International Journal of Intelligence and CounterIntelligence

ISSN: 0885-0607 (Print) 1521-0561 (Online) Journal homepage: www.tandfonline.com/journals/ujic20

Ukrainian Intelligence's Use of Telegram in Wartime

Peter Schrijver

To cite this article: Peter Schrijver (08 Jul 2025): Ukrainian Intelligence's Use of Telegram in Wartime, International Journal of Intelligence and CounterIntelligence, DOI: 10.1080/08850607.2025.2522222

To link to this article: https://doi.org/10.1080/08850607.2025.2522222

Published online: 08 Jul 2025.

International Journal of Intelligence and CounterIntelligence, 0: 1–27, 2025
ISSN: 0885-0607 print/1521-0561 online
DOI: 10.1080/08850607.2025.2522222

Routledge
Taylor & Francis Group

PETER SCHRIJVER

Ukrainian Intelligence's Use of Telegram in Wartime

Abstract: Since the start of Russia's full-scale invasion of Ukraine in 2022, the Main Directorate of Intelligence (HUR) has adopted a structured, public-facing communication strategy on Telegram that diverges from conventional intelligence practice. This approach integrates three recurring functions: projecting institutional legitimacy, targeting the adversary through disclosure, and mobilizing domestic publics. In doing so, the HUR turned intelligence communication into an ongoing process of public engagement rather than episodic outreach. These patterns underpin an emerging concept of *participatory intelligence communication*. The HUR's case demonstrates how, under high-intensity conflict, a state intelligence service may use digital platforms to coordinate narrative control, reinforce legitimacy, and enlist the public as contributors. While grounded in Ukraine's specific wartime conditions, these findings extend existing frameworks of intelligence communication and offer broader insight into how intelligence agencies may reconfigure their public role in wartime.

Peter Schrijver, M.A., is a researcher at the Faculty of Military Sciences of the Netherlands Defence Academy, Breda, the Netherlands. He is a lieutenant colonel in the Netherlands Army and has been deployed to Bosnia-Herzegovina and Afghanistan. The author can be contacted at p.schrijver@fgga.leidenuniv.nl.

INTRODUCTION

Intelligence services have traditionally operated behind a veil of secrecy to protect their methods, sources, and operational imperatives. This confidentiality has long been a cornerstone of intelligence work, but it now faces growing challenges in the digital age. The rapid circulation of information on social media, the influence of online discourse, and rising public demands for transparency have placed pressure on even the most secretive institutions.[1] Ukraine's Main Directorate of Intelligence (HUR) of the Ministry of Defense operates within this tension between secrecy-oriented intelligence practices and the demands of continuous public communication in a media-saturated wartime environment.

Amid the ongoing war between Russia and Ukraine, the HUR has embraced a public-facing strategy that departs from secrecy-driven norms. It shares intelligence-related content daily basis via Telegram and other social media platforms.[2] This approach is defined by sustained, interactive engagement with the public. In contrast, most Western intelligence agencies remain more restrained. During late 2021 and early 2022, the United Kingdom and United States selectively released intelligence about Russian troop movements near Ukraine's borders.[3] These announcements were episodic and strategically timed, designed to influence international opinion and deter aggression.[4] Most Western agencies continue to justify a cautious posture by citing legal and bureaucratic constraints, as well as fears of potential misuse or unintended consequences of shared information.[5]

By comparison, the HUR's strategy is broader and more dynamic. Using Telegram as a broadcast platform, the HUR disseminates multiple messages each day, often including operational footage and thematic intelligence updates. This divergence prompts questions about whether existing models of intelligence communication, largely developed in peacetime and Western contexts, adequately account for this form of persistent public engagement.

The HUR's communication strategy mirrors patterns observed by Olsson and Eriksson, identified within Swedish public agencies. These agencies increasingly use social media to engage the public through personalized content and informal communication styles.[6] In the context of intelligence, responsiveness to social media dynamics introduces both constraints and opportunities. Agencies must balance openness with the imperative to protect sensitive operations. When managed effectively, this visibility can support what scholars describe as an "effective intelligence lobby" in the public sphere, allowing agencies to counter criticism and assert their own voice rather than communicating solely through political or institutional superiors.[7] Scholars such as De Graaff and Hijzen argue that proactive communication is essential for intelligence services to build public legitimacy and counter negative perceptions.[8] As Hulnick observed over two decades

ago, carefully regulated openness can be as important in democratic societies as secrecy itself.[9]

The tension between secrecy and openness intensifies in the digital era. Platforms like Telegram, an application combining private messaging with public broadcasting, challenge intelligence services to reach mass audiences while maintaining operational discretion. Telegram has emerged as an especially important platform in the Russo-Ukrainian war: its scalability allows messages to reach millions of users, and it was already popular in Eastern Europe before the full-scale Russian invasion of Ukraine.[10] By 2023, 72% of Ukrainians cited Telegram as a primary news source, up from 63% the year before.[11] Recognizing this shift in information consumption, Ukrainian authorities adapted their communication strategies to maximize Telegram's potential despite concerns over the platform's Russian origins and its susceptibility to disinformation.[12] Telegram's structure, combining public broadcasting, group discussion, and private interaction, offers both flexibility and reach for Ukrainian agencies, including the HUR.

However, Telegram's utility comes with risks. Founded by Pavel Durov, the platform's Russian origins and relatively lenient moderation policies have raised concerns among Ukrainian officials about surveillance vulnerabilities and the spread of disinformation. These concerns intensified following Durov's arrest in France in 2024 and renewed scrutiny of Telegram's legal compliance and content regulation.[13] Despite these issues, Ukrainian agencies have continued to use Telegram for its immediacy, accessibility, and capacity for broad public engagement.

The HUR uses Telegram not only for one-way communication but also for two-way interaction. The agency uses the platform to enable rapid dissemination of updates while inviting public participation in intelligence efforts. For example, the HUR's official "Main Intelligence Bot" allows Ukrainian citizens to report enemy movements or suspected collaborators via chat, crowdsourcing reports on Russian troop movement from the population.[14] Information gathered through this type of chatbot has reportedly contributed to the destruction of enemy warehouses and equipment, directly integrating civilians into intelligence collection.[15] Similarly, the HUR's "I Want to Live" project provides Russian soldiers with a secure channel (via Telegram and other messaging applications) to arrange their surrender to Ukraine, offering guidance on how to safely defect under the Geneva Conventions.[16] These initiatives illustrate how the HUR uses Telegram to engage both supporters and adversaries. The public is not only a consumer of intelligence updates but also a contributor to intelligence operations and a target for influence, as the HUR seeks to encourage enemy defections.

Despite the growing relevance of social media in intelligence practices, research has largely focused on Western intelligence services, such as the

Central Intelligence Agency or Government Communications Headquarters, or military entities such as the Israel Defense Forces and the British Army.[17] These studies often highlight risk-averse and unidirectional communication strategies, which prioritize broadcasting safe, nonoperational content over interaction.[18] This cautious approach is understandable given concerns about operational security and political oversight. However, far less attention has been given to non-Western and wartime contexts, particularly Ukraine's experience, where more persistent and participatory strategies are emerging.[19] This case raises the question of whether existing conceptual frameworks, shaped largely in peacetime and Western environments, fully capture these developments. As Boichak argues, digital media afford opportunities for remote participation in wars, as they increasingly blur "the boundaries between military and civilian actors, physical and mediated battlefronts, and weapons and witnesses."[20]

A review of the HUR's Telegram communication reveals a strategy that carefully balances secrecy, immediacy, and transparency under wartime conditions. This approach raises the question of whether such activity reflects a reactive adaptation or signals a more systematic shift in how intelligence agencies engage with the public. The findings suggest that the HUR's activity may not fully align with existing models such as Petersen's tripartite framework of public intelligence communication.[21] Instead, a distinctive pattern appears to emerge: One that may require conceptualization on its own terms.

The discussion is structured as follows. First, it reviews the relevant theoretical literature, including models of public-facing intelligence communication. Next, the methodology section details the data collection and reflexive thematic analysis used to examine HUR's Telegram messages. This is followed by the findings, which are organized according to recurrent communication functions observed in the dataset. The article then develops a conceptual framework to account for these patterns and considers how this extends existing models. Finally, the conclusion discusses the broader theoretical and practical implications of mediatized intelligence communication, including issues of intelligence legitimacy, operational risk, the role of visual evidence and intercepted audio, and potential future developments in intelligence–public engagement.

