The Journal of Applied Operational Intelligence 2024 Vol 1 No 1 pp 41-62, DOI: 10.5750/jaoi.v1i1.2266

Assessing Deception Projection via OSINT: The Case of the Ukraine 2022 Counter-Offensive

*William L. Mitchell**
Associate Professor, Norwegian Defence Language and Intelligence Academy, Norwegian Defence University College, Norway

Abstract

Introduction: As the intelligence community observed the evolution of open-source intelligence (OSINT) and the development of the extensive data landscape, several new challenges to traditional approaches to warfighting emerged. One of these challenges was the increasing intensity of the illusory truth effect and its effects on operational timeline planning. How effective are these Emerging Disruptive Technologies (EDT)-driven open sources in projecting a battlespace deception, and what are the limitations and risks? To offer a substantive answer to this question, this study will use the Russian war of aggression against Ukraine as a case study specifically focusing on a projected deception using OSINT in support of the Ukrainian Kherson Offensive, which began on August 29, 2022, and the Kharkiv Offensive, which started in September 2022.
Methods: The analysis aimed to identify and quantify instances where the Ukrainian deception storyline was repeated across various media outlets and social media platforms. It used an OSINT scraper to aggregate and filter the data. Then, a simple quantitative analysis was used to cross-reference the intensity of the illusory truth effect with the Russian operational timeline for troop movements, and a conclusion was drawn.
Results: The number of 'hits' scrapped during a specific period was unexpectedly high, indicating a high level of engagement from both mobile and desktop devices. The data revealed a clear connection between increasing illusory truth intensity and Russian troop movements in the field. The study also pointed out the limitations of large-scale social media data in confidently establishing cause-and-effect relationships between influence and physical actions. It also demonstrated how the growing risk of the illusory truth effect, driven by OSINT and unrestricted military access to social media, could potentially compromise the compartmentalised operational command and control of military organisations through the personal devices of individuals involved in the command-and-control processes.

*Corresponding author: e-mail: wmitchell@mil.no

Conclusion: In an information environment enhanced by EDT, the illusory truth effect is a powerful tool for deceptive projection in the information domain. This effect is amplified if access is gained to compartmentalised operational decision-making processes within the target warfighting organisation. Consequently, from an operational security perspective, the intelligence community must address the threat of an illusory truth breach of command & control processes via OSINT collection in an EDT-enhanced information environment.

Keywords: Deception, Intelligence, OSINT, Ukraine, EDT, C2, Operational Planning, Information environment, Convergence, Russia, Military, Warfighting, Battlespace, Illusory Truth

Introduction

The conflict between Russia and Ukraine has undeniably been a significant geopolitical event that has commanded global attention since its inception. It commenced with Russia's annexation of Crimea in 2014, widely recognised as a blatant breach of international law, leading to a marked deterioration in Russian-Ukrainian relations. This annexation triggered a conflict in eastern Ukraine that has persisted for years, laying bare deep-seated historical, political, and cultural divisions between the two nations. As the conflict has endured, it has encompassed a fusion of traditional military strategies and modern digital-era innovations, shaping a complex battlespace with conventional and unconventional warfare methods.

With its unique blend of traditional and modern warfare, this conflict is a critical case study for Western militaries of military evolution (Hartunian, 2023), highlighting the need for modern warfare dynamics and the integration of traditional combat with cutting-edge technology (Franke, 2024). The conflict underscores the significance of cyber warfare, intelligence operations, unmanned systems, and the strategic use of information to shape public perception and operational effectiveness. It also demonstrates the necessity of agile command structures, logistics resilience, and adaptive strategies in response to evolving threats. Western militaries can study these factors to enhance operational readiness and modernise doctrines (Fedorchak, 2024; Watling & Reynolds, 2023; Zabrodskyi et al., 2022). A striking aspect of this protracted conflict has been the utilisation of Emerging Disruptive Technologies (EDT) in open-source intelligence (OSINT) and social media, which has fundamentally transformed the landscape for military and intelligence operations.

Since the Russian military aggression began in 2014, there has been significant advancement in EDT-driven OSINT, reflecting broader technological trends. OSINT entails gathering and analysing information from publicly available sources to generate actionable intelligence. It has evolved considerably

and is now crucial in law enforcement, national security, and cyber intelligence. The development of OSINT has been characterised by increasing sophistication and its seamless integration with modern technologies, mainly social media platforms (Miller, 2018; Steele, 2007). With the advancement and accessibility of technologies such as artificial intelligence, machine learning, and data analytics, OSINT has evolved to provide unprecedented real-time insights into battlespace situational awareness and enemy movements. This potential of OSINT to provide real-time insights, which was impossible even a decade ago, underscores its power and relevance in modern warfare (Ziółkowska, 2018). These technologies have empowered operatives and analysts to sift through vast information generated on social media platforms, websites, global news reports, and satellite imagery, synthesising them into actionable intelligence in impossible ways even a decade ago (Ponder-Sutton, 2016).

Focusing on the 2022 Ukrainian deception operations provides a compelling case study against this EDT and OSINT backdrop. One particularly significant military operation was the Ukrainian "Kherson first" deception, a stratagem aimed at diverting and misleading Russian forces regarding Ukraine's military objectives. Ukraine effectively obscured its plans for a substantial counter-offensive in Kharkiv by creating a false narrative prioritising attacks on Kherson (Dylan et al., 2022). This skilful orchestration of disinformation enabled Ukrainian forces to achieve strategic surprise, leading to the successful recapture of territory and earning international recognition.

The question at the heart of this study is: How influential are these EDT-driven open sources in projecting a battlespace deception, and what are the emerging risks and limitations? To provide a comprehensive response to this question, this study will concentrate on Ukraine's potential use of OSINT to deceive Russia in support of the Ukrainian Kherson Offensive, which commenced on 29th August 2022, as a diversion, and the Kharkiv Offensive, which began in September 2022.

What does this Study Bring to this Existing EDT-Driven OSINT Literature?

