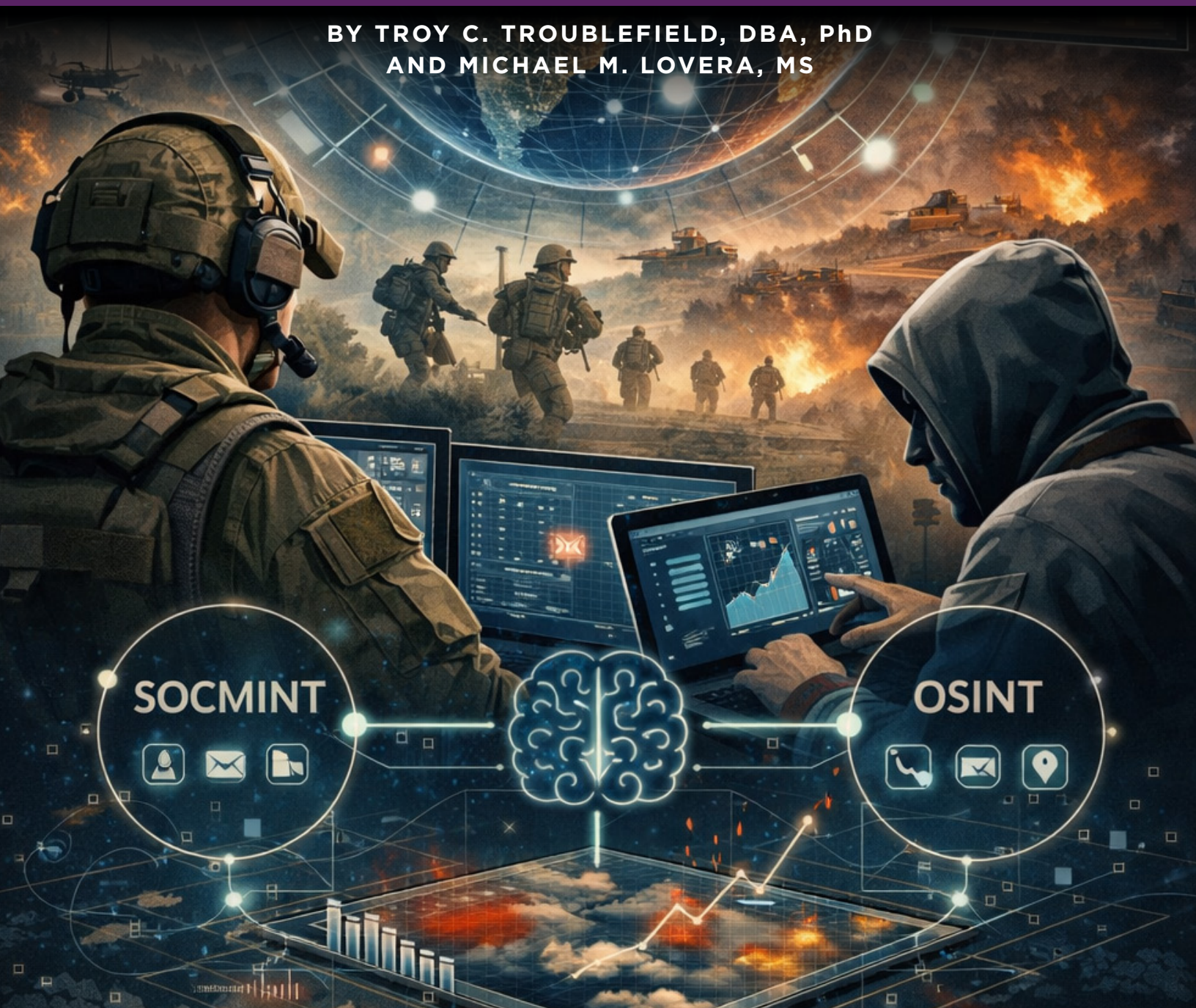
OCCASIONAL PAPER

JSOU PRESS

LEVERAGING SOCIAL MEDIA INTELLIGENCE AND OPEN-SOURCE INTELLIGENCE FOR AI-DRIVEN PREDICTIVE ANALYTICS IN IRREGULAR WARFARE

BY TROY C. TROUBLEFIELD, DBA, PhD
AND MICHAEL M. LOVERA, MS



On the cover:

AI-enabled fusion of social media intelligence and open-source intelligence in irregular warfare has the ability to transform the modern irregular warfare battlespace. Multisource digital data, network analytics, and predictive models converge to map decentralized adversary networks, forecast narrative and behavioral shifts, assess population sentiment, and support precision decision-making across the cognitive, informational, and physical dimensions of the modern battlespace. Source: Image generated by author using ChatGPT, March 26, 2026.

JSOU Press
Melanie Casey, Editor in Chief
Beth DeGeorge, Editor
Alina Alvarez Perez, Editor
Arianna Czesler, Designer
Rebecca Kurk, Designer

Digital Version

JSOU Report 26-7
Published April 2026

Leveraging Social Media Intelligence and Open-Source Intelligence for AI-Driven Predictive Analytics in Irregular Warfare

BY TROY C. TROUBLEFIELD, DBA, PhD AND MICHAEL M. LOVERA, MS

JSOU PRESS

Abstract

In an era of persistent irregular conflict, social media intelligence (SOCMINT) has evolved as a subdiscipline of open-source intelligence (OSINT). As hybrid threats expand to include both attributed and non-attributed gray-zone actors, there are substantial implications when it comes to AI predictive analytics, narrative forecasting, and the follow-on analysis to support policymakers and operations personnel. Within the irregular construct, characterized by non-state actors, asymmetric tactics, and sub-threshold violence, SOCMINT and OSINT provide critical data streams that enhance machine learning models for understanding insurgent networks, violent extremist narratives, and population-centric dynamics. How do these intelligence domains inform AI-driven predictive systems in support of special operations, psychological operations (PSYOP), counterinsurgency (COIN), and countering violent extremism (CVE) missions? Analysis explores operational frameworks, methodological integration, and implications for irregular warfare (IW) practitioners while addressing challenges including adversarial manipulation, information authenticity, and ethical governance in complex operational environments.

Introduction

Advancements in IW have historically catalyzed broader military evolution. The adoption of guerrilla tactics by American revolutionary militias, for example, foreshadowed the end of conventional line-formation battles. In the 21st century, this pattern continues with the leveraging of OSINT by Ukrainian forces, allowing them to execute "find, fix, finish" missions with notable effectiveness against the Russian Federation. This dynamic underscores the deeply symbiotic relationship between the information environment and IW.

SOCMINT and OSINT are critical components in understanding and addressing irregular operations within warfare. SOCMINT focuses on extracting actionable insights from social media platforms, offering visibility into insurgent networks, ideological narratives, population sentiment, and operational planning. OSINT complements this by leveraging publicly available data such as local media, academic research, and human rights documentation to provide historical, geopolitical, and cultural context. Together, these intelligence disciplines enable a nuanced understanding of irregular threats, bridging real-time signals with broader contextual analysis. The ability to rapidly circulate intelligence and operational lessons through the information domain is not merely beneficial—it is fundamental to achieving strategic objectives. These objectives include shaping perceptions, influencing key audiences, and, ultimately, destabilizing an adversary's coalition and will to fight.[1] In response, advanced intelligence frameworks such as SOCMINT and OSINT, combined with AI, are redefining how IW intelligence is gathered, analyzed, and acted upon.

The shift toward AI-driven intelligence represents a paradigm change in IW, empowering analysts with tools that extract granular insights from decentralized networks, predict adversarial behavior, and interpret evolving population sentiment.

