


Birdwatchers on social media: The mediatisation of intelligence organisations


Peter Schrijver¹, Lotte Nietzman², Peter B.M.J. Pijpers³

¹Pschrijver@mindef.nl

¹  <https://orcid.org/0009-0004-6526-0150>

²  <https://orcid.org/0009-0004-4939-1409>

^{1,2}Faculty of Military Sciences, Netherlands Defence Academy, Hogeschoollaan 2, 4818 CR, Breda, The Netherlands

³  <https://orcid.org/0000-0001-9863-5618>

³Law of Armed Conflict and Military Operations – ACIL, University of Amsterdam, Nieuwe Achtergracht 166, 1018 WV, Amsterdam, The Netherlands

Abstract

War has always affected the physical and cognitive dimensions of life; however, recent developments in Ukraine and Gaza have increased the emphasis on warfare making use of the virtual realm. Military actions now extend beyond traditional battlefields, significantly impacting virtual and cognitive dimensions through cyberspace and social media. This study examines how intelligence and security services in Ukraine, Israel, and the United Kingdom employ mediatisation—the process whereby mass media shapes public discourse—to achieve their objectives in modern warfare. Through comparative analysis of these three intelligence landscapes, the research explores how these organisations, despite being part of larger national security systems, pursue their own organisational interests. The study reveals that intelligence services use mediatisation for multiple purposes: engaging citizens, justifying operations, and projecting strength to domestic and international audiences. The results show a marked shift from secretive practices to open, public-facing communication strategies. The UK Defence Intelligence provides daily situational updates, the Israel Defence Forces Spokesperson's Unit releases sensitive intelligence to shape narratives, and Ukrainian military intelligence publishes intercepted communications to undermine adversaries. This selective disclosure via social media represents a significant departure from conventional secrecy, reflecting the growing importance of information warfare. While this approach offers benefits in shaping narratives and countering adversaries, it poses risks to operational security. The study underscores the complex balance that intelligence agencies must strike between transparency and protecting sources and methods in the digital age, highlighting how communication serves as a tool for informing the public, justifying actions and discrediting adversaries.

Keywords:

intelligence, UK DI, IDF spokesperson's unit, HUR, mediatisation

Article info

Received: 20 September 2024

Revised: 22 November 2024

Accepted: 26 November 2024

Available online: 28 January 2025

Citation: Schrijver, P., Nietzman, L. and Pijpers, P.B.M.J. (2025) 'Birdwatchers on social media: The mediatisation of intelligence organisations', *Security and Defence Quarterly*, 49(1). doi: [10.35467/sdq/196516](https://doi.org/10.35467/sdq/196516).

Introduction

War has always affected the physical and cognitive dimensions of life; however, recent developments in Ukraine and Gaza have increased the emphasis on warfare making use of the virtual realm. Military and intelligence actions now extend beyond the traditional battlefield, significantly impacting both virtual and cognitive dimensions through cyberspace and via social media with the aim of influencing the perceptions of target audiences.

Intelligence services have traditionally operated in near-total secrecy, deliberately keeping their activities out of the media and public view. Historically, protecting their sources and methods has been their top priority. Consequently, as [Petersen \(2019, p. 317\)](#) notes, “public-facing communication has been an almost absent topic in intelligence studies.”

Since the end of the Cold War, however, a new perspective has emerged among liberal international relations theorists that hiding the truth makes (international) cooperation difficult and increases the chances of conflict ([Pew Research Center, 2015](#)). The revealing of mass surveillance techniques by Edward Snowden in 2013 was another push for greater transparency.

The foundation of the analytic collective Bellingcat—a pioneer in the use of open-source investigations—in 2014 not only demonstrated that intelligence gathering and analysis are no longer the sole purview of government agencies, but also brought a new level of transparency to intelligence work ([Vox, 2024](#)). According to its founder, Elliot Higgins, Bellingcat’s work should be seen as a reflection of the technology that has changed the world in the last 15 years—referring to the use of smartphones, online platforms, and social media as new ways of sharing information ([Vox, 2024](#)). Today, anybody with a mobile phone and internet connection can collect or analyse intelligence ([Zegart and Morell, 2019, p. 85](#)).

As a result of these developments, intelligence organisations around the world are becoming much more visible as they realise they could actually use new media to their advantage and simultaneously understand that they need to be more transparent and open to scrutiny if they are to maintain public support ([Magen, 2017, p. 272](#)). The shift away from the traditional practice of keeping intelligence methods and sources secret represents a notable change in the intelligence community’s approach. The effect of greater openness on public confidence in intelligence organisations is, however, not straightforward. Intelligence agencies’ efforts to inform the public sometimes provoke unintended reactions, including scepticism and (unfounded) conspiracy theories ([McLoughlin *et al.*, 2020, p. 233](#)).

This shift also involves the process of mediatisation, which is understood as a reciprocal dynamic where mass media and social media not only influence society and organisations but are also leveraged by organisations, such as intelligence agencies, to further their own objectives ([Maltby, 2012, p. 255](#)). Through mediatisation, intelligence services can shape and frame public discourse, using media channels to amplify their specific perspectives. Mediatisation sets the societal conditions and norms for how media influences behaviour and expectations ([Hjarvard, 2008, p. 105](#)), creating an environment in which intelligence agencies can communicate with the public. In this article, the focus is on how intelligence agencies actively use social media to both influence and respond to public sentiment.

Intelligence communication—defined by Petersen (2019, p. 317) as “the strategic use of information by intelligence agencies to engage with and influence the public”—plays a central role in this process. It is the practical application of mediatisation by intelligence agencies, using the tools and norms established by mediatised society to achieve specific objectives. It serves two intertwined purposes: to inform the public with transparency and credibility, and to influence society by shaping narratives that align with organisational goals (Dylan and Maguire, 2022, pp. 61–62). This approach reflects a shift from purely covert operations to visible intelligence communication.

While all states’ military and intelligence agencies are subject to some sort of mediatisation, each nation, whether an ally or an enemy, still operates within unique security and sociocultural circumstances. Surprisingly, although the relationship between intelligence agencies and the public is becoming increasingly significant in Western societies, literature shows a notable scarcity of studies examining the direct relationship between these influential governmental institutions and the public through online and social media platforms (Avidar and Magen, 2023, p. 2). Studying and comparing the security agencies of other countries can provide insights into not only the communication strategy of the specific organisation at hand but also the wider social and cultural environment of their respective nations (Avidar and Magen, 2023, p. 7).

This article investigates how and for what purposes intelligence and security services in the United Kingdom, Israel, and Ukraine employ mediatisation to pursue their organisational objectives within the context of modern warfare. These cases were selected due to their involvement in current conflicts and their distinct approaches to intelligence dissemination on social media under overt and identifiable accounts. The cases offer a diverse yet comparable set of examples that provide insights into the use of intelligence material in social media communications. By comparing these cases, the study aims to shed light on the varying communication strategies. Other organisations or states were not included in order to maintain a manageable scope and focus on cases directly relevant to ongoing conflicts.

As regards intelligence, the following definition is used: Intelligence is the product resulting from the collection, evaluation, and analysis of available information concerning the intentions and capabilities of hostile or potentially hostile elements. This definition, originating from Hulnick’s (2004) discussion on intelligence, is largely based on the US Army Doctrine Publication (ADP) 2-0 definition. In this article, the focus is on information conveyed, either directly or indirectly, by intelligence agencies through their social media communications. This includes information that is typically not publicly available, gathered covertly or declassified, and selectively released to the public with the aim of shaping narratives and informing audiences.

The next section introduces the main theoretical concepts, focusing on mediatisation and communication strategies in conflicts. Drawing on the work of researchers, such as Bernd Hirschberger, a theoretical framework is developed. The article’s main body examines three cases: the United Kingdom, Israel, and Ukraine. Recognising that states organise and structure their intelligence services differently, examples of intelligence shared via social media are analysed. Following these examples, the theoretical framework is applied to study them, comparing the three cases and discussing the implications of their communication methods. This analysis does not seek to evaluate what is just, right, or true; rather, it aims to investigate analytically the tactics employed by each organisation in disseminating intelligence on social media. The article concludes with reflections on how intelligence services use social media to achieve their organisational objectives in contemporary conflicts.