INTELLIGENCE COMMUNICATION IN A MEDIATIZED ENVIRONMENT

Intelligence communication, defined by Petersen as "the strategic use of information by intelligence agencies to engage with and influence the public," has traditionally balanced secrecy with controlled disclosure, prioritizing discretion over public engagement.[22] However, contemporary media dynamics, particularly the increased use of social media during the last

twenty years and transparency expectations from public interest groups, have influenced how agencies manage their public messaging.[23] What has also changed is the ability of intelligence services to control information. Other players, such as open-source research collectives keen on publishing their research results, have also put pressure on intelligence services and their inclination toward secrecy.[24] These shifts have intensified debates on how intelligence services balance secrecy with public engagement and adapt to a media environment that favors immediacy and interactivity.[25]

Public-facing intelligence communication has emerged as an adaptation to these pressures, enabling agencies to engage audiences while maintaining institutional control. Beyond traditional media statements, intelligence organizations increasingly use websites, mobile applications, and social media platforms not only to broadcast information but also to solicit public participation.[26] Petersen argues that this shift reflects a broader bureaucratic challenge, the so-called *performativity gap*, where institutions struggle to meet high public and political expectations of control and effectiveness despite inherent operational limitations.[27] In this context, intelligence communication has become a strategic tool for managing this gap, reinforcing institutional legitimacy, and demonstrating relevance in an era of expanding oversight, evaluation, and public scrutiny. This broader transformation suggests that intelligence agencies are no longer peripheral to public discourse but have become active participants within a competitive, mediatized environment.[28]

To situate this study, the literature review is organized into two areas. First, it examines mediatization as a framework for understanding how intelligence agencies adjust their communication strategies in response to media logic, including the challenge of balancing secrecy with increasing expectations for transparency. Second, it reviews existing models of public-facing intelligence communication, particularly Petersen's typology of awareness, advice, and coproduction. Together, these frameworks provide important context for analyzing the HUR's communication practices, both as a potential extension of existing approaches and as a possible departure from them.

Mediatization and Intelligence Communication Adaptation

Mediatization refers to the process by which institutions adapt their behavior to the logic of the media environment.[29] As Krotz outlines, mediatization involves a dynamic interaction in which institutions adjust to evolving media outlets while also attempting to shape these platforms to align with their interests.[30] This dual relationship becomes particularly pronounced in intelligence communication, specifically in relation to state intelligence services communicating with the public.[31] This is where the traditionally secretive nature of intelligence work intersects with the expectations of

transparency within contemporary media environments, as noted by Magen.[32]

Strömbäck's stages of mediatization offer a useful framework for understanding this shift.[33] Initially, institutions used media channels as a one-way channel to disseminate information. Over time, the media gained autonomy, and institutions began taking media agendas into account. Eventually, the media developed its own logic, sometimes conflicting with institutional priorities. For example, during election campaigns, political parties might prefer to focus on detailed policy proposals, but media outlets often prioritize conflict narratives and personality-driven coverage that generates higher audience engagement, forcing politicians to adapt their messaging accordingly. The final stage of mediatization, as outlined by Strömbäck, involves institutions actively adapting their strategies to align with (social) media expectations.[34] This final stage reflects not merely a reaction but internalization, where media logic becomes embedded in institutional behavior.

This dynamic is particularly evident in the context of digital conflict communication. Zeitzoff's work emphasizes the role of social media and messaging applications in accelerating conflict dynamics. Social media platforms, including Facebook and Telegram, do not simply disseminate content; they are used actively by state and nonstate actors to shape narratives and exert influence.[35] In this environment, as Maltby has argued, mediatization allows institutions to circumvent traditional state bureaucracies, achieving greater speed and independence.[36] Her case study of the British Army's relations with the media during the 2003 invasion of Iraq demonstrates how mediatization enabled the British Army to assert its own voice, despite its subordination to the UK Ministry of Defense.[37] Together, these conditions establish the structural basis on which intelligence communication strategies emerge, prompting some services to prioritize public involvement and selective, albeit limited, forms of transparency.

A key challenge emerging from mediatization is how intelligence services manage the tension between operational secrecy and public visibility. In response, many have adopted strategies of selective disclosure, releasing information when it serves strategic objectives while retaining control over sources and methods.[38] Rather than choosing between secrecy and openness, agencies engage in tactical transparency: calibrated releases of information that reinforce credibility, preempt adversary narratives, or demonstrate institutional competence.

One such practice is coercive intelligence disclosure: the deliberate release of intelligence to shape decisions, deter adversaries, or reinforce public narratives.[39] This can be used to establish *narrative superiority,* where the timing and content of intelligence releases are calibrated to support a

preferred framing of events.[40] Disclosures of this kind may preempt adversary messaging, reassure allies, or signal foresight and credibility to domestic audiences. Even when the underlying sources remain classified, the performance of knowledge becomes a public tool of influence.[41]

By controlling the timing and content of disclosures, agencies attempt to preempt adversary propaganda, reassure allies and domestic audiences, and demonstrate their own effectiveness.[42] Such transparency is inherently performative: it projects an image of foresight and authority, even as the sensitive sources behind the intelligence remain secret.[43] The mediatized environment amplifies this dynamic; agencies know that disclosed intelligence will circulate rapidly online and inform public opinion.[44] However, such efforts at openness remain constrained. They are typically top–down communications, tightly vetted and episodic in nature, rather than a continuous dialog with the public.[45]

While some intelligence agencies are experimenting with more sustained engagement with the public on social media, traditional intelligence communication emphasizes control, and limits interactivity with external audiences.[46] To understand better these varying approaches to intelligence–public engagement, the next section examines Petersen's typology of intelligence communication.

Intelligence Communication Frameworks: Awareness, Advice, Coproduction

In response to the tensions and practices outlined above, researchers have developed models to categorize how intelligence agencies engage with the public. An influential framework is Petersen's tripartite model, which defines three concepts of intelligence communication aimed at the public.[47] Communication as *awareness* refers to one-way dissemination of information to broaden public knowledge of the agency or situation. In this mode, the public is treated as a passive audience, and the goal is to enhance the agency's visibility or legitimacy.[48] For example, an intelligence service might release annual reviews or historical reports to showcase its role and build trust.

Communication as *advice* involves providing warnings or assessments to inform external decisionmaking.[49] Here the public (or policymakers) is the recipient of specific guidance, such as in terror alerts or travel warnings where intelligence insights are shared so that citizens and authorities can take preventive actions. This advisory communication positions the agency as an expert counselor to society during crises.[50]

Finally, communication as *coproduction* entails active collaboration between intelligence agencies and external partners.[51] In coproduction, the public (or select groups like private companies and other government

agencies) become participants in the intelligence process, contributing information or resources, a form of cocreation. A classic example includes intelligence agencies partnering with companies that develop digital products and services (software, hardware, cloud, cybersecurity) on collaborative cybersecurity initiatives.[52]

Petersen's framework is valuable for highlighting increasing degrees of public involvement, from the minimal engagement of awareness to the shared responsibilities of coproduction. It also emphasizes the strategic intent behind intelligence communication: building legitimacy (awareness), informing policy or public safety (advice), and making use of capabilities outside the Intelligence Community (IC; coproduction). This typology provides a useful baseline for understanding how intelligence agencies have traditionally structured their public engagement, particularly in democratic and institutionalized settings.

Some of the functions associated with awareness invite comparison with practices historically studied under the label of propaganda, particularly in how states seek to shape public perception during conflict. Efforts to reinforce legitimacy or mobilize support have long featured in strategic state messaging. As Zelizer notes, the term "propaganda" is often reserved for adversarial actors, while comparable activities by allied or domestic institutions are reframed as public diplomacy or strategic communication.[53] This context highlights why certain communicative aims may resemble earlier persuasive traditions. However, in this research, *intelligence communication* is adopted as the more appropriate analytic framework, one that foregrounds institutional agency and the structured engagement of the public by intelligence services through modalities such as awareness, advice, and coproduction.

