



Universiteit
Leiden
The Netherlands

From shadows to screens: digital outreach strategies in intelligence and law enforcement

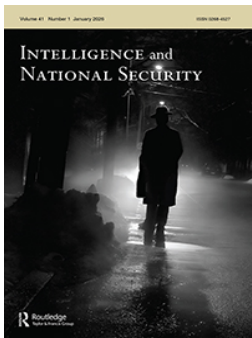
Schrijver, Peter; Wielders, Bart

Citation

Schrijver, P., & Wielders, B. (2026). From shadows to screens: digital outreach strategies in intelligence and law enforcement. *Intelligence And National Security*, 1-29.
doi:10.1080/02684527.2026.2669810

Version: Publisher's Version
License: [Creative Commons CC BY 4.0 license](#)
Downloaded from: <https://hdl.handle.net/1887/4308085>

Note: To cite this publication please use the final published version (if applicable).



From shadows to screens: digital outreach strategies in intelligence and law enforcement

Peter Schrijver & Bart Wielders

To cite this article: Peter Schrijver & Bart Wielders (25 May 2026): From shadows to screens: digital outreach strategies in intelligence and law enforcement, *Intelligence and National Security*, DOI: [10.1080/02684527.2026.2669810](https://doi.org/10.1080/02684527.2026.2669810)

To link to this article: <https://doi.org/10.1080/02684527.2026.2669810>



© 2026 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group.



Published online: 25 May 2026.



Submit your article to this journal [↗](#)



View related articles [↗](#)



View Crossmark data [↗](#)

RESEARCH ARTICLE

 OPEN ACCESS



From shadows to screens: digital outreach strategies in intelligence and law enforcement

Peter Schrijver  and Bart Wielders 

ABSTRACT

A growing number of intelligence and law enforcement organisations are augmenting traditional tradecraft with digital outreach to engage isolated or distrustful populations. This article examines this shift through two campaigns: Ukraine's Main Intelligence Directorate (HUR) 'I Want to Live' project for Russian defectors and the Royal Netherlands Marechaussee (RNLM) 'Call to Victims' program for Eritrean witnesses. Using Telegram analysis and practitioner interviews, the study demonstrates how agencies adapt commercial marketing logic to security goals. The findings identify a 'digital funnel' model, which streamlines the transition from broad public messaging to secure intake, facilitating engagement with populations traditionally difficult to access.

ARTICLE HISTORY

Received 5 January 2026
Accepted 1 May 2026

KEYWORDS

Digital outreach;
intelligence; social media;
Ukraine; Russia; Netherlands;
Eritrea

Introduction

Intelligence and law enforcement organisations have traditionally relied on covert and interpersonal methods to make contact with potential informants, witnesses, defectors, and other individuals who rarely interact with state institutions. These methods were grounded in personal networks, intermediaries, and the slow cultivation of trust.¹ Alongside these covert approaches, agencies also used public-facing tools such as printed notices, reward schemes, and broadcast crime appeals.² While these forms of outreach helped raise awareness, they offered limited possibilities for targeted or private engagement.

The broader shift towards digital communication has altered these conditions. Social media and messaging applications have expanded the range of individuals who can be approached, creating new routes for contacting those who previously remained beyond institutional reach.³ What distinguishes contemporary outreach from earlier broadcast appeals is the ability to reach individuals directly through their personal devices (e.g., smartphones), linking broad campaign messaging with immediate, private interaction.⁴ These changes reshape how agencies attempt to establish contact and reduce uncertainty for potential sources and contacts, without removing the need for secrecy or operational caution.

CONTACT Peter Schrijver  p.schrijver@fgga.leidenuniv.nl

© 2026 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group.

This is an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. The terms on which this article has been published allow the posting of the Accepted Manuscript in a repository by the author(s) or with their consent.

Understanding these shifts is relevant for research on state authority, conflict, and border governance, where access to non-cooperative populations that remain beyond the reach of conventional methods is a recurring challenge. In this context, a growing number of intelligence and law enforcement organisations have begun using digital tools to reach specific audiences and solicit contact. Agencies publish procedural guidance, circulate targeted messages, and provide accessible communication channels. Existing research on state authority in the digital age spans three primary domains: (1) strategic communication and information warfare, which explores how states use media for influence operations; (2) digital policing, which examines online community engagement and surveillance; and (3) traditional studies of intelligence recruitment, which focus on physical tradecraft and interpersonal dynamics.⁵ While existing literature addresses community engagement and physical tradecraft, it offers little insight into how digital platforms are used to solicit contact from hard-to-reach groups, such as enemy combatants or irregular migrants. Specifically, there remains a gap in understanding how organisations transition the ‘first contact’ phase from physical encounters to mediated digital environments. An important distinction must be drawn at the outset. Public-facing digital outreach of the kind examined in this article is not a substitute for clandestine human intelligence (HUMINT) practices such as the covert recruitment and handling of sources. The logic of covert source handling relies on sustained access, behavioural leverage, and operational control that cannot be replicated through public or semi-public communication. Rather, the digital outreach practices analysed here address a different and earlier phase: the solicitation of initial contact from individuals who might otherwise never engage with state authorities. This article therefore examines digital outreach as a complement to, rather than a replacement for, traditional tradecraft.

To examine how this outreach works in practice, this study analyses two cases: the Ukrainian Main Intelligence Directorate (HUR)⁶ and the Royal Netherlands Marechaussee (RNLN).⁷ Although they operate in different contexts, both organisations face the problem of engaging groups that do not readily interact with state authorities. For the HUR, this includes Russian military personnel who may consider surrendering during the Russo-Ukrainian war. Its ‘I Want to Live’ campaign uses platforms such as a website, the Telegram messaging application and a chatbot to address Russian military personnel, their families, and the wider Russian-speaking public, while providing a specific avenue through which soldiers can signal intent to surrender.⁸ For the RNLN, the Netherlands’ military police and border control agency, the challenge concerns individuals travelling along irregular migration routes. Its ‘Call to Victims of Human Trafficking from the Horn of Africa’ initiative sought to reach Eritrean migrants who might provide information on smuggling and extortion networks.⁹

In both contexts, outreach initially takes place through personal digital devices rather than face-to-face interaction. The analytical value of pairing such dissimilar cases lies in a ‘most-different’ comparison; if similar patterns are observed in a peacetime law-enforcement investigation and a wartime intelligence operation, it suggests a general organisational mechanism rather than a context-specific tactic.

The central question guiding this study is: how do intelligence and law enforcement organisations use digital strategies to reach groups that would normally remain hard to access? To conceptualise how such outreach practices are structured, digital outreach can be understood in relation to broader structural societal processes, particularly

mediatisation and digitalisation. Mediatisation refers to the adaptation of organisational communication to media logic, while digitalisation refers to the expansion of digital infrastructures that enable continuous, networked, and device-based interaction. As media logic becomes internalised, organisations increasingly adapt content, timing, and format to the expectations of platforms such as Telegram, Instagram, and Facebook.¹⁰ Digital communication enables widely circulated messages that include immediate, private contact options, creating a pathway between public messaging and individualised interaction.¹¹

Across the two cases, the analysis points to a recurring operational sequence through which organisations convert broad public messaging into progressively more private forms of contact. This article refers to this sequence as a ‘digital funnel’, an analytical concept developed from the material to capture how platform communication, trust threshold reduction, and the solicitation of contact from otherwise inaccessible groups are staged over time. The term ‘digital funnel’ is deliberately adapted from the marketing concept of a conversion funnel, in which broad initial awareness is progressively narrowed toward a specific desired action. This terminology reflects the article’s core argument: that the organisations examined here have adapted commercial marketing logic to security and intelligence objectives. Alternative framings drawn from intelligence studies, such as ‘intelligence collection techniques’, would mischaracterise the phenomenon, which is rooted in outreach and solicitation rather than analysis or collection.

The remainder of this article outlines the methodological approach, presents both cases, analyses their outreach practices, and discusses their convergence, including ethical implications of digital recruitment in conflict and law enforcement settings.

Methods

Instead of a symmetrical comparison, this study uses two complementary cases with different data profiles. For the HUR’s wartime military campaign, the analysis draws primarily on public-facing digital output, supplemented by a practitioner roundtable conducted in Kyiv in 2026. For the RNLM’s peacetime investigative outreach program, the analysis draws on practitioner interviews and desk research. Combining these two disparate cases provides a holistic understanding of digital outreach, capturing its application in both high-intensity conflict and domestic law enforcement.

Research objectives

Each case study serves a specific purpose within the overall research design. The analysis of the HUR’s ‘I Want to Live’ campaign examines how a wartime intelligence organisation uses a public-facing digital channel to solicit contact from enemy combatants. The analysis of the RNLM’s ‘Call to Victims’ campaign examines how a peacetime law enforcement organisation uses targeted digital advertising to solicit witness testimony from a distrustful migrant community. Together, the cases address the research question from two contrasting operational contexts, enabling the identification of shared patterns that transcend specific settings.

Data collection

The data collected for this study consist of Telegram posts, semi-structured interviews, a practitioner roundtable, and additional documents such as press releases and campaign websites. For the 'I Want to Live' case, 192 Telegram posts were collected in a dataset. The dataset covers the first three months (6 August – 6 November) of Ukraine's 2024 offensive in Russia's Kursk oblast and includes all public posts shared via the channel t.me/hochu_zhyt (t.me/hochu_zhyt (t.me/I want_to live)), which is run by Ukraine's Coordination Headquarters for the Treatment of Prisoners of War, under the direction of military intelligence (HUR). The full dataset was collected using a scraping tool and includes all publicly available messages from the campaign's Telegram channel during the selected timeframe.¹²

The analysis of the HUR case was additionally informed by a practitioner roundtable conducted at the Coordination Headquarters for the Treatment of Prisoners of War (*Koordshtab*; *Ukrainian abbreviation*) in Kyiv on 30 March 2026, at which five representatives discussed the procedures and results of the project. Participants consented to the use of this material for publication on condition of anonymity. Notes are held by the authors.¹³

For the 'Call to victims of human trafficking from the Horn of Africa' case, four semi-structured interviews were conducted with five respondents between February and April 2025. The interviews followed a topic guide structured around the campaign's design, execution, adaptation, and evaluation. Respondents were selected on the basis of their direct involvement in the campaign and included: two members of the criminal investigation team responsible for witness interviews (DR002, DR003); two members of the investigation communication team responsible for campaign design, platform selection, and advertising (DR004, DR005, interviewed jointly); and a cultural mediator who advised on messaging and translation (DR001). Respondent codes are used throughout to preserve anonymity while enabling traceability of quoted material. The interviews were recorded and transcribed verbatim, yielding 52 pages of transcripts which were coded using NVIVO. Interviews were conducted in Dutch; select quotations have been translated into English to illustrate the findings. To ensure accuracy and validity, transcripts were returned to participants for member checking.