Theoretical framework

Naturally, the media play an increasing role in international politics in general. The rise of digitalised (social) media has further increased the possibilities and relevance of parties engaging in external communication, including in crisis and conflict (Hirschberger, 2021, p. 14). This development in (social) media changes is conceptualised by the mediatisation approach (Krotz, 2018, p. 86). Strömbäck (2008, p. 234) argues that mediatisation is a multidimensional concept in which it is possible to distinguish four distinct phases. In the first phase, the media is the main source of information. In the second, media is becoming an independent power with its own agency. In the third, the power increases even more and the media creates its own logic away from political logic, while in the final phase, political entities follow media logic. The mediatisation of politics can be described as a process in which the reciprocal independence of the media from politics and society contrasts with the independence of politics and society from the media (Strömbäck, 2008, p. 241). This development is accentuated by Hoskins and O’Loughlin (2015, p. 1320) in their article “Arrested war: The third phase of mediatisation,” where they identify the “arrested war” phase as a period during which mainstream media and governments adapt to and harness digital media dynamics to regain control over the narrative.

Zeitsoff (2017, pp. 1970–1991) examines social media’s transformative role in conflict, showing how it has become a vital tool for governments, military forces, and intelligence agencies. He first notes that social media’s low communication barriers allow insurgents, activists, and citizens to reach global audiences, enabling those with limited resources to widely broadcast narratives. This democratisation of information was evident in the 2019 Hong Kong protests, where Telegram facilitated protest coordination and mobilisation (Urman *et al.*, 2021, p. 3). He further explains that rapid information dissemination on social media reshapes the pace of conflict, often escalating tensions more quickly than traditional media. The 2020 Belarusian protests illustrate this acceleration, as platforms like Telegram intensified public sentiment and urgency (Mateo, 2022, p. 26). Another key insight involves conflict actors adapting to the influence of social media. Governments and insurgents now adjust their strategies, as demonstrated in Syria, where the Assad regime shifted from strict media control to actively using social media to monitor dissent and promote its narrative (Rey, 2017, p. 89). Finally, Zeitsoff (2017) highlights the strategic value of social media as a real-time data source, allowing actors to gauge and influence conflict dynamics. During the 2012 Gaza Conflict, Israel monitored public sentiment by tracking hashtags like #GazaUnderAttack, in order to adjust its communication strategy in response (Bartlett and Reynolds, 2015, p. 25). These insights reveal how social media has reshaped interactions and strategies in modern conflicts.

Armed forces and intelligence services can use (social) media to interact with belligerent parties to inform a larger audience (including the public), and also in a more malign manner to influence or even manipulate target audiences (Maltby, 2021, pp. 255–268) argues that media act as both a rationale and an interface for communicating within the military but also between the military and their audiences. Her research shows that the mediatisation of conflict enables the British army to assert its voice independently, despite its subordination to the UK Ministry of Defence (MoD). Military media management strategies, she notes, are increasingly designed to appeal to reassure and garner support from multiple audiences (p. 264).

Hence, mediatisation represents a broader societal transformation in which media logic shapes the communication strategies of security organisations, including the military and intelligence actors. Strategies such as branding and shaming manifest this logic, offering

distinct yet complementary approaches to influencing public perception and shaping conflict narratives.

Branding and shaming are interrelated in their reliance on media's agenda-setting power and emotional resonance to communicate effectively. A common method for shaping the image of a conflict is to attribute negative behaviour to an adversary, a practice often referred to as "shaming" or "naming and shaming" (Krain, 2012, pp. 574–589). This approach is particularly successful when it evokes feelings of outrage or concern, making it easier for critics to question the legitimacy of the opponent and assign blame (Hirschberger, 2021, p. 25). Conversely, "branding" focuses on positive communication, typically aimed at enhancing the image of the communicator rather than targeting the opponent. Theories of branding align closely with marketing principles, emphasising the importance of actors defining their "brand," image, or reputation to influence audience perceptions (Hirschberger, 2021, p. 27).

These strategies are most effective when viewed through the lens of mediatisation, which not only enables but necessitates their use. Mediatisation provides the structural framework within which branding and shaming operate, leveraging media logic to amplify narratives and influence audiences. As Strömbäck (2008, p. 240) argues, mediatisation represents a significant shift where media becomes a central actor, not merely a conduit, in shaping how messages are constructed and received. This dynamic is particularly pronounced in the age of social media, where low communication barriers allow conflict actors to engage audiences directly, creating fertile ground for both branding and shaming to flourish.

The interplay between branding, shaming, and mediatisation is evident in contemporary conflicts, such as those in Ukraine and Gaza. For instance, during the conflict between Israel and Palestine, social media has been used strategically to influence public opinion through emotionally engaging narratives designed to spread rapidly and shift perceptions (Hirschberger, 2021, p. 13). Thus, mediatisation, as an overarching concept, encompasses branding and shaming as interrelated communication strategies. By creating targeted or emotionally engaging narratives that spread rapidly online, these strategies enable actors to reach and influence large audiences, shaping their perceptions effectively. In the age of social media, the battle for narratives is increasingly waged in digital spaces.

Three cases

Communication during conflicts is complex and occurs in a variety of constellations. It is influenced by numerous factors, such as the number of actors involved and the variety of channels used. Naturally, cultural differences also affect communication styles. Increasingly, intelligence and security services engage in strategic communication and image work through platforms like social media (McLoughlin *et al.*, 2020, p. 233). The overall research approach adopts a case study methodology, examining how intelligence and security services use intelligence-derived content as part of their public communication strategies on social media.

Regarding the UK Defence Intelligence (DI), the research method involves a thematic analysis of a sample of UK DI's intelligence updates on the Russo-Ukrainian war during 2023. This analysis categorises and interprets recurring themes, such as Russian military activities, leadership, and personnel issues. Through this approach, patterns within UK DI's public communication are identified to illustrate how the agency uses social media to inform and influence public discourse.

The case of the Israel Defence Forces (IDF) Spokesperson's Unit is examined by analysing the IDF's public release of intelligence-derived information. The analysis focuses on how the IDF has used sensitive information (e.g. recordings of intercepted calls) since 7 October 2023. These releases were identified from a dataset of tweets published by the IDF between October 2023 and June 2024.

Similarly, the discussion on Ukrainian military intelligence service (HUR) analyses the use of intercepted communications and sensitive intelligence shared on social media. This approach involves tracking and categorising these communications to understand how HUR uses intelligence disclosures as a tool to degrade the Russian war effort and shape the conflict narrative. These intercepted communications were identified from a dataset of tweets published by the HUR between February 2022 and February 2023.

In sum, the research design uses qualitative, case-based methods to investigate how different intelligence services incorporate social media into their public-facing strategies. Each case illustrates specific techniques of information selection, categorisation, and narrative construction to shape public perceptions in distinct conflict settings.

UK Defence Intelligence: Tweeting on the war

In the intelligence sphere of the United Kingdom, discussions of intelligence activities have gradually shifted towards the need for more openness, as observed by [Lomas and Ward \(2022, p. 10\)](#). Building on this trend, former Government Communications Headquarters (GCHQ) director Omand ([Omand, 2022, p. 248](#)) stressed the necessity for governments to provide enough background information about their intelligence and security organisations to build public trust. This change has driven UK intelligence agencies, including the traditionally secretive GCHQ, to actively engage with the public. GCHQ, responsible for providing signals intelligence (SIGINT) and information assurance to the British government and armed forces, now uses social media, public speeches, and media interviews to clarify its role and potentially enhance public understanding ([Lomas and Ward, 2022, p. 13](#)).

In a 2022 Royal United Services Institute (RUSI) report on the future of open-source intelligence in the United Kingdom, it is argued that amidst a "crowded environment which adversaries are seeking to pollute with disinformation," an increasing number of stakeholders are recognising the need for transparency. This transparency is important not only for improving domestic discourse but also for undermining the misleading narratives being spread both locally and internationally ([Centre for Emerging Technology and Security, 2022](#)).

However, the effect of greater openness on public confidence in intelligence organisations is not straightforward. GCHQ and other agencies' efforts to inform the public sometimes provoke unintended reactions, including scepticism and aversion. Some social media users have connected GCHQ's social media engagement with established conspiracy theories like "chemtrails" and "pizzagate" ([McLoughlin *et al.*, 2020, p. 242](#)). The first refers to a notion that the vapour trails left by aeroplanes are, in fact, chemical substances dispersed by the government to manipulate the population. The second concerns a fabricated scandal alleging that members of the American Democratic Party participated in a child exploitation network (The Independent, 2016). Thus, the increased volume of publicly accessible information about UK intelligence bodies does not automatically lead to the British public grasping the role of these organisations. This gap between heightened transparency and public comprehension underlines the difficulties intelligence services

face in their attempts to engage meaningfully with citizens (Lomas and Ward, 2022, p. 22).