Social media has played a crucial role in the Ukraine-Russia war, serving as a platform for information warfare, propaganda dissemination, and public engagement. Both state and non-state actors have used it to influence public perception, mobilise support, and spread misinformation. Current studies primarily focus on the role of social media in shaping public discourse regarding the Ukraine-Russia conflict (Brodovskaya et al., 2018; Galus & Nesteriak, 2019; Kuźmiński, 2022; Li et al., 2023). This study will differ in that it focuses on the role of social media within military planning processes designed to influence the physical domain of the battlespace and the adversary's operational timelines.

Another body of relative research focuses on the emerging limitations of big data collection and processing processes. For example, it emphasises the importance of having the right starting point. It is crucial to ask the right questions to ensure the collection and analysis of the correct data, with AI and big data amplifying the 'garbage in – garbage out' concern (Weir, 2015). Additionally, there are limitations with veracity control of the automated processes, where manual validation is overwhelmed by volume and variety (Lozano et al., 2015).

Emerging risk research focuses on decision-making. OSINT-related AI can improve decision-making by enhancing speed and effectiveness, but it introduces new uncertainties that can lead to catastrophic miscalculations, especially in crises (Hoffman & Kim, 2023; Kostenko et al., 2023; Whitty, 2022). This same risk will be amplified in warfighting environments where adversaries, as part of the environment, are humans working to disrupt and distort your situational understanding. Ukrainian and Russian entities actively employ misinformation and propaganda to do precisely that, confuse and disrupt operational timelines while enhancing perceptions of strengths or weaknesses. To add to this risk, more operational information is publicly available, further blurring the lines between civilian and military sensors (Karalis, 2022). This is an issue reinforced by the many cases of civilians unwittingly posting positions of strategic assets or even unwittingly providing battle damage assessment pictures and videos seconds after a strike in the Ukraine-Russian war.

This study, in addition to the novelty of explicitly focusing on the warfighting application of OSINT for deception in a battlespace, will also highlight a new operational security risk concerning the accurate assessment of operational timelines and the need for command-and-control systems to balance the speed offered by rapid OSINT exploitation and the possibility of corrupting battlespace intelligence processes. It will also identify a new methodological limitation related to assessing the impact of projecting deception through social media based on big data in the physical domain. Concluding a validation process involving classified sources and proper all-source validation would still be required to establish cause-and-effect certainty between projected stories and military actions.

Theoretical Framework and Key Concepts

The concept of convergence is crucial in understanding how the military, as part of society, must adapt to rapid societal changes driven by advances in science and technology within its operational environments (Arnold & Greer, 2016; Kim & Cho, 2022; Segal et al., 1974). Technological development and military transformation are closely linked in a continuous cycle. As new technologies emerge, military forces adapt to utilise these innovations, which drives further technological advancements. Today's military integrates

mobile technologies and platforms based on network-centric warfare (NCW) principles, which emerged in the early 2000s alongside the widespread use of the internet (Alberts et al., 2000; Cebrowski & Garstka, 1998). This connectivity improves communication, situational awareness, and decentralised command structures (Smith, 2012). The military must adapt to technological advancements and societal changes to remain effective in today's global landscape.

The Emerging Big Data Landscape

The internet's rapid growth has led to the rise of social media and mobile technologies, greatly enhancing OSINT capabilities. Platforms like X (Twitter), Facebook, and Instagram generate vast user-generated content, democratising access to information. This expansion has broadened the availability and scope of data that can be used for intelligence purposes (Crawford, 2012). Additionally, the emergence of mobile technologies allows for real-time access and sharing of information, enabling rapid collection and analysis of data on the go. These developments seamlessly integrate into "big data," where data's sheer volume, variety, and velocity require sophisticated tools and techniques for processing and interpretation (Lozano et al., 2015). By utilising big data analytics, intelligence agencies can extract meaningful insights from this information, uncovering patterns and trends that enhance decision-making and strategic planning in various contexts.

To understand this big data landscape, this paper draws on Miah Hammon-Errey's 2024 understanding, which notes three emerging categories of relevant technology: Data Abundance refers to the ever-expanding volume of data in society; Digital Connectivity refers to the effectiveness of digital networks in connecting people, places, and ideas; and Ubiquitous Technology refers to the pervasiveness of technology in our lives and how we interact with it (Hammon-Errey, 2024) (see Figure 1).

One of the key players in the big data landscape is social media platforms, which generate vast amounts of real-time data. This data offers unprecedented opportunities for collecting and analysing open-source information combined with mobile technology, significantly influencing psychological phenomena such as the *illusory truth effect*. The illusory truth effect has been widely studied and documented in cognitive psychology and behavioural science. The classic study "*The Illusion of Truth*" by Hasher, Goldstein, and Toppino in 1977 demonstrates how repeated exposure to statements increases their perceived truthfulness. The researchers conducted multiple experiments to investigate the illusory truth effect and examined factors such as repetition, source credibility, and varying time intervals between exposure and assessment (Hasher et al., 1977).

In 2019, Brashier and Marsh extensively discussed the illusory truth effect, providing a detailed analysis of the underlying mechanisms and factors that

