbuka yang dapat diakses oleh berbagai aktor, baik negara maupun non-negara.

Secara teoritis, kemajuan OSINT lebih baik dipahami sebagai perkembangan dalam praktik intelijen dan proses untuk melepaskan monopoli produksi pengetahuan keamanan daripada sebagai bentuk demokratisasi yang sepenuhnya revolusioner. Meskipun OSINT telah mengurangi dominasi negara dalam pengumpulan dan analisis informasi strategis, itu tidak serta-merta menyelesaikan masalah penting seperti kekurangan sumber daya, kualitas, dan kebenaran informasi, serta kebutuhan untuk berintegrasi dengan sumber intelijen rahasia. Oleh karena itu, OSINT tidak dapat dianggap sebagai pengganti intelijen konvensional; sebaliknya, itu dapat dianggap sebagai instrumen yang membantu *Human Intelligence* (HUMINT), *Signal Intelligence* (SIGINT), dan *Imagery Intelligence* (IMINT).

OSINT tidak hanya berfungsi sebagai alat untuk mendeteksi ancaman dalam perang hibrida Rusia-Ukraina, tetapi juga menjadi tempat perebutan cerita dan informasi. Jurnalis investigasi, komunitas OSINT, media, dan masyarakat sipil berkontribusi pada verifikasi informasi melalui teknik geolokasi dan analisis lintas sumber. Ini memungkinkan mereka untuk membangun basis fakta yang mempengaruhi opini publik internasional. Namun, pada saat yang sama, ruang informasi juga berfungsi sebagai media untuk praktik disinformasi, propaganda, dan operasi deception, yang merupakan ciri khas perang hibrida kontemporer.

Kasus Ukraina menunjukkan bahwa keberhasilan sistem peringatan dini tidak hanya tergantung pada kemampuan untuk mendeteksi ancaman melalui OSINT, tetapi juga pada kemampuan institusional dan kemauan politik untuk mengubah informasi yang diperoleh menjadi kebijakan dan tindakan pencegahan yang efektif. Jika tidak diikuti oleh mekanisme respons yang memadai, informasi yang akurat tidak akan memiliki nilai strategis. Oleh karena itu, pada akhirnya, keberhasilan peringatan dini bergantung pada kemampuan negara dan aktor terkait untuk memasukkan informasi ke dalam proses pengambilan keputusan.

Secara keseluruhan, penelitian ini menyatakan bahwa OSINT telah menciptakan model produksi informasi yang lebih terbuka dan terlibat, yang telah mengubah dunia studi intelijen dan keamanan internasional saat ini. Namun, demokratisasi informasi OSINT hanya akan menghasilkan visibilitas yang tidak memiliki efek strategis jika tidak didukung oleh integrasi

dengan intelijen tertutup, mekanisme verifikasi yang kuat, dan kerangka respons politik yang kuat. Akibatnya, untuk menghadapi ancaman keamanan yang semakin kompleks dan hibrida di era digital, sangat penting bagi Ukraina dan komunitas internasional untuk membangun sistem peringatan dini yang dapat disesuaikan dan terintegrasi yang melibatkan OSINT, intelijen konvensional, dan kemampuan respon institusional.

5. DAFTAR PUSTAKA

Aldhous, P., & Miller, C. (2022). *How Open-Source Intelligence Is Helping Clear The Fog Of War In Ukraine*. BuzzFeed News. https://www.buzzfeednews.com/article/peteraldhous/osint-ukraine-war-satellite-images-plane-tracking-social

Azzahra, K., Triyanti, A., & Desi, Y. (2025). Media sosial dan tantangan di era digital. *Jurnal Pengabdian Masyarakat dan Riset Pendidikan, 4*(1), 1625–1629. https://doi.org/10.31004/jerkin.v4i1.1793

Anjelina, D. (2023). Fenomena Serangan Siber Rusia Terhadap Ukraina: Sebagai Pembelajaran Bagi Indonesia Dalam Pengembangan Pertahanan Siber. *Jurnal Pertahanan & Bela Negara*. https://doi.org/10.33172/jpbh.v13i3.14307

Adlini, M. N., Dinda, A. H., Yulinda, S., Chotimah, O., & Merliyana, S. J. (2022). Metode Penelitian Kualitatif Studi Pustaka. *Edumaspul: Jurnal Pendidikan*. https://doi.org/10.33487/edumaspul.v6i1.3394