Petersen's framework assumes formal, episodic, and risk-averse public engagement, typically through institutional channels. While it has proven useful for analyzing public-facing strategies in countries like Denmark and the United Kingdom, its ability to reflect communication practices under wartime conditions, where public participation may be continuous, informal, and operationally embedded, remains untested.

This limitation becomes evident when examining intelligence communication in high-intensity conflict, where agencies may use open platforms not just to inform or collaborate with the public but to mobilize them directly. The Ukrainian case thus provides an opportunity to evaluate whether Petersen's categories are sufficiently elastic to accommodate this kind of sustained, participatory engagement.

METHODOLOGY

This study examines how the HUR employs persistent public-facing communication strategies via its official Telegram channel. Telegram was

selected as the research focus due to its prominence in the Russian and Ukrainian information environment. The platform's broadcasting capabilities allow organizations to disseminate messages to unlimited subscribers, effectively transforming messaging applications into mass media outlets.[54] From the early months of the invasion, war-related content has flourished on Telegram rather than on platforms such as Twitter/X or Facebook. All key Ukrainian government and security organizations maintain an active presence on Telegram, which by now has approximately one billion users worldwide.[55]

Using a scraping tool, 2,606 messages were collected from the HUR's verified Ukrainian-language Telegram channel (t.me/DIUkraine) between 24 February 2022 (the start of the Russian full-scale invasion) and 24 February 2024. By February 2024, the channel had amassed over 240,000 followers. The dataset encompasses battlefield updates, operational footage, intercepted Russian communications, special project announcements, civilian appeals, and support solicitations.

All posts were analyzed by the author using reflexive thematic analysis (RTA). This approach, developed by Braun and Clarke, treats the researcher's interpretive role as integral to the analytic process.[56] RTA was selected for its flexibility and its emphasis on the researcher's interpretive role, allowing for context-sensitive analysis of how intelligence communication constructs meaning under wartime conditions. Coding was conducted over multiple readings of the dataset, guided by contextual awareness and sustained reflection. Notes were maintained throughout to document analytical decisions and theme development. An iterative strategy was applied, combining inductive and deductive elements to examine content, tone, and communicative purpose.[57] Most Telegram posts are brief and focused, with a single thematic emphasis typically dominating each entry. The identified themes and their approximate frequency are summarized in Table 1 in the next section, although these percentages should be considered indicative rather than precise, as thematic prominence cannot be straightforwardly quantified.[58] For example, a theme mentioned only briefly and superficially in one post is not directly comparable to another theme developed at length in a subsequent post.

The coding process was shaped by sustained reading of the dataset and guided by questions about how different types of messaging contributed to the HUR's overall communication strategy. Initial codes included categories such as operational highlights, adversary targeting, public appeals, and symbolic messaging. These were later consolidated under broader functional headings to support interpretation of the HUR's overarching strategy on Telegram.

The analysis did not follow a predefined theoretical framework, but it was inevitably shaped by underlying assumptions about the communicative role of

Table 1. Categories of HUR Telegram content, 24 February 2022–24 February 2024.

Function	Themes	No. of posts	Proportion of posts (%)
1. Projecting organizational legitimacy	Branding of HUR success	821	31.50
	Media performances	319	12.24
	Eulogization of fallen soldiers	54	2.07
2. Targeting the adversary	Communication interceptions	634	24.33
	Shaming and doxing	446	17.11
	Appeals to Russian military/public	23	0.88
3. Engaging and mobilizing the public	Advice and appeals to the Ukrainian public	150	5.76
	Crowd funding and donations	78	2.99
Miscellaneous	Other content (uncategorized)	81	3.11
Total		2,606	100.00

intelligence in wartime.[59] The researcher's positionality, including a background in intelligence (studies) and interest in mediatized communication, played a role in shaping analytical focus. Decisions on relevance and granularity of themes were interpretive, influenced by the wartime context of the material and the strategic environment in which the HUR operates. A reflexive stance was maintained throughout, recognizing that meaning is constructed through interpretation.[60]

This study is limited by its exclusive focus on public-facing communication and by the context-specific nature of wartime Ukraine, which may limit generalizability to other institutional settings or periods of peacetime. Despite these limitations, this research provides an empirically grounded analysis of intelligence communication in high-intensity conflict. The following section presents the findings, organized by the communicative functions observed in the HUR's Telegram strategy.

OBSERVED FUNCTIONS OF THE HUR'S TELEGRAM STRATEGY

The analysis of the HUR's Telegram posts reveals a consistent and structured communication strategy that appears to serve multiple public-facing functions. Rather than an ad hoc reactive wartime adaptation, the HUR's messaging exhibits patterned use of Telegram to fulfill several overlapping aims. These include efforts to maintain institutional legitimacy, target the adversary through disclosure of information, and actively engage the public.

These functions emerged inductively from thematic coding of the Telegram posts. Although initially identified as distinct patterns, they often reinforce one other and evolve over time, suggesting a strategic use of public communication in the conflict context. Table 1 provides an overview of the main content categories derived through the coding process, grouped according to the functions observed in the HUR's public messaging. The figures are intended to indicate the relative prominence of different communicative purposes over the two-year period.

As Table 1 shows, the *projecting organizational legitimacy* function accounts for the largest share of the HUR's Telegram output (approximately 46% when combining its subcategories). *Targeting the adversary* is a close second (about 42%), while *engaging and mobilizing the public* makes up a smaller but still meaningful portion (around 9%, with a residual ~3% of posts not fitting neatly into these categories). This breakdown suggests that the HUR's communication strategy prioritizes self-representation and adversary pressure, while still incorporating calls for public participation. The following subsections illustrate each of these functions in more detail, with examples of Telegram posts corresponding to the themes outlined in Table 1.

Projecting Organizational Legitimacy

A prominent feature of the HUR's Telegram activity is the consistent projection of institutional legitimacy. Roughly 46% of posts serve to construct and reinforce the HUR's public identity. This includes highlighting operational success (*branding*), sharing leadership media appearances, and commemorating fallen personnel. These messages collectively portray the HUR as a capable and embedded national actor.

Branding of HUR success (821 messages) emerges as the dominant category, displaying the agency's operational effectiveness and ingenuity. Branding, in the context of communication by actors during a conflict, refers to an approach where an actor promotes a positive image of itself to shape perceptions and influence audiences.[61] Essentially, the HUR uses Telegram as a platform for reputation management, systematically highlighting successful missions, special units' achievements, and intelligence operations in a continuous narrative that emphasizes organizational competence and effectiveness. Notably, this branding effort began almost immediately after the Russian invasion. The HUR's first public statements in late February 2022 set the tone with frequent, assertive updates that underlined the agency's capabilities and resolve:

> We work 24/7, determine the location of the occupier's manpower and equipment, destroy it without mercy! After all, he crossed all physical and moral boundaries, encroached on the most precious thing we have—the life and well-being of Ukrainians! The enemy will be destroyed! Glory to Ukraine! Death to enemies![62]

A characteristic of these branding posts is the use of *visual frame building*: combat footage, images, or intercepted audio providing direct evidence of success.[63] A key aspect of this strategy is branding specialized HUR units, such as Group 13, known for maritime drone operations. Its documented achievements include the destruction of three Russian naval vessels in the

Black Sea: the *Ivanovets* corvette (1 February 2024), the amphibious landing ship *Tsezar Kunikov* (14 February 2024), and the patrol ship *Sergei Kotov* (5 March 2024).[64] Footage from Magura V sea drones visually confirmed these strikes, while intercepted Russian naval communications, in which personnel discussed the damage, further substantiated the claims.[65]

Other examples of success branding include the recapture of Zmiinyi (Snake) Island in the Black Sea in July 2022. The HUR's posts framed this event as a collaborative triumph of Ukrainian defense, restoring freedom of navigation in the Black Sea.[66] This operation relied on coordinated strikes involving Neptune missiles, Bayraktar TB2 drones, and the newly acquired High Mobility Artillery Rocket System.[67] It was presented as a collaborative effort between the HUR and other Ukrainian forces, such as the Sluzhba Bezpeky Ukrainy (Security Service of Ukraine; SBU), and underlined the agency's role in high-stakes military achievements.[68]

Further, the HUR has promoted its cyber capabilities through successful operations by groups such as Blackjack and the BO team, with a notable example occurring in early 2024 when it disrupted Russian military communication servers in Moscow.[69] This operation was openly attributed to cyber units of the HUR, defying the traditional secrecy associated with intelligence activities.[70] Cybersecurity expert Stefan Soesanto commented that public acknowledgment of cyberattacks is normally the hallmark of hacktivists and cybercriminals, as state actors have rarely engaged in such self-attribution.[71] However, the HUR departs from this general rule by openly claiming responsibility for its cyber operations.

