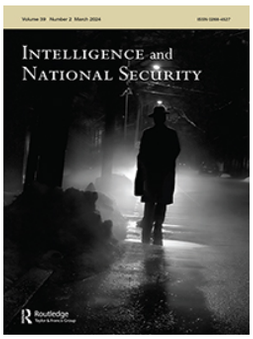

Routledge
Taylor & Francis Group

Intelligence and National Security

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/fint20

Beyond counterintelligence: understanding the SBU's social media outreach on Telegram during wartime

Peter Schrijver

To cite this article: Peter Schrijver (28 Feb 2024): Beyond counterintelligence: understanding the SBU's social media outreach on Telegram during wartime, Intelligence and National Security, DOI: 10.1080/02684527.2024.2321692

To link to this article: https://doi.org/10.1080/02684527.2024.2321692

Published online: 28 Feb 2024.

INTELLIGENCE AND NATIONAL SECURITY
https://doi.org/10.1080/02684527.2024.2321692

Routledge
Taylor & Francis Group

ARTICLE

Beyond counterintelligence: understanding the SBU's social media outreach on Telegram during wartime

Peter Schrijver

ABSTRACT

This study examines the Security Service of Ukraine's (SBU) use of its Telegram channel for social media outreach during the Russo-Ukrainian war. It employs a qualitative thematic analysis of Telegram posts published between February 2022 and October 2023 to investigate the SBU's communication strategies. The study identifies the SBU's focus on themes such as collaboration and treason, showcasing its operational successes, and countering Russian espionage in its social media messaging. The findings provide insights into the SBU's approach to engaging the Ukrainian public, in contrast with traditional concepts of intelligence communication, and emphasise its role in influencing public discourse.

ARTICLE HISTORY
Received 29 January 2024
Accepted 18 February 2024

KEYWORDS
Intelligence; social media; Russo-Ukrainian war; influence; communication

1. Introduction

On 24 February 2022, as Russia launched its full-scale invasion of Ukraine, the Security Service of Ukraine, known by its acronym SBU (Служба безпеки України, Latinised as Sluzhba Bezpeki Ukraini), posted a defiant message on its Ukrainian-language Telegram channel: '*Dear citizens of Ukraine! Since the morning of today, Russian troops have been attacking peaceful Ukrainian cities from various directions, including from the side of the temporarily occupied Donbas and Crimea, as well as the northeastern region. Martial law has been introduced in Ukraine. This is a necessary step for the sake of the security of the state and our victory. All state authorities, the entire force unit, SBU employees, special agents of the Special Operations Centre 'A' together with the Armed Forces of Ukraine and colleagues from the State Border Service are working to the maximum for the most effective protection of our country and your safety. Together we will win! Glory to Ukraine!*"[1]

While the message was undoubtedly poignant, the SBU's direct address to Ukrainian citizens through a social media channel was not unprecedented. The SBU is Ukraine's primary security agency, responsible for counterintelligence, combating terrorism and organised crime, and safeguarding state secrets. It first established a social media presence in 2014, communicating with external audiences through accounts on YouTube, Twitter, and Facebook. The SBU further expanded its social media reach in 2019 by creating Instagram and Telegram accounts, and in 2023 it added a channel on the messaging app Viber to its inventory (see Figure 1).

From the outset, the SBU leveraged social media platforms to disseminate notable content. A prominent example was its disclosure of intercepted communications on YouTube in 2014. These intercepts suggested Russian involvement in the downing of MH-17 over the eastern Donbas region in July 2014. The SBU released this sensitive intelligence on the very day the plane was shot down.[2] The international investigative collective Bellingcat acknowledged the significance of these intercepts in identifying the transport of a Russian Buk missile launcher, which was used to bring down the Malaysian Airlines flight.[3] While exercising caution in drawing initial conclusions, the international Joint Investigation Team (JIT) eventually endorsed the validity of the intercepts publicly