Analysis

The data were analysed using reflexive thematic analysis (RTA), a method suitable for identifying both explicit and implicit patterns in qualitative material.¹⁴ For the 'I Want to Live' case, each message was coded for its dominant communicative theme, using a coding frame developed iteratively during the analysis. The coding criteria focused on the primary communicative function of each message: what action or response it appeared designed to elicit, and what framing devices it employed (e.g., dissent, internal military tensions, surrender appeals, or public shaming of misconduct). Messages were assigned to a single dominant theme based on their most prominent function, though many contained secondary elements. Following an iterative process of review and comparison, six dominant themes were identified as structuring the campaign's output. For the 'Call to Victims' campaign, the interview transcripts were scanned line-by-line and coded for emergent themes.

Limitations and considerations

Several limitations regarding the datasets must be acknowledged. The Telegram data for the HUR case was collected from a state-operated platform during wartime, raising inevitable concerns about narrative framing and selective disclosure. The analysis therefore focuses on communicative patterns rather than the factual accuracy of the content. Furthermore, the dataset captures only public-facing content and does not include private interactions (e.g., chatbots or hotline calls), limiting conclusions about audience conversion rates, though practitioner accounts from the Coordination Headquarters provided limited insight into post-contact procedures.

Conversely, the interview data for the RNLM campaign provides an insider perspective but is limited to the viewpoint of the government agency. The authors were unable to interview witnesses to capture the recipients' perspective. Finally, the analysis of both cases is shaped by the context-sensitive coding process of reflexive thematic analysis, which is interpretive by design.¹⁵ In addition, the analysis faces inherent challenges in quantification: a theme briefly mentioned in one reference cannot be directly equated with another theme that receives extensive, detailed treatment in a subsequent reference.¹⁶

'I Want to Live' campaign

The 'I Want to Live' campaign is a communication initiative established by Ukraine's Main Intelligence Directorate (HUR) in September 2022 and is part of Ukraine's wider effort to shape perceptions of the war through digital communication.¹⁷ It is administered through the Coordination Headquarters for the Treatment of Prisoners of War and is intended to provide a mechanism through which Russian military personnel can signal their intention to surrender.¹⁸ The campaign is one of several digital projects operated by the Coordination Headquarters, which together form an integrated system addressing different audiences and functions, including the search for missing personnel, the facilitation of prisoner exchanges, and outreach to Ukrainian citizens held in Russian captivity.¹⁹ The campaign operates alongside military activity and has been maintained throughout successive phases of the war, including during the Ukrainian operation in the Russian Kursk oblast in 2024.²⁰

The campaign uses several digital channels to disseminate information and facilitate contact. Its main platforms include a website (www.hochuzhit.com), a Telegram channel, messaging applications such as WhatsApp, a 24-hour telephone hotline, and automated chatbots. These tools are used to distribute guidance on how to surrender safely, explain legal protections afforded under international humanitarian law, and outline possible next steps following detention.²¹

Information is provided in Russian and is designed to be accessible via applications and networks familiar to Russian military personnel and the wider Russian-speaking public. Telegram is used extensively by Russian military personnel for both official and personal communication, and the campaign makes use of this platform to reach its intended audience.²² Communications are distributed in the form of text messages, audio recordings, and videos. In some cases, content is also made available for forwarding within peer groups or private chats.²³

The website and Telegram channel offer practical details on the surrender process. These include telephone numbers, instructions for initial contact, and clarification of legal rights. Enquiries can be made anonymously. The campaign presents its process as structured and predictable, with reference to legal frameworks and international oversight mechanisms.²⁴

One element of the campaign involves the publication of video statements by Russian prisoners of war or soldiers who have surrendered. These individuals speak in their own words, often describing how they were treated following surrender. In several cases, soldiers recount the conditions that influenced their decision to disengage from combat.²⁵ These accounts are published on Telegram and occasionally re-shared by third-party channels. In addition to testimonial material, the campaign has released intercepted phone conversations between Russian soldiers and family members. These recordings refer to logistical shortages, dissatisfaction with leadership, or discussions of potential withdrawal.²⁶

The campaign also demonstrates a high degree of operational responsiveness. During specific military operations, such as the August 2024 offensive in Kursk oblast, the campaign's activity was closely aligned with battlefield developments. Messages were directed at Russian units positioned in towns near the frontline, encouraging them to make contact before Ukrainian advances reached their positions. In parallel, the campaign addressed residents in the region, asking them to report on the presence of specific military formations.²⁷ This form of geographic targeting was used to tailor the content to the immediate circumstances of both soldiers and civilians.

The campaign also distributes content intended to clarify its structure and reinforce awareness of available procedures. These posts include statistics on past surrenders, updates on prisoner exchanges, and summaries of legal protections. Messages are often brief, formatted for mobile viewing, and include images, hashtags, or direct links to further resources. While the 'I Want to Live' campaign is managed by a Ukrainian state body, its materials are framed to appear informal and accessible. Messaging is written in conversational Russian, with references to familiar contexts or shared experiences. The use of digital platforms enables interaction beyond formal military channels and allows users to initiate contact at their discretion.

The campaign remains active and continues to release content at regular intervals. Its focus on surrender procedures, soldier testimonies, and communication places it within a wider set of information activities undertaken by the Ukrainian government and civil society during the war.²⁸ It addresses both military personnel and, at times, their families, offering contact points and explanatory content without requiring in-person engagement.

Data released by Ukrainian authorities and practitioners indicate that the campaign receives a steady and growing volume of requests. By October 2025, the project reported 52,000 applications, 50 million website visits, of which 43 million originated from within the Russian Federation, and over one billion advertisement views across its platforms. The project confirmed more than 400 surrenders and defections processed directly through its channels, though practitioners indicated the actual number to be higher.²⁹

The preceding figures described the project's cumulative reach since its start in 2022. The following indicators relate specifically to the 192 Telegram posts analysed in this study, all of which were published during the first three months of Ukraine's 2024 offensive in Kursk oblast. Between 6 August and 6 November 2024, the 192 Telegram

Table 1. Thematic distribution of Telegram posts, 6 August to 6 November 2024.

Theme	Number	Percentage	Description
Shaming	54	28.1 per cent	Content that exposes moral, legal, or operational failures by Russian authorities.
Dissent	48	25.0 per cent	Posts that emphasise internal fractures within the Russian military, especially between regular and Chechen units.
Testimonial	30	15.6 per cent	First-hand accounts from surrendered Russian soldiers.
Project promotion	27	14.1 per cent	Promote the 'I Want to Live' and 'I Want to Find' initiatives
Intercepts	13	6.8 per cent	Conversations between Russian soldiers revealing low morale, command failures, or ethnic discrimination.
Miscellaneous	20	10.4 per cent	Posts that do not clearly fall into the above categories but still support the campaign's strategic goals.
Total	192	100.0 per cent	

posts garnered over 14.2 million views, with an average of 74,016 views per post.³⁰ These messages also accumulated 55,652 likes, 35,856 shares, and 8,032 comments, pointing to a high level of public interaction. The most widely shared post reached more than 1.6 million views, suggesting that specific messages, particularly those announcing mass surrenders or exposing unit-level dissent, achieved viral reach.³¹ These engagement patterns support the interpretation that the campaign circulated widely and resonated with its intended audience, providing a quantitative foundation for the qualitative thematic analysis that follows.

Thematic analysis of the 'I Want to Live' Telegram content

This section presents the findings of a qualitative analysis of the 'I Want to Live' Telegram campaign. Six dominant themes were identified as structuring the campaign's output. These are summarised in [Table 1](#), with indicative percentages based on the primary theme per message. These figures should be interpreted as approximate estimates of the campaign's editorial focus rather than precise statistical measurements.

Each theme reflects a distinct strategic function within the campaign's broader psychological and informational objectives. Selected examples in the following subsections illustrate how these themes were deployed to influence Russian military personnel and the wider Russian-speaking public.

Shaming

Shaming is the most frequently observed strategy on the 'I Want to Live' Telegram channel. These messages focus on (perceived) moral, legal, or operational failures by Russian military and political actors. The aim is to weaken their credibility by provoking emotional responses such as outrage or disillusionment among Russian audiences, thereby encouraging defection. As Krain (2012) and Hirschberger (2021) observe, exposing wrongdoing during conflict can shift public perception and contribute to the erosion of institutional legitimacy.³²

One post refers to Russia's policy of pardoning convicts in exchange for military service. It presents the case of Azamat Iskaliyev, a man previously imprisoned for murdering his wife, who was released early to serve in the armed forces.³³ After his release, he fatally stabbed a woman in Saratov, Russian Federation. The post frames this as a failure of military and legal oversight, arguing that military service did not rehabilitate the offender but allowed him to avoid accountability and reoffend.

Another post employs shaming to contrast Ukrainian and Russian conduct in the treatment of prisoners of war. It cites comments by Danielle Bell, Head of the UN Human Rights Monitoring Mission in Ukraine, who described the widespread torture of Ukrainian POWs in Russian captivity as the worst abuse she had witnessed in her twenty-year UN career.³⁴ The post claims that more than 95 per cent of Ukrainian prisoners have been subjected to torture, labelling these actions as war crimes. In contrast, Ukraine is presented as complying with international law, providing humane treatment to Russian POWs and allowing access for international observers. This comparison positions Ukraine as adhering to the Geneva Conventions while portraying Russia as systematically violating international norms.