Notwithstanding this scepticism about the public presence of intelligence organisations, recent online behaviour of the UK DI demonstrated a shift in the use of intelligence. It moved from a traditional model that primarily supported government and military decision-making to proactive public communication (Centre for Historical Analysis and Conflict Research (CHACR), 2022). This shift became evident with the public release of details on Russia’s military build-up near Ukraine’s borders during the winter of 2021/2022 (CHACR, 2022). Subsequently, the UK DI published approximately 130 intelligence updates during the first months of the Russo-Ukrainian war through the British Defence Ministry’s Twitter account @DefenceHQ, providing the public with awareness of the situation (CHACR, 2022). Despite criticisms regarding the selectivity or accuracy of these updates, they have been extensively utilised by journalists and the public, marking a shift in how intelligence is used to inform and influence public discourse (CHACR, 2022).

Throughout the ongoing war, the UK DI has persistently continued to share updates. A 3-month sample from 2023, covering the months of April, August, and December, included a total of eighty-three DI updates. Daily updates were published online in April and August 2023, while December 2023 saw a total of twenty-two updates. This selected subset underwent thematic analysis, a method used to systematically identify, organise, and interpret patterns or “themes“ within qualitative data. Through this approach, recurring themes within the DI updates were identified by examining the content for common topics, patterns, and nuances in how information was communicated. By analysing each update iteratively and reflexively, the analysis provided insight into the broader trends and priorities within UK DI’s public communication. This process allowed for categorisation into themes, such as military developments, leadership, and personnel, which reflect the areas where UK DI focused its messaging to inform and influence public discourse.

Though the subset is not exhaustive, insights were used to form an understanding of the entire UK DI social media communication in the context of the Russo-Ukrainian war. Table 1 presents a visual representation.

Table 1. Thematic analysis based on a subset (N = 83) of UK DI’s updates published on X/Twitter in April, August, and December 2023.

Theme	Characteristics	Prevalence
Military developments	Comments on Russian Federation (RF) military activities	29
Leadership	RF leadership changes, plans, and reorganisation	17
Personnel	RF recruitment, morale, and casualty figures	12
Information environment	RF narratives about Ukraine, cyber-attacks	7
Conditions in Ukraine, including occupied territories	Behaviour of occupation authorities, state of the energy infrastructure	7
Ukrainian military performance	Insights into defensive efforts, counterattacks, and assessments of (drone) strikes	6
Miscellaneous	Information regarding Belarus, RF economy, and other varied topics	5
Total		83

From this thematic analysis, it becomes apparent that the UK DI primarily contributed updates related to battlefield development in the Russo-Ukrainian war. For instance, typical posts in August 2023 contained remarks about Russian units having trouble fending off Ukrainian assaults: “struggling with battle fatigue and attrition in forward deployed regiments which have been in intense combat for over eight weeks” ([UK Ministry of Defence, 2023a](#)). Another example highlighted the Russian use of one-way attack unmanned aerial vehicles in strikes against Ukrainian port infrastructure on the Danube River ([UK Ministry of Defence, 2023b](#)). Additionally, the UK DI frequently reported on Russian leadership changes—both political and military. In mid-January 2023, the UK DI noted that the “Russian Chief of the General Staff (CGS) General Valery Gerasimov took personal command of the special military operation in Ukraine,” suggesting that “Gerasimov was pushing the limits of how far Russia’s political leadership would tolerate failure” ([UK Ministry of Defence, 2023c](#)).

The focus in the analysed subset of updates is mostly concentrated on (poor) Russian performance on the battlefield, leadership changes, and activities in the information environment, including cyber operations. Ukrainian military activity receives less attention, although the UK DI did produce updates on the aftermath of Ukrainian strikes with drones or other means ([UK Ministry of Defence, 2023d](#)). In doing so, the UK DI supported Ukrainian claims about the success of their attacks. Furthermore, the UK DI provided comments on the situation in Ukraine, describing the oppressive behaviour of occupation authorities towards the population, sham referendums, the dangers of mined areas, and the state of Ukrainian energy infrastructure due to continued Russian attacks ([UK Ministry of Defence, 2023e](#)).

Although presented as “Intelligence Updates,” the origin of intelligence in the UK DI’s daily updates remains unspecified. It is unlikely that the UK DI would prematurely release secret information publicly. As these updates do not cite sources and merely “marry up what’s already available in the Twittersphere,” the UK DI seems to primarily comment on known events in the Russo-Ukrainian war ([CHACR, 2022](#)). However, the UK DI might release declassified information originally sourced from classified materials, particularly when similar data is available from open sources like commercial imagery or unencrypted communications ([CHACR, 2022](#)). This would effectively mask UK DI’s release of information derived from its own secret collection assets ([CHACR, 2022](#)).

Although a pattern can be discerned from the content that UK DI chooses to distribute among its followers, the updates lack further analysis or background context for the presented findings. UK DI itself states in generic terms that by publishing intelligence assessments on Twitter it wants “to help explain the conflict” ([UK Government, 2023](#)). Interestingly, this lack of detailed sourcing and background information does not significantly impact external audiences. Since the onset of the Russian (re-)invasion in February 2022, British intelligence researcher Lomas has observed that the UK DI’s reporting ranks among “some of the most shared content on @Defence HQ’s timeline since the MoD joined Twitter in 2008” ([CHACR, 2022](#)). According to Lomas, the success of UK DI’s online material lies in its ability to present a straightforward series of facts regarding the situation on the ground ([CHACR, 2022](#)).

Israel Defence Forces Spokesperson’s Unit: Shaming Hammas with intelligence

Shifting focus from the approach of British intelligence during the Russo-Ukrainian war to Israeli strategies reveals a common thread in today’s intelligence

operations: the strategic use of information to shape perceptions. Scholarly research has examined the presence—or absence—of Israeli intelligence services in the public domain. A leading figure in this field is ([Magen, 2015](#), p. 253), who has analysed the motives and tactics of these services in their interactions with the media and public over the past 50 years. Her research identified four main strategies employed by these agencies.

The first strategy involves maintaining a veneer of secrecy, where intelligence agencies avoid direct media interactions and instead use intermediaries like the Prime Minister's Office to communicate indirectly. The second strategy, termed the “if you only knew” tactic, involves the selective disclosure of information to cover up operational failures, justified by the claim that releasing information could jeopardise future operations against dangerous adversaries ([Magen, 2015](#), p. 253). The third strategy is the utilisation of patriotic sentiments and collaboration with allied politicians to influence media narratives (p. 255). And the fourth and final strategy identified by Magen (p. 258) is the deliberate manipulation of information, including the use of disinformation campaigns and psychological tactics to steer media narratives. Magen notes that evolving societal and media dynamics pose fresh challenges to intelligence operations in the public domain, requiring adaptive strategies for media interaction. The era of unchallenged secrecy and fear-based tactics has waned, with Magen (p. 247) emphasising a critical balance between the public's right to information and the government's duty to protect national security.

Historically, intelligence services have sought to operate under the radar to shield their activities from public view, viewing intelligence as a critical asset to be safeguarded. However, [Magen \(2017, p. 272\)](#) points out that the rise of social media has diminished the ability of intelligence agencies to control information, increasing the necessity to proactively address the public's desire to know. In response, the Israeli intelligence agencies are now proactively utilising media platforms to pursue their goals, and thus recognising the need for a more engaged and responsive approach (p. 273).

During the recent ongoing operations in Gaza, the IDF strategically employed information as a tool in their tactical operations. This approach was prompted by the renewed phase of the Israeli-Palestinian conflict initiated by Hamas through their devastating attack on Israel on 7 October 2023, which primarily targeted civilians. As part of their information strategy, the IDF distributed several news releases that acknowledged close cooperation between the IDF and the Israel Security Agency (ISA) in their battle against Hamas. Specific contributions reported by the IDF Spokesperson's Unit include the ISA's questioning of detained Hamas operatives and the elimination of Hamas commanders ([Israel Defense Forces \(IDF\), 2023](#)).