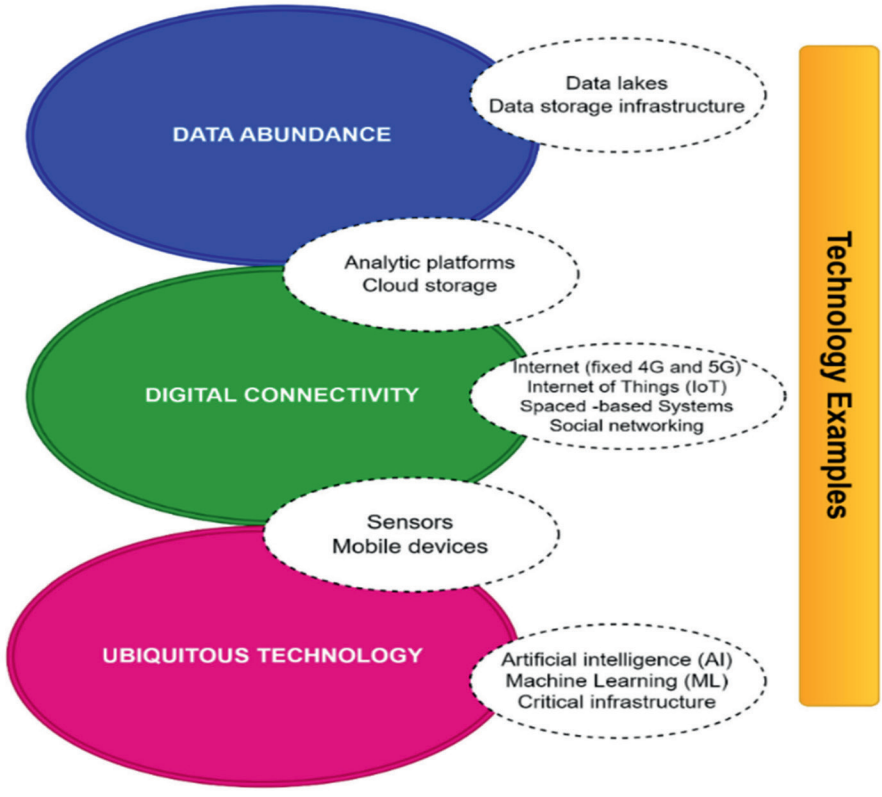

Figure 1. Big data landscape
Note: Original design by Susan Beale (Hammond-Errey, 2024, p. 24).

influence this bias. The authors delved into cognitive processes such as fluency, familiarity, and accessibility contributing to the illusory truth effect. They also examined the implications of this phenomenon for decision-making, information processing, and belief formation (Brashier & Marsh, 2019). Against the extensive data landscape, these dynamics significantly enhance opportunities for misinformation and deception across OSINT channels.

The Increasing Validity of OSINT

OSINT is, by definition, available to both sides in an operational environment and consists of publicly available sources for information. EDT in the form of network data technologies such as 4G and 5G has led to an explosion of general information and its amplification in the public domain quantitively and qualitatively. With the widespread adoption of mobile phones, individuals can easily capture, record, and share information through various channels such as social media platforms, websites, and blogs. EDT via A.I. and big data management is increasing the validity of OSINT through accessible real-time

big data and open-source analysis, highlighting the importance of information from open sources for decision-makers in the military, political, and humanitarian crisis domains (Susnea, 2018). The rapidly growing volume of information available for collection and real-time analysis in operational settings intensifies the illusory truth effect of OSINT. This effect is essential in situations like misinformation and advertising, as repetition of information increases familiarity, leading our brains to mistake it for truth. Notably, the illusory truth effect applies whether the repeated information is true or false, underscoring the need to critically evaluate frequently repeated information (Hassan & Barber, 2021; Nadrevic, 2022; Udry & Barber, 2023). The illusory truth effect theory highlights the power of repetition and familiarity in shaping beliefs and perceptions and selling the desired 'story', for example, to a *deception* target to achieve the desired outcome.

Deception

Deception, as used in this study, refers to intentionally providing false information to manipulate the target's perception of reality (Clark & Mitchell, 2024). Deception has long been a component of political and military conflicts. It is inherent in intentional human behaviour aimed at gaining an advantage (Caddell, 2004; Harrington, 2009). Deception has always been a central and often defining element in the historical context of warfighting strategies and tactics (Wanasika & Adler, 2011). It is also engaged in terms of a more modern instrumental understanding of policy (Godson & Wirtz, 2002) or discussions on military doctrine (Starry, 2012). Common to all are the fundamental dynamics of deception.

The fundamental dynamics of deception work within the context of what is truth, and therefore, truth paradoxically plays a vital role in deception by establishing a foundation of perceptions and beliefs. When an opponent then accepts these, they can be exploited in support of a deception plan. For that plan to work, active denial protects the integrity of the deception. Deception often requires deceit or the fabrication of the false as truth (Clark & Mitchell, 2024). This study examines the dynamics of deception applied tactically by the Ukrainian forces against the Russian military forces.

Before the current era of EDT-driven open-source transformation, deception created an illusory effect by synchronising projections across multiple adversarial collection channels such as Human Intelligence (HUMINT), Signal Intelligence (SIGINT), or Image Intelligence (IMINT). OSINT was considered the least valid of the channels as it was unclassified and required validation from classified channels. Therefore, any deception storyline projected through open sources monitored by the adversary had to be supported by corresponding narratives collectible by adversarial classified channels such as SIGINT and HUMINT to enhance credibility and create a robust illusory effect. Applied in a military context, it involves intentionally or partially

revealing false or misleading information about operational timelines. An operational timeline is a schedule of activities carried out by a military force during a specific operation, campaign, or exercise *in time and space*. Military commanders rely on operational timelines when planning and executing complex operations (ADP 3-90, 2019; JP 01-3, 2021).

Misleading and ambiguity are two primary forms of deception relevant to operational timelines. Misleading deceptions purposely project a story that reduces the adversary's ambiguity and misleads the adversary toward a specific action or preconceived direction. Alternatively, ambiguity, increases deceptions, and seeks to lead the adversary away from the truth, creating doubt and increases the range of incorrect alternatives that the adversary must consider (Clark & Mitchell, 2024). So, what types of false or misleading information are typically used in a battlespace when projecting a story' across known channels to deceive and achieve operational surprise?

Studies of deception, all directly and indirectly through review of historical cases or in discussions of deception dynamics, have highlighted modes of operational surprise, and they usually fall into three overarching categories: normative surprise (unexpected style or behaviour) for the times. (Whetham, 2009); time and space (Wanasika & Adler, 2011); and perceptions of strength or weakness (Caddell, 2004).

In his classic deception work in the late 1960s, Barton Whaley used five modes of *Surprise* that reflect these categories and are historically relevant to operational timelines of modern warfighting (Whaley, 2007):

1) Place – or the 'where?' of coming operations.
2) Time – or the 'when' of coming operations.
3) Strength – or the 'who' of coming operations.
4) Intention – or the 'what' of coming operations.
5) Style – or the 'how' of coming operations.