CONTACT Peter Schrijver p.schrijver@mindef.nl; peterschrijver01@gmail.com

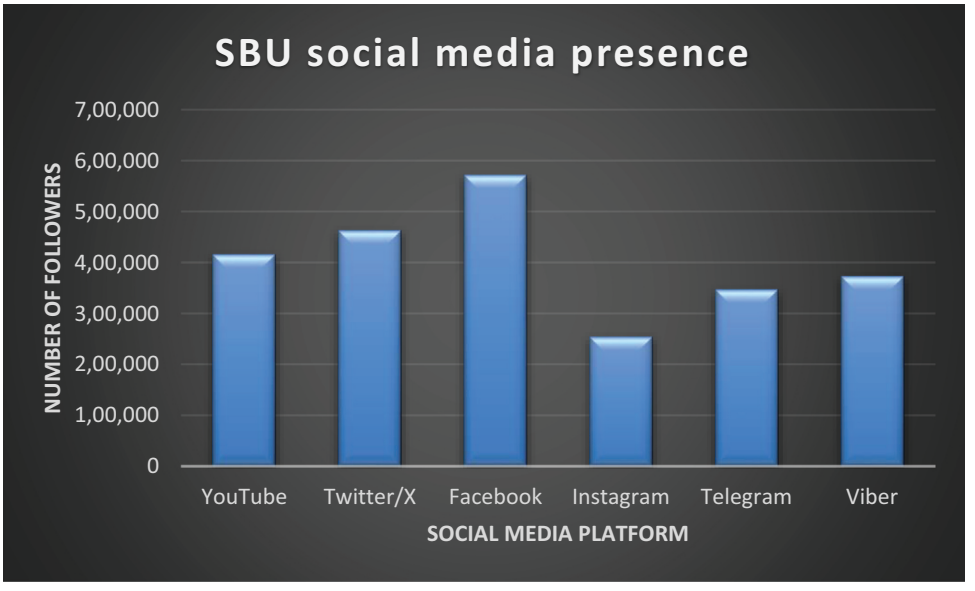

Figure 1. Number of followers per SBU social media account, December 2023.

released by the SBU: '*Immediately on 17 July 2014, it became apparent that the SBU - a security service in Ukraine that is responsible for intelligence and investigation - had access to relevant tapped telephone conversations. Taped conversations were made public that same evening*.'[4]

The release of incriminating evidence of Russian involvement in the downing of flight MH17 occurred in a year when the SBU's reputation was at an all-time low due to accusations of corruption, incompetence, and Russian infiltration.[5] The SBU's standing had improved slightly after the Maidan Revolution of February 2014, which had led to the ousting of pro-Russian president Viktor Yanukovych. The new government replaced the SBU leadership and initiated reforms.[6] However, the service still faced many challenges and criticisms following the annexation of Crimea by Russia and the outbreak of war in the Donbas region later that year.[7] Amidst this turmoil and criticism, the SBU made a counterintuitive decision to establish dedicated social media channels. The Russian large-scale invasion in February 2022 did not temper the SBU's social media presence, as the service continued to publish a daily stream of content with news on its operations.[8]

Intelligence services have significantly invested in using social media platforms for information collection and sentiment analysis. This has been labelled as social media intelligence (SOCMINT).[9] While SOCMINT has received academic attention, research focusing on the specific use of social media as a means of communication with the public, particularly during wartime, remains limited. This research focuses on the question of what sort of content the SBU has posted since the start of the Russian large-scale invasion (time frame of 24 February 2022 to 26 October 2023). It examines how the service uses its Telegram channel to inform and mobilise its audience, as well as to counter the propaganda and disinformation spread by the Russian forces. To achieve this, all posts made on the SBU's Ukrainian-language Telegram account within the specified time frame were analysed to identify recurring themes in the messaging. Telegram is a popular application in Ukraine and is used by the Ukrainian president, media outlets, journalists, citizens, and the military to communicate and share information about the war with Russia. The content released by the SBU on its Telegram channel is cross-posted to other SBU social media accounts across platforms such as Facebook, X (formerly Twitter), Instagram, YouTube, and the messaging app Viber.

The article is structured as follows. The next section examines the current state of knowledge regarding the use of social media by intelligence services. The outcomes of a qualitative thematic

analysis are then presented to gain an understanding of the recurring themes in the SBU's social media messaging on Telegram. This analysis is followed by an assessment that aims to determine the level of congruence between the SBU's social media strategy and concepts of intelligence communication, as outlined by scholar Petersen.[10] The objective of this analysis is to determine the SBU's strategy in effectively communicating with external audiences.

2. Intelligence and social media

Intelligence organisations use social media for a variety of reasons, depending on their goals and strategies. One main reason is to collect open-source intelligence (OSINT) from social media platforms like Facebook, Twitter, YouTube, and blogs, which is a passive form of social media engagement. This specific area of research has given rise to a distinct subdiscipline known as social media intelligence (SOCMINT), which is related to open-source intelligence (OSINT).[11] SOCMINT is an important tool for the police and security and intelligence services when they are seeking to map relationships between persons, personas and networks, and determine how they influence or are influenced. Furthermore, such intelligence provides insight into location, movement, financing and intentions of their suspects and opponents.

A second reason for intelligence services to use social media is to influence public opinion and the perception of outside audiences. As Lowenthal states, intelligence organisations may engage in covert actions, such as influence operations, to manipulate the beliefs of specific target audiences by spreading propaganda or disinformation.[12] Extensive research has documented the principles of Russian information confrontation, which involves the participation of Russian intelligence organisations such as he FSB, SVR, and GRU. These services have been repeatedly accused of employing social media bots and trolls to disseminate false or divisive information to interfere with elections and political processes in other countries.[13] To avoid detection, attribution, or maintain plausible deniability, these services and associated organisations typically carry out their operations under the guise of Advanced Persistent Threat (APT) actors.[14] Likewise, Western intelligence and security agencies have been known to conduct covert actions on social media platforms, operating under pseudonymous accounts to counter jihadist propaganda.[15]

However, these covert operations are in contrast with the overt nature of the SBU's social media-based communication practices, which are the subject of this research. While it is not within the scope of this study, it is worth noting that the SBU or other Ukrainian intelligence services may also engage in covert (cyber-enabled) influence operations.