Traditionally, the ISA has been a secretive organisation responsible for internal security, with a particular focus on countering terrorism and political subversion. However, according to one of its members, during the last decade, the ISA has gradually shifted towards greater openness. Previously, the prevailing perception was that “everything is secret,” but over time, the ISA embraced a more transparent approach ([Avidar and Magen, 2023, p. 5](#)).

Besides the ISA's activities, detailed insights into the operations of other Israeli intelligence units have also been disclosed. According to the IDF website and associated social media posts, a military intelligence unit known as “Unit 504” conducted approximately 30,000 telephone conversations with Palestinian leaders since the renewed phase of the conflict ensued on 7 October 2023. These leaders were urged to encourage evacuations among their constituents. Additionally, the unit sought information regarding the whereabouts of Hamas fighters ([i24NEWS English on X, 2023](#)). Unit 504 also reported the interrogation

of three hundred captured Hamas militants, swiftly sharing relevant information about tunnels and other relevant details with IDF units in the field.

Beyond these activities of Unit 504, the Israeli efforts at the intersection of intelligence and influence operations have expanded even further. Notably, since the attacks of 7 October 2023, the IDF Spokesperson's Unit has shared sensitive intelligence derived from human intelligence (HUMINT) and SIGINT sources. This approach contrasts with that of the UK DI, which does not allude to the origins of its updates.

For example, the IDF has published recordings of telephone conversations on social media between Israeli HUMINT operators and established Palestinian contacts. In these recordings, Palestinians shared information about Hamas members obstructing civilian evacuations—for instance, by confiscating car keys or preventing people from leaving altogether ([Hagari, 2023c](#)). The IDF Spokesperson's Unit has also published online intercepted phone calls in which Palestinian civilians complained about Hamas' misconduct, such as fighters seizing humanitarian aid and fuel ([Hagari, 2023d](#)). Further, the Israelis released audio recordings of an Israeli operator assuring the manager of the Shifa Hospital in Gaza regarding the free passage of persons from the premises of the hospital ([Hagari, 2023b](#)). The IDF released this conversation in November 2023 at a time when it was accused of blocking civilians from leaving this area. Additionally, the IDF released an intercepted conversation between two Hamas militants discussing a failed rocket launch that hit a hospital in Gaza—an incident initially attributed by international media outlets to the Israeli Air Force ([Hagari, 2023a](#)).

These examples are noteworthy because the Israelis deliberately choose to share information gathered through intelligence means (HUMINT and SIGINT) on social media platforms. This strategy aims to portray Hamas negatively worldwide, despite the potential risks involved. It raises questions about the confidential relationship between the HUMINT operators and their Palestinian contacts. Will these contacts continue to share information with their Israeli handlers if they fear their conversations might end up on Facebook? Furthermore, there are concerns about the secrecy of Israeli interception systems. An intelligence principle holds that if opponents are aware of eavesdropping capabilities, they may think twice before sharing information over channels, such as telephone lines ([Clark, 2016](#), p. 62).

Despite these concerns, the Israelis have continued the release of sensitive intelligence online. In March 2024, IDF spokesman Rear Admiral Daniel Hagari disclosed intercepted telephone conversations that implicated United Nations Relief and Works Agency (UNRWA) employees in cooperating with Hamas during the capture and subsequent hostage-taking of Israeli women on 7 October 2023. Hagari explained that despite the “difficult content,” the military chose to release the audio recordings of UNRWA staff who participated in the 7 October 2023 onslaught to “remind and not forget. Know that these women and girls in Hamas captivity are in danger.” He emphasised that the continued hostage-holding by Hamas necessitated Israel's continued operations in Gaza ([IDF Spokesperson's Unit, 2024](#)).

Ukrainian Military Intelligence: Communicating with COMINT

A third case in which intelligence is used in social media communications concerns the Main Intelligence Directorate of the Ukrainian Ministry of Defence, HUR MO.

Its approach also runs counter to the conventional wisdom that intelligence agencies should maintain a low profile to prevent drawing undue attention to their secretive operations. In this context, the “Intelligence Laboratory Express,” a Russian publication specialising in intelligence studies, highlighted the HUR as an outlier in early 2024. The journal described the HUR as “notably visible in the media,” asserting that its activities are “primarily aimed at achieving media success” and contain “clear propaganda elements” ([Intelligence Express Laboratory \(LIEKS\), 2024](#)).

This portrayal, while critical and shaped by the current Russo-Ukrainian conflict, brings attention to a significant point: the HUR’s widespread presence across six social media and messaging platforms, including Facebook, X/Twitter, Telegram, and Viber. The HUR makes use of these channels to share in-depth military information, humanise the conflict through personal accounts of its operatives, emphasise humanitarian activities, and actively interact with its followers ([Schrijver, 2024](#)).

The HUR is not unique in this approach. Similarly, the Ukrainian Security Service (SBU) manages numerous accounts across various social media platforms, posting updates about operational successes, law enforcement activities, and the apprehension of individuals suspected of collaborating with Russian forces ([Kaul, 2023](#)). To illustrate the extensive online activity of the HUR and SBU: both services published over 5,600 Telegram messages in the 2-year period following Russia’s large-scale invasion of Ukraine in February 2022.

The HUR’s social media accounts frequently document operations against Russian forces, particularly those conducted by Special Operations Forces (SOF) under its command, such as Group 13, Artan, and Timur. These units have gained attention for their activities, including Group 13’s destruction of three Russian naval vessels in the Black Sea: the corvette Ivanovets on 1 February 2024, the amphibious landing ship Tsezar Kunikov on 14 February 2024, and the patrol ship Sergei Kotov on 5 March 2024 ([Crimea.Realities, 2024](#)). The HUR has shared footage on social media showing attacks on these ships, reportedly captured by onboard cameras of Magura V maritime drones, also known as Unmanned Surface Vessels (USVs). Additionally, the HUR has released what it described as intercepted communications between Russian navy personnel discussing these incidents ([Ukrainska Pravda, 2024](#)).

This approach of openly disseminating sensitive intercepts, globally recognised as highly classified communications intelligence (COMINT), has challenged the conventional wisdom that intelligence services should prioritise protecting their collection methods. The HUR’s strategy has prompted a re-evaluation of this long-standing principle in intelligence circles.

The use of communication intercepts by the HUR in its social media postings in the aftermath of the attacks on Russian navy vessels, however, did not present a novel approach by the Ukrainian HUR. During the first 2 years of the Russian invasion, the HUR disseminated more than six hundred posts on its social media accounts containing the Ukrainian language hashtag #ГУРперехоплення (HURperekhoplennya; HURinterception). Besides that, the HUR also published material from other intelligence sources. On 1 March 2022, the HUR began to publish a series of lists with information on Russian and Belarusian military units ([Defence Intelligence of Ukraine, 2022a](#)).

These records included names, ranks, birthdays, and other personal information of military personnel. The HUR reported that the lists comprised names of service members who participated in or aided the Russian invasion ([Schrijver, 2024](#)). The intelligence service sought to encourage the surrender of enemy personnel with “doxing”—publishing

personally identifiable information online—and justified it by claiming that those people had contributed to Russia’s illegal invasion ([Jensen and Watts, 2022](#)).

Notwithstanding these examples, the release of communication intercepts to the public remains the most prevalent form of classified intelligence released by the HUR. The intercepted communications published by the HUR primarily consist of global system for mobile communications (GSM) signals captured through base transceiver stations under Ukrainian control. Despite Russian military regulations prohibiting the use of mobile phones, even within Russian borders, these interceptions continue to occur. This suggests that the Russian leadership may not be effectively enforcing their own policies or implementing sufficient measures to prevent this form of information leakage ([BBC News, 2023](#)). Russian soldiers, especially on the front lines, still find ways to acquire phones, sometimes stealing them from the Ukrainian population, to call home or colleagues ([Enea, 2022](#)).

The recorded conversations can be categorised as COMINT, because it entails the interception and analysis of the communications of government officials, military personnel, and other groups or individuals. In principle, similar to the Israeli case, if it becomes public knowledge that an entity has access to this information, then that tends to mean the end of this access ([Clark, 2016](#), p. 62). Despite concerns over losing access to intelligence sources, the HUR is continuing to release social media messages containing audio recordings of which the majority fits into three main categories: alleged Russian war crimes, Russian disillusionment in the war, including plans for desertion, and the weakness or corruption of the Russian military leadership ([Rothman *et al.*, 2024](#), p. 83). The novelty in the approach is that the HUR uses intercepted communication as content for its social media channels.