Machine learning (ML) and natural language processing (NLP) technologies amplify intelligence operations by identifying pre-violence indicators, mapping insurgent digital footprints, evaluating the resonance of adversarial narratives, and foreseeing strategic adaptations by irregular actors. SOCMINT enables real-time intelligence collection and analysis by monitoring social network activity, encrypted communications, and propaganda dissemination while OSINT provides critical geopolitical context through academic research, human rights documentation, and economic data.[2] Together, the integration of these systems strengthens operational capabilities, enabling practitioners to decode complex IW environments that traditional intelligence alone cannot effectively address.

The importance of multisource data fusion, combining SOCMINT, OSINT, human intelligence (HUMINT), signals intelligence (SIGINT), and geospatial intelligence (GEOINT), further establishes AI-powered platforms as indispensable for IW intelligence. These systems unify disparate data streams, aligning the cognitive dimension with ground-truth validation and operational insights.[3] Predictive modeling and feature engineering across behavioral, network, and narrative metrics provide actionable outputs for COIN, CVE efforts, and PSYOP. As adversaries employ advanced deception techniques (e.g., deepfakes, encrypted channels, bot networks), the ability to annotate malign networks, track their expansion, and convey this to the target system is paramount to cognitive resilience in friendly populations and avoiding unintended collateral harm (i.e., blowback). The ongoing evolution of these technologies highlights the essential role of AI in shaping the future of IW intelligence.

SOCMINT enables real-time intelligence collection and analysis by monitoring social network activity, encrypted communications, and propaganda dissemination while OSINT provides critical geopolitical context through academic research, human rights documentation, and economic data.

Social Media Intelligence and Open-Source Intelligence for Irregular Warfare Operations

SOCMINT plays a critical role in irregular operations by systematically extracting actionable insights from conventional and encrypted platforms, such as Telegram, Signal, X, and local networks like VKontakte or WeChat. In IW, SOCMINT enables network identification, sentiment analysis, narrative tracking, and early warning detection to penetrate the cognitive domain of non-state actors and influence operations. Paired with OSINT, which provides socio-cultural, historical, and geopolitical context through public datasets like media reports, non-governmental organization (NGO) documentation, and ethnographic studies, these intelligence tools form a cohesive framework for understanding and countering

adversaries in asymmetric environments. This hybrid approach ensures nuanced threat mapping while enabling both real-time action and strategic decision-making.

Social Media Intelligence in Irregular Operations

In IW, the role of SOCMINT involves systematically collecting, analyzing, and exploiting data from diverse social media platforms, including encrypted messaging services (Telegram, Signal), regional platforms (VKontakte, WeChat), and global mainstream networks (X, Facebook, Instagram). Unlike traditional intelligence approaches focused on state actors with hierarchical command systems, SOCMINT in irregular contexts operates with priorities distinctively suited to the asymmetrical nature of such conflicts. These include network identification, where insurgent, terrorist, and violent extremist organization (VEO) cells are mapped through advanced social graph analysis to discern operational structures; narrative tracking, which monitors how ideological messages, recruitment content, and propaganda evolve and propagate to shape adversarial messaging; sentiment analysis, assessing public attitudes toward groups like governments, coalitions, or other adversaries, and their competing narratives; and early warning indicators, which detect mobilization efforts, operational planning signals, or coordinated threats.

SOCMINT demonstrates unparalleled operational value by penetrating the cognitive domain, revealing insights into adversary morale, strategic intent, and communication strategies that are often invisible to conventional intelligence disciplines. By leveraging SOCMINT in tandem with OSINT, which offers contextual depth via sources such as local news, ethnographic research, and NGO reporting, IW practitioners craft a cohesive framework to understand adversaries in real time and account for socio-political dimensions of their activities.

By leveraging SOCMINT in tandem with OSINT, irregular warfare practitioners craft a cohesive framework to understand adversaries in real time and account for socio-political dimensions of their activities.

For example, while SOCMINT provides actionable signals on insurgent narratives or mobilization efforts, OSINT contextualizes these insights by framing them within historical grievances, economic tensions, or communal conflicts. This dual approach creates not only a precise operational picture but also ensures nuanced anticipation of enemy action, further enabling COIN, CVE, and PSYOP efforts.[4]

The integration of SOCMINT and OSINT is further enhanced using AI frameworks, which enable predictive analytics for irregular operations. Through ML models, SOCMINT fuels advanced systems that detect pre-violence indicators such as spikes in hate speech, geographic coordination in messaging, or escalation in propagandist

rhetoric. AI tools like graph neural networks (GNNs) enable mapping of insurgent networks, identifying "hub nodes" that represent influential leaders, "bridge nodes" that connect operationally distinct groups, and key ideological amplifiers who are central to recruiting and radicalization campaigns.[5] These insights not only inform targeting efforts, such as the disruption of critical nodes through surgical operations, but also provide structured outputs to measure operational success through battle damage assessments (BDAs), moving away from traditional anecdotal metrics.

AI also scales narrative-tracking functions through NLP models that monitor public receptiveness to competing messages, helping practitioners adapt PSYOP to neutralize extremist narratives and foster favorable sentiment among local populations. Additionally, the integration of analytical tools like multimodal transformers further optimizes SOCMINT capabilities by analyzing adversarial messaging across multimedia formats such as text, video, and audio, with applications extending beyond sentiment tracking to pre-positioning of counternarratives.

In IW, the modern battlefield is cognitively driven, with the information space playing a pivotal role in shaping both operational dynamics and strategic objectives. SOCMINT, paired with advanced AI-driven analytics and harmonized with OSINT context, ensures that IW practitioners penetrate these cognitive domains effectively, enabling decision-makers to influence perceptions, preempt adversarial plans, and dynamically adjust strategies in response to rapidly evolving threats.

Open-Source Intelligence for Irregular Threat Understanding

OSINT is a cornerstone in the intelligence architecture of IW, offering valuable insights through publicly available datasets, including local media outlets, diaspora communities, academic research on conflict zones, NGO reports, satellite imagery, and digital repositories documenting insurgent activity. Its contributions are multi-dimensional, providing historical context, geopolitical framing, and socio-cultural understanding essential for decoding the operational signals identified through SOCMINT. For instance, OSINT enables IW practitioners to contextualize SOCMINT-derived indicators, such as spikes in recruitment propaganda, within broader narratives of socio-political grievances, resource competition, or human rights violations.[6]

Key OSINT sources in COIN and CVE operations include localized news coverage that reveals grievance narratives linked to political or governance failures; academic ethnographies that probe deep tribal, sectarian, or communal fault lines; and human rights reports documenting state oppression that fuels recruitment efforts among disenfranchised populations. Additionally, economic data highlighting resource disparities, territorial disputes, or logistical vulnerabilities complement OSINT efforts by framing insurgent motivations in terms of material conditions, not solely ideological drivers. Together, these inputs help practitioners identify recruitment triggers, analyze underlying causes of unrest, and

strategically address vulnerabilities driving radicalization.

The symbiotic relationship between OSINT and SOCMINT is pivotal to IW intelligence. While SOCMINT enables real-time operational signals, such as monitoring insurgent communication trends, detecting mobilization signals, or tracking propaganda dissemination, OSINT delivers the underlying scaffolding necessary for accurate interpretation of these signals. For example, SOCMINT may pinpoint a surge in online recruitment activity after an economic disruption, but OSINT contextualizes this by highlighting local unemployment patterns or resource scarcity that exacerbates grievances. Together, these domains form a cohesive intelligence framework, empowering IW operations that span from tactical interventions to strategic influence campaigns. When further integrated into AI-driven platforms, OSINT enhances predictive analytics capabilities, allowing practitioners to anticipate insurgent recruitment patterns, map foreign fighter flows, and evaluate how adversarial narratives resonate with population sentiment.