A third objective of an intelligence service's use of social media could be to actively engage with stakeholders and enhance transparency and accountability. This can be done through identifiable accounts used by a service to communicate its accomplishments and challenges to the public and other relevant parties, debunk disinformation, and reach out to potential employees.[16] Engagement can help to build trust and reputation among audiences and to address concerns or criticisms they may have. McLoughlin et al. researched the social media engagement of the UK's Government Communications Headquarters (GCHQ) on Twitter. They concluded that it allowed the agency to reach out to a '*young tech-savvy generation of potential recruits*', while also pointing out that this engagement had its limitations, damaging GCHQ's brand identity due to prevailing conspiracy theories on the service.[17] A study on social media engagement by intelligence agencies within the European Union (EU) revealed a wide spectrum of online presence, from '*extremely active*' to completely absent.[18] However, the research did not specify the reasons behind each agency's unique approach to social media communication. A 2015 investigation into social media engagement by U.S. intelligence agencies found that interactivity with audiences was minimal and much of the content was replicated from other government agencies and lacked substantive information.[19]

Despite previous research activities, the overt social media engagement by intelligence services in wartime has received little academic attention. Hence, the Security Service of Ukraine (SBU) is an interesting case, as it has built up experience with this type of engagement since 2014, when the

service launched several social media channels amid a developing war with the Russian Federation. Since the large-scale Russian invasion in 2022, the SBU has appointed a designated spokesperson to share information with the public and issue warnings about security threats. In its dissemination of content, the service goes beyond the posting of trivial information or historical facts. The SBU has openly communicated about its counterintelligence and counter-corruption missions, including the apprehension of its own personnel accused of power abuse. According to SBU-researcher Kaul, the level of communication and openness, including admitting its own faults, marks a significant shift in post-Soviet security behaviour.[20]

3. Exposing of collaboration and celebrating success: SBU's social media engagement on Telegram

With regard to the ongoing large-scale Russian invasion of Ukraine, analysts have noted in general terms that the use of telecommunications infrastructure by the Ukrainian government, specifically through the successful incorporation of smartphones, social media and messaging apps, provided the Ukrainians with a significant advantage in terms of information over the Russian invaders.[21] Nevertheless, the role of Ukrainian intelligence services' use of social media has received little attention.

3.1. Method

To understand the recurring themes the SBU addresses on its Telegram channel (t.me/SBUkr), a qualitative thematic analysis was conducted. Telegram combines aspects of messaging and social media platforms, providing features for individual or group chats, either privately or publicly. The application also enables the maintenance of channels with an unlimited number of subscribers, allowing users to create and subscribe to public channels that function like broadcast stations, disseminating messages, media and files to a large audience.[22] Telegram has been popular for years in Russia and Ukraine and has around 700 million users worldwide.[23] Besides the SBU, all other key Ukrainian government and security organisations maintain a Telegram channel. Early reports from the war in Ukraine indicated that the events of the war were not to be found on platforms such as Twitter/X. Instead, Telegram became the place to be for both Russians and Ukrainians.[24]

Using a scraping tool all Telegram messages posted by the SBU from the start of the large-scale Russian invasion on 24 February 2022 to 26 October 2023 (≈20 months) were collected. This dataset consists of 2,574 Telegram posts that the service has published on its Ukrainian language channel, which had amassed over 347,000 followers by December 2023.[25] This material was coded and themes were identified using reflexive thematic analysis (RTA), which combines the possibilities of inductive and deductive approaches.[26] RTA is a method of qualitative data analysis that involves identifying, analysing and reporting patterns or themes within the data.[27] Thematic analysis is well suited for this dataset, since it can accommodate exploration of the content, tone and purpose of the SBU's posts and examination of how the service constructs its communication strategy using a bottom-up approach.

Given the relatively short length of most Telegram posts, each typically contains a single dominant theme. The observed themes and their characteristics are described in Table 1, including the percentage of occurrence for each theme. However, these percentages are indicative and should not be treated as exact numbers due to the non-straightforward nature of the frequency and prevalence of certain themes in the SBU's Telegram posts. For instance, a theme that is briefly and superficially mentioned in one Telegram message is not directly measurable and comparable to another theme that is referenced in detail and depth in the next message.[28] Nonetheless, the top two themes in the table – *Collaboration and Treason* and *Branding of SBU Success* – are predominantly referenced in the dataset over the entire 20 months of SBU Telegram posting. The other themes are ranked in order, providing an indication of the topics the SBU considers most crucial to communicate to external audiences.

Table 1. Thematic analysis of SBU telegram content (2574 messages), 24 February 2022 till 26 October 2023.