Media performances. Over the course of 2022 to 2024, Ukraine's HUR engaged in extensive media outreach. During this period, the agency republished 319 media appearances on its social media accounts. Key figures such as director Kyrylo Budanov, deputy director Vadym Skibitskyi, and spokesperson Andriy Yusov regularly appear in television interviews and press conferences. For example, Budanov has discussed the strategic impact of naval drone strikes on the Russian Black Sea Fleet, presenting them as a significant factor in limiting enemy operations.[72] Such media appearances reinforce the HUR's image as a credible and authoritative voice in the conflict.

High-profile operations, such as the defection of a Russian Mi-8 helicopter pilot, have also been publicized through the media.[73] During a press conference, the pilot expressed his opposition to Russia's actions and detailed his journey to Ukraine.[74] The HUR framed this event as a significant intelligence victory, although the subsequent death of the pilot in Spain underscored the risks associated with such operations.[75]

Eulogization of fallen soldiers (54 messages). A smaller category of identity construction involves commemorating the HUR's fallen. The agency uses the hashtag #ГУРпамятає (#HURremembers) to highlight their bravery,

resilience, and perseverance. A poignant example from November 2023 is a eulogy for Andriy "Yankee" Yaremchuk, whose sacrifice "in the battle for his country's freedom exemplifies the utmost patriotism and courageous leadership." His commitment, reflected in his return from the French Foreign Legion to defend Ukraine, "inspired a legacy of bravery and selflessness."[76]

These posts serve more than a commemorative function, as they also reinforce the connection between fallen soldiers, their local communities, and their families. By recognizing the support networks behind the soldiers, the HUR positions itself as an institution embedded within the broader Ukrainian society. This framing contributes to a collective narrative of sacrifice and national unity.

Taken together, these messages shape perceptions of the HUR as a legitimate, competent, and emotionally engaged institution. Rather than offering sporadic updates, the agency systematically reinforces its image through visual evidence, symbolic gestures, and consistent narrative framing.

Targeting the Adversary

A substantial portion of the HUR's Telegram messages, over 42%, focus on publicly revealing information about the Russian military and its conduct. This includes intercepted communications, identification of individuals, and narrative strategies aimed at lowering enemy morale and legitimacy. There are three recurring primary themes: *communication intercepts*, *shaming and doxing of enemy personnel*, and *appeals to the Russian military and population*.

Communication intercepts. Over two years, the HUR released 634 Telegram messages featuring intercepted conversations between Russian military personnel, their relatives, or other affiliated individuals. Although Russian regulations forbid mobile phone use among service members, many soldiers, especially on the front lines, acquire phones, sometimes stolen from Ukrainian civilians, to contact home.[77]

Ukraine's control over parts of the cellular network and interception capabilities allows the HUR to capture a lot of these communications.[78] By broadcasting them, the HUR knowingly risks tipping off the Russians about what communications channels are compromised. This deliberate disclosure of communication intercepts marks a tradeoff, where operational security is compromised to achieve a broader informational effect. The HUR has *weaponized* these intercepts to delegitimize Russian actions.[79]

The content of the intercepted calls serves multiple purposes for Ukraine's narrative. Intercepted conversations often highlight alleged Russian war crimes. For example, an intercept from April 2022 revealed an order to execute Ukrainian prisoners of war in the Popasna area of Luhansk Oblast.[80] Then, on 23 May 2023, the HUR intercepted the audio of two soldiers from the by Russia annexed Donetsk People's Republic, discussing rape, extortion,

and looting by members of their unit.[81] Later in June, an intercept revealed the Russians captured a Ukrainian crewmember of a tank, interrogated him, and then shot him, "as they did not leave prisoners alive."[82] Another recording detailed Russian soldiers using phosphorus ammunition, a potential violation of the Geneva Conventions.[83]

Intercepts also capture the disillusionment of Russian soldiers. Numerous recordings reveal complaints about poor living conditions, inadequate supplies, and the high human cost of the war. For instance, a Russian soldier in Kharkiv reported in August 2022 that his unit was encircled with no food or water, while another lamented that only seventy-two out of 300 personnel in his unit had not been killed or wounded.[84] On 4 September, Russian soldiers objected about the poor state of newly arrived units: "[T]hey arrive without proper clothing, no sleeping bags, or anything."[85] In another intercept, a Russian serviceman said that mobilized colleagues with serious diseases, such as acquired immune deficiency syndrome, tuberculosis, and hepatitis, are forced to stay on the front lines.[86]

The HUR also exposes systemic issues within the Russian military, including corruption and leadership failures. On 14 September 2022, a Russian military member in the Kharkiv area complained about the incompetence of his superiors: "[T]here is no organization at all, I thought it was an army, but there is no army."[87] Similarly, on 28 November, a military officer described his commanding officers as idiots who were hiding themselves in the rear area.[88] Furthermore, intercepts have revealed officers demanding bribes for leave permissions.[89] These revelations erode the image of the Russian military as a unified and competent force.

By weaponizing these intercepts, the HUR turns the enemy's own words into ammunition against them, strategically using Russia's own communications to reveal war crimes, poor morale, and leadership failures, allowing Russian soldiers' own complaints and admissions to damage their military's reputation without Ukraine having to make these claims themselves. It is important to note the boldness of this approach. Every time the HUR releases an intercept, it presumably tips off Russian counterintelligence about specific compromised communication channels. The fact that the HUR continued to release hundreds of them implies either that the intelligence value of those particular intercepts had a short shelf life, or that the informational impact outweighed the loss of intelligence advantage. This represents a shift in intelligence philosophy: valuing immediate influence over longer-term collection capabilities.

Shaming and doxing (446 messages). The theme of *shaming and doxing* is aimed at both undermining Russian morale and drawing attention to misconduct. Early in the conflict, the HUR began publishing lists of Belarusian and Russian military personnel, including personal details such as names, ranks, and dates of birth.[90] The intelligence service justified this tactic

of doxing, the act of publishing personally identifiable information online, to encourage enemy personnel to surrender and as a response to Russia's illegal invasion. This strategy, while controversial, reflects the HUR's efforts to use doxing as a tool in the ongoing conflict.[91]

Furthermore, a method for shaping perceptions of a conflict is to assign blame for negative actions to an actor, a practice often referred to as *shaming*.[92] This approach is effective when it provokes emotions such as outrage or concern, as it can weaken the perceived legitimacy of the opponent and make it easier to assign responsibility.[93]

In April 2022, the HUR released information about the alleged use of mobile crematoria in Mariupol, claiming that Russian forces used these to dispose of civilian casualties and obscure the true scale of their own losses.[94] The HUR also uses historical and environmental narratives to criticize Russian actions. On the anniversary of the downing of Malaysia Airlines Flight 17, the agency described the incident as part of a broader pattern of Russian aggression.[95] Similarly, the destruction of the Kakhovskaya Hydro Power Plant in 2023 was labeled an act of ecocide, aimed at highlighting the environmental and humanitarian toll of the war. On 18 June 2023, the HUR accused Russia of "nuclear blackmail" at the Zaporizhzhia Nuclear Power Plant (ZNPP), detailing safety violations and the "terrorizing" of the staff members. Andriy Yusov, a HUR spokesperson, stated that "a whole series of norms and standards of nuclear safety at the ZNPP are no longer ensured by the occupation authorities."[96]

The shaming strategy extends to exposing systemic issues in Russian society, including disparities in conscription practices. For instance, the HUR highlighted the disproportionate recruitment of ethnic minorities in Russian Federation regions such as Buryatia and Dagestan, while wealthier urban Russians avoided mobilization.[97] These messages appear designed not only to challenge the moral legitimacy of the Russian war effort but also to exacerbate internal tensions within the adversary state

While the themes *communication intercepts* and *shaming and doxing* differ in format and source material, both serve a similar narrative purpose. Each functions as a means of discrediting the adversary, either by exposing institutional dysfunction or by assigning responsibility for violence and misconduct. Intercepts rely on captured audio to highlight poor morale, ethical and judicial breaches, or corruption, often anonymized but framed to shame collectively. Doxing personalizes this strategy by naming and visually identifying specific individuals. Together, these approaches contribute to the HUR's effort to isolate the adversary morally and position Russia as acting outside accepted norms of conduct.