AI Predictive Analytics in Irregular Warfare Operations

Predictive analytics models powered by SOCMINT and OSINT are critical tools in IW operations, enabling practitioners to anticipate adversary actions, assess risks, and optimize strategic responses across key mission sets. These models integrate advanced ML algorithms to detect pre-violence indicators, such as spikes in rhetoric or geographic keyword clustering, providing early warnings of potential threats. Additionally, by mapping network structures and analyzing communication patterns, these systems identify high-value nodes including influencers, bridge connectors, or narrative amplifiers, essential for disrupting insurgent or extremist networks with targeted interventions. Furthermore, these tools enhance influence operations by predicting shifts in population sentiment and adversarial narrative resonance, allowing operators to dynamically adapt psychological campaigns and counter-messaging strategies to neutralize extremist propaganda effectively.[7]

> **SOCMINT enables real-time operational signals...OSINT delivers the underlying scaffolding necessary for accurate interpretation of these signals.**

Threat Forecasting and Pre-Violence Detection

ML algorithms analyze historical attack patterns, social media chatter intensity, and contextual triggers (political events, religious holidays, military operations) to forecast insurgent activity. Features such as message frequency spikes, violent rhetoric escalation, and geographic keyword clustering serve as leading indicators of imminent operations.[8] AI models can predict improvised explosive device emplacement locations, suicide bomber recruitment phases, and militant

mobilization windows, enabling proactive force protection and preemptive interdiction.

GNNs have emerged as critical tools within IW analytics, enabling the accurate identification and mapping of organizational structures within decentralized insurgent networks. By training these models on SOCMINT data, AI systems can uncover intricate relationships among insurgents by analyzing communication patterns, content-sharing behaviors, and temporal coordination. These advanced capabilities classify key network roles into three categories:

1. **Hub nodes:** high-influence individuals responsible for coordinating operational cells
2. **Bridge nodes:** individuals who connect otherwise separate groups within the network and facilitate operational communication or resource sharing
3. **Ideological amplifiers:** content creators whose propaganda or recruitment materials drive radicalization and mobilization across broader audiences.[9]

Targeting these identified critical nodes transforms IW operational strategy and creates openings to degrade adversarial capabilities systematically. For instance, when using layered kinetic effects, such as precision air strikes, alongside non-kinetic approaches like PSYOP, the structural integrity of insurgent networks can be undermined without resorting to inefficient attritional models. This strategy maximizes operational impact by disrupting vital connections and leadership nodes, directly impairing the adversary's ability to coordinate, expand, or regroup effectively.

Furthermore, this data-driven approach changes how the intelligence community evaluates mission success. Traditional metrics reliant on anecdotal evidence or unrepeatable operational successes are replaced with the precise language of BDAs. BDAs enable intelligence practitioners to quantify the adversarial network's systemic degradation objectively, assessing measurable impacts such as reduced operational capabilities, compromised communication flows, or diminished recruitment pipelines. This rigorous methodology ensures that assessments are both consistent and applicable across diverse IW contexts, bolstering decision-making processes and enabling adaptable strategies to counter evolving threats.

AI systems can uncover intricate relationships among insurgents by analyzing communication patterns, content-sharing behaviors, and temporal coordination.

Narrative Warfare and Influence Operations Assessment

NLP models assess narrative resonance, tracking how competing storylines (government legitimacy, sectarian grievance, foreign intervention framing) propagate through populations. In PSYOP, sentiment analysis functions as an early gauge, helping to predict which messages will be effective and which will fall flat. This initial feedback directly informs campaign design. However, this process is analogous to a corporation like Nike testing a new marketing slogan:

While positive initial sentiment is a good sign, it is only a starting point. To ensure a campaign's success, the assumptions drawn from that sentiment must be rigorously tested and confirmed through ongoing intelligence and continuous adaptation.[10]

Analytical Frameworks for Irregular Warfare Intelligence

Multi-source data fusion architectures combine diverse intelligence sources, such as SOCMINT, OSINT, HUMINT, SIGINT, and GEOINT, to deliver comprehensive situational awareness in IW contexts. AI-driven platforms facilitate this integration through advanced techniques like entity disambiguation, temporal synchronization, and source reliability scoring, enabling more accurate threat detection and understanding. Predictive modeling, rooted in features like behavioral patterns, network dynamics, and narrative metrics, further enhances operational decision-making. Specialized ML architectures, including temporal convolutional networks (TCNs), graph attention networks (GATs), and multimodal transformers, optimize data fusion by analyzing complex insurgent activities and countering adversarial manipulation strategies.

Multi-Source Data Fusion Architectures

In the context of IW, effective intelligence assessments rely on the integration of SOCMINT and OSINT with other critical intelligence disciplines such as HUMINT, SIGINT, and GEOINT.[11] AI-powered fusion platforms act as a central mechanism to combine these multisource inputs into a unified operational picture, enhancing the accuracy and timeliness of IW decision-making. HUMINT provides essential ground-level insights and serves as a validation mechanism for the information extracted from SOCMINT platforms, ensuring that online indicators correspond to actionable realities on the ground. Meanwhile, SIGINT refines analysts' understanding of communication patterns and reveals details about adversarial coordination within targeted networks, such as encrypted transmissions or frequency spikes. GEOINT, on the other hand, enables the precise geolocation of activities by leveraging geo-tagged posts or imagery, helping intelligence analysts correlate digital activities with physical locations.

AI-powered fusion platforms act as a central mechanism to combine these multisource inputs into a unified operational picture, enhancing the accuracy and timeliness of irregular warfare decision-making.

This multi-modal integration resolves ambiguities that are often present when relying on a single intelligence source, as each discipline complements the limitations of others. For instance, SOCMINT might identify an insurgent propaganda effort on social media, but its full operational significance might only be uncovered through the corroboration provided by SIGINT interceptions or HUMINT reporting.

AI platforms enhance this synergy by employing confidence scoring mechanisms that assess the reliability and consistency of various sources, ensuring that actionable intelligence is presented with high accuracy. Additionally, these platforms use advanced tools like temporal synchronization to align intelligence inputs in real time, enabling practitioners to deliver a coherent, multi-dimensional perspective on adversarial capabilities and intent. This holistic approach not only strengthens situational awareness but also fosters more informed and agile responses to the dynamic challenges of IW.[12]

Feature Engineering for Irregular Threat Detection

Predictive analytics in IW leverages features extracted from SOCMINT and OSINT data streams to identify emerging threats, assess network behavior, understand narrative trajectories, and anticipate adversary actions. These features fall into three key domains: behavioral indicators, network dynamics, and narrative metrics. Behavioral indicators provide early warning signals by analyzing patterns such as operational security (OPSEC) degradation, which often precedes attacks, cross-platform coordination highlighting operational readiness, and the dissemination of martyrdom content, which is strongly associated with imminent suicide operations. These indicators allow for proactive interdiction strategies to disrupt adversarial plans at their formative stages.

Network dynamics focus on understanding the structural elements and evolution of insurgent or extremist networks. Features such as sudden fragmentation within a network can signal leadership elimination,

Predictive analytics in irregular warfare irregular warfare leverages features extracted from SOCMINT and OSINT data streams to identify emerging threats, assess network behavior, understand narrative trajectories, and anticipate adversary actions.

while increased bridging activity between previously isolated cells may indicate heightened levels of coordination or resource sharing. Additionally, patterns in foreign fighter integration reveal global recruitment and logistical flows, essential for anticipating transnational threats. These dynamics provide actionable insights, enabling operational strategies to disrupt critical nodes and pathways within adversary networks.

Narrative metrics are equally vital in tracking the cognitive domain. Advanced analytics measure the intensity of grievance narratives to evaluate the velocity of radicalization within a target population. Counter-narrative effectiveness is assessed by monitoring sentiment shifts, gauging the impact of PSYOP on neutralizing extremist messaging. Furthermore, attribution of information operations is supported through linguistic stylometry, which identifies unique adversarial text patterns and links them to specific actors. Combined, these narrative insights inform the design of tailored influence campaigns to limit adversarial

propaganda's spread while amplifying countervailing messages.