The first category is aimed at examples of alleged Russian war crimes: on 20 April 2022, the HUR disclosed an intercept ordering the execution of Ukrainian Prisoners of War (POWs) in Luhansk Oblast, with instructions to permanently eliminate most of them while sparing the highest-ranking ([Defence Intelligence of Ukraine, 2022b](#)). Following this, further intercepts exposed Russian forces looting equipment and dismissing their setbacks. By 23 May 2022, discussions among Donetsk People’s Republic (DPR) forces allied with the Russians revealed serious abuses, including acts of violence and theft ([Defence Intelligence of Ukraine, 2022c](#)). An intercept from June 2022 revealed the execution of a Ukrainian tank crew member, highlighting a policy of not sparing lives ([Defence Intelligence of Ukraine, 2022d](#)). Additionally, on 2 August 2022, a Russian’s use of banned phosphorus munitions was recorded, in violation of international laws ([Defence Intelligence of Ukraine, 2022e](#)).

The second category of intercepts illustrates the demoralisation within the Russian military. On 21 June 2022, a Russian man discussed the imminent threat of encirclement and substandard support from rear units ([Defence Intelligence of Ukraine, 2022f](#)). And on 21 August 2022, an officer highlighted the extensive refusal to fight among troops, hoping for an imminent withdrawal ([Defence Intelligence of Ukraine, 2022g](#)).

The third category contains examples of weak or corrupt Russian leadership. These audio intercepts released by the HUR provided a window into the mindset of Russian military personnel towards their leadership during the conflict in Ukraine. On 14 September 2022, a Russian military member in the Kharkiv area complained about the incompetence of his superiors: “there is no organization at all, I thought it was an army, but there is no army” ([Defence Intelligence of Ukraine, 2022h](#)). Similarly, on 28 November 2022, a military officer described his commanding officers as idiots who were hiding

themselves in the rear area while sending their troops on dangerous missions: “there is a minefield in front of you, start an attack” ([Defence Intelligence of Ukraine, 2022i](#)). On 26 December 2022, a Russian military member near Donetsk talked about the cowardice of staff officers, deserters, and the vain hope of withdrawal from the combat zone ([Defence Intelligence of Ukraine, 2022j](#)).

The authenticity of the audio intercepts released by the HUR is suggested by the language and discourse used within them ([Tikkanen, 2024](#), p. 107). However, one cannot rule out the possibility that audio experts may have altered the content. As a result, it is difficult to establish absolute confidence in the reliability of the intelligence material shared by the HUR. Nevertheless, the HUR intentionally selects and releases portions of intercepted audio that align with its communication strategy, aiming to stimulate public discussion on specific themes that it deems relevant.

Analysis

In modern warfare, public perception forms an integral part of the battleground, with information and narrative control becoming as crucial as traditional military assets. Military and intelligence organisations are using communication strategies to shape public opinion and counter opposing narratives. The UK DI, IDF Spokesperson’s Unit, and Ukraine’s HUR demonstrate this trend. Table 2 presents a comparison of how theories about communication strategies and mediatisation apply to these recent cases. It examines the tactics used by each organisation to disseminate intelligence on social media channels, focusing on three key areas: branding, shaming, and the influence of social media through mediatisation.

It is important to note here that these three categories are interrelated and that the third category (mediatisation) can best be understood as an overarching society-wide concept, entailing communication strategies as branding and shaming. Branding and shaming for their part are interrelated as well in the sense that branding can be viewed as a part of shaming. Indeed, when attributing certain negative behaviour to an adversary, the communicator itself is by comparison automatically framed more positively. This, however, should be seen as an additional effect of shaming, not as the main purpose. The main difference between the two, therefore, lies in the fact that branding most of the time is attributed to the communicator himself, and shaming is attributed to the opponent ([Hirschberger, 2021](#), p. 20).

Branding: An observer of the UK DI’s social media posts in the early months of the war suggested that the organisation uses intelligence updates for publicity ([Michaels, 2022](#)). These updates gain significance from their official source, rather than from their superior analysis. As an analyst observed, “the stuff you see on these twice-a-day slides is just skimming the surface” ([Washington Post, 2022](#)). A primary goal seems to be placing the UK DI and MoD in the spotlight ([Michaels, 2022](#)). Hence, the material published online on the ongoing Russo-Ukrainian war by the UK DI can be seen as a branding tool, bolstering both UK DI and MoD’s reputations as credible and authoritative sources. This aligns with Lomas’ observation that “strong engagement with the media has also developed trust which has paid dividends” ([CHACR, 2022](#)).

The IDF Spokesperson’s Unit and Ukraine’s HUR, unlike UK DI, are directly involved in ongoing conflicts. When it comes to social mediaposts in which intelligence (e.g. communication intercepts) is released, they appear to focus less on promoting their own positive qualities as communicators and much more on shaming their opponents. This difference

Table 2. Theories about communication strategies and mediatisation applied to recent cases of the UK DI, IDF Spokesperson's Unit, and Ukrainian HUR disseminating intelligence in their social media communication.

Theory and cases	Case 1: UK DI	Case 2: IDF Spokesperson's Unit	Case 3: Ukrainian HUR
Branding: promotion of positive qualities of the communicator	Spotlight UK DI and UK MoD; reinforce reputation as credible and authoritative	Not applicable	Not applicable
Shaming: undermining legitimacy of an opponent	Reports on Russian military shortcomings and operational failures; details of oppressive tactics in occupied territories	Portray Hamas negatively; and undermine Hamas' legitimacy in the ongoing conflict	Intercepted communications highlight poor living conditions of soldiers and corruption of commanders
Mediatisation: influence of social media	Bypasses traditional gatekeepers; interplay of information dissemination and institutional positioning	Enhances IDF's institutional prominence; reciprocal media relationship	Continuous reinforcement of Ukraine's conflict narrative

in approach highlights how branding strategies can vary significantly among military and intelligence organisations.

Transitioning to Shaming: The analysed sample of UK DI's social media posts reveals a focus on Russian military weaknesses. These posts offer detailed assessments of Russian operational failures, logistical hurdles, and strategic blunders. Additionally, the intelligence service provides insights into the situation in Ukrainian territories occupied by Russia, detailing the oppressive tactics used by Russian-installed authorities and the organisation of illegitimate referenda. This approach aligns with the concept of shaming as a means of undermining an opponent's legitimacy. [Hirschberger \(2021\)](#) explains shaming as a tactic whereby one points out an opponent's bad behaviour or mistakes to damage their reputation and erode their standing. The UK DI primarily focuses on Russian operations, particularly their negative aspects. Ukrainian operations are much less discussed in the material. This imbalance further indicates that the releases are not intended to provide a holistic overview of the ongoing conflict. Rather, they aim to cast the Russians in a negative light. This subjectivity contrasts with and dilutes the idea of asserting oneself as a reliable intelligence supplier.

The IDF Spokesperson's Unit's release of communication intercepts and taped recordings is not primarily focused on branding its own organisation. Rather, these disclosures aim to portray Hamas in a negative light. This approach forms part of a broader Israeli governmental effort to demonstrate that Hamas prioritises self-preservation over civilian safety. By disseminating such information, the IDF seeks to influence public perception and challenge Hamas's legitimacy in the ongoing conflict. However, this tactic raises ethical concerns regarding the use of intercepted communications and taped recordings for public consumption. It could potentially compromise operational security or expose Palestinians to retaliation from Hamas for communicating with the Israeli military.

In a similar vein, the Ukrainian HUR employs shaming tactics in its steady release of communication intercepts on an almost daily basis. From its collection of Russian communications, Ukrainian military intelligence carefully selects those that underscore the poor living conditions of Russian soldiers, instances of corruption among commanders, and discussions about war crimes committed by Russian forces, including looting, rape,

and executions (Schrijver, 2023). Basically, the interceptions have been weaponised to degrade the Russian war effort in an attempt to negatively influence people's perceptions of the Russian military. This tactic mirrors Israel's approach, aiming to evoke negative emotions about the opponent.

Mediatisation: The concept of mediatisation is evident in the strategies employed by various military and intelligence organisations in their communication efforts. The UK DI, for instance, uses social media to circumvent traditional gatekeepers such as the news media. This approach allows UK DI to directly influence public discourse, support Ukraine, and confront Russian disinformation (Centre for Emerging Technology and Security, 2022). However, these releases also bring attention to UK DI and MoD themselves, demonstrating the interplay between information dissemination and institutional positioning. This strategy illustrates modern conflict communication, where intelligence services actively participate in shaping media narratives and raise their own profiles through social media.