Projecting an operational timeline deception is communicating a story that will contribute to the adversary's situational understanding in a manner that is advantageous to you. Therefore, it should be plausible and fit the adversary's assessed beliefs and expectancies. Furthermore, it should reinforce the adversary's assessed desires and fears (Wirtz, 2000). Once a good storyline is built, it must be communicated to the adversary in a manner that does not raise suspicion via their intelligence collection channels and assessment processes.

Deception Channels

Deception channels are the 'known' adversarial collection sensors and sources in a conflict situation that can be exploited or fed falsehoods as truth. Its role can best be understood within the context of Boyd's Observe, Orient, Decide, and Act (OODA) model, focusing on the first two phases of the model that

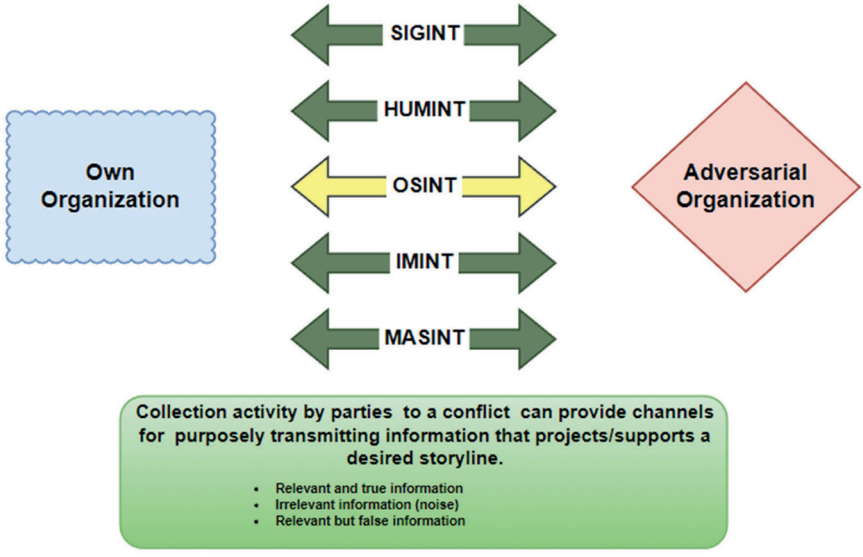

Figure 2. Channels for deception projection
Note: Adapted from Clark and Mitchell (2024, p. 149).

represent the intelligence processes driving the decision-making and action phases through observation and orientation. When planning to project a deception, clearly understand how the adversary can collect and orient in the OODA loop. Projection methodology that underlies deception planning requires a desired outcome or situation after the deception, an idea of what the deception target must do to achieve that outcome, a plausible story for the target to believe, and a reasonable way *(channels)* to project that story (Clark & Mitchell, 2024). Therefore, to project any deception, deception planners must understand their capabilities and their adversary's capabilities for observing and orienting to the operational environment (see Figure 2).

This paper focuses on how the increased availability of OSINT information affects the projection of deception. It explores how the illusion of truth is heightened through social media riding the infrastructure of mobile networks, indicating that people are more likely to believe repeated information and how this can significantly impact the operational environment. It follows basic logic that though managing and combating misinformation poses a challenge, deliberately utilising the same technological dynamics that drive misinformation, OSINT can become a crucial channel for projecting operational deceptions.

Method and Research Design

This paper employs a single case study design to investigate social media's and traditional media's role in contributing to the Ukrainian counter-offensive

deception from 1st April 2022 to 31st August 2022. This approach allows for an in-depth exploration of the specific case and the mechanisms within a defined timeframe. The data for this study were collected through open-source web scraping from 1st April 2022 to 31st August 2022, which is considered the operational timeline for the Ukrainian counter-deception. The scraping focused on English and Russian Cyrillic sources to capture a broad spectrum of media coverage and content relevant to the Ukrainian counter-offensive deception, focusing on social media platforms such as Reddit, X, and Facebook.

The search terms used in the scraping process were consistent throughout the study. These terms were chosen to capture mentions and discussions surrounding the Ukrainian counter-offensive and related deceptive narratives. The essential English search term(s) were: "*Kherson AND Counter-Offensive.*" The key search term(s) in Russian were: "*Херсон AND контрнаступлен*" (See Annex A, B). The analysis aimed to identify and quantify instances where the Ukrainian deception narrative was repeated across various media outlets and social media platforms. The primary metric used was the number of 'hits' or mentions related to the projected deception story/narrative in the data set.

Data Collection and Analysis

1. Aggregation: All the collected data were combined into two central databases in an Excel-readable file format - one for English and another for Russian/Cyrillic by MegaScrape, a custom-built data scraping tool specifically designed for researching the correlation between information warfare and deception tactics. It is used to analyse historical and contemporary articles and social media posts. MegaScrape efficiently gathers and processes large volumes of multimedia content, addressing the need for extensive data collection across various platforms (Foresights AB, 2024).
2. Filtering: The data were filtered to remove irrelevant mentions and noise, ensuring that only relevant mentions of the Ukrainian counter-offensive deception narrative were retained.
3. Coding: Each mention was coded based on its source (social media platform or news outlet) and language (English or Russian).
4. Repetition Analysis: The frequency of mentions and reposts/duplicates was tracked over the specified operational time to understand the intensity of the deception storyline projection. This was further analysed to illustrate how the repetition significantly bolstered the perceived veracity and impact of the deception narrative, accentuating its influence.

Research Limitations

The data collection had two areas for improvement. The first area for improvement was that the Russian Telegram was not included in the data

scrape, even though the initial plan was to collect it separately. However, mitigating this weakness was the combined number of English and Russian hits for the period being significantly higher than expected (20,000 plus). Telegram postings are often repeated on Reddit or other platforms. To facilitate the management of the data and ensure the quality of our analysis, a strategic decision was made to exclude Telegram from the data returns, as the collected data was more than sufficient for the exploratory purpose of this research.

The second area for improvement is that the database does not monitor physical communication in the operational environment. For example, pamphlets were distributed in Ukraine to advise the local population to keep their distance from Russian military positions and hardware in a specific geographical area in Kherson to support the deception storyline. There is currently no solution, but it serves as a reminder that physical messaging is still available to project deception and likely contributes to desired effects locally that social media can quickly amplify.