By integrating these predictive features, AI-driven systems empower IW practitioners to craft more precise and impactful strategies. These tools provide real-time decision support, enabling IW forces to neutralize threats effectively while adapting dynamically to changes in adversary behavior and narratives.

Machine Learning Architectures for Irregular Warfare

Specialized AI architectures have revolutionized intelligence workflows in IW by enhancing the ability to detect, analyze, and counter unconventional threats. TCNs capture long-range dependencies in insurgent activity cycles, seasonal operational patterns, and the evolution of broader campaigns by identifying periodic trends or emerging spikes in activity tied to specific events.[13]

This allows intelligence analysts to forecast key operational periods and prioritize resource allocation accordingly. GATs provide a tailored approach to modeling heterogeneous insurgent networks, mapping nodes that represent individuals, locations, and ideological factions with varying relationship complexities, such as direct communications, shared goals, or overlapping resources. This functionality enables the identification of critical network components, such as high-influence operators or connecting nodes critical to hierarchical or decentralized systems.[14]

Multimodal transformers further enhance the analysis of SOCMINT-relevant data by integrating and interpreting text, imagery, video, and audio from propaganda materials. By assessing sophisticated production techniques and coherence in messaging across multiple media types, these AI models evaluate the strategic aims of adversarial influence campaigns, helping practitioners design counternarratives and assess adversary communication hierarchies.[15] Additionally, robust adversarial models provide vital capabilities for addressing deliberate manipulation efforts, such as fake accounts, bot-driven amplification, and the circulation of deceptive information. These models actively detect and counter these efforts, ensuring intelligence accuracy while bolstering the credibility of operational insights.[16]

In collaboration with broader multisource data fusion architectures that integrate SOCMINT, OSINT, HUMINT, SIGINT, and GEOINT, these AI-powered systems provide a unified operational framework. They utilize tools like entity disambiguation, temporal synchronization, and reliability scoring to enhance situational awareness and threat assessments. When combined with predictive feature engineering across behavioral, network, and narrative metrics, models like TCNs, GATs, and multimodal

Specialized AI architectures have revolutionized intelligence workflows in irregular warfare by enhancing the ability to detect, analyze, and counter unconventional threats.

transformers refine intelligence workflows by identifying patterns and relationships, capturing temporal dynamics, and countering adversarial manipulation strategies with precision. This synergy ensures robust, adaptable intelligence operations suited to the complexities of modern IW environments.

Operational Case Applications in Irregular Warfare

COIN population sentiment monitoring uses SOCMINT analytics to track grievances and predict insurgent recruitment surges, enabling targeted intervention by civil affairs (CA) and PSYOP teams.[17] OSINT-SOCMINT fusion models play a key role in forecasting foreign fighter flow patterns by analyzing travel logistics, recruitment signals, and coordination routes. Influence campaign effectiveness and VEO evolution are assessed through AI-driven sentiment tracking, network analysis, and predictive modeling, allowing proactive adaptations to messaging and counternarratives.[18]

Counterinsurgency Population Sentiment Monitoring

During operations in Afghanistan and Iraq, SOCMINT analytics revealed that population grievance escalation correlated with specific military operations or governance failures.[19] AI models trained on local language social media predicted which districts would experience insurgent recruitment surges, enabling CA and PSYOP teams to preempt radicalization through targeted engagement programs.[20]

Foreign Fighter Flow Prediction

European counterterrorism agencies utilized OSINT-SOCMINT fusion models to address the growing challenge of foreign fighter mobilization toward conflict zones like Syria and Iraq. By monitoring discussions on travel routes, analyzing logistical coordination signals, and mapping recruitment network activity, predictive analytics enabled accurate forecasting of border-crossing patterns. This intelligence supported the development of interdiction strategies, including targeted enforcement at critical transit points and the adaptation of entry/exit screening protocols to identify suspicious movements effectively. Furthermore, these models play a role in disrupting broader recruitment processes by revealing the digital and logistical pathways that insurgent groups leverage to mobilize fighters. By combining real-time SOCMINT signals with contextual OSINT data, agencies were able to preempt operational threats and adjust law enforcement tactics to minimize the flow of foreign fighters into active conflict zones.[21]

Influence Campaign Effectiveness Assessment

U.S. Special Operations Command (USSOCOM) effectively employs AI-driven SOCMINT analytics to enhance the real-time evaluation of PSYOP campaign effectiveness. Through sentiment tracking, AI systems pinpoint which messages resonate most strongly with target audiences, enabling PSYOP strategists to emphasize impactful narratives and refine fewer effective ones. Network analysis reveals organic amplifiers—individuals or groups with significant

outreach potential—who can be recruited as surrogates to disseminate favorable messaging and expand influence campaigns. Predictive models add a proactive dimension by forecasting adversarial counter-messaging strategies, allowing operators to pre-position tailored narratives that undermine opposition efforts. Additionally, this dynamic adaptability ensures campaigns remain relevant to evolving operational contexts, strengthening the cognitive dimension of IW through sustained influence and information dominance.[22]

Violent Extremist Organization Evolution Tracking

AI models analyzing jihadist SOCMINT effectively identified a critical shift in Islamic State of Iraq and Syria (ISIS) strategic messaging, transitioning from territorial caliphate narratives to insurgency and virtual caliphate frameworks following its territorial losses. This predictive insight enabled CVE practitioners to proactively address resurgent themes through pre-positioned counternarratives, undermining their traction before they could mobilize widespread support. By closely monitoring digital communications and propaganda flows, these models further revealed the narrative tactics ISIS employed to sustain legitimacy among its global supporters, even as its physical presence diminished. Moreover, this intelligence informed tailored intervention strategies that targeted specific audience groups vulnerable to such messaging, enhancing the precision of CVE efforts. As a result, CVE operations leveraged these predictive capabilities to disrupt ISIS's ability to consolidate influence within virtual networks, thereby reducing recruitment effectiveness and global outreach.[23] This predictive insight enabled CVE practitioners to pre-position counternarratives addressing resurgent messaging themes before they achieved widespread traction.

Challenges in Irregular Warfare Intelligence Environments

Adversarial actors in IW are increasingly adept at countering intelligence efforts through encryption, disinformation, and deceptive tactics, requiring AI models to detect and adapt to manipulation attempts. Operating in low-resource language and cultural contexts necessitates methods like transferring learning, synthetic data, and validation by native experts to ensure analytical accuracy.[24] Ethical considerations are critical in population-centric operations, demanding strict standards for data collection, safeguards against misuse, and measures to prevent discrimination or misclassification. Additionally, addressing deepfakes and fabricated content requires robust authenticator systems to maintain the integrity of SOCMINT analysis.

Adversarial Awareness and Deception

Irregular adversaries in IW demonstrate increasing sophistication in countering intelligence collection by employing methods such as encrypted messaging, ephemeral content, and deception campaigns that include false accounts and disinformation. Honeypots, deliberately manipulated data or systems designed to lure and mislead analysts, further complicate intelligence efforts, often expending valuable resources and time.[25] To combat

these tactics, AI models need advanced adversarial learning capabilities to detect and adapt to such manipulation attempts while ensuring analytical accuracy. These systems must account for emerging threats like deepfakes and bot-driven amplification, integrating authenticity verification mechanisms to maintain the intelligence streams. Additionally, robust adversarial frameworks are necessary to analyze malicious SOCMINT patterns effectively, neutralize manipulated narratives, and provide actionable intelligence for operational decisions.