Similarly, the IDF has adapted their communication to media logic (i.e. based on attention and emotion, rather than on political rationale), particularly that of social media platforms. This reflects a new understanding that information can be as crucial as traditional military assets (Massa and Anzera, 2023, p. 364). By releasing intercepted communications via these channels, the IDF, like the UK MoD, bypasses traditional media gatekeepers, enabling direct engagement with audiences in Israel and abroad.

Ukraine's HUR also leverages digital channels to maintain a presence in the information environment, consistently promoting the Ukrainian narrative of fighting a just war against an invader, whose ruthlessness is repeatedly emphasised through the release of communication intercepts (Tikkanen, 2024, p. 107). Further, the service emphasises Russian failures. This approach aligns with Strömbäck's (2008) concept of reciprocal media-political institution relationships, where the HUR not only shapes media coverage through information releases but also benefits from the resulting publicity. However, it is important to note that the HUR's efforts are part of a larger coordinated information strategy involving multiple Ukrainian state and non-state organisations (Ekman and Nilsson, 2023, p. 7). The effectiveness of this approach can vary depending on the target audience, with different narratives resonating differently in Ukraine, Russia, and Western countries.

These examples illustrate how intelligence organisations are adapting to the mediatised landscape, using social media platforms to directly engage with audiences, shape narratives, and position themselves in the public eye.

Conclusions

Communication during conflicts is complex and occurs in a variety of constellations. It is influenced by multiple factors, including the speed with which information can be disseminated via social media, which enables rapid and wide distribution of intelligence that may even outpace traditional media and enemy propaganda. This rapid dissemination raises further considerations about the risks of politicisation and the potential perception of intelligence releases as propagandistic, rather than as sources of factual reporting from conflict zones. Intelligence services must consider how their communications might be interpreted—particularly when aimed at shaping public narratives, rather than merely informing.

Additional factors influencing communication include the trustworthiness of disclosed information, as intelligence releases via social media may raise questions about authenticity and the risk of manipulation as well as the operational risks associated with using

intelligence for strategic communications. Moreover, the decision to release such information is shaped by the specific conflict context and the societal and cultural background of the states concerned. The stakes for Israel and Ukraine, for example, are higher than for the United Kingdom, as public opinion and national engagement with the conflict play significant roles in guiding communication approaches.

Nevertheless, a shift from the traditional practice of protecting intelligence methods and sources is evident. This research reveals that sensitive intelligence material has become content for social media campaigns, signalling a substantial shift in operational paradigms. Intelligence is being used as a strategic communication tool not only to inform but also to influence public opinion, counter enemy narratives, and justify military actions. This suggests a novel approach where the perceived benefits of public disclosure outweigh the risks of revealing capabilities and, potentially, sources. Yet, such disclosures remain selective and contextual, as intelligence agencies weigh both benefits and risks of shaping narratives in line with public opinion and engagement levels.

A dominant trend, therefore, is that intelligence services are grappling with the balance between operational secrecy and the potential benefits of public disclosure. Selective transparency is on the rise, but so too are the associated risks, including the exposure of sensitive sources or methods, particularly in the release of HUMINT and SIGINT materials by agencies, such as the IDF and HUR. This study adopted a comparative approach, focusing on three cases selected for their involvement in ongoing conflicts and their distinct approaches to intelligence sharing on social media through overt and identifiable accounts. As a result, the findings of this study cannot be generalised to cases beyond its scope. Nonetheless, agencies must carefully weigh the impact on their reputations and the risk of eroding public trust if their communications are perceived as overly influenced by national agendas, rather than grounded in objective reporting. This balancing act between strategic influence and maintaining public trust underscores the evolving role of intelligence agencies in the age of information warfare.

Mediatization plays a key role in this process, especially for organisational reputation-building purposes. Social media platforms are well suited to this objective, as they allow intelligence agencies to bypass traditional gatekeepers, including investigative journalism and conventional (print) media. By using social media, these agencies are not just gathering information but are also actively shaping the narrative of conflicts to align with their own agendas. While intelligence organisations operate within a broader national military and security system, they still pursue their own organisational interests through the use of social media.

This approach underscores the changing nature of information warfare and the increasing importance of information as a strategic asset, blurring the lines between covert intelligence operations and public influence campaigns. Within the information warfare spectrum, which ranges from communication to indoctrination, intelligence agencies assess that their information can be strategically employed to build trust and amplify emotional resonance with target audiences (Clack and Johnson, 2021, p. 1).

Funding

This research received no external funding.

Author Contributions

Conceptualization, P.S., L.N., and P.P.; Investigation, P.S.; Writing—original draft preparation, P.S., L.N., and P.P.; Writing—review and editing, P.S., L.N., and P.P. All authors read and agreed to the published version of the manuscript.

Data Availability Statement

The data presented in this study is available on request from the corresponding author.

Disclosure statement

No potential conflict of interest was reported by the authors.

References

- Avidar, R. and Magen, C.** (2023) 'Negative spaces as a strategic decision: The case of the Israeli Security Agency', *Public Relations Review*, 49(2), pp. 2–7. doi: [10.1016/j.pubrev.2023.102315](https://doi.org/10.1016/j.pubrev.2023.102315).
- Bartlett, J. and Reynolds, L.** (2015) *The state of the art 2015: A literature review of social media intelligence capabilities for counter-terrorism*. London: Demo.
- BBC News** (2023) *Makiivka: Russia blames missile attack on soldiers' mobile phone use*. Available at: <https://www.bbc.com/news/world-europe-64159045> (Accessed: 3 June 2024).
- Centre for Emerging Technology and Security** (2022) *The future of open-source intelligence for UK national security*. Available at: <https://cetas.turing.ac.uk/publications/future-open-source-intelligence-uk-national-security> (Accessed: 18 September 2024).
- Centre for Historical Analysis and Conflict Research (CHACR)** (2022) *In-depth briefing 28: Weaponising the truth? UK intelligence, public information and Ukraine*. Available at: <https://chacr.org.uk/2022/04/26/in-depth-briefing-28-weaponising-the-truth-uk-intelligence-public-information-and-ukraine/> (Accessed: 25 May 2024).
- Clack, T. and Johnson, R.** (2021) *The world information war: Western resilience, campaigning, and cognitive effects*. London: Routledge.
- Clark, R.M.** (2016) 'The protection of intelligence sources and methods'. *The Intelligence: Journal of US Intelligence Studies*, 22(2), pp. 55–69.
- Crimea.Realities** (2024) *Three times hit, once destroyed: the combat path of the Russian corvette 'Sergey Kotov'*. Available at: <https://ru.krymr.com/a/bojevoy-put-rossiyskogo-korveta-sergey-kotov-/32848566.html> (Accessed: 20 September 2024).
- Defence Intelligence of Ukraine (@DI_Ukraine)** (2022a) '#ОкупантиРФ !! Кожний українець повинен знати...', Twitter. 1 March. Available at: https://x.com/DI_Ukraine/status/1498576358976503812 (Accessed: 20 September 2024).
- Defence Intelligence of Ukraine (@DI_Ukraine)** (2022b) '#ГУРперехоплення "Плених в Попасной приказано убити..."', Twitter. 20 April. Available at: https://x.com/DI_Ukraine/status/1516863387401080833 (Accessed: 19 September 2024).
- Defence Intelligence of Ukraine (@DI_Ukraine)** (2022c) '#ГУРперехоплення Згвалтування, мародерство, масові злочини...', Twitter. 23 May. Available at: https://x.com/DI_Ukraine/status/1528637578475347968 (Accessed: 13 November 2024).
- Defence Intelligence of Ukraine (@DI_Ukraine)** (2022d) '#ГУРперехоплення "Одного в плен взяли танкиста..."', Twitter. 2 June. Available at: https://x.com/DI_Ukraine/status/1532442740138688514 (Accessed: 13 November 2024).
- Defence Intelligence of Ukraine (@DI_Ukraine)** (2022e) '#ГУРперехоплення "'О, фосфор полетел" Окупант розповідає...', Twitter. 2 August. Available at: https://x.com/DI_Ukraine/status/1554436854015033345 (Accessed: 19 September 2024).

Defence Intelligence of Ukraine (@DI_Ukraine) (2022f) ‘#ГУРперехоплення “Силовики, алкаші. Хорошого нічого...”’, Twitter. 21 June. Available at: https://x.com/DI_Ukraine/status/1539252939356880900 (Accessed: 19 September 2024).