The study visualises and interprets, utilising frequency counts and time-series analysis to show how the repetition of the Ukrainian deception narrative across different media platforms reinforced the illusion of the counter-offensive. Graphs and charts represent the narrative's distribution and repetition patterns. This analysis aims to demonstrate the significant role of social media in supporting the Ukrainian deception. Through repetitively disseminating specific narratives, these platforms contribute to the illusory truth effect via the OSINT domain.

Case Study: Ukraine-Russian War 2022

In the period up to the writing of this paper, two distinct Ukrainian counteroffensives were completed. They strongly suggested that the Ukrainian Armed Forces (UAF) used a deception plan projected in the information domain across open sources targeting the Russian Armed Forces (RuAF) and projecting the story that Kherson would be the main focus of the UAF counter-attack to get RuAF to weaken the Kharkiv front by sending their best troops to the Kherson front.

Counteroffensive 1, the deception and feint: Kherson Region Offensive 29th August 2022

On 29th August 2022, Ukraine launched an offensive in the Kherson region. Some believed it was to improve the UAF's position for future counteroffensives. Reports indicate that by early September 2022, UAF offensives had made progress across three fronts in Kherson, pushing back some Russian forces and encountering heavy opposition. At the same time, the UAF began an offensive in the northeastern region of Kharkiv (Bowen, 2022a).

Counteroffensive 2: Kharkiv Offensive 8th September 2022

On 8th September 2022, the Ukrainian Armed Forces exploited a weak spot in Russian defences, capturing several towns and launching a successful

counteroffensive. This led to almost 400 square miles of liberation and a rapid advance, causing Russian forces to disintegrate. By September 11, Ukraine had retaken over 1,000 square miles of territory in the Kharkiv region. The key objectives were the hubs of Lyman and Bakhmut, which would impact the conflict's trajectory (Bowen, 2022b) (see Figure 3).

Since the Kharkiv Counteroffensive was more successful than even the Ukrainians expected, liberating more than 1000 square miles in a little over a week, it is reasonable to assume the deception worked and contributed significantly to the successful operation. The Ukrainian deception was designed to mislead the Russians rather than increase situational ambiguity, specifically to get them to move some of their best troops from Kharkiv to Kherson before attacking Kharkiv. The story they created played to both Russian fears of losing the strategic land bridge to Crimea as well as their desire to believe that Kherson was, because of this fact, the primary objective of Ukraine. The Russian fears and desires are reflected in how Ukraine engaged the Whaley's modes of surprise, which can be applied to their deception

Figure 3. Ukraine gains in kharkiv counter-offensive

Note: Source Institute for the Study of War (21:00 GMT, 12 September 2022).

Table 1. Ukrainian deception objectives

Mode of surprise	Projected story
Place	Major Ukrainian counter-offensive against Russian occupiers coming in Kherson Oblast.
Time	Kherson Oblast is the Ukrainian first counter-offensive priority.
Strength	Ukrainian main strength will be on a counter-offensive in Kherson Oblast.
Intention	Ukrainians want to retake the whole of Kherson Oblast to cut the strategic land bridge between Russia and Crimea.
Style	Land offensive by armoured brigades and riverine/amphibious operations.

Note: Refers to Barton Whaley's (2007) modes of surprise presented in Section IV.

operation (see Table 1). Ukrainians targeted the Russian intelligence and leadership, as well as the general media and social media, to specifically convince Russia to redeploy its best troops from the Kharkiv Oblast frontline to the Kherson Oblast frontline in to weaken the Russian defenses in Kharkiv Oblast.

Results

During the Period of Ukrainian Deception Projection, What Were the Dynamics of English Language Media and Social Media Relative to the Storyline?

Ukrainian officials hinted at a potential counteroffensive in the south in early April. By 25th June 2022, Russian troops were redeployed to southern Ukraine, including Kherson. By 1st September 2022, significant engagements and advances were confirmed in Kherson. On 6th September 2022, Ukrainian forces launched a surprise counteroffensive in Kharkiv Oblast, linked to diverting Russian units to Kherson.

During the Ukrainian deception from 1st April 2022 to the end of August 2022, there were 16,930 hits on stories in English media and social media scraping referencing a possible Ukranian counter-offensive in Kherson, of which 12,344 were repostings. The highest intensity was shortly before the start of the Kharkiv counter-offensive, with nearly 7,101 hits. This intensity increased as the media and social media spectrum expanded, going from 64 unique sources in April 2022 to 2,104 by the end of August 2022, and the corresponding increases in reposts, from 27 in April to 4,997 in August (see Table 2).

The deception story projection trend through the period indicates a consistently increasing intensity and echo, with a significant jump from June

Table 2. English language projection overview

Month	Hit summary	Unique	Reposts/duplications
April	91	64	27
May	1292	427	865
June	1697	352	1345
July	6749	1639	5110
Aug	7101	2104	4997
Total	16930	4586	12344

Note: Data summarised from Annex A, UKR Deception 2022 DB English. English Language input terms included "Kherson AND Counter-offensive" from 1st April – 31st August 2022.

2022 to July 2022 and peaking just days before the Ukrainians launched their Kharkiv counter-offensive in the first week of September 2022.

According to the illusory truth effect theory, expanding the number of unique broadcasters and corresponding reposting will increase the story's believability. Therefore, operational activities occurring from June to July are of particular interest, as it appears there was a significant spike in believability within the Russian intelligence community that caused them to act.

During the Period of Ukrainian Deception Projection, What Were the Relative Dynamics of Russian Language Media and Social Media?

During the Ukrainian deception from 1st April 2022 to the end of August 2022, there were 3,412 hits on stories in Russian media and social media scraping referencing a possible Ukranian counter-offensive in Kherson, of which 968 were repostings. The highest intensity was shortly before the start of the Kharkiv counter-offensive, with nearly 1,668 hits. This intensity increased as the media and social media spectrum expanded, going from 66 unique sources in April 2022 to 1,151 by the end of August 2022 and the corresponding increases in reposts, from 13 in April 2022 to 517 in August 2022 (see Table 3).