A further instance of shaming is found in a post that shows systemic abuse within the Russian military, focusing on the widespread use of punitive confinement in pits and basements. Servicemembers are subjected to harsh punishments, including beatings, deprivation of food or water, and public humiliation, for refusing orders, raising complaints, or returning from failed operations. These acts are described as routine, not exceptional. They are portrayed as part of a longstanding military tradition rooted in coercion and dehumanisation.³⁵ The decision over life or death, the post claims, is often left to local commanders with no recourse to legal standards. The practice is depicted as incompatible with modern values and used as a tool to enforce obedience through fear. Soldiers who do not comply are urged to seek help via the project and avoid further participation in such a system.

Another post uses shaming to depict the Russian military leadership as directly complicit in the deaths of its own soldiers. The message, framed around an '*epidemic of suicides on the battlefield*', accuses Russian commanders and propagandists of driving soldiers toward suicide as an alternative to surrender.³⁶ The post references disturbing footage from drones and claims that suicide instructions, allegedly distributed in place of basic medical supplies, reflect a broader disregard for soldier welfare. Russian officers are portrayed as sending troops into repeated, unsupported assaults, while denying them evacuation or basic aid. By contrast, the message claims Ukraine offers a '*mutually beneficial deal*': life, humane treatment, and eventual exchange under international oversight.³⁷ The post concludes by citing examples of conscripts in the Kursk region who surrendered instead of following such directives. According to the message, they later returned home alive.

Dissent

Messaging associated with the dissent theme frequently mentions friction within the Russian military, particularly between regular units and Chechen formations, often referred to as 'Kadyrovtsy' units. The term *Kadyrovtsy* refers to units under the control of Ramzan Kadyrov, head of the Chechen Republic within the Russian Federation.

A message circulating in the early stages of the Kursk offensive serves a dual purpose: to encourage surrender and to foment distrust among Russian military personnel.³⁸ It portrays Russian conscripts as victims of abandonment by their own commanders, accusing leadership of reporting false victories to Moscow while leaving soldiers to die or be captured. The post draws a sharp line between regular units and Chechen forces, mocking the latter, referred to as *'TikTok troops'*, for allegedly fleeing at the first sign of danger and setting up conscripts to fail.³⁹

Another post targets pro-Kremlin propagandists, including Anastasia Kashevarova, accusing them of protecting elite units while disregarding the fate of ordinary conscripts. The message criticises efforts to downplay Ukraine's offensive in Kursk and suggests that disinformation from official media outlets has directly contributed to battlefield confusion and surrender. It positions the Kadyrov-affiliated forces as privileged and theatrical, while portraying young conscripts as poorly equipped and abandoned.⁴⁰ References to the mythologising of Soviet-era heroism, such as the WWII myth of the *'28 Panfilov heroes'*, are used to argue that these narratives obscure the contemporary failures of Russian military planning and leadership.⁴¹

A third post suggests that resentment between units has escalated into acts of sabotage. It reports, without confirming, that some regular Russian troops have begun leaking the positions of Chechen forces to Ukrainian intelligence as an act of retaliation. This rumour is used to illustrate the extent of distrust and disintegration within the chain of command, implying that breakdowns in cohesion are not only rhetorical but operational.⁴² The post concludes by presenting surrender as a rational response to a military system marked by betrayal, favouritism, and disinformation.

Collectively, these messages use incidents and imagery to construct a picture of division and mistrust within Russian forces. By foregrounding the Chechen units' strained relations with other military elements, the communication not only signals operational vulnerabilities but also amplifies scepticism about the coherence and morale of the Russian war effort.

Testimonials

These posts feature interviews with surrendered Russian soldiers and prisoners of war. The accounts are used to cast doubt on the Russian war effort, humanise defectors, and affirm Ukraine's adherence to international norms.

For example, in one testimonial, a Russian soldier who had surrendered to Ukrainian forces discusses how the Ukrainians gave him and other soldiers *'water to drink from the last bottle'* and *'a smoke'* and how they had *'expected a completely different attitude'*.⁴³ Another post features the testimony of Vladimir Vasilyevich Kuleshov from Orel, Russia. After losing his job due to sanctions, he signed a contract with the Russian Ministry of Defence and was deployed to Luhansk oblast in eastern Ukraine just four days later as a deputy platoon commander.⁴⁴ Promised officer training, he instead faced frontline combat with minimal preparation. His platoon of thirty suffered near-total losses during a single operation against elite Ukrainian formations *'Kraken'* and *'Artan'*.⁴⁵ Captured during this offensive, Kuleshov expressed surprise at the discipline and conduct of Ukrainian troops, contrasting it with the disorganisation of the Russian side. In captivity, he met

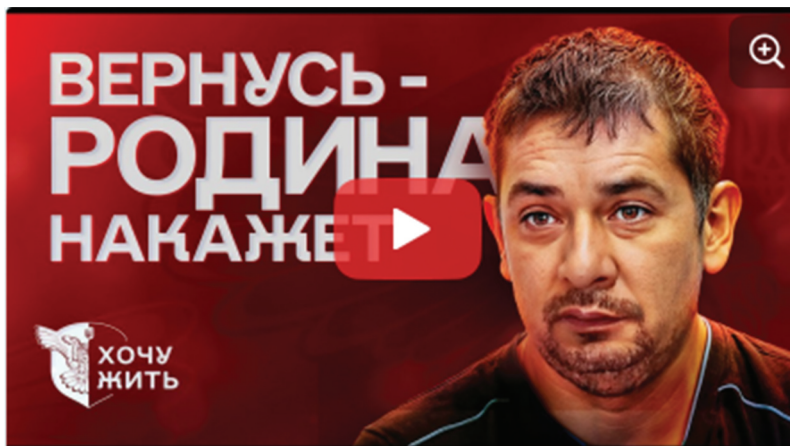


Figure 1. Screenshot of the interview with Russian Major Bykov, who surrendered himself and his unit, <https://www.youtube.com/watch?v=EPkA5lkdpzl>.

fellow Russian soldiers who had been awaiting prisoner exchanges for years, while others, particularly Kadyrov-affiliated personnel and conscripts, were swiftly repatriated.

An additional example draws attention to a Russian officer characterised as a *'unique phenomenon'*.⁴⁶ Major Mikhail Fedorovich Bykov, known by the call sign *'Navigator'*, is a Russian aviation officer who was mobilised into the motorised rifle troops and assigned to the border with Ukraine, where he was unexpectedly placed in command of conscripts (see Figure 1).⁴⁷ After becoming surrounded, Bykov chose to surrender to preserve his unit. He expresses concern about punishment but argues that saving his men justified the decision. His account portrays ethical decision-making as rare within the Russian military, reinforcing the project's message that defection can be morally defensible.

Together, these posts construct a narrative in which surrender becomes a rational and ethically grounded act. By foregrounding humane treatment, empathy, and operational failure on the Russian side, the testimonials aim to erode loyalty among frontline soldiers while strengthening Ukraine's normative claims. As scholar Grauer argues, surrender becomes more likely when soldiers expect humane treatment.⁴⁸ The testimonial content directly targets these expectations, reinforcing the logic of self-preservation.

Project promotion

Posts in this category aim to promote the operational availability and credibility of the 'I Want to Live' and 'I Want to Find' initiatives.⁴⁹ The former addresses Russian soldiers directly, offering surrender as a life-preserving option. The latter supports Russian relatives searching for missing personnel.

One post marks October 2024 as a record month for applications to 'I Want to Live' project, citing 6,533 new requests and a cumulative total of 38,528. The message also reports on POW identifications, prisoner exchanges, and casualty confirmations, underlining the project's transparency and procedural structure.⁵⁰

Another post provides a two-year overview, noting over 40,000 inquiries from Russian military personnel via Telegram, WhatsApp, chatbots, and hotline. It explains the

registration and detention process and outlines the legal protections available to surrendered soldiers, including the possibility of asylum in Ukraine or third countries. These posts are logistical and informative, reinforcing the project's reliability and reach.⁵¹

Communication intercepts

Messages categorised under the intercepts theme and labelled with the hashtag *#Listening_to_the_Occupiers* typically feature wiretapped and intercepted conversations between Russian military personnel.

One example features a conversation between a Russian soldier named Viktor and his wife.⁵² Viktor reports that commanders have left the unit without supplies, no food, water, or communication. Soldiers attempting to flee are shot by their own side and consider self-injury or suicide by grenade to escape the front. There is no proper medical care, wounded personnel are not evacuated. Furthermore, the intercepts describe soldiers as desperate to leave the war zone but fearful of reprisals.⁵³

Another example of an intercept ticks multiple themes the 'I Want to Live' project emphasises. This intercepted call between a soldier and his wife reveals deep frustration, resentment, and emerging awareness about the unequal treatment and perceived futility of the war.⁵⁴ The soldier describes that he is stationed on the front lines for two years without rotation, while his commander has taken multiple vacations.

A key theme is ethnic discrimination: the soldier, identified as Buryat in the post, states that his Russian commander consistently assigns him the most dangerous tasks, suggesting that ethnic minorities are being disproportionately exposed to risk.⁵⁵ The soldier asserts that the war benefits only political leaders and high-ranking commanders, not ordinary people. His concluding statement: *'I don't see what kind of motherland I am defending here'*, underscores a sense of betrayal and alienation.⁵⁶ The post positions this call as an example of growing disillusionment within the Russian ranks, particularly among those from non-Slavic regions.

Miscellaneous

This final category includes content that does not fit neatly into the other themes but still contributes to the campaign's strategic objectives. Posts include information on captured Russian soldiers, warnings to foreign fighters from Asia and Africa considering enlistment in Russian forces, and anticipatory messages about upcoming Russian mobilisation waves.⁵⁷

One example, in Korean, specifically addresses North Korean soldiers first being observed in the Kursk oblast in late 2024. Similar to regular 'I Want to Live' messages addressed to Russian military personnel; this post also called upon North Korean soldiers to surrender themselves voluntarily.⁵⁸ By 2026, practitioners at the Coordination Headquarters estimated that at least 27,000 foreigners from 135 nations were serving within the Russian armed forces, prompting the project to expand its website to five languages.⁵⁹

What is notable is the direct coordination between the 'I Want to Live' project and physical military operations. During the Kursk oblast offensive, the Ukrainians directed messages toward Russian soldiers active in towns and villages at risk of being overrun by

the Ukrainian army.⁶⁰ However, this coordination went even further. Before Ukrainian troops entered Russian villages, the project was already communicating with residents, requesting them to report the locations of Kadyrov's 'gangs' or forces.⁶¹ The project's staff actively used social media to warn about impending encirclements by the Ukrainian army, creating psychological pressure. These messages were designed to dissuade Russian soldiers from combat by presenting surrender as a viable alternative.