Complementing these tactics, a smaller set of messages focuses on direct appeals to Russian military personnel and civilians, combining psychological pressure with the presentation of alternatives.

Appeals to the Russian military and population (twenty-three messages). While quantitatively the smallest category, it is one in which the HUR directly appeals to Russians. In this theme, the HUR employs various strategies. In its communications, the HUR employs a dual approach of incentives and deterrence. The service reaches out to Russian military personnel through the "I Want to Live" project, providing detailed surrender instructions and guaranteeing humane treatment under the Geneva Conventions.[98] Simultaneously, the HUR issues warnings to those complicit in aggression against Ukraine, including messages about attacks by "unknown perpetrators" on Russian pilots.[99] These communications serve as both deterrence and psychological warfare, creating unease among Russian personnel, while offering a clear alternative to continued involvement in the war.

Taken together, these adversary-targeted messages reflect an assertive and strategic use of intelligence for public influence. Rather than using intercepted or collected material solely for internal or covert advantage, the HUR selectively releases content intended to degrade adversary morale, expose misconduct, and shape perceptions. While much of this content adopts a confrontational posture, such as discrediting Russian leadership or identifying individuals, some messages pursue behavioral influence more subtly, offering enemy personnel a pathway to disengagement or defection.

Engaging and Mobilizing the Public

A smaller but meaningful portion of HUR's Telegram content (just under 9%) focuses on engaging the public directly. These messages either provide guidance and safety information to civilians or highlight forms of public support for the agency's operations. While less frequent than operational or adversary-targeting content, they reflect a consistent communicative effort to include citizens in the wartime information environment. Two main themes can be identified: *advice and appeals to the Ukrainian public* and *crowdfunding and civil support initiatives*. Through these, the HUR seeks to inform, recruit, and rally the public in support of intelligence and security goals.

Advice and appeals to the public (150 messages). A significant portion of the HUR's posts is directed at ordinary Ukrainian citizens, offering guidance, requests, or warnings to aid the country's defense and resilience. This category can be seen as the HUR stepping into a public safety role via its communications. One prominent example is the HUR's promotion of the "Main Intelligence Bot," which allows citizens to report enemy movements and suspected collaborators.[100] Further, on occasions such as national holidays (e.g., Independence Day) or when anticipating heightened Russian cyber activities, the HUR posted detailed cybersecurity advice.[101] This included urging people to secure their devices, use two-factor authentication,

be cautious of phishing attempts, and rely on verified information sources to avoid disinformation traps. These posts read like public service announcements, in tone and structure, that one might expect from a cybersecurity agency or police unit, indicating how the HUR also takes on the mantle of protecting the digital front at the citizen level.

Additionally, the HUR's channel directly addresses fake narratives circulating in the information space by debunking them and directing people toward verified Ukrainian government channels.[102] For example, the HUR has exposed fabricated narratives, such as a Russian guide encouraging collaboration with occupying forces.[103] This is part of a broader Ukrainian strategy where multiple agencies work to inoculate the public against Russian propaganda.[104] The HUR's involvement underscores that intelligence agencies are actively engaged in the information verification battle, not just collecting secrets.

Some messages target Ukrainians living under Russian occupation, providing instructions such as how to evacuate safely or how to signal compliance to avoid retribution while covertly resisting.[105] The HUR also shared emergency contact numbers for humanitarian help and advice for those forcibly conscripted by Russia on how to surrender or escape when possible.[106]

Throughout these public-directed communications, the tone is often reassuring yet firm. The HUR portrays itself as watching out for citizens' safety and as a conduit for citizens to contribute to victory. The underlying message is that Ukraine's defense is a collective effort, and intelligence is not confined to professionals in secret rooms. This reflects a participatory ethic: intelligence success is tied to public involvement.

Crowdfunding and civil support initiatives (seventy-eight messages). Another notable way the HUR engages the public is by collaborating with the civilian population and diaspora for material support. Posts in this category highlight partnerships with Ukrainian civil society organizations, charities, and even cultural groups that contribute resources to the HUR or the broader IC.

The HUR maintains close ties with civil society and is thus able to secure financial and material support through crowdfunding and donations. These contributions enhance the agency's operational capacity and strengthen its connection with the public. For example, the Come Back Alive fund supplied thirteen pickup trucks valued at $353,000, while the Serhiy Prytula Foundation donated unmanned aerial vehicles for reconnaissance missions.[107] These resources have been instrumental in enabling the HUR to conduct special operations.

Cultural initiatives also play a role in engaging the public. Music groups such as Dance on the Congo Square, a Ukrainian collective, have raised substantial funds for military equipment and support for injured personnel.[108] They raised over 1.8 million hryvnias (approximately 44,000

USD) to support the children of fallen intelligence officers as part of a larger charity tour across twenty-two European cities. Sports events, such as mixed martial arts competitions, further highlight the HUR's efforts to connect with various segments of society.[109]

Civil–military cooperation is a key component of the HUR's activities, particularly in humanitarian aid. The HUR's Special Forces, including the Kraken unit, work alongside local aid groups to support civilians in areas reclaimed from occupation. In late 2023, these joint efforts provided aid to about 7,000 people across several newly liberated villages in the Kharkiv and Donetsk regions.[110] They distributed supplies, such as food packages, medicine, and medical equipment, with a specific focus on supporting a medical center and a hospital in these areas.

Together, these messages portray the public not only as an audience but as a valued part of the wider defense effort. The HUR's consistent inclusion of public participation in its messaging reinforces its embeddedness in civil society and contributes to an atmosphere of shared national purpose.

The patterns across these three functions (i.e., projecting organizational legitimacy, targeting the adversary, and engaging and mobilizing the public) suggest that the HUR's use of Telegram reflects more than a reactive communication posture. Rather, the agency appears to have adopted a structured approach to digital engagement that integrates operational visibility, adversary pressure, and public involvement. The following section draws on these findings to consider whether they represent a distinct model of intelligence communication and how this model relates to existing theoretical frameworks.

THE EMERGING CONCEPT OF PARTICIPATORY INTELLIGENCE COMMUNICATION

The analysis of HUR's Telegram communications suggests the emergence of a communication model that extends beyond existing typologies in the literature. This approach builds on existing concepts of mediatization and coproduction, yet represents a more sustained, functionally embedded, and operationally integrated form of public engagement. In the case of the HUR, the agency uses its accounts on social media to involve the public actively in its wartime intelligence efforts. This includes crowdsourced reporting (e.g., urging citizens to send tips on enemy positions via dedicated chatbots), the selective release of intelligence (publishing intercepted communications, battlefield footage, and lists of enemy personnel), and ongoing, daily updates that keep the public informed and engaged. Through these means, the HUR diffuses the line between the intelligence apparatus and its audience: the public is not merely consuming information but is also contributing to the intelligence cycle and the broader campaign against the adversary.

This approach shares elements with established frameworks, particularly Petersen's typology of awareness, advice, and coproduction, which also explicitly includes open public participation in security communication, such as tip lines and suspicious activity reporting.[111] However, Petersen's observations are rooted in peacetime contexts such as counterterrorism and cybersecurity, where participation tends to follow formal, structured channels. The HUR's approach, by contrast, demonstrates a broad and continuous mobilization of the public through open platforms, positioned as an essential element of wartime operations. Whereas Petersen's model reflects structured participation designed to support long-term resilience, the HUR's strategy integrates public input into immediate tactical and symbolic outcomes. This participation is both practical and persistent, integrated into both messaging and operational outcomes.