The deception story projection trend through the period indicates a consistently increasing intensity and echo, with a significant jump from June to July and peaking just days before the Ukrainians launched their Kharkiv counter-offensive in the first week of September.

In July 2022, pro-Russian media and military analysts discussed Kherson's strategic importance and the potential implications of a Ukrainian offensive. They emphasised the need to strengthen defences and prepare for a significant confrontation. In August 2022, Russian-appointed officials in Kherson urged civilians to evacuate due to the anticipated Ukrainian attack. This was portrayed as a necessary precaution against the increasing threat from Ukrainian forces. In September 2022, pro-Russian sources reported on Ukrainian advances and the effectiveness of their operations, particularly the

Table 3. Russian language projection overview

Month	Hit summary	Unique	Reposts/duplications
April	79	66	13
May	292	240	52
June	276	216	60
July	1097	771	326
Aug	1668	1151	517
Total	3412	2444	968

Note: Data summarised from Annex B, UKR Deception 2022 DB Russian. Russian Language input terms included "Херсон AND контрнаступление" for the period of 1st April – 31st August 2022.

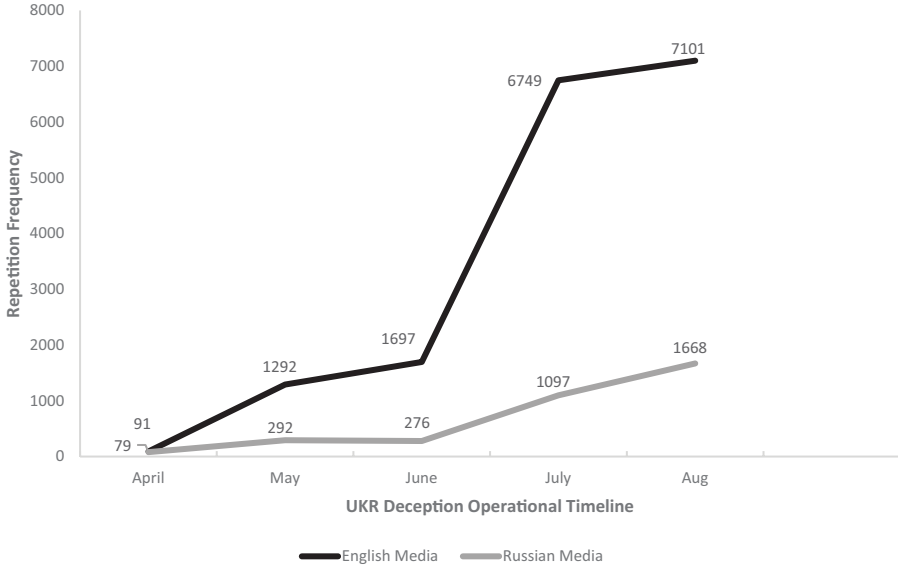

Figure 4. Comparative deception story repetition frequency vs. operational period

Note: Visualisation of hit summary data from Table 2 and Table 3.

use of HIMARS artillery systems to target Russian logistics and command centres. These reports highlighted the vulnerabilities in Russian defences and the challenges posed by the Ukrainian offensive.

With the English language data collected, according to the illusory truth effect theory (Whaley, 2017), expanding the number of unique broadcasters and corresponding reposting will increase the story's believability. Therefore, Russian military operational activities from June to July are of interest, as there was a significant spike in believability in both languages (see Figure 4).

How do the Russian Troop Movements Match the Projection of the Deception Storyline?

As the Ukrainians were conducting a misleading deception plan, they had specific objectives concerning the Russians' understanding of time and space for the coming Ukrainian offensive. The main objective was to get the Russians to weaken the defenses on the Kharkiv front by moving some of their best troops to the Kherson front. This objective was accomplished. So, cross-referencing fundamental Russian troop movements in time and space with the storyline projection via OSINT should offer some insight into the deception projection's effects.

Some of the critical operational timeline troop movements noted through OSINT platforms began in June with the Russian 1st Guards Tank Army, which was redeployed from Kharkiv to Kherson starting in June 2022 Then, from June 2022 to August 2022, the Russian 20th Combined Arms Army moved elements from Kharkiv to Kherson. More significant troop movements were noted by late August, including the Russian 76th Guards Air Assault Division, which moved to Kherson in late August 2022, and the Russian 106th Guards Airborne Division (Stephanenko et al., Aug 30). Finally, one of the more elite units, the 45th Guards Spetsnaz**.** Engaged in Kherson by August 2022.

Figure 5 illustrates a relationship between the increasing Russian troop movement activity and the increasing intensity of the deception projection across OSINT channels in both English and Russian.

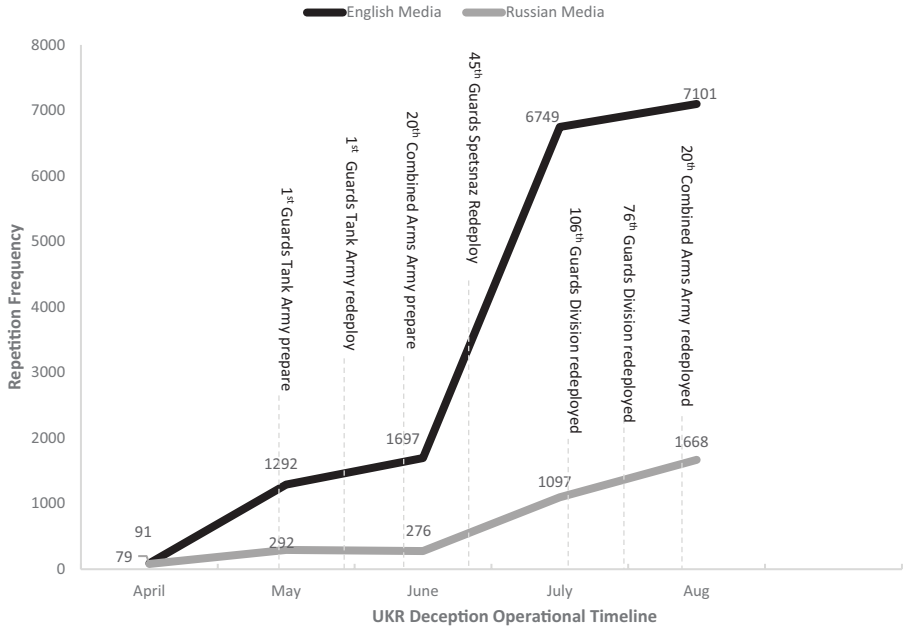

Figure 5. Deception story repetition frequency vs. russian troop movements
Note: Visualisation of hit summary data from Table 2 and Table 3 against Russian troop movements.