Böhm, I., & Lolagar, S. (2021). Open source intelligence. *International Cybersecurity Law Review, 2*, 317 - 337. https://doi.org/10.1365/s43439-021-00042-7

Colley, T., & Dylan, H. (2025). The war on open-source intelligence. *The Washington Quarterly, 48*(3), 147–162. https://doi.org/10.1080/0163660X.2025.2554477

Collier, S., & Walsh, P. F. (2024). Commercial satellites, OSINT, and the war in Ukraine: Redefining the intelligence-policy nexus. *Intelligence and National Security*, *39*(2), 189–207. https://doi.org/10.1080/02684527.2023.2254131

DHNS. (2022, February 3). *New satellite images show massive Russian forces near Ukraine border*. Deccan Herald. https://www.deccanherald.com/archives/new-satellite-images-show-massive-russian-forces-near-ukraine-border-1077624-1450848

Dover, C. (2023). Verification in the digital age: How open-source intelligence challenges disinformation in contemporary conflicts. *Media, War & Conflict*, *16*(3), 312–329. https://doi.org/10.1177/17506352231164091

Edwards, J. (2021, December 28). *Satellite images track new Russian military deployments near Ukraine*. Military Times. https://www.militarytimes.com/flashpoints/2021/12/27/satellite-images-track-new-russian-military-deployments-near-ukraine/

Evangelista, J. R. G., Sassi, R. J., Romero, M., & Napolitano, D. (2020). Systematic Literature Review to Investigate the Application of Open Source Intelligence (OSINT) with Artificial Intelligence. *Journal of Applied Security Research*, *16*(3), 1–25. https://doi.org/10.1080/19361610.2020.1761737

Firdaus, M., Argenti, G., & Gustianti, N. (2025). Invasi militer Rusia ke Ukraina pada tahun 2022: Tujuan, alasan, dan implikasi. *Jurnal Ilmiah Wahana Pendidikan, 11*(9.D), 142–154.

Fowler, M. (2024). Intelligence and operational warning: lessons from Ukraine. *Journal of Policing, Intelligence and Counter Terrorism, 19*, 501 - 518. https://doi.org/10.1080/18335330.2024.2319128

Ghioni, R., Taddeo, M., & Floridi, L. (2023). Open source intelligence and AI: a systematic review of the GELSI literature. *AI & SOCIETY*. https://doi.org/10.1007/s00146-023-01628-x

Ghofur, M. J. U., & Nikhlis, N. (2025). Early detection of data theft on mobile devices using machine learning. *Jurnal Ilmiah Sistem Informasi (JUSI), 4*(2), 110–129. https://doi.org/10.51903/fz0xzt26

Gunawan, F., Imilda, & Keumala, T. M. M. (2024). Analisis information gathering target daftar pencarian orang menggunakan metode open source intelligence pada Kejaksaan Tinggi Aceh. *Jurnal Sistem Komputer (SISKOM), 4*(1), 10–21.

Gustafson, K., Lomas, D., & Wagner, S. (2024). Intelligence warning in the Ukraine war, Autumn 2021 – Summer 2022. *Intelligence & National Security*, *39*(3), 1–20. https://doi.org/10.1080/02684527.2024.2322214

Giegerich, B., & Terlikowski, M. (2023). Open-source intelligence and the war in Ukraine: Democratic revolution or tactical evolution? *International Affairs*, *99*(4), 1435–1452. https://doi.org/10.1093/ia/iiad120

Gustafson, K., Lomas, D., Wagner, S., Abdalla, N., & Davies, P. (2024). Intelligence warning in the Ukraine war, Autumn 2021 – Summer 2022. *Intelligence and National Security, 39*, 400 - 419. https://doi.org/10.1080/02684527.2024.2322214

Husein, M., & Sudiarto, T. D. (2024). Diplomasi luar negeri Indonesia yang bebas dan aktif dalam perang Rusia-Ukraina selama masa presidensi G20 di Indonesia. *Arus Jurnal Sosial dan Humaniora, 4*(3), 1237–1245.