Low-Resource Language and Cultural Contexts

Many IW environments involve challenges stemming from low-resource languages, dialects, and complex cultural contexts that are poorly represented in AI training datasets. To overcome these limitations, transfer learning from high-resource languages can be employed and allow AI models to adapt insights from well-documented linguistic data to areas with fewer resources. Additionally, synthetic data augmentation techniques expand training datasets by creating realistic examples of speech or text, improving the model's accuracy in diverse linguistic environments. Human-in-the-loop validation by native speakers ensures that AI systems correctly interpret nuances of language and culture, reducing risks of misclassification or cultural misinterpretation. This multi-faceted approach not only enhances intelligence workflows but also builds trust and operational effectiveness in IW contexts characterized by linguistic and cultural diversity.[26]

Ethical Considerations in Population-Centric Operations

IW is fundamentally population-centric, as its success hinges on cultivating legitimacy and support among civilian populations. However, the extensive use of SOCMINT introduces significant ethical challenges, including risks of civilian privacy violations, the potential misidentification of non-combatants as threats, and the misuse of intelligence by repressive government partners to target political dissidents. To mitigate these risks and ensure ethical operations, robust frameworks and safeguards must be implemented throughout SOCMINT processes. These frameworks demand adherence to strict standards of necessity and proportionality in data collection, ensuring that intelligence actions are measured and warranted based on operational relevance and severity.[27]

Protections against the misuse of intelligence by partner nations are imperative, as IW often involves multinational collaborations where local authorities may exploit shared intelligence to suppress dissent or marginalize ethnic, tribal, or religious groups. Additionally, bias audits must be routinely conducted to verify that AI-driven SOCMINT models do not inadvertently reinforce discriminatory practices or systemic biases against specific populations. Without such audits, predictive analytics may classify vulnerable communities unfairly, exacerbating societal rifts and undermining IW objectives.

Transparency also plays a critical role in maintaining accountability and legitimizing intelligence operations. Mechanisms such as oversight committees and interpretability

models allow stakeholders to review targeting decisions, ensuring that interventions adhere to ethical imperatives and avoid collateral harm. Collectively, these safeguards align IW intelligence efforts with international norms and human rights while protecting the trust of civilian populations, a crucial factor for sustainable strategic success in population-based IW environments.

Attribution and Information Authenticity

Deepfakes, fabricated evidence, and synthetic personas significantly degrade the reliability of SOCMINT streams, particularly in IW where adversaries exploit these tools to deliberately distort intelligence environments. To counter such challenges, provenance verification systems employ metadata analysis and cryptographic integrity checks to trace the origin and authenticity of digital information, reducing the risk of misinterpretation.[28] Blockchain-based authentication further strengthens data integrity by creating immutable, transparent transaction records that can validate the authenticity and source of SOCMINT artifacts. Forensic media analysis complements these efforts by using AI-driven tools to detect manipulation in images, audio, and videos, enabling intelligence practitioners to differentiate between legitimate content and adversarial disinformation. Combined, these measures ensure SOCMINT remains a reliable and actionable component of IW intelligence frameworks while minimizing vulnerabilities created by adversarial deception.

Mechanisms such as oversight committees and interpretability models allow stakeholders to review targeting decisions, ensuring that interventions adhere to ethical imperatives and avoid collateral harm.

Internet-Based Psychological Operations and Irregular Warfare Intelligence Integration

The proliferation of internet-based PSYOP aligns seamlessly with the intelligence frameworks discussed, particularly in the realm of IW. Modern IW places the cognitive domain at the forefront of conflict. Adversaries increasingly utilize the digital environment to shape perceptions, propagate ideological narratives, and mobilize populations against opposing forces. Integrating advanced SOCMINT and OSINT analytics with AI frameworks provides critical capabilities to address these dynamics. Internet-based PSYOP relies heavily on these intelligence disciplines to enhance precision-targeting, adapt strategies in real time, and counter adversarial messaging efforts effectively.[29]

The Role of Social Media Intelligence in Internet-Based Psychological Operations

SOCMINT's operational insights are invaluable to internet-based PSYOP campaigns. By systematically analyzing social media platforms, integrating encrypted messaging applications (e.g., Telegram

or Signal), region-specific platforms (e.g., VKontakte or WeChat), and mainstream networks (e.g., X, Facebook, or Instagram), SOCMINT enables real-time detection of evolving adversary narratives and sentiment shifts. For PSYOP practitioners, SOCMINT fulfills several critical roles:

1. **Narrative identification and dissemination:** SOCMINT monitors ideological evolution, recruitment materials, and propaganda flows to identify emerging adversary narratives. NLP-driven models assess how these narratives resonate across cultural and demographic lines, allowing PSYOP teams to counteract propaganda by pushing tailored counter-messaging.
2. **Sentiment analysis of target populations:** SOCMINT tracks and measures public attitudes toward government forces, insurgent groups, or coalition operations, offering rich data for PSYOP stratagem adjustments. Highlighting emotional triggers and grievance narratives aid in preempting radicalization or social dissent.
3. **Early warning mechanisms:** SOCMINT surfaces signals of mobilization or coordination tied to adversarial campaigns, enabling PSYOP teams to deploy countermeasures before insurgents capitalize on population unrest.

Through SOCMINT's capabilities, PSYOP efforts gain visibility into the cognitive dimensions of conflict, targeting populations with precision while thwarting insurgent messaging campaigns.[30]

Open-Source Intelligence's Contribution to Contextualizing Psychological Operations Efforts

OSINT complements SOCMINT by enriching internet-based PSYOP with deeper contextual intelligence. Open-source channels such as local media coverage, NGO reports, and academic research into sociopolitical dynamics allow PSYOP teams to better understand the historical and cultural dimensions that underpin adversarial messaging strategies. For example, in COIN operations, OSINT might identify grievances stemming from human rights abuses or resource shortages, narratives that insurgents exploit in recruitment materials.[31]

The integration of OSINT ensures that internet-based PSYOP campaigns stay culturally relevant and contextually accurate. Predictive models trained on OSINT inputs enable tailored engagement for specific populations, amplifying PSYOP messages that resonate while countering adversaries' exploitation of societal fault lines.[32]

AI Predictive Analytics: Enhancing Strategic Adaptability in Psychological Operations

AI enhances internet-based PSYOP by driving predictive analytics frameworks capable of anticipating adversary behavioral patterns and population responses. Algorithms leveraging SOCMINT and OSINT can forecast several critical parameters.

1. **Narrative trajectories:** NLP models assess adoption rates of adversarial narratives, allowing PSYOP strategists

to pre-position counternarratives before extremist messaging gains traction.

2. **Network dynamics:** AI-driven graph analytics identify key influencers or amplifiers within digital networks, offering PSYOP teams precise targets for engagement or disruption.
3. **Behavioral readiness:** Predictive models process OPSEC patterns, cross-platform coordination signals, and martyrdom content to detect upcoming insurgency operations, enabling preemptive messaging campaigns.

Through predictive intelligence, internet-based PSYOP campaigns remain agile and dynamically adapt to shifts in adversarial tactics and audience sentiment.[33]

Countering Adversarial Manipulation in the Digital Space

Internet-based PSYOP must navigate complex adversarial efforts to deceive and disrupt intelligence collection. Irregular actors deploy OPSEC tactics (e.g., encrypted messages, ephemeral content, etc.), initiate disinformation campaigns, and create honeypots to mislead analysts. AI models tailored for adversarial robustness play a crucial role here. Such models detect manipulated SOCMINT streams (e.g., deepfakes, bot activity, etc.), validate information authenticity, and help identify malicious narratives embedded within adversarial propaganda.[34] Furthermore, ethical frameworks integrated into AI-driven PSYOP workflows eschew biases, prevent collateral harm on non-combatant populations, and implement transparency mechanisms to ensure accountability during targeting decisions.

Operational Synergy: Fusion Architectures for Psychological Operations

The fusion of SOCMINT, OSINT, and other intelligence domains, facilitated by advanced AI frameworks, empowers internet-based PSYOP teams with multidimensional insights critical for modern IW. By integrating HUMINT, SIGINT, and GEOINT, AI platforms effectively create unified operational pictures that validate and refine intelligence. HUMINT confirms the credibility of narratives and key actors derived from digital signals, while SIGINT corroborates detected communication patterns to uncover adversarial coordination dynamics. GEOINT adds crucial spatial analysis, pinpointing insurgent movements and recruitment hotspots through geotagged data.