Theme	Characteristics	Pct.
Collaboration, treason	• Accusation or apprehension of Ukrainians (including members of DNR/LNR government and military units) collaborating with Russian authorities. • Messages about alleged treacherous activities, such as posting Russian propaganda, blogging and maintaining bot farms.	28.4 per cent
Branding of SBU success	• Successes of special forces wing SBU Alfa, SBU cyber operations. • Announcements of national festive and commemorative days. • Successful prisoner of war (POW) exchanges.	16.9 per cent
Russian espionage, sabotage	• Warnings of Russian espionage and sabotage activities, arrests of spies.	13.6 per cent
SBU law enforcement	• Posts about the SBU tackling crime: extortion, smuggling, forgery fraud, corruption and exposure of military service evasion schemes.	13.4 per cent
Shaming of Russians, Russian behaviour.	• Indictments of Russian businessmen, propagandists, parliamentarians and military officers who have facilitated or committed alleged war crimes. • Confiscation of Russian business assets in Ukraine. • Video testimonials of Russian POWs expressing disappointment with their own leadership and the war.	12.1 per cent
Communication intercepts	• Raw intelligence (communication intercepts) in which Russian military members express discontent with their circumstances due to lack of material and clothing and unexpected Ukrainian resistance. • References to war crimes or corrupt and dysfunctional leadership.	8.3 per cent
Advice and appeals to the public	• Advice to the public to be vigilant during festive days, warnings about Russian campaigns and recommendations to follow trusted Ukrainian government sites. • Appeals to disconnect IP cameras; refrain from sharing any footage of Russian missile strikes. • Report treason, war crimes or Russian troop presence to chatbots and applications, e.g., eVorog.	4.5 per cent
Miscellaneous	• Calls for applications of new personnel, information about exercises, leadership changes.	2.7 per cent

3.2. Qualitative thematic analysis of the SBU's Telegram content in wartime

As explained, the SBU is Ukraine's main intelligence and counterintelligence agency of Ukraine. It plays a crucial role in the ongoing conflict with Russia. In its social media messaging on Telegram, eight recurring themes can be discerned (see Table 1).

Collaboration and Treason is the predominant theme in the SBU's social media messaging. Ukrainians who are collaborating in any way with the Russian occupation forces are singled out. A few illustrative Telegram messages alluding to this subject are as follows. On 23 October 2023, the SBU reported that it had neutralized an 'anti-Ukrainian underground team', that was directing Russian missiles and guided aerial bombs at residential buildings in Kherson. As a result of their treason, enemy shelling injured 10 civilians. According to the SBU investigation, the organiser and leader of the local anti-Ukrainian underground group was a former businessman who, after the capture of the city in 2022, switched to the side of the enemy.[29] In this message, the alleged treason is quite straightforward, since the SBU suspects the apprehended persons of guiding Russian missiles to Kherson. However, treason of a milder nature is also taken seriously. In August 2023, the SBU reported on its Telegram channel that it had detained two female officials of a regional energy company in Mykolaiv in southern Ukraine for denying the existence of Ukraine and expressing support for the Russian invasion. According to the SBU, the officials had also justified rocket attacks on Odesa. The SBU reported that the women were facing charges under two articles of the Criminal Code of Ukraine and could be sentenced to up to eight years in prison with property confiscation.[30]

Harsh words were spoken by the SBU about Ukrainians who have supported the organisation of illegal referendums in the occupied territories of Ukraine in September 2022. The Russian authorities organised these referendums to attempt to legitimise the annexation of parts of Ukraine under their control. In one of its Telegram messages the SBU commented on one of the persons suspected of collaboration: *In the ranks of the invading institution, she carried out Moscow's instructions to hold*

a fake plebiscite in the autumn of 2022. To do this, she visited the homes of local residents and urged them to participate in a pseudo-referendum and 'vote' in favour of the aggressor country. During such raids, the collaborator was accompanied by armed occupiers who helped her intimidate the residents of the village and 'beat out' from them signatures in support of the Kremlin.[31] The SBU deems these acts a significant betrayal of Ukraine's national interests. Perpetrators are facing up to 10 years prison, warned the SBU. In this respect, this type of messaging within the theme *Collaboration and Treason* can be seen as a means for the SBU to discourage Ukrainians involved in collaboration.

Branding of SBU Success is the second theme that is dominant in SBU Telegram messaging. This theme reflects the SBU's attempts to showcase its achievements and boost its reputation among the public. In mid-October 2023, the SBU posted a typical branding message in which the service proudly reported that its special forces unit SBU Alfa disabled 57 units of equipment and weapons of the Russian armed forces, including tanks, anti-aircraft missile defence systems, BMP armoured vehicles, artillery systems and surveillance systems. '*We destroy the occupiers until complete Victory!*', the post reads, and it is illustrated with first-person view (FPV) footage of kamikaze drones slamming into Russian equipment.[32] Another example is the SBU's use of Telegram to highlight its contribution to the successful exchange of Ukrainian prisoners of war with Russia and the return of Ukrainian children who were taken to the Russian Federation.[33] Again, an example of a distinctive branding post in August 2023: '*I am proud that Russians know that I am an employee of the SBU. Let them be afraid!*', said Olympic sabre fencing champion and student at the SBU Academy Olga Harlan. Harlan gained international media attention after she refused to shake hands with her Russian opponent during the World Fencing Championship in Milan in July 2023.[34]