Discussion

In the context of answering the main research question, how effective are these EDT-driven open sources in projecting a battlespace deception? The results are mixed. The Ukraine Counteroffensive in 2022 saw a significant impact from the EDT-enhanced OSINT information domain, contributing to the illusion of truth surrounding the 'Kherson counter-offensive first' narrative. As seen in Figure 5, the intensity of the deception storyline correlates with increased Russian troop movement activity, peaking before the start of the Kharkiv counter-offensive.

However, this analysis' limitation becomes apparent: We cannot establish a direct cause-and-effect relationship from the scraped OSINT data in the cognitive domain to specific actions in the battlespace with certainty; at best, the heightened Russian troop activities and movements confirm the generation of illusory truth effects as they move toward September, and we can assume that the troop movement activities themselves began to contribute to the self-reinforcement of the deception storyline.

The precise causal links between troop movements and deception storylines can only be verified with validated troop movement timings in the intelligence reports driving the Russian troop movement orders. Any direct cause-and-effect could be determined by cross-referring the reports' content with OSINT-driven storyline projection. In short, classified sources for validation are still required to clarify the strength of the cause-effect relationship between OSINT projection and resulting actions.

It also points out a possible risk to operational security and the compartmentalised military decision-making processes within the command and control of the military organisation, emerging from the widespread access to social media within the military organisation. If the illusory truth effect accesses these compartmentalised processes, they risk becoming corrupted, including the internal verification and validation of intelligence used for planning. Once information streams from OSINT-driven social media are transformed into other forms of reporting (intelligence or patrol reports from units) by military personnel, it becomes something other than OSINT as it moves up the analytical chain, constantly gaining validity. This is a risk compounded by the sheer number of military personnel involved in the military planning process having constant access to their favourite social media news sources.

Implications for Policy and Practice

OSINT has transformed from merely providing tip-offs, to a platform for classified collection. With the rise of EDT and the abundance of data, digital connectivity, and widespread technology, OSINT has become a crucial platform for threat analysis and understanding the relationship between

information and physical domains. Intelligence organisations should allocate ample resources to facilitate this transition within their structures and processes. This may also involve developing new functions for integrating networks, big data processing, and analytical platforms.

As a result of this transformation, an essential aspect that intelligence organisations must consider is that we have the technological ability to collect and analyse vast amounts of data from the internet. The more historical data attributed to behavioural systems, whether persons, organisations, or states, will become collectable cognitive 'patterns of life' within the information environment that can be exploited to predict physical behaviour. All systems, physical or cognitive, have a pattern of life to discover. There are no exceptions.

Finally, this case study illustrates the significant challenge military organisations face in maintaining operational security during planning. The widespread use of mobiles as sensors within the military creates a vulnerability that adversaries could exploit in the information domain. Policies governing access to personal mobile devices during wartime are needed, especially for personnel involved in decision-making processes. These policies should consider how OSINT could undermine validated reporting that informs decision-making and influences the situational understanding of operational decision-makers. This underscores the importance of implementing strict policies regarding using personal devices with internet access within warfighting organisations, particularly for intelligence and situational awareness reporting personnel.

Conclusion

The number of hits gathered during the specific period and on the particular operational topic was unexpectedly high, suggesting a high level of engagement from both mobile and desktop devices, particularly among military personnel in the battlespace via social media.

One potential area for further investigation is the impact of EDT-enhanced OSINT doctrinal command and control systems and intelligence processes within military organisations. For instance, the significant increase in OSINT focus between June and July coincided with initial signs of Russian troop movement preparations. The extensive use of OSINT began to influence their decision-making processes, reinforcing the narrative projection and leading to more operational responses, thus magnifying the impact in the information domain.

Given the prevalence of mobile devices in the battlespace, it is conceivable that regular access to social media for information may have directly influenced military processes through reporting. If this is the case, the illusory truth effect could gain access to compartmentalised decision-making processes, making it a powerful tool for deceptive projection. Moreover, amplifying and repeating information from sources in the battlespace is crucial for shaping operational

planning and timelines. It allows the enhanced illusory truth effect to influence operational planning structures through personnel, leveraging increased familiarity, accessibility, and fluency.

When we examine the Ukraine 2022 counteroffensive deception, it is no secret that the Russian intelligence apparatus has been prone to significant mistakes in this war and has struggled to provide accurate and timely battlespace intelligence for targeting on an operational level through 2022. This raises the possibility that the success was not only due to the Ukrainian Armed Forces better utilising an EDT-enhanced OSINT domain to project a deception but also that the target of the deception (Russia) being weak in the classified collection at that point in the conflict, was easily manipulated into relying heavily on the EDT-driven OSINT domain. This powerful combination possibly led to their undoing in Kharkiv due to the belief that "something is better than nothing", upon which they subsequently based their operational decisions.

Future research should examine limiting the threat of an illusory truth breach of warfighting command-and-control processes via OSINT collection in an EDT-enhanced information environment.

Retention Rights

Data Statement

Restricted Data

Due to ethical/commercial issues, data underpinning this publication cannot be made openly available. Further information about the data and conditions for access are available from the Language and Intelligence Academy, Norwegian Defence University College. Inquiries may be sent to fhs.sesk@mil.no.