How OSINT shaped reporting on the war in Ukraine - Centre for Information Resilience. (2025, March 4). Centre for Information Resilience; CIR. https://www.info-res.org/eyes-on-russia/articles/how-osint-shaped-reporting-on-the-war-in-ukraine/

Hassan, I., & Pomerantsev, P. (2023). Hybrid warfare and the battle for the narrative: OSINT, disinformation, and civil society in Ukraine. *Journal of Democracy*, *34*(1), 78–92. https://doi.org/10.1353/jod.2023.0005

Hartono, A. (2022). Evaluasi Layanan Perpustakaan Perguruan Tinggi Seni di Tengah Pandemi: Studi Kasus Layanan UPT Perpustakaan ISI Yogyakarta. *ABDI PUSTAKA: Jurnal Perpustakaan dan Kearsipan*. https://doi.org/10.24821/jap.v2i1.6987

Karakikes, A., & Kotis, K. (2025). AI-assisted OSINT/SOCMINT for safeguarding borders: A systematic review. *Information, 16*(12), 1095. https://doi.org/10.3390/info16121095

Kivimäki, V.-P. (2026). *Open Source Information as a Window into the War in Ukraine* (K.

Liuhto & J. Sipilä, Eds.). Springer Nature Switzerland. https://doi.org/10.1007/978-3-032-11892-9

Kotaridis, I., & Benekos, G. (2023, September 21). https://securityanddefence.pl/pdf-170901-94539?filename=Integrating+Earth.pdf&utm_source=consensu

Lavinia, N., & P. (2023). Urgensi Pemanfaatan Open Source Intelligent (Osint) Dalam Upaya Pencegahan Aksi Terorisme Di Indonesia. *Jurnal Sosial Humaniora Terapan*. https://doi.org/10.7454/jsht.v6i1.1105

Marleku, A. (2025). Public intelligence as a strategic tool: The role of real-time intelligence disclosure in the Ukraine War. *Security and Defence Quarterly, 50*(2). https://doi.org/10.35467/sdq/205566

Mitchell, W. (2025). Assessing Deception Projection via OSINT: The Case of the Ukraine 2022 Counter-Offensive. *Journal of Applied Operational Intelligence*. https://doi.org/10.5750/jaoi.v1i1.2266

Niu, J., Stillman, M., Seeberger, P., & Kruspe, A. (2024). A dataset of Open Source Intelligence (OSINT) Tweets about the Russo-Ukrainian war. *ArXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2409.01052

Norman, G. (2022, February 2). *Russia-Ukraine conflict: Satellite images reveal extent of Moscow's military buildup*. Fox News. https://www.foxnews.com/world/russia-ukraine-conflict-satellite-images-reveal-extent-of-military-buildup

Omand, D. (2022). The new age of open-source intelligence: How social media and digital tracking reshaped the war in Ukraine. *Foreign Affairs*, *101*(3), 24–31.

Open Source Intelligence: Pengertian, Manfaat, Kegunaan, Contoh, dan Masalah Hukum. (2023). Indonesiana.id. https://www.indonesiana.id/read/169276/open-source-intelligence-pengertian-manfaat-kegunaan-contoh-dan-masalah-hukum

Paluvi, R., & Nasution, M. I. P. (2025). Pemrosesan dan analisis big data: Peluang dan tantangan dalam dunia industri. *Jurnal Sains Student Research, 3*(3), 341–350. https://doi.org/10.61722/jssr.v3i3.4744

Parawita, A., Yura, E., Andrian, E., Pratama, F. A., Nasar, & Barella, Y. (2025). Konflik Rusia-Ukraina (Sejarah, resolusi, serta manajemen konflik). *Maeswara: Jurnal Riset Ilmu Manajemen dan Kewirausahaan, 3*(1), 147–161. https://doi.org/10.61132/maeswara.v3i1.1611

Putra, S., & Kusumastuti, B. (2023). Potensi Ancaman Penggunaan OSINT Menyebabkan Kegagalan Pengambilan Keputusan Akibat Informasi Hoax. *Jurnal Kajian Stratejik Ketahanan Nasional*, *6*(2). https://doi.org/10.7454/jkskn.v6i2.10081

Puyvelde, D. V., & Rienzi, F. T. (2025). The rise of open-source intelligence. *European Journal of International Security*, 1–15. https://doi.org/10.1017/eis.2024.61

Ramadhani, S. (2025). Analisis penyebaran informasi palsu dan ujaran kebencian di media sosial Indonesia: Studi kasus berita hoax dan hate speech. *PUBLISTIK: Riset Jurnalistik dan Komunikasi Media, 2*(1), 28–34.