The third recurring theme in the SBU's messaging involves warnings about Russian *Espionage and Sabotage*, as well as reports of the arrests of suspected spies and saboteurs. This theme was particularly prevalent in the SBU's social media engagement during the first six months of the invasion. For instance, in early August 2022, the SBU reported the detention of members of a Russian sabotage and intelligence group, part of the Russian military intelligence service (GRU), who were allegedly planning to assassinate the Ukrainian Minister of Defence and the head of Defence Intelligence (HUR).[35]

The fourth theme in SBU's Telegram messaging is *Law Enforcement*. In these posts, the SBU reports on its operations against extortion, smuggling, forgery and fraud. The SBU also detains alleged corrupt Ukrainian government employees, including personnel from within its own ranks. Furthermore, the SBU exposes military service evasion schemes. For example, in April 2023, the SBU posted about a group of suspects from Vinnytsia, Lviv and Odesa who helped young Ukrainians to dodge conscription by means of fake documents and offered help to illegally cross the borders of Ukraine.[36] This is seen as a serious offence, since these schemes enable military-aged males to leave Ukraine and therefore drain the Ukrainian armed forces potential for recruitment and mobilisation of new personnel. Ominously, the SBU warns that perpetrators involved in evasion schemes face up to nine years in prison and confiscation of property.[37]

The theme of *Shaming Russians* in the SBU's messaging strategy involves scorning Russian businesspeople, parliamentarians, military personnel and propagandists who contribute to the Russian war effort. A special category within this theme is the publication of video testimonials of Russian prisoners of war (POWs). These videos were regularly published by the SBU in the first months of the invasion and received international criticism due to the exposure of POWs to public scrutiny, which is forbidden by international humanitarian law (IHL). In these videos, the Russian POWs express their disappointment with their own leadership and the war in general: '*the Russian Federation does not even take away the corpses of soldiers*', complains a captured soldier in a video published in mid-March 2022 on Telegram.[38] The SBU supplemented these testimonials with messages directed towards the families of captured Russian soldiers. In these messages, the families were offered the opportunity to call helplines and contact their loved ones. This was one of the few posts by the SBU that directly addressed the Russian public.[39] Furthermore, the SBU reported in May 2022 that it had confiscated the phone of a Chechen fighter loyal to Chechen leader Ramzam

Kadyrov. Reportedly, they had created videos of themselves firing their weapons against pine trees instead of fighting the Ukrainian army, prioritising flashy content over actual combat. The SBU used this material to degrade Chechen forces loyal to Ramzan Kadyrov and label them as '*TikTok troops*'.[40]

Another prominent theme in the first months of the invasion, was the publication on the SBU Telegram channel of more than two hundred excerpts of communication intercepts. This theme - *Communication Intercepts* - pertains to the disclosure of voice files containing conversations between Russian military personnel or with their family members or persons otherwise related. The intercepted conversations published by the SBU are interceptions of GSM traffic through base transceiver stations (BTS) controlled by the Ukrainians. Russian service members are prohibited from using mobile phones on active service, even on Russian territory, meaning that from a formal point of view, Russian command should be taking measures to block this channel of leakage.[41] However, Russian soldiers, especially on the front lines, still find ways to acquire phones, sometimes stealing them from the Ukrainian population, to call home.[42] Although the language and discourse used in the audio files suggest that the audio fragments released by the SBU are genuine intercepts, the possibility cannot be ruled out that SBU specialists may have modified the contents.[43] Therefore, achieving absolute certainty about the reliability of the intelligence material released by the SBU is a challenging undertaking. Furthermore, the SBU only released excerpts of audio material which it deemed suitable for release to promote public discourse on themes that suited its communication strategy.

Consequently, the intercepts selected by the SBU for release on Telegram and its other social media channels reflected Russians' despair with their dire circumstances, due to lack of sufficient equipment, clothing and ammunition, corruption in military leadership and unexpected Ukrainian resistance. Also very prominent were candid discussions of Russian military service members about war crimes they either perpetrated themselves or witnessed. In one of the intercepts published by the SBU in April 2023, a Russian soldier admits to killing Ukrainian POWs by cutting their throats. The SBU states that it has identified the soldier responsible and is working to ensure he faces punishment.[44] In January 2023, another example of an intercept published by the SBU alluded to the misconduct of the Russian military in the north-eastern region of Ukraine: *When we surrendered Lyman, we cut everyone there, the fuckers… We raped them, cut them, shot them there. In Lyman, in Torsk, everyone just went and was shot. All men, who were younger, were taken there, and the women, these young people: all of them were killed, they were cut, they were shot*. The SBU stated that the words of this Russian had been documented and that overall, the service had started 21,000 criminal proceedings based on the facts of violations of the laws and customs of war by the Russian army.[45]