Defence Intelligence of Ukraine (@DI_Ukraine) (2022g) ‘#ГУРперехоплення “МЫ УЖЕ ВСЁ, У НАС ЛЮДИ СДАЮТСЯ...”’, Twitter. 21 August. Available at: https://x.com/DI_Ukraine/status/1561234801830551557 (Accessed: 13 November 2024).

Defence Intelligence of Ukraine (@DI_Ukraine) (2022h) ‘#ГУРперехоплення !! “Я ДУМАЛІ, ТУТ АРМІЯ, А ТУТ НЕ АРМІЯ...”’, Twitter. 14 September. Available at: https://x.com/DI_Ukraine/status/1569929787010945026 (Accessed: 13 November 2024).

Defence Intelligence of Ukraine (@DI_Ukraine) (2022i) ‘#ГУРперехоплення !! “ВСЕ “ВОЕННЫЕ ПОЛИЦИИ” ЗАБИТЫ...”’, Twitter. 28 November. Available at: https://x.com/DI_Ukraine/status/1597262175021989890 (Accessed: 13 November 2024).

Defence Intelligence of Ukraine (@DI_Ukraine) (2022j) ‘#ГУРперехоплення !! “МЫ НОЧЬЮ ЕЩЕ 20 НАШИХ...”’, Twitter. 26 December. Available at: https://x.com/DI_Ukraine/status/1607418465110851585 (Accessed: 13 November 2024).

Dylan, H. and Maguire, T.J. (2023) ‘Secret intelligence and public diplomacy in the Ukraine war’, *Survival* 64(4), pp. 33–74. doi: [10.1080/00396338.2022.2103257](https://doi.org/10.1080/00396338.2022.2103257).

Ekman, I. and Nilsson, P.E. (2023) ‘Ukraine’s information front: strategic communication during Russia’s full-scale invasion of Ukraine’, *FOI Sweden*. Available at: <https://www.foi.se/rest-api/report/FOI%20Memo%208173> (Accessed: 25 May 2024).

Enea (2022) *The mobile network battlefield in Ukraine – part 2*. Available at: <https://www.enea.com/insights/the-mobile-network-battlefield-in-ukraine-part-2/> (Accessed: 30 August 2023).

Griffin, A. (2016) ‘What is pizzagate? The Hillary Clinton conspiracy theory that led to a man opening fire in a restaurant’, *The Independent*, 5 December 2016. Available at: <https://www.independent.co.uk/tech/pizzagate-what-is-it-explained-hillary-clinton-paedophile-conspiracy-gunman-fake-news-a7456681.html> (Accessed: 20 September 2024).

Hagari, D. (@IDFSpokesperson) (2023a) ‘Attached is a recording of a conversation between Hamas operatives regarding the Islamic Jihad failed rocket launch on the hospital on October 17, 2023’, *Twitter*. Available at: <https://x.com/IDFSpokesperson/status/1714541413944250869> (Accessed: 19 September 2024).

Hagari, D. (@IDFSpokesperson) (2023c) ‘Over the past few days, soldiers and officers from Unit 504 of the IDF’s intelligence directorate (J2) have notified residents in the northern Gaza Strip of the need to evacuate to the south for their safety >> <https://t.co/oUcu68koBo>’, *Twitter*. Available at: <https://twitter.com/IDFSpokesperson/status/1717467662618337778> (Accessed: 8 December 2023).

Hagari, D. (@IDFSpokesperson) (2023b) ‘Following the repeated calls by the IDF to Gazan residents to evacuate from northern Gaza for their own safety, the IDF is enabling a passage from the Shifa, Rantisi and Nasser hospitals’, *Twitter*. Available at: <https://x.com/IDFSpokesperson/status/1723642738820714849> (Accessed: 19 September 2024).

Hagari, D. (@IDFSpokesperson) (2023d) ‘In a call that took place yesterday, on November 2nd with an official in the Medical System in Gaza, it was revealed again that Hamas is holding the fuel reserves in the Gaza Strip and is using it >> <https://t.co/eXADezfwFo>’, *Twitter*. Available at: <https://twitter.com/IDFSpokesperson/status/1720346785124688241> (Accessed: 8 December 2023).

- Hirschberger, B.** (2021) *External communication in social media during asymmetric conflicts: A theoretical model and empirical case study of the conflict in Israel and Palestine*. Bielefeld: Verlag transcript.
- Hjarvard, S.** (2008) 'The mediatization of society', *Nordicom Review*, 29, pp. 102–131.
- Hoskins, A. and O'Loughlin, B.** (2015) 'Arrested war: The third phase of mediatization', *Information, Communication & Society*, 18(11), pp. 1320–1338. doi: [10.1080/1369118X.2015.1068350](https://doi.org/10.1080/1369118X.2015.1068350).
- Hulnick, A.S.** (2004) *Keeping us safe: Secret intelligence and homeland security*. Westport, CT: Praeger.
- Intelligence Express Laboratory (LIEKS)** (2024) *LIEKS–Glavnaya*. Available at: <https://intelligence-express.ru> (Accessed: 7 August 2024).
- Israel Defense Forces (IDF)** (2023) *Over 500 Hamas and Islamic Jihad terrorists were apprehended by the IDF and ISA over the past month*, IDF press release. Available at: <https://www.idf.il/en/mini-sites/hamas-israel-war-24/all-articles/over-500-hamas-and-islamic-jihad-terrorists-were-apprehended-by-the-idf-and-isa-over-the-past-month/> (Accessed: 14 June 2024).
- Israel Defense Forces (IDF) Spokesperson's Unit** (2024) *IDF releases recordings of UNRWA employees from October 7: 'We have hostages, I caught one'*. Available at: <https://www.youtube.com/watch?v=tJVLBsCTe2A> (Accessed: 28 July 2024).
- i24NEWS English on X** (2023) *Unit 504 maneuvers support, gathers intelligence to incriminate targets, influences and leads the effort to evacuate the population to southern Gaza*. Available at: https://x.com/i24NEWS_EN/status/1726612014758281697 (Accessed: 19 September 2024).
- Jensen, E. and Watts, S.** (2022) *Ukraine symposium – doxing enemy soldiers and the law of war*, Lieber Institute West Point. Available at: <https://lieber.westpoint.edu/doxing-enemy-soldiers-law-of-war/> (Accessed: 19 September 2024).
- Jurek, A., Mulvenna, M.D. and Bi, Y.** (2015) 'Improved lexicon-based sentiment analysis for social media analytics'. *Security Informatics*, 4(1), pp. 1–13. doi: [10.1186/s13388-015-0024-x](https://doi.org/10.1186/s13388-015-0024-x).
- Kaul, E.C.** (2023) *Ukraine's current counterintelligence capabilities*. Available at: <https://www.ponarseurasia.org/ukraines-current-counterintelligence-capabilities/> (Accessed: 15 May 2024).
- Krain, M.** (2012) 'J'accuse! Does naming and shaming perpetrators reduce the severity of genocides or politicides?', *International Studies Quarterly*, 56(3), pp. 574–589. doi: [10.1111/j.1468-2478.2012.00732.x](https://doi.org/10.1111/j.1468-2478.2012.00732.x).
- Krotz, F.** (2018) 'Explaining the mediatization approach', in Olsson, T., Hill, A. and Bødker, B. (eds.) *Critical perspectives on media, power and change*. London: Routledge, pp. 85–102.
- Lomas, D.W.B. and Ward, S.** (2022) 'Public perceptions of UK intelligence: still in the dark?', *The RUSI Journal*, 167(2), pp. 6–17. doi: [10.1080/03071847.2022.2090426](https://doi.org/10.1080/03071847.2022.2090426).
- Magen, C.** (2015) 'Media strategies and manipulations of intelligence services: the case of Israel', *International Journal of Press/Politics*, 20(2), pp. 247–265. doi: [10.1177/1940161214556514](https://doi.org/10.1177/1940161214556514).
- Magen, C.** (2017) 'Strategic communication of Israel's intelligence services: countering new challenges with old methods', *International Journal of Strategic Communication*, 11(4), pp. 269–285. doi: [10.1080/1553118X.2017.1334207](https://doi.org/10.1080/1553118X.2017.1334207).
- Maltby, S.** (2012) 'The mediatization of the military', *Media, War & Conflict*, 5(3), pp. 255–268. doi: [10.1177/175063521244479](https://doi.org/10.1177/175063521244479).