The thematic analysis of the content on 'I Want to Live' channel serves multiple and intertwined communicative functions. A substantial proportion of its content, particularly posts categorised under shaming, dissent, and intercepts, targets enemy morale, exploits internal divisions, and undermines confidence in Russian military leadership. At the same time, the channel's project promotion and testimonial content performs a distinct operational function: the direct solicitation of surrender and the provision of procedural guidance for defection.

This combination of strategic influence and operational outreach is consistent with what Schrijver (2025) terms participatory intelligence communication. In this mode of engagement, intelligence-related content is selectively disclosed to shape adversary behaviour while simultaneously offering a practical pathway for those willing to act on it.⁶² While elements of the channel's output overlap with what Western military doctrine classifies as psychological operations, applying that label to the campaign as a whole would flatten its dual character. The 'I Want to Live' project operates both as an influence instrument and as a functioning operational interface for surrender coordination, and it is this combination, rather than either function in isolation, that defines its distinctive logic. The analytical focus of this article is on the latter dimension: the mechanisms through which initial contact is established and managed through a staged digital process.

'Call to victims of human trafficking from the Horn of Africa' campaign

In contrast to the high-intensity information environment of the Russo-Ukrainian war, the 'Call to Victims of Human Trafficking from the Horn of Africa' represents a targeted law enforcement initiative operating within a peacetime legal framework. Launched by the RNLM in October 2024, the campaign was managed jointly by the RNLM's criminal investigation brigade and the Netherlands Police's investigation communication team.

The primary objective was to identify potential witnesses among Eritrean migrants travelling through Libya along the Central Mediterranean Route (CMR) to Europe. This initiative formed part of a broader investigation aimed at mapping migrant smuggling and extortion networks. It built upon previous efforts by the RNLM and the Netherlands Police targeting organised criminal groups and Libyan militias involved in the exploitation of migrants.⁶³

The aim of the 'Call to Victims of Human Trafficking from the Horn of Africa' Campaign was to generate statements from victims or witnesses to support the investigation. The target audience consisted of individuals who fled from Eritrea to the EU via the Central Mediterranean Route through Libya between 2016 and 2024, and who resided in the EU. The team knew from previous investigations that this was a hard-to-reach demographic:

'We rely on witnesses. Reaching out to them is one thing, but convincing them to share their story is another'.⁶⁴

The circumstances in the country of origin and the migrants' experiences during their journey meant that the team had to overcome significant mistrust from victims and witnesses towards authorities in general and the police in particular. This made trust a crucial element in the campaign's efforts to engage the target audience convincingly.

The campaign utilised several channels to disseminate information and facilitate contact. Its main components included advertisements on Meta (Facebook and Instagram), a webpage, messaging applications such as WhatsApp, Viber, and IMO, a telephone line, and an email address. Information was provided in Tigrinya, English, and Dutch and designed to be accessible through applications familiar to migrants from the Eritrean community. The campaign employed Facebook and Instagram to reach its target audience, as these platforms are extensively used within the Eritrean community. Communications were distributed through Meta advertisements, text, images, and videos. The content was made available for sharing within peer groups.

Because the investigation team anticipated that the target audience would need some persuasion to actively contact the RNLM, a retargeting strategy was used for Facebook and Instagram ads. This strategy involved two phases. In the first phase, video advertisements were placed on Facebook and Instagram. These ads, in Tigrinya and English, included a brief call for witnesses, contact details for reaching the RNLM in their own language, and a link to the webpage for further information. In the second phase, a follow-up advertisement was shown to individuals who had viewed the initial ad for at least 3 seconds. This second ad, also in Tigrinya and English, featured a still image, the same call for witnesses, a short explanation of the RNLM, contact details in their own language, and a link to the webpage. Both advertisements highlighted the option to testify anonymously under certain conditions.

The webpage offered a more detailed call for witnesses, information about the targeted criminal network, and updates on the new investigation, emphasising the successful arrest of several suspects in previous cases. It also explained how a potential witness can contact the RNLM and what to expect upon contact. The webpage also provided an option to securely report or submit photographic and video materials.

A key component of the webpage is a video testimony from a witness who fled Eritrea and had contact with detectives from the RNLM. The witness speaks in Tigrinya about their experience with the RNLM. They also describe the circumstances that prompted their flight from Eritrea, recount their journey to the EU, and detail the abuse they endured at the hands of smugglers and human traffickers. The witness shares a personal motivation for giving testimony (*'I don't want those who come after me to suffer the same fate as me'*⁶⁵) and encourages others to come forward and share their experiences.

The campaign ran from 7 to 31 October 2024, though the webpage remains accessible. Engagement data from Meta show extensive reach. The adverts on Meta were viewed by over a million unique individuals. The webpage received over 5,000 unique clicks. The RNLM and Police reported receiving numerous potential witnesses and noted that the campaign's results were favourable compared to similar initiatives.⁶⁶ Individuals who interacted with the advertisements on social media were not automatically identified.

Table 2. Thematic distribution of practitioner interviews.

Theme	References	Percentage	Description
Platform selection	23	15,9 per cent	References regarding social media platform selection.
Messaging strategy and challenges	29	20 per cent	References discussing elements of the messaging strategy.
Ethical and legal considerations	26	17,9 per cent	Comments on ethical and legal considerations, dilemmas and constraints.
Balancing openness and secrecy	28	19,3 per cent	Discussions on the open nature of outreach on social media vs the confidentiality of an investigation.
Adaptation	22	15,2 per cent	References regarding the adaptation of the campaign.
Lessons learned	17	11,7 per cent	Reflections on lessons learned.
Total	145	100 per cent	

Positive identification occurred only when a person voluntarily initiated contact and proceeded to the telephone intake interview conducted by the front office.

Thematic analysis of the call to victims campaign: a practitioner's view

This section presents the findings of the reflexive thematic analysis of the 'Call to Victims' campaign practitioner interviews. Six themes were identified, representing a practitioner's perspective. The themes are summarised in [Table 2](#).

Platform selection

The RNLM team chose to use Meta (Facebook and Instagram) as their advertising channels, with WhatsApp, IMO, and Viber serving as communication platforms. Four main factors influenced their platform selection: 1) budget, 2) advertisement format, 3) monitoring options, and 4) platform demographics. The available budget determined which platforms could be utilised for the campaign. Using more platforms would have spread the budget too thin and shortened the campaign duration. It would also have increased the risk of reaching the same individual multiple times through different channels, reducing the potential to generate views from unique persons within the same budget. The advertisement format was also a crucial factor. The team briefly considered banner ads but concluded that to persuade people to respond to the advertisement, they needed space to explain, address distrust, and encourage engagement, so they opted for a video format instead.

The third deciding factor was the monitoring options offered by the different advertisement platforms. Given the chosen retargeting strategy, the team needed to monitor unique video ad views in Phase One to determine who would be retargeted in Phase Two. This was a key factor in the decision to remain on a single advertising platform. Additionally, various platforms provide distinct options for monitoring and retargeting. The possibility of retargeting on video was an important deciding factor.

The fourth factor influencing platform choice was platform demography, defined as the characteristics of users across platforms. To maximise visibility and reach as many unique viewers as possible, the team needed to select the platform most frequently used by their target audience. For this purpose, the team relied on publicly available open-source reports on social media use among specific demographics and on advice from a

cultural mediator. It quickly became clear that Facebook was the most commonly used platform among the target audience.⁶⁷ Other platforms were considered but not selected due to lower daily usage (YouTube) or targeting the wrong age group (TikTok and Snapchat). In particular, the younger TikTok and Snapchat audiences posed a potential challenge for the investigation team when it came to interviewing a minor as a witness.⁶⁸

Messaging strategy and challenges

Mapped against established marketing frameworks, the campaign structure closely resembles the initial stages of the McKinsey customer journey model: awareness, consideration, evaluation, and conversion/closure.⁶⁹ See Table 3.

The Meta advertisements aimed to raise awareness of the campaign and encourage people to click the link and visit the website. The retargeting strategy focused on the consideration phase, while the website provided additional information to support the evaluation process, including whether to proceed and contact the RNLM or to upload photos or videos (conversion/closure).

To raise awareness, video was used to prompt people to watch the advertisement and visit the website. This posed a dilemma for the team, as the pool of available footage was limited. News outlets were reluctant to sell video for this purpose, and a large number of videos on social media could not be verified. The team overcame this obstacle using police footage of previous arrests, supplemented with stock photos and animations. Next, retargeting was used to influence the consideration and evaluation phase:

People who had watched at least the first three seconds of the video would later be shown another ad. Because often someone watches something and then thinks, “nah, forget it”. Especially in this case, if people felt anxious, they could decide not to proceed. But then, after a few days, they would see another ad. In that way, we tried to really pull them into the funnel.⁷⁰

The next stage involved the webpage, which was vital for overcoming distrust during the evaluation phase. To build trust, the team relied on cultural awareness, language, and Cialdini’s principles of persuasion.⁷¹ To enhance cultural understanding, the team engaged a cultural mediator with expertise in Eritrean culture and Tigrinya. This mediator advised the team on tailoring their message to connect effectively with the target audience. The team recognised a significant language and cultural barrier:

We wanted to seek advice from that cultural mediator on how we could best reach those people, and with which texts. We can translate something directly, but from our own perspective, it might come across very differently than when you put it in Tigrinya. That was something we really had to think about.⁷²

With the team’s permission, the mediator adapted text, without changing the meaning, for the video script, social media posts, and the webpage.⁷³ Using Tigrinya was essential

Table 3. Campaign stages and customer journey.

	Stage 1	Stage 2	Stage 3	Stage 4
Campaign	Advertisement	Retargeting	Webpage	Contact
Customer Journey	Awareness	Consideration	Evaluation	Conversion

to reaching the target audience, engaging them, and building trust. However, using Tigrinya posed several challenges for the team. Firstly, the pool of available translators was limited, which constrained the campaign's duration and reach. Secondly, on many advertising platforms, Tigrinya was not a supported language, making it harder to select the target audience.⁷⁴

The team and the cultural mediator had to navigate several trade-offs between the investigation and marketing perspectives. From a marketing perspective, the communication team wanted short, to-the-point messages to persuade the target audience. In contrast, the investigation team and the prosecutor emphasised the importance of legal correctness in phrasing.