The SBU's communications under the *Advice and Appeals to the Public* theme directly address Ukrainian citizens. This messaging typically calls for heightened vigilance during festive periods, alerts the public to Russian disinformation campaigns, and advices against engaging with pro-Russian Telegram channels. At the end of May 2022, the SBU warned that the Russian special services were using smartphone games to gather information about strategically important objects by enticing young participants to take photos of the terrain, military objects and critical infrastructure in exchange for digital money.[46] Moreover, the SBU asked the public to disconnect IP cameras and to refrain from sharing any footage of Russian missile and drone strikes that could compromise Ukrainian security and defence. The SBU also used its Telegram channel to open the cyber front: *If you notice any vulnerable points in the cyber protection of Russian objects (bugs, backdoors, logins and passwords), be sure to report them to the chatbot. These can be vulnerabilities in e-mail, websites, online banking, management systems, computer networks, certification centres, keys, messengers, social networks. Ukrainian cyber experts will use this information to fight the occupier!*

On 28 February 2022, just a brief time after the Russian invasion started, the SBU presented a chatbot capability that enables citizens to share information concerning Russian forces inside Ukraine. This bot has improved the SBU's ability to support military intelligence in finding Russian soldiers and equipment, and it has likewise been valuable in gathering data about collaborators and infiltrators.[47] The SBU repeatedly addressed the Ukrainian people, not only by asking them to cooperate but also by asking

them to provide information and participate in the war effort.[48] In a post that exemplifies this strategy, three different chatbots were promoted and Ukrainians were asked to report information on traitors, collaborators and enemy agents. It was explained that this would enable the SBU to collect high-quality evidence that would make it possible to bring the perpetrators to justice. *The testimonies of residents are very important to us! If you have information about the accomplices of the enemy, as well as Internet agents who spill important data to the aggressor or distribute content in social networks in support of him, use the chatbot ➡ t.me/Traitor_Search_bot. If you have information about the positions or movements of enemy equipment, write to the chatbots: Security Services of Ukraine ➡ t.me/stop_russian_war_bot and the Ministry of Digital Transformation ➡ t.me/evorog_bot. Let us protect Ukraine together!*[49] In October 2022, Ilia Vitiuk, the chief of the cyber security department, reported that the SBU had received over 100,000 messages from Ukrainians via its Telegram bot. Vitiuk claimed that after verification, this information enabled several hundred strikes by artillery forces on Russian convoys and military leadership.[50]

The last theme *Miscellaneous* contains a wide range of messages, varying from calls for applications of new SBU personnel to information about exercises and leadership changes within the SBU.

3.3. Not bound by secrecy

The thematic analysis of more than 2,500 Telegram posts establishes that in its social media engagement, the SBU emphasises operations against alleged collaborators, traitors and criminals. Additionally, its own success is regularly accentuated, which corresponds to the behaviour of other Ukrainian government and security organisations with a strong online presence that was gradually developed in the years prior to the Russian invasion. The SBU presence on Telegram is distinctive in its use of raw intelligence such as communication intercepts, which is not in keeping with the occasional trickle or leaking of intelligence to support a specific political outcome.[51] Rather, it fits into a pattern of a wider Ukrainian governmental narrative strategy, that leaves no opportunity unused to disgrace the Russian opponent and underscore Ukrainian resilience and bravery.[52] The SBU's adherence to this strategy indicates a willingness to move beyond the traditional view that intelligence organisations should operate covertly and discreetly to avoid public scrutiny.[53] Declassified intelligence can be used to inform the public and seize the moral high ground.[54]

Furthermore, the recurring messages about indictments of Russian officials and statements by Russian POWs about the alleged dreadful state of the Russian military support Ukrainian communication strategies to shame its adversary. Reports on counterintelligence and sabotage operations are a logical theme in the SBU's social media strategy, as these are the main tasks of the SBU. Finally, as shown in the thematic analysis of SBU Telegram content, the service makes an effort to involve the Ukrainian population in its daily operations by promoting multiple channels (chatbots, hotlines, applications) to collect information on collaborators, spies and the whereabouts of the Russian enemy, while also asking the public to report weaknesses in Russian cyber security.

In summary, the SBU uses social media engagement on Telegram to expose collaboration, treason, and crime, as well as to celebrate its own success and degrade the Russian adversary. The SBU also involves the Ukrainian population in its daily operations. The themes established in these posts are the building blocks that can be used to identify the concept of intelligence communication that the SBU adheres to.

4. The SBU's concept of intelligence communication

In this section, various concepts of intelligence communication with the public are introduced and subsequently analysed in the context of the SBU's social media engagement with Ukrainian audiences.

Petersen's 2019 study identified three distinct approaches employed by Western intelligence services for public communication.[55] Unlike previous research that primarily focused on communication with political or military superiors, Petersen's work delved into communication intended for

audiences beyond governmental circles.[56] These approaches extend beyond social media interactions and encompass public engagement through websites, media outlets, community programmes, and partnerships. Each of these three concepts represents a unique perspective on effective public communication.