- Massa, A. and Anzera, G.** (2023) 'The platformization of military communication: The digital strategy of the Israel defense forces on Twitter', *Media, War & Conflict*, 16(3), pp. 364–383. doi: [10.1177/17506352221101257](https://doi.org/10.1177/17506352221101257).
- Mateo, E.** (2022) "All of Belarus has come out onto the streets": exploring nationwide protest and the role of pre-existing social networks', *Post-Soviet Affairs*, 38(1–2), pp. 26–46. doi: [10.1080/1060586X.2022.2026127](https://doi.org/10.1080/1060586X.2022.2026127).
- McLoughlin, L., Ward, S. and Lomas, D.W.B.** (2020) 'Hello, world: GCHQ, Twitter and social media engagement', *Intelligence and National Security*, 35(2), pp. 233–251. doi: [10.1080/02684527.2020.1713434](https://doi.org/10.1080/02684527.2020.1713434).
- Michaels, J.** (2022) *Ukraine: the daily intelligence event*, Royal United Services Institute. Available at: <https://rusi.org/explore-our-research/publications/commentary/ukraine-daily-intelligence-event> (Accessed: 19 September 2024).
- Mortensen, P.B.** (2012) 'It's the central government's fault: elected regional officials' use of blame-shifting rhetoric', *Governance*, 25(3), pp. 439–461. doi: [10.1111/j.1468-0491.2012.01585.x](https://doi.org/10.1111/j.1468-0491.2012.01585.x).
- Omand, D.** (2022) 'How spies think: ten lessons in intelligence', *Journal of Intelligence, Conflict, and Warfare*, 4(3), pp. 244–250. doi: [10.21810/jicw.v4i3.4201](https://doi.org/10.21810/jicw.v4i3.4201).
- Petersen, K.L.** (2019) 'Three concepts of intelligence communication: awareness, advice or co-production?', *Intelligence and National Security*, 34(3), pp. 317–328. doi: [10.1080/02684527.2019.1553371](https://doi.org/10.1080/02684527.2019.1553371).
- Pew Research Center** (2015, 23 November) *Trust in government: 1958–2015*. Available at: <https://www.pewresearch.org/politics/2015/11/23/1-trust-in-government-1958-2015/> (Accessed: 18 September 2024).
- Rey, M.** (2017) 'Preventing a mobilization from spreading: Assad and the electronic war', in Lenze, N., Schriwer, C. and Abdul Jalil, Z. (eds.) *Media in the Middle East: activism, politics, and culture*. Cham: Springer, pp. 89–106.
- Riemer, O. and Sobelman, D.** (2023) 'Coercive disclosure: the weaponization of public intelligence revelation in international relations', *Contemporary Security Policy*, 44(2), pp. 276–307. doi: [10.1080/13523260.2022.2164122](https://doi.org/10.1080/13523260.2022.2164122).
- Rothman, M., Peperkamp, L. and Rietjens, S. (eds.)** (2024) *Reflections on the Russia-Ukraine war*. Leiden: Leiden University Press. doi: [10.24415/9789087284343](https://doi.org/10.24415/9789087284343).
- Schimmelfennig, F.** (2001) 'The community trap: liberal norms, rhetorical action, and the eastern enlargement of the European Union', *International Organization*, 55(1), pp. 47–80. doi: [10.1162/002081801551414](https://doi.org/10.1162/002081801551414).
- Schrijver, P.** (2023) 'The wise man will be master of the stars: the use of Twitter by the Ukrainian military intelligence service', *Irregular Warfare Initiative*. Available at: <https://irregularwarfare.org/articles/the-wise-man-will-be-master-of-the-stars-the-use-of-twitter-by-the-ukrainian-military-intelligence-service/> (Accessed: 7 August 2024).
- Schrijver, P.** (2024) 'From the shadows to the social sphere: Ukraine's strategy of engagement', *Irregular Warfare Initiative*. Available at: <https://irregularwarfare.org/articles/from-the-shadows-to-the-social-sphere-ukraines-strategy-of-engagement/> (Accessed: 1 July 2024).
- Strömbäck, J.** (2008) 'Four phases of mediatization: an analysis of the mediatization of politics', *The International Journal of Press/Politics*, 13(3), pp. 228–246. doi: [10.1177/1940161208319097](https://doi.org/10.1177/1940161208319097).
- Tikkanen, R.** (2024) *Intercepted phone calls at the Russo-Ukrainian war: cyberoperation or propaganda campaign?* Available at: <https://www.theseus.fi/handle/10024/854656> (Accessed: 10 July 2024).

UK Government (2022) *Defence Intelligence – communicating probability*. Available at: <https://www.gov.uk/government/news/defence-intelligence-communicating-probability> (Accessed: 19 June 2024).

UK Ministry of Defence GB (@DefenceHQ) (2023a) '(2/5) 58 CAA is highly likely struggling with battle fatigue and attrition in forward deployed regiments which have been in intense combat for over eight weeks', *Twitter*. Available at: <https://x.com/DefenceHQ/status/1686249944670216192> (Accessed: 13 November 2024).

UK Ministry of Defence GB (@DefenceHQ) (2023b) '(1/4) In the last two weeks, Russia has conducted several waves of strikes against Ukrainian ports on the Danube River using Iranian-produced one-way attack uncrewed aerial vehicles (OWA UAVs)', *Twitter*. Available at: <https://x.com/DefenceHQ/status/1687340228422283265> (Accessed: 20 June 2024).

UK Ministry of Defence GB (@DefenceHQ) (2023c) '(1/4) On 11 January 2023, Russian Chief of the General Staff (CGS) General Valery Gerasimov took personal command of the “special military operation” in Ukraine', *Twitter*. Available at: <https://x.com/DefenceHQ/status/1642055052629012480> (Accessed: 20 June 2024).

UK Ministry of Defence GB (@DefenceHQ) (2023d) 'Latest defence intelligence update on the situation in Ukraine – 31 August 2023. Find out more about defence intelligence's use of language: [#StandWithUkraine](https://ow.ly/FX8K50PGclJ) <https://t.co/zgmtfOkEIT>', *Twitter*. Available at: <https://x.com/DefenceHQ/status/1697117712776913027> (Accessed: 13 November 2024).

UK Ministry of Defence GB (@DefenceHQ) (2023e) 'Latest defence intelligence update on the situation in Ukraine – 17 August 2023. Find out more about defence intelligence's use of language: [#StandWithUkraine](https://ow.ly/QXHl50PAcvZ) <https://t.co/quzREoEomm>', *Twitter*. Available at: <https://x.com/DefenceHQ/status/1692049325780595013> (Accessed: 13 November 2024).

Ukrainska Pravda (2024) *Ukrainian intelligence intercepts Russian pilots' discussion of TsezarKunikov warship: wreckage and patch of oil*. Available at: <https://www.pravda.com.ua/eng/news/2024/02/14/7441839/> (Accessed: 20 September 2024).

Urman, A., Ho, J.C. and Katz, S. (2021) 'Analyzing protest mobilization on Telegram: the case of 2019 anti-extradition bill movement in Hong Kong', *PLoS One*, 16(10), p. e0256675. doi: [10.1371/journal.pone.0256675](https://doi.org/10.1371/journal.pone.0256675).

Vox (2024) *Fighting the spread of online disinformation: an interview with Bellingcat founder Eliot Higgins*. Available at: <https://www.voxweb.nl/english/fighting-the-spread-of-online-disinformation-an-interview-with-bellingcat-founder-eliot-higgins> (Accessed: 20 September 2024).

Washington Post (2022) *How UK intelligence came to tweet the lowdown on the war in Ukraine*, 22 April. Available at: <https://www.washingtonpost.com/world/2022/04/22/how-uk-intelligence-came-tweet-lowdown-war-ukraine/> (Accessed: 6 July 2024).

Zegart, A. and Morell, M. (2019) 'Spies, lies, and algorithms: why US intelligence agencies must adapt or fail', *Foreign Affairs*, 98(3), pp. 85–96. Available at: <https://www.foreignaffairs.com/united-states/spies-lies-and-algorithms> (Accessed: 30 May 2023).

Zeitsoff, T. (2017) 'How social media is changing conflict', *Journal of Conflict Resolution*, 61(9), pp. 1970–1991. doi: [10.1177/0022002717721392](https://doi.org/10.1177/0022002717721392).