So sometimes it's about the legal side, and in terms of communication, you generally want to stay at B1 level. And with these Eritrean target groups, that was also the goal. But sometimes you're stuck with certain terms you can't avoid – terms that an average Dutch person might not even understand.⁷⁵

Additionally, the situation in the country of origin posed another challenge. The team had to consider the presence of both supporters and opponents of the Eritrean regime within the target population. To avoid diplomatic sensitivities, the team chose to phrase the reason someone had fled as neutrally as possible.

For the webpage design and content, the team explored ways to move the target audience from the evaluation phase to the conversion phase, such as making contact with the investigation team or uploading photo or video evidence. The team applied two of Cialdini's principles of persuasion: social proof (people follow the lead of similar others) and authority (people defer to experts who provide shortcuts to decisions requiring specialised information).⁷⁶

For social proof, the team added a video testimonial to the webpage. In the video, an Eritrean witness, speaking in Tigrinya, recounts personal experiences from their flight to the EU.

That was a very important element, because from our experience, we see that real stories from victims and bereaved relatives can trigger people. The story of someone who has actually gone through it is often a crucial factor for others to come forward, to share what they know.⁷⁷

In addition, the video helped overcome fear and distrust of the RNLM and the police. The witness described their experiences interacting with the RNLM and outlined the process that would follow once contact was established.

For authority, the webpage and the video included an explainer on the RNLM, including background information, core tasks, and *modus operandi*. To boost credibility, a press release was issued alongside the campaign, allowing people to verify its legitimacy. An essential element in bolstering authority was the arrests made in previous investigations.

That worked in our favour, the arrests that had already taken place. With those, we could demonstrate that we were taking action. We had already apprehended two key figures. We were able to show this through the arrests and accompanying images.⁷⁸

By including the arrest footage, the team demonstrated that the RNLM was a credible and competent authority.

Ethical and legal considerations

During the campaign, the team faced several ethical dilemmas and legal considerations. The team had to carefully manage the expectations of people who reached out to provide information and might expect something in return, such as financial compensation or commitments toward an asylum application.

'During each interview, it is emphasised that we appreciate the individual providing a statement, but we cannot make any promises regarding their residence status. We cannot intervene in that matter, nor can we make any commitments'.⁷⁹

Another complication is the possibility that relatives or friends of the witness might still be in transit or even captivity, using the same route. Providing information and assisting an investigation into a migrant smuggler could later affect those relatives or friends by potentially closing a route.

Re-experiencing trauma was also an ethical dilemma for the team. When asking people to provide detailed statements about specific events, there is a risk that they may relive those events. People who reached out therefore had the option to reconsider whether to proceed and provide a witness statement after the first contact with the RNLM, thereby extending the evaluation phase.

We ask whether the person would like more time to think about it. In some cases, people make use of that opportunity. Others, however, immediately say: "Oh no, I don't need to think about it. I want to give my statement now". Those individuals would actually prefer that you had already been at their door yesterday with the interview set, rather than waiting until next week.⁸⁰

From a legal perspective, the campaign was designed in accordance with the *Aanwijzing opsporingsberichtgeving* 2017 (Directive on investigative public announcements 2017).⁸¹ The directive states that public announcements are an investigative tool. The Public Prosecution Service and the police can utilise investigative announcements to seek the public's assistance in gathering information to establish the truth, enforce judicial decisions, prevent criminal offences, or promote other interests related to the criminal enforcement of the rule of law. This campaign falls into the category of 'establishing the truth' by calling for witness or victim testimony.

Although social media advertisements can have a global reach, the campaign faced limitations. The team had to obtain permission from the Public Prosecutor's Office to run the advertisements outside the Netherlands. For reciprocity reasons, the team was allowed to run the advertisements only within the EU.⁸² Furthermore, for the investigation team to conduct the interviews, it was essential that the witnesses or victims lived within the EU.

Balancing openness and secrecy

An intriguing aspect of this campaign is that it blends the openness and high visibility of a social media outreach effort with the inherent confidentiality of an ongoing investigation. This means that at some point, the campaign must transition from open to confidential status to protect victims and witnesses and preserve the integrity of the investigation. After contact was made, the team had to decide whether the person would be regarded

as a regular witness (ready to give a statement, handled by the investigation team), a protected witness (ready to provide a statement but requiring additional protection, managed by the protected witnesses team), or an informant (not ready to give a statement but willing to provide information under the condition of anonymity, handled by the criminal intelligence team). To facilitate this, a front office was set up to process and screen all incoming calls, emails, and app messages. The front office was staffed by an interpreter and a member of the RNLM's intelligence department, who had experience of all three processes. The Front Office triaged all incoming information and assigned each person to the appropriate team while preserving confidentiality.

That worked out really well in the sense that we received regular updates saying how many people had approached us in terms of numbers, but without names or phone numbers. They only gave us the witnesses who actually did want to give a statement to us.⁸³

The front office served as the point where the campaign shifted from open to confidential (see Figure 2). It was a crucial element in maintaining secrecy and safeguarding the identities of sources.

The open nature of the social media campaign sometimes posed challenges in safeguarding potential witnesses and sources. The campaign received likes and reactions on the advertisements. All reactions had to be translated and verified, adding to the demands on limited translation resources. The team also encountered situations where people responded to the ads by openly posting '*I know more*', potentially risking their safety.⁸⁴

To verify the credibility of each potential witness or source, the team conducted a telephone intake interview. During the interview, a team member used a dedicated template to evaluate the coherence, details, and relevance of the information to the investigation's aim.

In terms of reliability, you quickly notice whether they really have something substantive to say, or whether they just want to extract information. And there were indeed some of those, but fortunately they were already filtered out in the preliminary stage.⁸⁵

Disinformation was also a consideration for the team. Not because they feared being supplied with disinformation; that was something to be processed and filtered out during intake. The team, however, acknowledged that the spread of disinformation could affect the target audience's willingness to contact the RNLM.⁸⁶ A final concern was the handling of witnesses under duress. The team recognised the possibility of being approached by persons under threat from criminal groups or state actors.

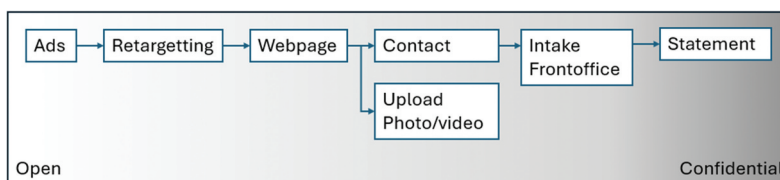


Figure 2. Campaign process. From open to confidential.

Adaptation

Although the campaign's duration was limited to three and a half weeks, there were opportunities to adapt to improve efficiency and effectiveness. Due to the short time-frame, no changes were made to the messaging strategy, including the advertisements and the webpage.⁸⁷ A minor adjustment was made to the allocation of the advertisement budgets for the retargeting strategy. After the campaign start, the team decided to allocate more funding to the first phase to broaden the initial outreach. This came at the expense of the retargeting budget in the second phase, but allowed the campaign to reach more unique viewers.⁸⁸ Another procedural adaptation concerned the interview protocol for female victims or witnesses who might have encountered sexual violence during their journey. The team recognised that, to lower the threshold for discussing these experiences and build trust, it was necessary to have a female investigator, a specialised vice investigator, and a female interpreter on call to conduct these interviews.⁸⁹

Lessons learned

During and after the campaign, the team identified several lessons learned. Running a digital outreach initiative in this context was a first for the RNLM, so many aspects had to be developed for the first time, particularly web care and follow-up. Advice and support from the police communications team were invaluable in managing advertising accounts, dedicated phone numbers, email addresses, and the overall scope of the campaign. Adding more languages or countries for advertising would require additional budget and translation resources. A larger target audience could also result in more front-office intakes and more interviews for the investigation team. The team therefore had to carefully balance its information needs with the available budget and resources.

Each country was so many euros extra. An extra language, or an extra site, an extra banner, an extra week. Everything comes down to money. Well, plus the wider you make the funnel, the more people you also have to put behind the phone.⁹⁰

An important lesson learned was the need for a dedicated repository for RNLM's operational photos and videos to support future outreach initiatives. During the campaign, it became clear that certain specific, hard-to-obtain footage could not be used, either because the rights holder would not grant permission or the footage could not be verified. For future campaigns, it is essential that the RNLM maintain a database of its own verified photos and videos.⁹¹

Ultimately, the team reflected on a successful campaign that produced a satisfactory number of witnesses. The campaign generated significant interest among partner organisations, both in the Netherlands and internationally.

And now we are at the tipping point. After conducting many interviews and hearing relevant witnesses from the media strategy, we are converting that into case files. So now we start building the evidence. That is happening right now. So, you generate information, and now we want to actually arrest those guys. Wherever they may be.⁹²

Discussion and conclusion

This article examines how intelligence and law enforcement organisations utilise digital strategies to reach groups that are typically hard to access through conventional means. Through the analysis of the Ukrainian HUR's 'I Want to Live' campaign and the Royal Netherlands RNLN's 'Call to Victims', this study identifies an emerging variant in outreach practice: the extension of contact-making from the 'shadows' of physical interaction to the 'screens' of digital platforms. This development does not signal the obsolescence of traditional human intelligence (HUMINT) or investigative methods, but rather represents an expansion of the operational toolkit.

The analysis highlights how operational context shapes the design and use of digital outreach strategies. The HUR campaign is ongoing and adaptive, operating against the high-intensity backdrop of the Russo-Ukrainian war. Its content shifts in response to battlefield developments through a metrics-driven feedback loop.⁹³ In contrast, the RNLN campaign was limited and time-bound, constrained by a specific investigative mandate and budget. Rather than producing comparable practices, these differing contexts illuminate how a shared operational problem, establishing initial contact with distrustful and physically inaccessible audiences, is addressed under divergent conditions.