The first concept, communication as awareness, seeks to balance the need for democratic accountability with national security. This concept is not aimed at asking the public to act or even mobilise its knowledge. Instead, this concept consists of statements by intelligence executives or in official publications.[57] The key message of this concept of communication is the commitment to a certain level of openness by an intelligence service since it is important to justify the need for intelligence work. However, this message is always coupled with the need for secrecy, because otherwise services would not be able to function.[58] A typical example of this communication concept is the 'Transparency Initiative' launched by the Director of U.S. National Intelligence James Clapper (2010–2017) in 2015, designed to enhance public understanding of the mission of intelligence services and assure the public that secret activities were adequately supervised and overseen.[59]

Another concept established by Petersen that intelligence communication can be seen as a form of advice, which means that an agency can encourage the public to do take certain actions based on threat information.[60] For example, in France the Plan Vigipirate is a government-led terrorism alert system that defines the level of vigilance and security measures to be implemented in times of heightened terrorist threat.[61] The United States and other European nations have similar programmes.[62] The core question with regard to these systems is determining the amount and type of information necessary for the public to make informed decisions about what actions to take to prevent and respond to threats. Petersen argues that this concept, communication as advice, parallels the first concept, communication as awareness, in being unidirectional. It positions agencies as possessing secret expertise and proficiency in making judgments for the common good, reinforcing an '*expert-amateur hierarchy*' between the services and the public.[63]

The third concept is communication as co-production. Unlike the previous concept of communication as advice, which maintains a clear separation between sender (intelligence service) and receiver (general public), this concept recognises the importance of decentralised security management, which involves cooperation between services in the public and private spheres.[64] This more egalitarian concept encourages collaboration between intelligence services and the private sector, particularly in areas such as cybersecurity, where private companies, such as Microsoft and Mandiant and their regular publications about cyber threats, contribute or even lead in defining potential threats.[65] This concept of intelligence communication emphasises learning and incorporating new knowledge from the civil and private sectors and aims to engage citizens and companies in identifying and managing emerging threats. It challenges the traditional hierarchical structure of state intelligence expertise and opens up the possibility of public participation in interpreting present and future risks.[66]

Drawing upon the thematic analysis of the SBU's Telegram content, it can be said that the SBU employs Petersen's second concept of communication as advice. In addition to publishing branding messages focused on its own performance and the shaming of Russian officials and military personnel, the SBU consistently updates Ukrainian citizens on a wide range of tangible and intangible threats. However, the SBU takes its social media engagement further by asking the public to assist the service. The security service does not present itself as omniscient, but repeatedly emphasises its reliance on Ukrainian society. This is not merely an empty statement, as the SBU has opened multiple chatbots and hotlines for public communication. In this respect, the SBU aligns with governmental cybersecurity agencies that closely collaborate with companies in the technology sector, recognising the need for private and civilian involvement in mitigating cyber threats, identifying common challenges and discussing best practices.[67] Thus, the SBU's communication extends beyond providing advice to encompass learning, cooperation, and an understanding of the Ukrainian public's potential contributions.

Incidentally, this approach is not without controversy. While beyond the scope of this article, the active involvement of civilians in the wartime collection of information on enemy troops is a contentious issue. Some argue that it may violate the humanitarian rules of war due to the blurred lines between combatants and non-combatants.[68] Regardless, of these debates, the mutual communication between the SBU and the Ukrainian public is continuing, at any rate for the time being.

The SBU's policy to cooperate with the civilian population in order to collect information fits into Petersen's concept of communication as co-production. However, this does not fully explain the SBU's strategy of incorporating the disclosure of raw, sensitive intelligence into its social media messaging. The public release of intercepted communications, in which Russian military personnel discuss low morale, weak leadership, or hint at misconduct against Ukrainian civilians and military personnel, challenges traditional notions that intelligence material should remain confidential and outside the public sphere to avoid jeopardising future collection. This is particularly true for communication intercepts, as public awareness of an entity's access to this information often signals the end of such access.[69]

Despite the risk of losing intelligence sources, the SBU's decision to utilize this sensitive material in the public domain aligns with a broader Ukrainian government strategy. Ukraine sees a public relations advantage in releasing intercepted material that embarrasses the Russian military and exposes details of Russian atrocities on the battlefield. This lends additional credibility to Ukraine's protest against the injustice of the Russian invasion, not only to Western audiences but also to its own population. The SBU's selective disclosure of sensitive intelligence in this attributable manner on its own social media channels is viewed as another tool to support the strategic narrative that Ukraine is waging a just war against a disgraceful foreign invader, outweighing the risks associated with the disclosure of this material.