Reuters. (2022, February). *Satellite images show troops at the Ukraine border ahead of Russia-Belarus drills*. INQUIRER.net. https://newsinfo.inquirer.net/1550877/satellite-images-show-troops-at-ukriane-border-ahead-of-russia-belarus-drills

RFE/RL. (2021, December 7). *Boots On The Ground: Satellite Images Reveal Russian Troop Buildup Near Ukrainian Border And In Crimea*. RadioFreeEurope/RadioLiberty; RFE/RL. https://www.rferl.org/a/russia-ukraine-troop-buildup-satellite-imagery/31598141.html

Riyanta, S., & Permatasari, D. A. (2025). Kontraintelijen pada era kontemporer dalam mencegah ancaman intelijen asing dan implikasinya terhadap ketahanan wilayah Ibu Kota Nusantara di Kalimantan Timur.

Rovner, J. (2023). Intelligence, warning, and the war in Ukraine: Why political response remains the weakest link. *Strategic Studies Quarterly*, *17*(2), 45–61.

Samudro, E. G., Sjamsoeddin, S., & Santoso, A. (2024). Sistem deteksi dini dalam pencegahan konflik sosial di Provinsi Daerah Istimewa Yogyakarta. *Civil and Military Cooperation Journal, 1*(1), 11–18.

Sarjito, A. (2024). Hoaks, disinformasi, dan ketahanan nasional: Ancaman teknologi informasi dalam masyarakat digital Indonesia. *Journal of Governance and Local Politics (JGLP), 6*(2), 175–186.

ScienceDirect. (2024). *early warning System - an overview | ScienceDirect Topics*. Www.sciencedirect.com. https://www.sciencedirect.com/topics/computer-science/early-warning-system

Sitanggang, Z. S. (2024). Analisis perkembangan jaringan terorisme dalam perspektif hukum dan ancaman global akibat penyebaran terorisme di Indonesia. *Jurnal Pacta Sunt Servanda, 5*(2).

Stone, H., Heslop, D., Lim, S., & Sarmiento, I. (2023). *early warning System - an overview | ScienceDirect Topics*. Www.sciencedirect.com. https://www.sciencedirect.com/topics/computer-science/early-warning-system

Sudiq, R. D., & Yustitianingtyas, L. (2022). Intervensi Rusia terhadap Ukraina pada tahun 2022 sebagai pelanggaran berat HAM. *Jurnal Pendidikan Kewarganegaraan Undiksha, 10*(3), 101–117.

Szymoniak, S., & Foks, K. (2024). Open Source Intelligence Opportunities and Challenges: a Review. *Advances in Science and Technology Research Journal*. https://doi.org/10.12913/22998624/186036

Udayana, A. (2025). Dampak perang Rusia-Ukraina terhadap hubungan diplomatik antara Indonesia dan Rusia. *Diplomacy and Global Security Journal, 2*(1), 108–136. https://doi.org/10.36859/dgsj.v2i1.3495

Van Beek, H., & Rietjens, S. (2024). Open-Source Intelligence in the Russia-Ukraine War. In M.

Rothman, L. Peperkamp, & S. Rietjens (Eds.), *Reflections on the RussiaUkraine War* (pp. 57–76). Leiden University Press; JSTOR. https://doi.org/10.2307/jj.13760045.7

Van Puyvelde, Fernando Tabárez RienziVan Puyvelde, Fernando Tabárez Rienzi, D. (2025, January 7). https://www.cambridge.org/core/services/aop-cambridge-core/content/view/21122432399ECB8078BF0D89A76D0586/S2057563724000610a.pdf/div-class-title-the-rise-of-open-source-intelligence-div.pdf?utm_source=consensus

Varzhanskyi, I. (2023). Reflexive Control as a Risk Factor for Using OSINT: Insights from the Russia–Ukraine Conflict. *International Journal of Intelligence and CounterIntelligence, 37*, 419 - 449. https://doi.org/10.1080/08850607.2023.2228489