The 'digital funnel': adapting marketing logic

Both cases demonstrate that effective outreach relies on adapting commercial marketing logic to security objectives. The HUR penetrated the Russian-language information environment via Telegram, while the RNLN targeted the Eritrean community through Meta (Facebook/Instagram). Crucially, both organisations employ a 'digital funnel' to manage the transition from public awareness to private contact.

This process begins in the open environment, where public messaging, using videos and advertisements, triggers initial attention. The 'I Want to Live' campaign illustrates how this early stage works in practice and at scale: by October 2025, the project had driven over 50 million visits to its website, 43 million of which originated from within the Russian Federation. Soldiers often encounter material through forwarded messages, channel recommendations, or incidental exposure, reflecting Telegram's architecture, which encourages circulation beyond the intended audience.

From this broad visibility, potential contacts move into a consideration phase, shifting from social media feeds to dedicated websites or guidance pages, such as the hochuzhit.com website of the 'I Want to Live' campaign or the RNLN campaign landing page. In the Ukrainian case, this aligns with a stage in which individuals assess whether surrender appears plausible, supported by FAQs, chatbots, and observable activity on the channel, all of which allow for risk-free information gathering.

The process culminates in a closed conversion stage, where interaction moves to messaging apps such as WhatsApp, Signal, IMO, or hotlines. Here, low-risk first contact, such as a question or a short message to a chatbot, marks the shift from tentative intent to active coordination. The data emphasise the necessity of this filtering process: from millions of initial impressions on the website, the HUR processed over 52,000 individual requests via chatbots and hotlines.⁹⁴ The RNLN case offers a specific insight into how this transition is managed: the 'front office'. This triage unit acts as a

human filter, verifying the relevance of the contact and protecting the source's identity. A comparable process operates on the Ukrainian side. Incoming contacts through chatbots and hotlines are screened using open-source analysis to establish the identity of the person making contact. Once verified, respondents are advised to remove the bot from their devices, and tailored individual communication channels are established to protect operational security.⁹⁵ This procedure mirrors the RNLM's front office triage in function, though it operates under wartime conditions and at considerably greater scale.

Viewed through this lens, the digital funnel performs a function that extends beyond audience targeting or message optimisation. Rather than primarily seeking to build interpersonal trust at the outset, both organisations aim to reduce the threshold of trust required to initiate contact. This is achieved by lowering perceived risk and uncertainty through procedural transparency, anonymity options, and staged escalation from public to private communication. Trust does not disappear from the process; instead, it is deferred. Interpersonal trust becomes relevant only after initial contact has been established, at a point where organisational safeguards and institutional procedures already structure the interaction.

The novelty of this process does not lie in the use of digital communication per se, intelligence and law enforcement agencies have maintained websites and social media accounts for years. What is distinctive is the deliberate sequencing: a staged pathway that converts broad public visibility into individualised, secure contact, structured around marketing logic. It is this designed progression from open to closed interaction, captured in the digital funnel concept, that represents a departure from both traditional broadcast appeals and conventional clandestine recruitment. The digital funnel occupies a space between these two modes: more targeted and interactive than a public appeal, yet more open and scalable than covert source cultivation.

Cultural intelligence

A key finding concerns the role of cultural competence. The HUR has an intrinsic advantage: a command of the Russian language, military culture, and Russian social context, allowing for the use of humour, slang, and cultural references (e.g., the '*28 Panfilov heroes*' reference to Soviet propaganda) to build credibility or foment dissent. This competence extends to the weaponisation of societal fissures; for example, the campaign actively exploits internal resentments between ordinary Russian conscripts and Chechen '*Kadyrovtsy*' units, framing the latter as privileged forces who loot or flee while conscripts are left to die.

This advantage is reinforced by Ukraine's prolonged exposure to the Russian information environment, which helped to shape the tone and the reach of its messaging. These conditions make it easier for the HUR to match content to audience expectations. The RNLM, lacking this access, had to construct competence through use of cultural mediators and translators. This difference underscores that digital tools are only as effective as the cultural nuance behind them; where the HUR could draw on deep contextual knowledge of and sustained operational experience with their Russian opponent, the RNLM had to construct this competence deliberately.

Ethical tensions: protection versus instrumentalisation

Ethical and legal regimes play a decisive role in shaping how digital outreach can be conducted and how far contact pathways can extend. In the RNLM case, outreach is embedded in a peacetime law-enforcement framework governed by strict legal directives prioritising the protection of victims and witnesses. Practitioner interviews highlighted the risk of '*secondary trauma*' (re-experiencing events) and the possibility that cooperation with authorities could endanger relatives still travelling along the same smuggling routes. Consequently, witnesses are hidden. Promises, such as guaranteed asylum, are also carefully avoided to manage expectations.

The HUR operates in a distinct ethical framework driven by the requirements of war. While the campaign frames its actions as compliant with International Humanitarian Law (IHL), it actively instrumentalises the target audience. The analysis shows that HUR publishes video testimonials of Russian POWs.⁹⁶ This raises ethical questions absent in the RNLM case: the potential pressure on prisoners to perform for the camera, the conflict with Article 13 of Geneva Convention III regarding protection from '*insults and public curiosity*', the risk that public exposure might endanger their eventual exchange, and the impact on their families in Russia.⁹⁷ Practitioners at the Coordination Headquarters state that all interviews with Russian prisoners of war are conducted on a voluntary basis and that prisoners typically approach the project themselves. Conversations are limited to personal experiences and avoid politically sensitive subjects. Staff note that the recordings also serve a protective function for the prisoners, allowing them to signal to family members in Russia that they are alive, given that Russian authorities routinely suppress information about captured personnel. These safeguards do not eliminate the ethical tension inherent in publishing testimonials from individuals in detention, but they indicate an awareness of the issue on the part of the operating organisation.⁹⁸

Digital risks

Finally, both cases illustrate the paradox of digital recruitment. The device that enables contact, the smartphone, is also a liability. For an Eritrean migrant or a Russian soldier, engaging with these campaigns leaves a digital trace that can be weaponised by their oppressors (smugglers or commanders). For instance, there have been documented cases of spoofed Telegram bots and websites, created by Russian intelligence services, which redirected inquiries from would-be defectors into state-controlled channels, compromising users' safety.⁹⁹ These incidents expose the fragility of the communicative infrastructure both campaigns depend on.

Conclusion

Digital outreach offers a growing number of intelligence and law enforcement organisations expanded reach, but it also demands organisational, group, and individual competencies that extend well beyond digital distribution. Success depends on the ability to design staged pathways that lower the threshold of trust required for initial engagement while managing the transition from public visibility to operational confidentiality. As demonstrated by the practitioner interviews in the Netherlands and the campaign data

from Ukraine, digital platforms function primarily as conduits. The decisive work occurs in the organisational structures and procedures that govern what happens once a potential source makes contact. The recruitment or investigative encounter, even when digitally mediated, remains a deeply human endeavour.

Taken together, the two cases point to a common operational logic despite their divergent contexts. Both organisations faced the same core problem: reaching a distrustful population that would not voluntarily approach adversary or state authorities. Both converged on a staged digital pathway to address it, and both produced measurable operational results. The HUR processed over 52,000 individual inquiries through its various contact channels, while the RNLM generated a sufficient number of witness statements to proceed with building criminal case files.¹⁰⁰ Yet the comparison also reveals that the conditions enabling this convergence are specific. The HUR could draw on native cultural and linguistic proximity to its target audience; the RNLM had to construct this competence externally. The HUR operated under wartime latitude that permitted instrumentalising approaches, including the publication of POW testimonials; the RNLM was bound by prosecutorial oversight and witness protection obligations that constrained both the reach and duration of its campaign. These differences suggest that the digital funnel functions as a design pattern whose implementation depends on the cultural, legal, and institutional resources available to the organisation in question. This point is underscored by Russian attempts to replicate the Coordination Headquarters' projects. According to Ukrainian practitioners, Russian imitations lack genuine institutional backing and function primarily as propaganda facades rather than operational intake systems. The contrast suggests that the digital funnel's effectiveness depends not on its visible digital surface but on the organisational infrastructure and procedural credibility behind it.¹⁰¹

These findings should not be generalised without qualification. Both campaigns were conducted by organisations with specific mandates, resources, and institutional cultures. Whether similar strategies could be adopted by other intelligence or law enforcement bodies depends on several conditions: the availability of cultural expertise, access to platforms used by the target audience, sufficient organisational capacity to process incoming contacts, and a legal framework that permits public solicitation. Not all organisations will meet these conditions, and the two cases studied here represent relatively advanced examples of digital outreach practice. Practitioners involved in the RNLM campaign assessed the initiative positively, noting that it produced favourable results compared to previous investigative approaches and generated interest among partner organisations in the Netherlands and beyond.¹⁰² A recipient or defector perspective remains unavailable for the HUR case, as no surrendered soldiers were interviewed for this study. However, the practitioner roundtable at the Coordination Headquarters offered operational insight into the project's results, intake procedures, and ethical safeguards, partially addressing the asymmetry between the two cases.

Future research could extend this analysis in several directions. Understanding how target audiences experience and evaluate digital outreach efforts remains a priority, as the present study captures only the organisational and content dimensions. Comparative research across a wider range of cases, including campaigns by other national intelligence services or international law enforcement bodies, would test the generalisability of the digital funnel model. The ethical dimensions of digitally mediated recruitment in conflict settings, where the line between voluntary engagement and coercion is blurred, warrant

sustained scholarly attention. Finally, longitudinal analysis of campaign effectiveness, tracking conversion rates from initial exposure through to operational outcomes, remains an open methodological challenge.

Disclosure statement

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

Notes on contributors

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 Royal Netherlands Army and has been deployed to the Balkans and Afghanistan.

Bart Wielders, M.A., is a researcher at the Faculty of Military Sciences of the Netherlands Defence Academy, Breda, the Netherlands. He works for the Royal Netherlands Marechaussee and has experience as a law enforcement and intelligence practitioner.