Telegram enables the HUR to incorporate the public into intelligence work at scale and with speed. The strategy encompasses three primary functions: *projecting institutional identity and legitimacy*, *targeting the adversary*, and *mobilizing civilian support*:

1. *Identity and authority construction*: The HUR employs communication to establish its reputation as competent, heroic, and dependable. By highlighting successful operations, honoring fallen officers, and projecting service-oriented values, the agency builds public trust and confirms its legitimacy. This strategic transparency addresses the credibility challenges often faced by intelligence organizations, supporting what scholars have termed an "intelligence lobby" effect.[112]
2. *Enemy exposure and pressur*e: A prominent feature in HUR's communications is the release of material designed to undermine adversary legitimacy and morale. This includes intercepted conversations, documentation of war crimes and corruption, and personal information about Russian military personnel.[113] These disclosures serve practical and symbolic purposes: they damage enemy credibility while reinforcing Ukraine's moral position. In this context, transparency functions as a tactical asset, rather than institutional openness.
3. *Public engagement and mobilization:* The HUR actively involves, primarily domestic, audiences in intelligence efforts. Its Telegram channel calls for public action, such as reporting enemy movements or using the "Main Intelligence Bot" and provides guidance for civilians in occupied territories. It also shares practical advice (e.g., cybersecurity tips and guidelines for civilians in occupied areas) to involve citizens in national defense and keep them safe. Furthermore, the HUR publicizes partnerships with civil society; for example, highlighting crowdfunding campaigns and donations of drones or vehicles from Ukrainian organizations and volunteers.[114] This dimension of engagement positions the public not as passive supporters but as distributed contributors to defense and intelligence operations.

These functions closely mirror communication strategies observed in other conflicts. For instance, Hirschberger's study of external communication in social media during the Israeli–Palestinian conflict finds that conflict actors commonly use public messaging to shape perceptions and rally popular involvement.[115] Similar patterns have been observed in Ukraine's broader wartime messaging. Karpchuk identifies three recurring themes in Ukraine's communications: first, mobilizing citizens to fight for victory; second, messages aimed at Western nations to secure financial and military support; and third, communications directed at Russian citizens to reveal the realities of war.[116] While the HUR operates with an intelligence-specific remit, its messaging aligns with these themes, particularly through its focus on exposing enemy conduct and reinforcing institutional credibility. This suggests narrative cohesion across state actors, even when formal coordination structures may not be evident.[117]

The HUR's Telegram outreach reflects elements of this pattern: it attempts to shape predominantly domestic perceptions of the war (through identity construction and narrative control), it targets the adversary with informational pressure, and it mobilizes the citizenry as part of the intelligence process. In doing so, the HUR uses transparency, not as an end, but as a means to achieve objectives: from legitimacy and influence to crowdsourced intelligence.[118]

In sum, the HUR's Telegram strategy represents a distinct wartime application of intelligence communication that goes beyond traditional frameworks. While it builds on coproduction principles, it operates at a greater scale, with more consistency, and deeper operational integration than peacetime models. The unique pressures of Russia's invasion have pushed the HUR to develop a communication approach that simultaneously builds domestic support, pressures the enemy, and harnesses public participation in intelligence work. Rather than treating civilians as auxiliary observers, the HUR incorporates them as active participants in intelligence production, tactical support, and strategic messaging. Through its daily updates, intercepted communications, and calls for citizen involvement, the HUR demonstrates how intelligence agencies in conflict zones can adapt to digital environments by diffusion of traditional boundaries between intelligence producers and consumers.

CONCLUSION

The HUR's use of Telegram during the war in Ukraine illustrates how intelligence services may communicate under conditions of sustained, high-intensity conflict. Departing from episodic, centrally managed updates, the agency adopted a continuous strategy that blended operational disclosure with public engagement.

This approach relied heavily on visual and audio content, such as footage of drone strikes and intercepted communications, that reduced reliance on narrative framing and reinforced message credibility in a contested information space.

Rather than functioning as isolated updates, the HUR's posts reflect a deliberate and structured effort to shape perception, reinforce legitimacy, and involve the public in wartime intelligence. These patterns suggest, not an improvised adjustment, but an integrated communication strategy with both tactical and symbolic dimensions.

This strategy, however, is not without complications. Regular public disclosure of intelligence carries risks: it may erode long-term collection capacity, blur boundaries between intelligence and influence operations, and expose civilian contributors to retaliation or surveillance.[119] The approach also complicates traditional boundaries between intelligence, strategic communication, and public diplomacy.

The HUR case offers a reference point for reconsidering how intelligence communication may function under extreme political and operational pressure. While its broader applicability remains uncertain, given Ukraine's specific context of existential threat, national mobilization, and a resilient digital infrastructure, it underscores the need to revisit assumptions about public-facing intelligence work.

DISCLOSURE STATEMENT

No potential conflict of interest was reported by the author(s).

REFERENCES

[1] Ruth Avidar and Clila Magen, "Negative Spaces as a Strategic Decision: The Case of the Israeli Security Agency," *Public Relations Review* 49, no. 2 (1 June 2023): 2, https://doi.org/10.1016/j.pubrev.2023.102315.

[2] Damien Van Puyvelde and Fernando Tabárez Rienzi, "The Rise of Open-Source Intelligence," *European Journal of International Security*, 7 January 2025, 11, https://doi.org/10.1017/eis.2024.61.

[3] Huw Dylan and Thomas J. Maguire, "Secret Intelligence and Public Diplomacy in the Ukraine War," *Survival* 64, no. 4 (4 July 2022): 34, https://doi.org/10.1080/00396338.2022.2103257.

[4] Dylan and Maguire, "Secret Intelligence and Public Diplomacy in the Ukraine War," 34.

[5] Clila Magen, "Media Strategies and Manipulations of Intelligence Services: The Case of Israel," *The International Journal of Press/Politics* 20, no. 2 (1 April 2015): 253, https://doi.org/10.1177/1940161214556514; Ben Scott, "The Strategic Disclosure of Intelligence Requires Stronger Guardrails," *Lawfare*, 1

August 2024, https://www.lawfaremedia.org/article/the-strategic-disclosure-of-intelligence-requires-stronger-guardrails.

[6] Eva-Karin Olsson and Mats Eriksson, "The Logic of Public Organizations' Social Media Use: Toward a Theory of "Social Mediatisation"," *Public Relations Inquiry* 5, no. 2 (2016): 187, https://doi.org/10.1177/2046147X16654454.

[7] Paul Lashmar, "From Silence to Primary Definer: The Emergence of an Intelligence Lobby in the Public Sphere," *Critical Sociology* 45, no. 3 (1 May 2019): 411, https://doi.org/10.1177/0896920518780987.

[8] Bob de Graaff and Constant Hijzen, "Zwijgen Is Zilver En Spreken Is Goud," *Justitiële Verkenningen* 44, no. 1 (2018): 148, https://www.proquest.com/scholarly-journals/zwijgen-is-zilver-en-spreken-goud/docview/2023993970/se-2.

[9] Arthur S. Hulnick, "Openness: Being Public About Secret Intelligence," *International Journal of Intelligence and CounterIntelligence* 12, no. 4 (1 December 1999): 463, https://doi.org/10.1080/088506099305007.

[10] "Telegram Global MAU 2022," *Statista*, https://www.statista.com/statistics/234038/telegram-messenger-mau-users/.

[11] Maria Hernandez, "Ukraine's Media Landscape in 2022: Martial Law Unavoidably Restricted Freedom of Expression and Telegram Emerged as the Primary News Source amidst War" (Report, Centre for Media Pluralism and Freedom, 11 January 2024), 1, https://cmpf.eui.eu/ukranian-media-landscape-in-2022/.

[12] Piyush Ghasiya and Kazutoshi Sasahara, "Messaging Strategies of Ukraine and Russia on Telegram during the 2022 Russian Invasion of Ukraine," *First Monday*, 12 August 2023, https://doi.org/10.5210/fm.v28i8.12873.

[13] "Telegram CEO Pavel Durov Faces Preliminary Charges for Allowing Crime on App | AP News," https://apnews.com/article/france-telegram-pavel-durov-arrest-6e213d227458f330ed16e7fe221a696c.

[14] "Головне Управління Розвідки МО України," Telegram, https://t.me/diukraine/3494.

[15] "How a Chatbot Has Turned Ukrainian Civilians into Digital Resistance Fighters," *The Economist*, 22 February 2023, https://www.economist.com/the-economist-explains/2023/02/22/how-a-chatbot-has-turned-ukrainian-civilians-into-digital-resistance-fighters.