This multisource integration not only enables PSYOP teams to craft precisely targeted messaging strategies, but it also continuously refines these strategies based on feedback loops from firing unit reports, which serve as initial indicators for evaluating the effectiveness of these campaigns. Additionally, predictive modeling tools, leveraging SOCMINT and OSINT data streams, help identify narrative adoption rates and key amplification nodes within digital networks, enabling dynamic adjustments to PSYOP operations. Together, these capabilities ensure decision-makers maintain robust situational awareness while

systematically degrading adversary influence in the cognitive domain of conflict.[35]

Future Directions: Autonomous Intelligence Support for Irregular Warfare

The future of intelligence support in IW will increasingly depend on integrating autonomous AI tools with established intelligence frameworks such as SOCMINT, OSINT, HUMINT, SIGINT, and GEOINT. By creating adaptable and scalable systems capable of real-time analysis, prediction, and action, AI-driven platforms will enhance decision-making across key domains of IW intelligence: the cognitive terrain, adversary network mapping, population sentiment analysis, and influence operations. Key advancements are expected to shape autonomous intelligence support in IW environments, ensuring operational superiority in increasingly complex conflict zones.

Cognitive Warfare Analytics

Irregular adversaries prioritize cognitive vulnerabilities, employing influence campaigns and narrative manipulation to undermine trust, disrupt societal stability, and win legitimacy within target populations. Autonomous intelligence models will develop deeper insights into the cognitive dimensions of conflict by analyzing neuropsychological influence mechanisms embedded in adversarial propaganda and messaging. For example, with deep sentiment mapping, AI can enhance sentiment models that detect emotional, cultural, and psychological triggers with adversarial content, allowing analysts to counteract narratives that exploit fear, anger, or socioeconomic grievances. With behavioral dynamics modeling, AI systems can monitor and predict cognitive responses to specific propaganda tactics across diverse demographic groups, enabling precision-tuned PSYOP campaigns tailored to neutralize adversarial messaging. These cognitive warfare advancements will help IW practitioners dominate the "information battle," influencing perceptions and preempting adversaries in the psychological domain.

> **The fusion of SOCMINT, OSINT, and other intelligence domains, facilitated by advanced AI frameworks, empowers internet-based PSYOP teams with multidimensional insights critical for modern irregular warfare.**

Federated Intelligence Platforms for Multinational Irregular Warfare

IW often occurs in coalition contexts, where intelligence gathering and sharing between partner nations must balance OPSEC and sovereignty concerns. Federated learning architectures will emerge as key enablers for coalition intelligence collaboration. By allowing distributed AI models to train across multiple data centers without centralized aggregation, federated learning provides significant benefits, like enhanced predictive accuracy and operational efficiency. Models integrate diverse SOCMINT and OSINT data streams

from multinational contributors, improving analytic output while preserving the confidentiality of raw data. Furthermore, intelligence fusion across coalition networks offers shared insights into insurgent patterns without exposing sensitive national intelligence equities. This approach will enable seamless collaboration in IW while maintaining security and interoperability among partners.

Edge AI for Tactical Deployment in Austere Environments

Special operations forces (SOF) frequently operate in areas with unreliable network infrastructure, necessitating localized intelligence technologies. Edge computing-based AI models will enable units to conduct real-time SOCMINT and OSINT analysis directly on tactical devices. Features such as compressed deep learning models and low-power computation specialize these systems for deployment in denied or disconnected environments, allowing operators the ability to extract local intelligence through the analysis of insurgent digital activity, propaganda dissemination, and encrypted coordination signals at the point of collection and the operational autonomy to undertake SOCMINT-driven PSYOP or tactical shifts informed by localized insights without relying on centralized databases. Edge AI ensures intelligence operations remain agile, adaptive, and sustainable in resource-constrained conflict zones.

Quantum Machine Learning for Enhanced Pattern Recognition

As irregular adversaries adopt more robust countermeasures like quantum-resistant encryption, autonomous intelligence must respond with advanced computational tools. Quantum ML will offer significant advantages in pattern recognition and encrypted communication inference, enabling IW practitioners to identify concealed insurgent networks despite sophisticated OPSEC mechanisms and decode adversary strategies hidden across complex SOCMINT and OSINT streams with improved computational speed and accuracy. Quantum-enhanced AI will propel IW intelligence into a new era of analytical power, overcoming future encryption and obfuscation tactics used by irregular adversaries.

Human–Machine Teaming in Intelligence Operations

While autonomous systems play an increasingly critical role, human analysts remain essential for contextual judgment, operational oversight, and decision-making in IW intelligence. Human–machine teaming represents a hybrid future where AI-powered tools augment, rather than replace, analysts. Key aspects of this collaboration include:

- **Hypothesis generation:** AI systems automatically surface insights, trends, and anomalies for analysts to validate and refine.
- **Bias mitigation:** Human involvement ensures ethical oversight and prevents AI-driven conclusions from reinforcing cultural or demographic biases.
- **Rapid operational integration:** Analysts apply AI-derived outputs in real time, adapting intelligence workflows dynamically to mission needs.

Human–machine teaming ensures intelligence remains accurate, ethical, and actionable within IW campaigns.

Ethical Safeguards in Autonomous Intelligence

As IW intelligence increasingly relies on autonomous systems, ethical frameworks must evolve to prevent misuse and collateral harm. AI systems will incorporate transparency mechanisms such as interpretability models and accountability protocols, allowing real-time bias audits where autonomous intelligence outputs undergo continuous evaluation for discriminatory pattens or misclassification risks and civilian protections allowing ethical thresholds to guide data collection and analysis and prevent violations of privacy or overreach by partner nations. These safeguards ensure trust in AI systems while aligning IW operations with international norms and population-centric priorities.

Overall, autonomous intelligence support for IW is set to transform how conflicts are analyzed, predicted, and influenced by integrating advanced AI tools across SOCMINT and OSINT streams. From deep cognitive warfare analytics to quantum-enhanced inference and edge computing, future systems will empower IW practitioners to dominate the information dimension while adapting dynamically to adversarial countermeasures. By combining federated learning, ethical safeguards, and human-machine teaming, the next generation of autonomous intelligence platforms will optimize collaboration, precision, and ethical compliance in the most complex IW environments.

From deep cognitive warfare analytics to quantum-enhanced inference and edge computing, future systems will empower irregular warfare practitioners to dominate the information dimension while adapting dynamically to adversarial countermeasures.

Discussion

In contemporary IW, the convergence of SOCMINT and OSINT with AI-driven predictive analytics has transformed intelligence frameworks. This integration offers unmatched precision in identifying, understanding, and countering threats posed by non-state actors, insurgents, and violent extremism. SOCMINT, through its real-time analysis of social platforms, enables network mapping, sentiment analysis, and narrative tracking, while OSINT provides essential socio-cultural and geopolitical contexts for interpreting these signals effectively. Together, these intelligence domains bridge the gap between real-time operational signals and broader contextual insights, creating a holistic approach to IW intelligence.

Multisource intelligence fusion is a cornerstone of modern IW operations, combining diverse inputs from SOCMINT,

OSINT, HUMINT, SIGINT, and GEOINT into unified analytical platforms. HUMINT validates digital narratives by grounding them in real-life observations, SIGINT corroborates adversarial communication networks, and GEOINT refines target locations using geotagged data. The synergy among these sources enables IW practitioners to craft cohesive messaging strategies for PSYOP while ensuring precision targeting to counter adversarial influence campaigns effectively.