Conflict of Interest Statement

The author declares that they have no conflicts of interest

References

ADP 3-90, U. A. (2019, July). *Offence and Defense*. Dept. of the Army. https://www.moore.army.mil/Infantry/199th/2-16/ABOLC/content/pdf/ADP%203-90%20Offense_Defense.pdf

Brodovskaya, E. V., Dombrovskaya, A. Y., & Karzubov, D. (2018). The communication structure of the ukrainian information flows about the crimea

development as a part of russia: Social-media analytics and discourse analysis. *Bulletin of the Moscow State Regional University*, 4. https://doi.org/10.18384/2224-0209-2018-4-923

Caddell, J. W. (2004). *Deception 101 – Primer on Deception*. https://doi.org/10.21236/ADA429106

Cebrowski, A. K., & Garstka, J. J. (1998). *Network Centric Warfare: Its Origins and Future* (Vol. 124, Issue 1).

Clark, R. M., & Mitchell, W. L. (2024). *Deception: Counterdeception and Counterintelligence*. https://doi.org/10.4135/9781071872642

Dylan, H., Gioe, D., & Little, J. (2022, December 10). *The Kherson Ruse: Ukraine and the Art of Military Deception*. Mordern War Institute. https://mwi.westpoint.edu/the-kherson-ruse-ukraine-and-the-art-of-military-deception/

Fedorchak, V. (2024). *The Russia-Ukraine War*. https://doi.org/10.4324/9781003351641

Foresights, A. B. (2024). *Customised Mega Scraper* [Graphic].

Franke, U. (2024). Transformation technologique et stratégique de la guerre. *Revue Défense Nationale*, *N° 871*(6), 32–40. https://doi.org/10.3917/rdna.871.0032

Galus, A., & Nesteriak, Y. (2019). *Digital media in a contemporary conflict – example of Ukraine*. *4*, 27–44. https://doi.org/10.14746/SSP.2019.4.2

Godson, R., & Wirtz, J. J. (2002). *Strategic Denial and Deception: The Twenty-First Century Challenge*. https://doi.org/10.4324/9781315130316

Hammon-Errey, M. (2024). *Big Data, Emerging Technologies and Intelligence*. Routledge.

Harrington, B. (2009). *Deception: From Ancient Empires to Internet Dating.*

Hartunian, E. (2023). US Army War College Russia-Ukraine War Study Project. *Parameters*, *53*(3). https://doi.org/10.55540/0031-1723.3234

Hoffman, W., & Kim, H. M. (2023). *Reducing the Risks of Artificial Intelligence for Military Decision Advantage*. https://api.semanticscholar.org/CorpusID:259598846

JP 01-3, J. C. of S. (2021, November). *DOD Dictionary of Military and Associated Terms*. Office of the Chairman, Joint Chiefs of Staff. https://irp.fas.org/doddir/dod/dictionary.pdf

Karalis, M. (2022, December 16). *Open-source intelligence in Ukraine: Asset or liability?* [Expert Comment]. Chatham House. https://www.chathamhouse.org/2022/12/open-source-intelligence-ukraine-asset-or-liability

Kostenko, O., Jaynes, T. L., Zhuravlov, D., Dniprov, O., & Usenko, Y. (2023). Problems of using autonomous military ai against the background of russia's military aggression against ukraine. *Baltic Journal of Legal and Social Sciences*, *4*, 131–145. https://doi.org/10.30525/2592-8813-2022-4-16

Kuźmiński, A. (2022). *The Methods of Disinformation in the Russia-Ukraine War*. *53*, 167–171. https://doi.org/10.55206/vtxc7801

Li, Q., Li, Q., Di, X., Chen, S., & Zhang, H. (2023). Influence of social bots in information warfare: A case study on @UAWeapons Twitter

account in the context of Russia–Ukraine conflict. *Communication and the Public*, 205704732311661–205704732311661. https://doi.org/10.1177/20570473231166157

Lozano, M. G., Franke, U., Rosell, M., & Vlassov, V. (2015). *Towards Automatic Veracity Assessment of Open Source Information*. 199–206. https://doi.org/10.1109/BIGDATACONGRESS.2015.36

Miller, B. H. (2018). Open Source Intelligence (OSINT): An Oxymoron? *International Journal of Intelligence and Counterintelligence*, *31*(4), 702–719. https://doi.org/10.1080/08850607.2018.1492826

Ponder-Sutton, A. M. (2016). *The Automating of Open Source Intelligence* (pp. 1–20). https://doi.org/10.1016/B978-0-12-802916-9.00001-4

Smith, C. R. (2012). *Network Centric Warfare, Command, and the Nature of War*. https://apps.dtic.mil/dtic/tr/fulltext/u2/a506221.pdf

Starry, M. D. (2012). *Deception and the Operational Level of War*.

Steele, R. D. (2007). *Open source intelligence* (pp. 147–165). https://doi.org/10.4324/9780203089323-20

Stephanenko, K., Hird, K., Barros, G., Mappes, G., & Kagan, F. (Aug 30). *Russian Offensive Campaign Assessment, August 30* (The Critical Threats Project 2022, p. 17). Institute for the Study of War.

Wanasika, I., & Adler, T. R. (2011). Deception as Strategy: Context and Dynamics. *Journal of Managerial Issues*, *23*(3). https://www.jstor.org/stable/23209121

Watling, J., & Reynolds, N. (2023). *Meatgrinder: Russian Tactics in the Second Year of Its Invasion of Ukraine* [Special Resources]. RUSI. https://www.rusi.org/explore-our-research/publications/special-resources/meatgrinder-russian-tactics-second-year-its-invasion-ukraine

Whaley, B. (2007). *Stratagem: Deception and surprise in war*. Boston: Artech House.

Whetham, D. (2009). *Just Wars and Moral Victories: Surprise, deception and the normative framework of European war in the later Middle Ages*.

Whitty, R. D. (2022). The Battle with Data: Realities of Bringing Artificial Intelligence to the Battlefield. *Expeditions with MCUP*, *2022*. https://doi.org/10.36304/expwmcup.2022.09

Zabrodskyi, M., Watling, J., Danylyuk, O., & Reynolds, N. (2022). *Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine: February–July 2022* [Special Resources]. RUSI. https://www.rusi.org/explore-our-research/publications/special-resources/preliminary-lessons-conventional-warfighting-russias-invasion-ukraine-february-july-2022

Ziółkowska, A. (2018). *Open Source Intelligence (OSINT) as an element of Military Recon*. *19*(2), 65–77. https://doi.org/10.5604/01.3001.0012.1474