[16] David Wallace and Shane Reeves, "The 'I Want to Live' Project and Technologically-Enabled Surrender," *Lieber Institute West Point*, 13 January 2023, https://lieber.westpoint.edu/i-want-to-live-project-technologically-enabled-surrender/.

[17] Michael Landon-Murray, "Social Media and U.S. Intelligence Agencies," *Journal of Strategic Security* 8, no. 3 (2015): 67–79, http://www.jstor.org/stable/26465246; Liam McLoughlin, Stephen Ward, and Daniel Lomas, "'Hello, World': GCHQ, Twitter and Social Media Engagement," *Intelligence and National Security* 35, no. 2 (2020): 233–51; Sarah Maltby, "The Mediatisation of the Military," *Media, War & Conflict* 5, no. 3 (1 December 2012): 255–68, https://doi.org/10.1177/1750635212447908.

[18] Landon-Murray, "Social Media and U.S. Intelligence Agencies," 78.

[19] Gregory Asmolov, "The Transformation of Participatory Warfare: The Role of Narratives in Connective Mobilization in the Russia–Ukraine War," *Digital War* 3, no. 1–3 (2022): 25–37, https://doi.org/10.1057/s42984-022-00054-5.
[20] Olga Boichak, "Digital War: Mediatized Conflicts in Sociological Perspective," in *The Oxford Handbook of Digital Media Sociology*, ed. Deana A. Rohlinger and Sarah Sobieraj (Oxford University Press, 2022), 511, https://doi.org/10.1093/oxfordhb/9780197510636.013.31.
[21] Karen Lund Petersen, "Three Concepts of Intelligence Communication: Awareness, Advice or Co-Production?," *Intelligence and National Security* 34, no. 3 (16 April 2019): 317, https://doi.org/10.1080/02684527.2019.1553371.
[22] Petersen, "Three Concepts of Intelligence Communication," 317.
[23] Damien Van Puyvelde, "Intelligence Accountability and the Role of Public Interest Groups in the United States," *Intelligence and National Security* 28, no. 2 (1 April 2013): 139, https://doi.org/10.1080/02684527.2012.735078; Landon-Murray, "Social Media and U.S. Intelligence Agencies," 67.
[24] Richard J. Aldrich and Christopher R. Moran, "Delayed Disclosure : National Security, Whistle-Blowers and the Nature of Secrecy," *Political Studies*, 28 March 2018, 25, https://doi.org/10.1177/0032321718764990.
[25] Clila Magen, "Strategic Communication of Israel's Intelligence Services: Countering New Challenges with Old Methods," *International Journal of Strategic Communication* 11, no. 4 (2017): 269, https://doi.org/10.1080/1553118X.2017.1334207.
[26] Petersen, "Three Concepts of Intelligence Communication," 317.
[27] Ibid., 318.
[28] Magen, "Strategic Communication of Israel's Intelligence Services," 272.
[29] Jesper Strömbäck and Frank Esser, "Mediatisation of Politics: Transforming Democracies and Reshaping Politics," in *Mediatisation of Communication*, ed. Knut Lundby (Berlin: De Gruyter, 2014), 375, https://doi.org/10.1515/9783110272215.375.
[30] Friedrich Krotz, "Explaining the Mediatisation Approach," *Javnost—The Public* 24, no. 2 (3 April 2017): 110, https://doi.org/10.1080/13183222.2017.1298556.
[31] Petersen, "Three Concepts of Intelligence Communication," 317.
[32] Magen, "Strategic Communication of Israel's Intelligence Services," 269.
[33] Jesper Strömbäck, "Four Phases of Mediatisation: An Analysis of the Mediatisation of Politics," *The International Journal of Press/Politics* 13, no. 3 (2008): 235, https://doi.org/10.1177/1940161208319097.
[34] Ibid., 240.
[35] Thomas Zeitzoff, "How Social Media Is Changing Conflict," *Journal of Conflict Resolution* 61, no. 9 (October 2017): 1970, https://doi.org/10.1177/0022002717721392.
[36] Maltby, "The Mediatisation of the Military," 263.
[37] Ibid., 264.
[38] Ofek Riemer and Daniel Sobelman, "Coercive Disclosure: The Weaponization of Public Intelligence Revelation in International Relations," *Contemporary Security Policy* 44, no. 2 (3 April 2023): 5, https://doi.org/10.1080/13523260.2022.2164122.

[39] Riemer and Sobelman, "Coercive Disclosure," 2.
[40] Huw Dylan and Thomas J. Maguire, "Secret Intelligence and Public Diplomacy in the Ukraine War," 47.
[41] Ibid., 47.
[42] Daniel Lomas, "In-Depth Briefing #28: "Weaponising the Truth": UK Intelligence, Public Information and Ukraine," *Centre for Historical Analysis and Conflict Research*, 26 April 2022, https://chacr.org.uk/2022/04/26/in-depth-briefing-28-weaponising-the-truth-uk-intelligence-public-information-and-ukraine/2025).
[43] Ofek Riemer, "Politics Is Not Everything: New Perspectives on the Public Disclosure of Intelligence by States," *Contemporary Security Policy* 42, no. 4 (2 October 2021): 556, https://doi.org/10.1080/13523260.2021.1994238.
[44] Peter Schrijver, Lotte Nietzman, and Peter B. M. J. Pijpers, "Birdwatchers on Social Media: The Mediatisation of Intelligence Organisations," *Security and Defence Quarterly*, 28 January 2025, 2, https://doi.org/10.35467/sdq/196516.
[45] Petersen, "Three Concepts of Intelligence Communication," 320; Avidar and Magen, "Negative Spaces as a Strategic Decision," 6.
[46] McLoughlin, Ward, and Lomas, "'Hello, World,'" 233; Landon-Murray, "Social Media and U.S. Intelligence Agencies," 67.
[47] Petersen, "Three Concepts of Intelligence Communication," 317.
[48] Ibid., 319.
[49] Ibid., 320.
[50] Ibid., 321.
[51] Ibid., 322.
[52] Ibid., 322.
[53] Barbie Zelizer, "Is Propaganda by Any Other Name Still Propaganda?," in *Media and Propaganda in an Age of Disinformation*, ed. Nelson Ribeiro and Barbie Zelizer, 1st ed. (Routledge, 2025), 34.
[54] Arash Dargahi Nobari et al., "Characteristics of Viral Messages on Telegram; the World's Largest Hybrid Public and Private Messenger," *Expert Systems with Applications* 168 (2021): 6, https://doi.org/10.1016/j.eswa.2020.114303.
[55] Katherine Li, "Telegram Hits 1 Billion Active Users as CEO Pavel Durov Takes Swipe at Meta-Owned Rival WhatsApp," *Business Insider*, https://www.businessinsider.com/telegram-celebrates-1-billion-active-users-pavel-durov-swipe-whatsapp-2025-3.
[56] Virginia Braun and Victoria Clarke, *Thematic Analysis : A Practical Guide* (London: SAGE, 2022), 12.
[57] David Byrne, "A Worked Example of Braun and Clarke's Approach to Reflexive Thematic Analysis," *Quality & Quantity* 56, no. 3 (1 June 2022): 1396, https://doi.org/10.1007/s11135-021-01182-y.
[58] Braun and Clarke, *Thematic Analysis: A Practical Guide*, 141.
[59] Ibid., 12.
[60] Ibid., 14.
[61] Bernd Hirschberger, *External Communication in Social Media during Asymmetric Conflicts: A Theoretical Model and Empirical Case Study of the Conflict in Israel and Palestine*, 1st ed., Vol. 108 Edition Politik (Bielefeld, Germany: transcript Verlag, 2021), 27, https://doi.org/10.14361/9783839455098.