One significant application of AI in IW is narrative warfare. NLP models now analyze the resonance of competing storylines, such as grievance-based narratives or foreign intervention framing, to predict their adoption among target populations. This insight allows PSYOP teams to develop tailored counternarratives and assess their impact dynamically, ensuring campaigns are continually refined based on real-world feedback. The iterative nature of this process helps avoid blowback while increasing cognitive resilience in populations likely targeted by adversarial propaganda.

Predictive modeling plays a pivotal role in anticipating adversarial behaviors in IW. ML algorithms analyze insurgent networks, attack patterns, and operational signals to detect pre-violence indicators such as recruitment spikes or coordination efforts. GNNs reveal organizational bottlenecks in decentralized networks, enabling IW practitioners to target high-value nodes for disruption, thereby degrading the adversary's systemic capabilities and shifting away from attritional strategies like the "whack-a-mole" approach. This data-driven methodology significantly enhances operational efficiency and strategic outcomes in IW environments.

However, adversarial manipulation of digital data streams presents growing challenges to intelligence collection. Deepfakes, bot-driven amplification, and disinformation campaigns pollute SOCMINT data, necessitating advanced adversarial robustness frameworks. AI models designed for authenticity verification, such as forensic media analysis and blockchain-based authentication, ensure that intelligence remains reliable despite adversarial deception tactics. The integration of ethical safeguards, including bias audits and transparency mechanisms, further bolsters operational integrity, reducing collateral damage to civilian populations and reinforcing trust in intelligence workflows.

> **Together, these intelligence domains bridge the gap between real-time operational signals and broader contextual insights, creating a holistic approach to irregular warfare intelligence.**

The adoption of edge AI technologies, designed for real-time analysis within austere operational environments, highlights the adaptability of current IW intelligence systems. Such tools allow SOF to analyze SOCMINT and OSINT signals autonomously, ensuring that intelligence is actionable even

in disconnected zones. Additionally, quantum ML and federated intelligence platforms promise breakthroughs in countering modern encryption technologies, facilitating coalition-wide data sharing without compromising national security equities.

Looking to the future, the role of autonomous intelligence systems in IW will likely expand, offering practitioners greater capabilities for preempting adversarial narratives, neutralizing insurgencies, and fostering stability among affected populations. By leveraging advanced AI-driven tools alongside human–machine teaming, intelligence frameworks can maintain situational adaptability while ensuring ethical oversight and contextual relevance. These advancements will redefine how IW campaigns unfold across both physical and cognitive domains, optimizing their precision and minimizing unintended harm.

Conclusion

The integration of autonomous intelligence systems into IW operations is set to revolutionize the way conflicts are anticipated, interpreted, and assessed. Advanced AI-driven technology empowers IW practitioners to exploit the information dimension effectively, from cognitive warfare insights to adversary network mapping and real-time sentiment analysis, ensuring comprehensive intelligence support. Platforms that leverage SOCMINT and OSINT analytics provide nuanced visibility into decentralized insurgent operations, ideological messaging, and population attitudes, while predictive models offer actionable foresight into emerging threats. This capability allows operators to not only address immediate risks but also proactively shape IW engagements before adversarial narratives dominate the conflict landscape.

Looking to the future, the role of autonomous intelligence systems in irregular warfare will likely expand, offering practitioners greater capabilities for preempting adversarial narratives, neutralizing insurgencies, and fostering stability among affected populations.

Future advancements in IW intelligence will emphasize adaptability to complex environments characterized by adversarial deception, low-resource language contexts, and ethically sensitive operations. Cognitive warfare analysis will improve PSYOP campaigns, using deep psychological modeling to neutralize adversarial narratives and reinforce stable governance. Federated learning platforms will ensure coalition-wide intelligence collaboration without compromising OPSEC, while edge computing will allow SOF to conduct localized intelligence analysis in austere operational areas. The rise of quantum ML will overcome encryption barriers and accelerate pattern recognition in highly secure insurgent networks, ensuring the

continued dominance of intelligence forces over adversarial countermeasures.

Ethical frameworks embedded into autonomous systems will also play a defining role in ensuring accuracy, fairness, and accountability in IW campaigns. Real-time bias audits, civilian protections, and transparency mechanisms will align intelligence workflows with international norms and population-centric priorities, avoiding collateral damage or misuse by partner states. Human–machine teaming will further enhance the interpretation and application of AI-generated outputs, blending computational precision with human contextual judgment to maintain ethical oversight and operational integration at all levels of IW intelligence.

Ultimately, the future of autonomous intelligence in IW promises a transformative capability to predict, adapt, and act efficiently and ethically across the information dimension. By harnessing cutting-edge technologies alongside transparent and collaborative frameworks, IW practitioners will optimize their operational precision while successfully countering the growing complexity of irregular threats in the modern battlespace.

About the Authors

Dr. Troy C. Troublefield

Dr. Troy C. Troublefield is a mission information support operations program manager for U.S. European Command. He retired as a psychological operations sergeant major after more than 30 years of service, where he served in multiple senior leadership roles throughout his career. He holds a BS from Touro University in Information Technology Management, an MBA with a concentration in Management of Information Systems from New York Institute of Technology, an MSSI from the National Intelligence University in Strategic Intelligence, a DBA from the International School of Management in International Business Management, and a PhD from Capital Technology University in cyberpsychology. He currently serves as an adjunct professor and dissertation chair for Capital Technology University for PhD students in cyberpsychology, cyber leadership, and forensic cyberpsychology.

Michael Lovera

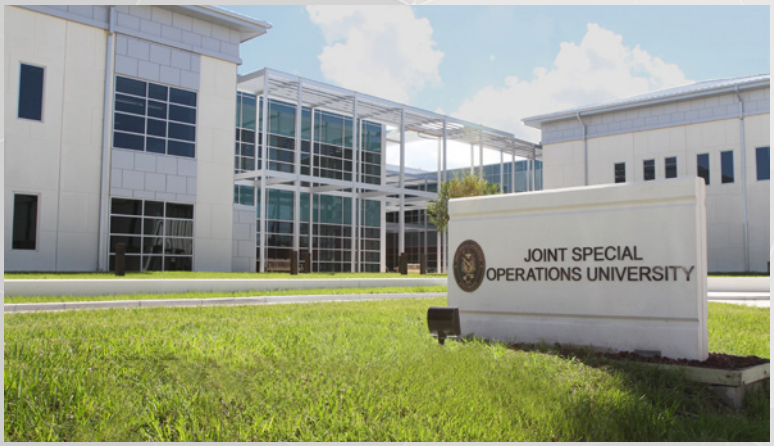
Michael Lovera is a seasoned intelligence professional and former U.S. Navy Chief Intelligence Specialist with over 13 years of experience in the targeting community. In his current role at U.S. Strategic Command, he leads the integration of intelligence to inform strategic planning, support global operations, and refine assessment methodologies. His background includes a decade as a targeting analyst, where he developed deep expertise in orchestrating layered effects across kinetic, cyber, and psychological operations. He holds a master of arts in international relations from the University of Oklahoma and is currently a juris doctor candidate. His primary research passion focuses on the integration of layered effects and the assessment of their impact, particularly at the intersection of steady-state and contingency operations. He has contributed to multiple strategic projects for the Institute for Defense Analysis and the RAND Corporation.