ORCID

Peter Schrijver  <http://orcid.org/0009-0004-6526-0150>

Bart Wielders  <http://orcid.org/0009-0009-6867-3539>

Notes

1. Cotter, "Police Intelligence: Connecting-the-Dots," 173.
2. Cornelissens and Ferwerda, *Burgerparticipatie in Opsporing*, 37. https://www.bureaubeke.nl/doc/pkenpw/bw.politiekunde30_Burgerparticipatie.pdf.
3. Zeitsoff, "How Social Media Is Changing Conflict," 1970.
4. Walsh, "Social Media and Border Security," 1138.
5. Buluc et al., "When Spies Go Public! Lessons Learnt," 1–16; Jeanis et al., "Law Enforcement and Social Media Usage," 570–83; and Lowenthal, *Intelligence: From Secrets to Policy*, 125.
6. While the agency's official English website uses the legacy abbreviation GUR, this text employs HUR to reflect the Ukrainian transliteration of Holovne Upravlinnya Rozvidky. This aligns with the style guides of The Kyiv Independent and Kyiv Post, which prioritise modern phonetic standards, transliterating the Ukrainian "Г" as "H" rather than "G," a convention the authors follow for linguistic consistency.
7. The Royal Netherlands Marechaussee (Koninklijke Marechaussee) is a gendarmerie-type organisation within the Dutch armed forces. Its core duties include border control, security, surveillance and close protection; international police tasks; and military policing. The RNLN conducts criminal investigations related to its mandate, including transnational organised crime.
8. Schrijver, "Ukrainian Intelligence's Use of Telegram."
9. Ministerie van Justitie en Veiligheid, "Call to Victims of Human Trafficking from the Horn of Africa – News Item – Royal Netherlands Marechaussee," nieuwsbericht, Ministerie van Defensie, October 7, 2024, 216, <https://doi.org/10/07/call-to-victims-of-human-trafficking-from-the-horn-of-africa>.
10. Jesper Strömbäck, "Four Phases of Mediatization: An Analysis," 240.
11. Jeanis et al., "Law Enforcement and Social Media Usage."
12. Data retrieved using the social media analytics tool Popsters (<https://popsters.com>), which collects engagement metrics (views, likes, shares, comments) from public-facing posts

- across platforms, including Telegram. The sample of 192 Telegram messages from the “I Want to Live” campaign was collected and analysed via Popsters in mid-February 2025.
13. Roundtable session with five representatives of the Coordination Headquarters for the Treatment of Prisoners of War (*Koordshtab*), Kyiv, March 30, 2026. Participants consented to the use of this material for research and publication on condition of anonymity. Notes held by the authors.
 14. Braun and Clarke, *Thematic Analysis: A Practical Guide*, 55.
 15. *Ibid.*, 146.
 16. *Ibid.*, 141.
 17. 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 (April 11, 2024): 21, <https://doi.org/10.37458/nstf.25.1.2>.
 18. “I Want to Live: How to Surrender in Ukraine? Single Center for Accepting Appeals on Surrender,” accessed 23 April 2025, <https://hochuzhit.com/>.
 19. Roundtable session, *Koordshtab*, March 30, 2026.
 20. “Проект «Хочу Жить»,” Telegram, accessed 10 June 2025, https://t.me/hochu_zhyt/1825.
 21. Per-Erik Nilsson and Kristina Hellström, *All Eyes on Ukraine: Strategic Communication in the Russo-Ukrainian War, 2023–2024*, text (FOI, 2025), 82, <https://www.foi.se/en/foi/reports/report-summary.html?reportNo=FOI-R-5758-SE>.
 22. “Telegram Has Become a Key Tool for the Russian Military.” *Meduza*, Accessed June 19, 2025, <https://meduza.io/en/feature/2024/08/28/telegram-has-become-a-key-tool-for-the-russian-military-why-does-moscow-continue-to-rely-on-a-dubai-based-civilian-messaging-app>.
 23. “I Want to Live: How to Surrender in Ukraine?” <https://hochuzhit.com/>.
 24. *Ibid.*
 25. Telegram, “Проект «Хочу Жить»,” *Telegram post*, 29 October 2024. Accessed April 9, 2025. https://t.me/hochu_zhyt/2028
 26. *Ibid.*
 27. Telegram, “Проект «Хочу Жить»,” *Telegram post*, 20 August 2024, Accessed April 9, 2025. https://t.me/hochu_zhyt/1825
 28. See note 17 above
 29. Roundtable session, *Koordshtab*, March 30, 2026.
 30. Data retrieved using the social media analytics tool Popsters (<https://popsters.com>), which collects engagement metrics (views, likes, shares, comments) from public-facing posts across platforms, including Telegram. The sample of 192 Telegram messages from the “I Want to Live” campaign was collected and analysed via Popsters in mid-February 2025.
 31. “Telegram: View @hochu_zhyt,” Accessed 24 June 2025. https://t.me/hochu_zhyt/1794.
 32. Matthew Krain, “J’accuse! Does Naming and Shaming Perpetrators,” 574; Hirschberger, *External Communication in Social Media*, 25. <https://doi.org/10.14361/9783839455098>.
 33. Telegram, “Проект «Хочу Жить»,” *Telegram post*, 10 October 2024, Accessed April 8, 2025. https://t.me/hochu_zhyt/1984
 34. Telegram, “Проект «Хочу Жить»,” *Telegram post*, 8 August 2024, Accessed April 8, 2025. https://t.me/hochu_zhyt/1775
 35. Telegram, “Проект «Хочу Жить»,” *Telegram post*, 24 September 2024, Accessed April 9, 2025. https://t.me/hochu_zhyt/1951
 36. Telegram, “Проект «Хочу Жить»,” *Telegram post*, 30 August 2024, Accessed April 8, 2025. https://t.me/hochu_zhyt/1864
 37. *Ibid.*
 38. Telegram, “Проект «Хочу Жить»,” *Telegram post*, 8 August 2024, Accessed April 8, 2025. https://t.me/hochu_zhyt/1776
 39. *Ibid.*
 40. Telegram, “Проект «Хочу Жить»,” *Telegram post*, 8 August 2024, Accessed April 8, 2025. https://t.me/hochu_zhyt/1777
 41. The legend of the “28 Panfilov heroes” refers to a Soviet wartime myth according to which 28 soldiers of General Ivan Panfilov’s division heroically held off a large

German tank force near Dubosekovo in November 1941, reportedly sacrificing their lives to defend Moscow. The story, widely circulated through Soviet media and education, was institutionalised as a symbol of selfless heroism. However, a 1948 investigation by the Soviet military prosecutor's office found that the account was largely fabricated. Despite this, the narrative remains part of Russia's official historical memory and continues to be referenced as a "*sacred legend*"; Dietmar Neutatz, "Der erfundene Heldentod: Die Legende von den 28 Panfilov-Männern," in *Erinnerungsorte des Zweiten Weltkriegs in der russischen und deutschen Erinnerungskultur*, ed. Guido Hausmann and Mischa Gabowitsch (Würzburg: Ergon-Verlag, 2019), 189–208.

42. Telegram, "Проект «Хочу Жить»," *Telegram post*, 16 August 2024, Accessed April 8, 2025. https://t.me/hochu_zhyt/1807
43. Telegram, "Проект «Хочу Жить»," *Telegram post*, 23 August 2024, Accessed April 9, 2025. https://t.me/hochu_zhyt/1835
44. Telegram, "Проект «Хочу Жить»," *Telegram post*, 5 November 2024, Accessed April 9, 2025. https://t.me/hochu_zhyt/2047
45. Kraken and Artan are special forces units affiliated with the Ukrainian military intelligence service, HUR.
46. Telegram, "Проект «Хочу Жить»," *Telegram post*, 29 October 2024, Accessed April 9, 2025. https://t.me/hochu_zhyt/2028
47. Ibid.
48. Grauer, "Why Do Soldiers Give Up?" 653.
49. "I Want to Find. Unified Center for Searching for Servicemen of the Russian Army in Ukraine," <https://hochunaiti.com/> (accessed April 22, 2025).
50. Telegram, "Проект «Хочу Жить»," *Telegram post*, 1 November 2024, Accessed April 9, 2025. https://t.me/hochu_zhyt/2040
51. Telegram, "Проект «Хочу Жить»," *Telegram post*, 8 October 2024, Accessed April 9, 2025. https://t.me/hochu_zhyt/1977
52. Telegram, "Проект «Хочу Жить»," *Telegram post*, 22 September 2024, Accessed April 9, 2025. https://t.me/hochu_zhyt/1945
53. Ibid.
54. Telegram, "Проект «Хочу Жить»," *Telegram post*, 13 September 2024, Accessed April 9, 2025. https://t.me/hochu_zhyt/1903
55. Member of the Buryat people, an indigenous ethnic group native to Siberia, primarily residing in the Republic of Buryatia in the Russian Federation, near Lake Baikal.
56. Telegram, "Проект «Хочу Жить»," *Telegram post*, 13 September 2024, Accessed April 9, 2025. https://t.me/hochu_zhyt/1903
57. Telegram, "Проект «Хочу Жить»," *Telegram post*, 15 August 2024, https://t.me/hochu_zhyt/1799 (accessed 7 May 2025); Telegram, "Проект «Хочу Жить»," *Telegram post*, 30 August 2024, https://t.me/hochu_zhyt/1866 (accessed 7 May 2025); Telegram, "Проект «Хочу Жить»," *Telegram post*, 12 September 2024, https://t.me/hochu_zhyt/1899 (accessed 7 May 2025).
58. Telegram, "Проект «Хочу Жить»," *Telegram post*, 23 October 2024. Accessed April 9, 2025. https://t.me/hochu_zhyt/2017.
59. Roundtable session, *Koordshtab*, March 30, 2026.
60. Telegram, "Проект «Хочу Жить»," *Telegram post*, 20 August 2024, Accessed April 9, 2025. https://t.me/hochu_zhyt/1825
61. Telegram, "Проект «Хочу Жить»," *Telegram post*, 18 August 2024, Accessed April 9, 2025. https://t.me/hochu_zhyt/1820
62. See note 8 above.
63. NOS, "OM: Eritrese Bende Mishandelde Migranten, Perste Nederlandse Familieleden Af," NOS, October 1, 2023, <https://nos.nl/artikel/2459405-om-eritrese-bende-mishandelde-migranten-perste-nederlandse-familieleden-af>.
64. DR002, "Interview 2."