[62] "Головне Управління Розвідки МО України," Telegram, https://t.me/diukraine/5.
[63] Ganga Dhanesh and Nadia Rahman, "Visual Communication and Public Relations: Visual Frame Building Strategies in War and Conflict Stories," *Public Relations Review* 47, no. 1 (15 December 2020): 5, https://doi.org/10.1016/j.pubrev.2020.102003.
[64] "Головне Управління Розвідки МО України," Telegram, https://t.me/diukraine/3403; "Головне Управління Розвідки МО України," Telegram, https://t.me/diukraine/3469; "Головне Управління Розвідки МО України," Telegram, https://t.me/diukraine/3552.
[65] "Головне Управління Розвідки МО України," Telegram, https://t.me/diukraine/3553.
[66] "Головне Управління Розвідки МО України," Telegram, https://t.me/diukraine/848.
[67] Sebastien Roblin, "Russia Slinks Away from Snake Island: How Ukraine Won the Battle," *Forbes*, https://www.forbes.com/sites/sebastienroblin/2022/06/30/russia-slinks-away-from-snake-island-after-ukrainian-bombardment/.
[68] "Головне Управління Розвідки МО України," Telegram, https://t.me/diukraine/847.
[69] "Головне Управління Розвідки МО України," Telegram, https://t.me/diukraine/3389.
[70] Stefan Soesanto, "Smoke, Mirrors, and Self-Attribution: Ukraine's Military Intelligence Service in Cyberspace," *RealClearDefense*, 2 March 2024, https://www.realcleardefense.com/articles/2024/03/02/smoke_mirrors_and_self-attribution_ukraines_military_intelligence_service_in_cyberspace_1015598.html.
[71] Ibid.
[72] "Головне Управління Розвідки МО України," Telegram, https://t.me/diukraine/2739.
[73] "Головне Управління Розвідки МО України," Telegram, https://t.me/diukraine/2777.
[74] "Ukraine Releases Video of Russian Pilot Who Defected," *YouTube*, 5 September 2023, https://www.youtube.com/watch?v=oExnHCz8hdo.
[75] Michael Schwirtz and Constant Méheut, "Russian Pilot Who Defected to Ukraine Is Believed Dead in Spain," *The New York Times*, 20 February 2024, https://www.nytimes.com/2024/02/20/world/europe/russian-pilot-maksim-kuzminov-spain.html.
[76] "Головне Управління Розвідки МО України," Telegram, https://t.me/diukraine/3006.
[77] "Makiivka: Russia Blames Missile Attack on Soldiers Mobile Phone Use," *BBC News*, January 4, 2023, https://www.bbc.com/news/world-europe-64159045.
[78] "The Mobile Network Battlefield in Ukraine – Part 2," *Enea*, 31 March 2022, https://www.enea.com/insights/the-mobile-network-battlefield-in-ukraine-part-2/.
[79] Raimo Tikkanen, "Intercepted Phone Calls at the Russo-Ukrainian War: Cyberoperation or Propaganda Campaign?" (MA thesis, JAMK University of Applied Sciences, 2024), 7, https://www.theseus.fi/handle/10024/854656.

[80] "Головне Управління Розвідки МО України," Telegram, https://t.me/diukraine/380.
[81] "Головне Управління Розвідки МО України," Telegram, https://t.me/diukraine/530.
[82] "Головне Управління Розвідки МО України," Telegram, https://t.me/diukraine/585.
[83] "Головне Управління Розвідки МО України," Telegram, https://t.me/diukraine/1031.
[84] "Головне Управління Розвідки МО України," Telegram, https://t.me/diukraine/720; "Головне Управління Розвідки МО України," Telegram, https://t.me/diukraine/1253.
[85] "Головне Управління Розвідки МО України," Telegram, https://t.me/diukraine/1254.
[86] "Головне Управління Розвідки МО України," Telegram, https://t.me/diukraine/3383.
[87] "Головне Управління Розвідки МО України," Telegram, https://t.me/diukraine/1327.
[88] "Головне Управління Розвідки МО України," Telegram, https://t.me/diukraine/1698.
[89] "Головне Управління Розвідки МО України," Telegram, https://t.me/diukraine/2941.
[90] "Головне Управління Розвідки МО України," Telegram, https://t.me/diukraine/15.
[91] Eric Jensen and Sean Watts, "Ukraine Symposium—Doxing Enemy Soldiers and the Law of War," *Lieber Institute West Point*, 31 October 2022, https://lieber.westpoint.edu/doxing-enemy-soldiers-law-of-war/.
[92] Matthew Krain, "J'accuse! Does Naming and Shaming Perpetrators Reduce the Severity of Genocides or Politicides?," *International Studies Quarterly* 56, no. 3 (1 September 2012): 574, https://doi.org/10.1111/j.1468-2478.2012.00732.x.
[93] Hirschberger, *External Communication in Social Media During Asymmetric Conflicts*, 25.
[94] "Головне Управління Розвідки МО України," Telegram, https://t.me/diukraine/313.
[95] "Головне Управління Розвідки МО України," Telegram, https://t.me/diukraine/2585.
[96] "Головне Управління Розвідки МО України," Telegram, https://t.me/diukraine/2442.
[97] "Головне Управління Розвідки МО України," Telegram, https://t.me/diukraine/1408.
[98] "Головне Управління Розвідки МО України," Telegram, https://t.me/diukraine/1637.
[99] "Головне Управління Розвідки МО України," Telegram, https://t.me/diukraine/3424.
[100] "Solutions to Win: Ukraine Unveils Revamped Main Intelligence Bot to Assist Occupied Territories in Fighting against Russian Regime," *Rubryka*, 20

February 2024, https://rubryka.com/en/2024/02/20/gur-zapuskaye-onovlenyj-golovnyj-bot-rozvidky-dlya-chogo-tse-rishennya/.

101 "Головне Управління Розвідки МО України," Telegram, https://t.me/diukraine/1149.

102 "Головне Управління Розвідки МО України," Telegram, https://t.me/diukraine/1481.

103 "Головне Управління Розвідки МО України," Telegram, https://t.me/diukraine/994.

104 Todd C. Helmus and Khrystyna Holynska, "Ukrainian Resistance to Russian Disinformation: Lessons for Future Conflict" (RAND Corporation, 3 September 2024), 9, https://www.rand.org/pubs/research_reports/RRA2771-1.html.

105 "Головне Управління Розвідки МО України," Telegram, https://t.me/diukraine/610.

106 "Головне Управління Розвідки МО України," Telegram, https://t.me/diukraine/612.

107 Defence Intelligence of Ukraine [@DI_Ukraine], Tweet posted March 15, 2024, Twitter, https://x.com/DI_Ukraine/status/1768581165508624505; "Головне Управління Розвідки МО України," Telegram, https://t.me/diukraine/2956.

108 "Головне Управління Розвідки МО України," Telegram, https://t.me/diukraine/3065.

109 "Головне Управління Розвідки МО України," Telegram, https://t.me/diukraine/3251.

110 "Головне Управління Розвідки МО України," Telegram, https://t.me/diukraine/3036.

111 Petersen, "Three Concepts of Intelligence Communication," 322.

112 Lashmar, "From Silence to Primary Definer," 411.

113 Tikkanen, "Intercepted Phone Calls at the Russo-Ukrainian War," 8.

114 Peter Schrijver, "From the Shadows to the Social Sphere: Ukraine's Strategy of Engagement," Irregular Warfare Initiative, 28 May 2024, https://irregularwarfare.org/articles/from-the-shadows-to-the-social-sphere-ukraines-strategy-of-engagement/.

115 Hirschberger, *External Communication in Social Media During Asymmetric Conflicts*, 130.

116 Natalia Karpchuk, "Information and Communication Policy in Wartime: The Case of Ukraine," *Historia i Polityka* 47, no. 40 (2022): 125.

117 Per-Erik Nilsson and Ivar Ekman, ""Be Brave Like Ukraine": Strategic Communication and the Mediatization of War," *National Security and the Future* 25, no. 1 (11 April 2024): 40, https://doi.org/10.37458/nstf.25.1.2.

118 Peter Schrijver, "Beyond Counterintelligence: Understanding the SBU's Social Media Outreach on Telegram during Wartime," *Intelligence and National Security* 39, no. 3 (15 April 2024): 525, https://doi.org/10.1080/02684527.2024.2321692.

119 Paul Burke, "The Issues in the Collection, Verification and Actionability of Citizen-Derived and Crowdsourced Intelligence during the Russian Invasion of Ukraine, 2022," *Strategic Panorama*, 15 November 2022, 100, https://doi.org/10.53679/2616-9460.specialissue.2022.09.