Notes

1. John Arquilla and David Ronfeldt, Networks and Netwars: The Future of Terror, Crime, and Militancy (Rand Corporation, 2001), https://apps.dtic.mil/sti/tr/pdf/ADA397612.pdf.
2. David Omand et al., "Introducing Social Media Intelligence (SOCMINT)," *Secret Intelligence* 26, no. 6 (2019): 77–94, https://doi.org/10.1080/02684527.2012.716965.
3. William J. Lahneman, "The Need for a New Intelligence Paradigm," *International Journal of Intelligence and CounterIntelligence* 23, no. 2 (2010): 201–225, https://doi.org/10.1080/08850600903565589.
4. Jamie Bartlett and Louis Reynolds, *The State-of-the-Art 2015: A Literature Review of Social Media Intelligence Capabilities for Counter-Terrorism* (Demos, 2015), https://demos.co.uk/wp-content/uploads/2015/09/State_of_the_Arts_2015-1.pdf.
5. Michael Glassman, and Min Ju Kang. "Intelligence in the Internet Age: The Emergence and Evolution of Open-Source Intelligence (OSINT)," *Computers in Human Behavior* 28, no. 2 (2012): 673–682, https://doi.org/10.1016/j.chb.2011.11.014.
6. Glassman and Kang, "Intelligence in the Internet Age," 680.
7. J.M. Berger and Jonathon Morgan, "The ISIS Twitter Census: Defining and Describing the Population of ISIS Supporters on Twitter," Analysis Paper No. 20 (The Brookings Project on U.S. Relations with the Islamic World, March 2015), https://www.brookings.edu/wp-content/uploads/2016/06/isis_twitter_census_berger_morgan.pdf.
8. Jacob R. Scanlon and Matthew S. Gerber. "Automatic Detection of Cyber-Recruitment by Violent Extremists," *Security Informatics* 3, no. 1 (2014): 5, https://doi.org/10.1186/s13388-014-0005-5.
9. Marc Sageman, *Understanding Terror Networks* (University of Pennsylvania Press, 2004), https://doi.org/10.9783/9780812206791.
10. Aaron F. Brantly, "The Cyber Deterrence Problem," in 2018 10th International Conference on Cyber Conflict (CyCon) (IEEE, 2018), 31–54, https://doi.org/10.23919/CYCON.2018.8405009.
11. Susan Henrico and Dries Putter. "Intelligence Collection Disciplines—A Systematic Review," *Journal of Applied Security Research* 20, no. 1 (2025): 46–70, https://doi.org/10.1080/19361610.2023.2296765.
12. Lahneman, "The Need for a New Intelligence Paradigm," 210.
13. Yangdong He and Jiabao Zhao, "Temporal Convolutional Networks for Anomaly Detection in Time Series," in Journal of Physics: Conference Series 1213, no. 4 (2019): 042050, https://doi.org/10.1088/1742-6596/1213/4/042050.
14. Jie Zhou et al., "Graph Neural Networks: A Review of Methods and Applications," *AI Open* 1 (2020): 57–81, https://doi.org/10.1016/j.aiopen.2021.01.001.
15. A. Vineela et al., "An Artful Multimodal Exploration in Discerning Fake News Through Text and Image Harmony," *Multimedia Tools and Applications* 84, no. 6 (2025): 37997–38016, https://doi.org/10.1007/s11042-025-20695-4.
16. Tao Bai et al., "Recent Advances in Adversarial Training for Adversarial Robustness," paper presented at International Joint Conference on Artificial Intelligence, April 21, 2021, https://doi.org/10.48550/arXiv.2102.01356.
17. Nathan Schneider, "ISIS and Social Media: The Combatant Commander's Guide to Countering ISIS's Social Media Campaign" (student paper, Naval War College, 2015), https://apps.dtic.mil/sti/pdfs/ADA621060.pdf.
18. Alexandros Karakikes and Konstantinos Kotis. "AI-Assisted OSINT/SOCMINT for Safeguarding Borders: A Systematic Review," *Information* 16, no. 12 (2025): 1095, https://doi.org/10.3390/info16121095.
19. Christopher Paul et al., Paths to Victory: Lessons from Modern Insurgencies (RAND Corporation, 2013), https://apps.dtic.mil/sti/tr/pdf/ADA586471.pdf.
20. Robert Dover, "SOCMINT: A Shifting Balance of Opportunity," *Intelligence and National Security* 35, no. 2 (2020): 216–232, https://doi.org/10.1080/02684527.2019.1694132.
21. Thomas Hegghammer, "Should I Stay or Should I Go? Explaining Variation in Western Jihadists' Choice Between Domestic and Foreign Fighting," *American Political Science Review* 107, no. 1 (2013): 1–15, https://doi.org/10.1017/S0003055412000615.
22. Ali Burak Daricili, and Nourhan El-Bayaa. " Using Artificial Intelligence in the Field of Intelligence Operations and Analysis," in Cyber Security in the *Age of Artificial Intelligence and Autonomous Weapons*, ed. Mehmet Emin Erendor (CRC Press, 2024): 43–57, https://doi.org/10.1201/9781003441700.
23. Charlie Winter, The Virtual 'Caliphate': Understanding Islamic State's Propaganda Strategy (Quilliam, 2015), https://counterideology2.wordpress.com/wp-content/uploads/2015/07/the-virtual-caliphate-understanding-islamic-states-propaganda-strategy.pdf.
24. Jeffrey White, "A Different Kind of Threat: Some Thoughts on Irregular Warfare," *Studies in Intelligence* 39, no. 5 (1996), https://apps.dtic.mil/sti/pdfs/ADA525282.pdf.
25. Loch Johnson, ed., *The Oxford Handbook of National Security Intelligence* (2nd Edition) (Oxford University Press, 2025), https://doi.org/10.1093/oxfordhb/9780197783160.001.0001.
26. White, "A Different Kind of Threat."
27. Mariarosaria Taddeo, "Information Warfare: A Philosophical Perspective," *Philosophy & Technology* 25, no. 1 (2012): 105–120, https://doi.org/10.1007/s13347-011-0040-9.

28. Bobby Chesney and Danielle Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security," *California Law Review* 107, no. 6 (2019): 1753, https://doi.org/10.15779/Z38RV0D15J.
29. M.D. Sazibur Rahman, The Art of Open-Source Intelligence (OSINT): Addressing Cybercrime, Opportunities, and Challenges (2025), https://dx.doi.org/10.2139/ssrn.5281845.
30. Matteo Bonfanti, "An Intelligence-Based Approach to Countering Social Media Influence Operations," *Romanian Intelligence Studies Review* no. 19–20 (2018): 47–68, https://www.ceeol.com/search/article-detail?id=874123.
31. Alcides Macêdo et al., "A Review of the Intersection Techniques on HUMINT and OSINT," *International Journal on Cybernetics & Informatics* (IJCI) 12, no. 1 (2023): 53, https://ijcionline.com/abstract/12123ijci05.
32. Babak Akhgar, "OSINT as an Integral Part of the National Security Apparatus," in Open-Source Intelligence Investigation: From Strategy to Implementation, eds. Babak Akhgar, P. Saskia Bayerl, and Fraser Sampson (Springer Charm International Publishing, 2017), 3–9, https://doi.org/10.1007/978-3-319-47671-1_1.
33. Natascha Harth et al., "Predictive Intelligence to the Edge: Impact on Edge Analytics," *Evolving Systems* 9, no. 2 (2018): 95–118, https://doi.org/10.1007/s12530-017-9190-z.
34. Karakikes and Kotis, "AI-Assisted OSINT/SOCMINT for Safeguarding Borders," 1095.
35. Henrico and Putter, "Intelligence Collection Disciplines—A Systematic Review," 55.

The Joint Special Operations University (JSOU) Press is the scholarly publishing arm of U.S. Special Operations Command (USSOCOM). Through unclassified, open-access materials and SOF-relevant thought leadership, the press supports both the university and USSOCOM in advancing the SOF warrior mind. SOF-specific publications and research, enterprise-wide engagement, and an annual Academic Call for Special Operations Papers facilitate screative, innovative solutions in alignment with command priorities.



JSOU provides relevant joint special operations-peculiar education programs that strengthen the SOF enterprise's impact on the joint force and the Nation.

Joint Special Operations University
7701 Tampa Point Blvd.
MacDill AFB, FL 33621
jsou.edu/press

JSOU PRESS