65. RNLM, "Call to Victims of Human Trafficking from the Horn of Africa," July 10, 2024, <https://english.marechaussee.nl/latest/news/2024/10/07/call-to-victims-of-human-trafficking-from-the-horn-of-africa>.
66. NP, *Rapportage Campagne KMar En OM*, 1–19.
67. DR001, "Interview 1."
68. DR003, "Interview 3."
69. DR004 and DR005, "Interview 4"; and David Court et al., "The Consumer Decision Journey," *McKinsey.Com*, <https://www.mckinsey.com/capabilities/growth-marketing-and-sales/our-insights/the-consumer-decision-journey>.
70. DR004 and DR005, "Interview 4."
71. Cialdini, "The Science of Persuasion," 76–81.
72. DR002, "Interview 2."
73. DR001, "Interview 1"; and DR002, "Interview 2."
74. DR004, DR005, "Interview 4."
75. Ibid.
76. Cialdini, "The Science of Persuasion."
77. DR004, DR005, "Interview 4."
78. Ibid.
79. DR003, "Interview 3."
80. Ibid.
81. Aanwijzing opsporingsberichtgeving, BWBR0040219, Veiligheid en Justitie (2017), <https://wetten.overheid.nl/BWBR0040219/2017-12-01/0/informatie>.
82. DR004, DR005, "Interview 4."
83. DR002, "Interview 2."
84. DR004, DR005, "Interview 4."
85. DR002, "Interview 2."
86. Ibid.
87. DR001, "Interview 1"; DR004, DR005, "Interview 4."
88. DR004, DR005, "Interview 4."
89. DR003, "Interview 3."
90. DR002, "Interview 2."
91. DR004, DR005, "Interview 4."
92. DR002, "Interview 2."
93. Peter Schrijver, "I Want to Live': Psychological Warfare," *Irregular Warfare Initiative*, November 4, 2024, <https://irregularwarfare.org/articles/i-want-to-live-psychological-warfare-for-the-modern-era/>.
94. Roundtable session, *Koordshtab*, March 30, 2026.
95. Ibid.
96. "Shielding Prisoners of War from Public Curiosity," *Humanitarian Law & Policy Blog*, June 28, 2022, <https://blogs.icrc.org/law-and-policy/2022/06/28/shielding-prisoners-of-war-from-public-curiosity/>.
97. "Украинский проект «Хочу жить», который помогает военным из РФ сдаться, провел среди военнопленных социологическое исследование. Результаты очень интересные. Но методология вызывает серьезные сомнения" [*The Ukrainian "I Want to Live" Project, Which Helps Russian Soldiers Surrender, Conducted a Sociological Survey Among POWs. The Results Are Interesting, But the Methodology Raises Serious Doubts*], *Meduza*, Accessed 7 May 2025, <https://meduza.io/feature/2023/07/06/ukrainskiy-proekt-hochu-zhit-kotoryy-pomogaet-rossiyskim-voennym-sdavatsya-v-plen-opublikoval-opros-voennoplennyh>.
98. Roundtable session, *Koordshtab*, March 30, 2026.
99. Проект «Хочу жить» [@hochuzhit_com], "Будьте внимательны!" Tweet, *Twitter*, October 1, 2024, https://x.com/hochuzhit_com/status/1846134016715395348.
100. DR002, "Interview 2"; NP, *Rapportage Campagne KMar En OM. Getuigenoproep Slachtoffers Mensenmokkel Gericht Op Eritrese Vluchtelingen* (2024), p. 19.
101. Roundtable session, *Koordshtab*, March 30, 2026.

102. DR002, "Interview 2."

Bibliography

- Aanwijzing opsporingsberichtgeving*. BWBR0040219. Veiligheid en Justitie. December 1, 2017. <https://wetten.overheid.nl/BWBR0040219/2017-12-01/0/informatie>.
- Braun, V., and V. Clarke. *Thematic Analysis: A Practical Guide*. London: SAGE, 2022.
- Buluc, R., R. Arcos, and C. Ivan. "When Spies Go Public! Lessons Learnt from the Instrumentalization of Intelligence for Strategic Communication in the Run-Up to the Russian-Ukrainian War." *Intelligence and National Security* 40, no. 1 (2025): 42–57. doi:10.1080/02684527.2024.2405255.
- Cialdini, R. B. "The Science of Persuasion." *Scientific American* 284, no. 2 (2001): 76–81. doi:10.1038/scientificamerican0201-76.
- Cornelissens, A., and H. Ferwerda. *Burgerparticipatie in Opsporing*. Amsterdam: Reed Business, 2010. https://www.bureaubeke.nl/doc/pkenpw/bw.politiekunde30_Burgerparticipatie.pdf.
- Cotter, R. S. "Police Intelligence: Connecting-the-Dots in a Network Society." *Policing & Society* 27, no. 2 (2017): 173–187. doi:10.1080/10439463.2015.1040794.
- Court, D., D. Elzinga, S. Mulder, and O. Jørgen Vetvik. "The Consumer Decision Journey." *McKinsey & Company*. 2009. <https://www.mckinsey.com/capabilities/growth-marketing-and-sales/our-insights/the-consumer-decision-journey>.
- Grauer, R. "Why Do Soldiers Give Up? A Self-Preservation Theory of Surrender." *Security Studies* 23, no. 3 (2014): 622–655. doi:10.1080/09636412.2014.935238.
- Hirschberger, B. *External Communication in Social Media During Asymmetric Conflicts: A Theoretical Model and Empirical Case Study of the Conflict in Israel and Palestine*. Edition Politik 108 ed. Bielefeld: transcript Verlag, 2021. 10.14361/9783839455098.
- I Want to Find. Unified Center for Searching for Servicemen of the Russian Army in Ukraine." Accessed April 22, 2025. <https://hochunaiti.com/>.
- I Want to Live: How to Surrender in Ukraine? Single Center for Accepting Appeals on Surrender." Accessed April 23, 2025. <https://hochuzhit.com/>.
- Jeanis, M. N., C. N. Muniz, and C. L. Molbert. "Law Enforcement and Social Media Usage: An Analysis of Engagement." *Policing: A Journal of Policy and Practice* 15, no. 1 (2021): 570–583. doi:10.1093/police/paz026.
- Krain, M. "J'Accuse! Does Naming and Shaming Perpetrators Reduce the Severity of Genocides or Politicides?" *International Studies Quarterly* 56, no. 3 (2012): 574–589. doi:10.1111/j.1468-2478.2012.00732.x.
- Lowenthal, M. M. *Intelligence: From Secrets to Policy*. 8th ed. Washington, DC: CQ Press, 2022.
- Meduza. "Telegram Has Become a Key Tool for the Russian Military. Why Does Moscow Continue to Rely on a Dubai-Based Civilian Messaging App?" *Meduza*, August 28, 2024. <https://meduza.io/en/feature/2024/08/28/telegram-has-become-a-key-tool-for-the-russian-military-why-does-moscow-continue-to-rely-on-a-dubai-based-civilian-messaging-app>.
- Meduza. ""Украинский проект «Хочу жить» ... провел среди военнопленных социологическое исследование" [The Ukrainian 'I Want to Live' Project ... Conducted a Sociological Survey among POWs]." *Meduza*, July 6, 2023. <https://meduza.io/feature/2023/07/06/ukrainskiy-proekt-hochu-zhit-kotoryy-pomogaet-rossiyskim-voennym-sdavatsya-v-plen-opublikoval-opros-voennoplennyh>.
- Neutatz, D. "Der Erfundene Heldentod: Die Legende Von Den 28 Panfilov-Männern." In *Erinnerungsorte des Zweiten Weltkriegs in der Russischen und Deutschen Erinnerungskultur*, edited by G. Hausmann and M. Gabowitsch, 189–208. Würzburg: Ergon-Verlag, 2019.
- Nilsson, P.-E., and I. Ekman. "'Be Brave Like Ukraine': Strategic Communication and the Mediatization of War." *National Security and the Future* 25, no. 1 (2024): 21–64. doi:10.37458/nstf.25.1.2.
- Nilsson, P.-E., and K. Hellström. "All Eyes on Ukraine: Strategic Communication in the Russo-Ukrainian War, 2023–2024." 2025. <https://www.foi.se/en/foi/reports/report-summary.html?reportNo=FOI-R-5758-SE>. Stockholm: FOI.
- NP [Nederlandse Politie]. *Rapportage Campagne KMar en OM: Getuigenoproep Slachtoffers Mensensmokkel Gericht op Eritrese Vluchtelingen*. 2024.

- Schrijver, P. "'I Want to Live': Psychological Warfare for the Modern Era." *Irregular Warfare Initiative*, November 4, 2024. <https://irregularwarfare.org/articles/i-want-to-live-psychological-warfare-for-the-modern-era/>.
- Schrijver, P. "Ukrainian Intelligence's Use of Telegram in Wartime." *International Journal of Intelligence & CounterIntelligence* (2025). doi:10.1080/08850607.2025.2522222.
- Shielding Prisoners of War from Public Curiosity." Humanitarian Law & Policy Blog. International Committee of the Red Cross. June 28, 2022. <https://blogs.icrc.org/law-and-policy/2022/06/28/shielding-prisoners-of-war-from-public-curiosity/>.
- Strömbäck, J. "Four Phases of Mediatization: An Analysis of the Mediatization of Politics." *International Journal of Press/Politics* 13, no. 3 (2008): 228–246. doi:10.1177/1940161208319097.
- van Justitie En Veiligheid, M. "Call to Victims of Human Trafficking from the Horn of Africa." *Royal Netherlands Marechaussee*, October 7, 2024. <https://english.marechaussee.nl/latest/news/2024/10/07/call-to-victims-of-human-trafficking-from-the-horn-of-africa>.
- Walsh, J. P. "Social Media and Border Security: Twitter Use by Migration Policing Agencies." *Policing & Society* 30, no. 10 (2020): 1138–1156. doi:10.1080/10439463.2019.1666846.
- Zeitzoff, T. "How Social Media Is Changing Conflict." *The Journal of Conflict Resolution* 61, no. 9 (2017): 1970–1991. doi:10.1177/0022002717721392.
- Проект «Хочу жить» [@hochuzhit_com]. "Будьте внимательны! [Be Careful!]." Twitter/X, October 15, 2024. https://x.com/hochuzhit_com/status/1846134016715395348.
- Проект «Хочу Жить» [I Want to Live Project]. "Telegram Channel Posts." T.Me/Hochu_Zhyt. August 6 November 6, 2024.