5. Reflection and concluding remarks

This research focussed on what type of social media content the SBU has posted on its Telegram channel since the start of the Russian large-scale invasion. SBU cyber chief Vitiuk described his department in September 2023 as: '*a mixture of intelligence officers, law enforcement officers, hackers and a SWAT team*'.[70] This characterisation aligns closely with the tenacious mindset that the wider SBU aims to portray. Its approach involves the strategic dissemination of content to achieve multiple objectives: apprehending traitors and collaborators, promoting its own achievements, discrediting the Russian invaders, warning Ukrainian citizens against Russian disinformation outlets, and encouraging them to contribute to the war effort.

Since 2014, the SBU has accumulated a decade of experience in overt and attributable social media messaging. One of the SBU's objectives behind this strategy was to transform its public image from a repressive and Russian-infiltrated agency to a modern and initiative-taking intelligence and security service.[71]

The social media practices of the SBU on Telegram, including repeated calls for cooperation with the Ukrainian public and particularly its release of raw intelligence in support of Ukrainian government narratives, is part of a wider development that encompasses the use of intelligence beyond its traditional territory of informing key policy makers and military commanders, using it for external influence.[72] In this regard, the disclosure of intelligence by the American and British governments of Russian troop build-up around Ukraine during the winter of 2021/2022 was a coordinated effort to shape international political discourse, exemplifying public diplomacy.[73] However, this is not comparable to the SBU's social media messaging on Telegram in the ongoing war. The SBU's messaging is continuous, appeals to the stamina of the population by highlighting success, warns Ukrainians not to collaborate with the enemy and directly asks citizens to contribute to the war effort. This underscores the SBU's efforts to defend against the invaders while bringing to light the wartime atrocities committed. Its messaging has strengthened international support for Ukraine, both among leaders and ordinary citizens.

This qualitative research has some limitations that should be considered when interpreting the findings and implications. One limitation is that the SBU's social media engagement does not reflect the full spectrum of intelligence and influence operations conducted by Ukrainian intelligence organisations. An additional limitation is that the research may have a biased view of social media – based engagement in the Russo-Ukrainian war, as it only examines the strategy of the SBU, without considering the counterstrategies and responses of other actors, such as Russia, NATO, or the EU.

However, the findings of this study have relevance in the context of the Russo-Ukrainian War. The SBU's approach in information warfare is marked by its prominent social media presence. This contrasts with the more subdued online profiles of other intelligence and security services, which preferably leave external communication to policymakers. The SBU assesses that within the information warfare spectrum, from communication to indoctrination, its information and intelligence can be employed to build trust and amplify emotional resonance.[74]

Notes

1. "Telegram: Contact @SBUkr."
2. Hauter, *Russia's Overlooked Invasion The Causes of the 2014 Outbreak of War in Ukraine's Donbas. With a Foreword by Hiroaki Kuromiya*., 174.
3. Higgins, "MH17 - The Open Source Evidence."
4. Veiligheid, "Onderzoek naar telecommunicatie – MH17 vliegramp – Openbaar Ministerie."
5. Kaul, "Ukraine's Current Counterintelligence Capabilities", 2.
6. Kaul, "The Evolution of the Security Services of Ukraine: Institutional Change in the Post-Soviet Security Apparatus", 175.
7. Kaul, 175.
8. Kaul, "Ukraine's Current Counterintelligence Capabilities", 4.
9. Omand, "Social Media Intelligence (SOCMINT)", 355.
10. Petersen, "Three Concepts of Intelligence Communication", 317.
11. Omand, Bartlett, and Miller, "Introducing Social Media Intelligence (SOCMINT)", 805.
12. Lowenthal, *Intelligence: From Secrets to Policy*, 235.
13. Treyger, Cheravitch, and Cohen, *Russian Disinformation Efforts on Social Media*, 107.
14. "The IO Offensive."
15. Omand, "Social Media Intelligence (SOCMINT)", 363.
16. Landon-Murray, "Social Media and US Intelligence Agencies: Just Trending or a Real Tool to Engage and Educate?", 67.
17. McLoughlin, Ward, and Lomas, "'Hello, World': GCHQ, Twitter and Social Media Engagement", 233.
18. Luțai, "European Intelligence Services Just Signed up on Social Media. An Analysis of Secret Services and Social Media Platforms", 216.
19. Landon-Murray, "Social Media and US Intelligence Agencies: Just Trending or a Real Tool to Engage and Educate?", 78.
20. Kaul, "Ukraine's Current Counterintelligence Capabilities."
21. "06 Integration of the Ukrainian Tech Sector for Civil Defense By Jerry England, TRADOC G-2 - Red Diamond Newsletters – Operational Environment and Threat Analysis Directorate."
22. Thomas and Bhat, "A Comprehensive Overview of Telegram Services-A Case Study", 290.
23. "Telegram Global MAU 2022."
24. Ford, "Ukraine, Participation and the Smartphone at War", 15.
25. "SBU_Telegram_Feb22-Oct23.Xlsx – Google Spreadsheets."
26. Byrne, "A Worked Example of Braun and Clarke's Approach to Reflexive Thematic Analysis", 1396.
27. Campbell et al., "Reflexive Thematic Analysis for Applied Qualitative Health Research."
28. Braun and Clarke, *Thematic Analysis : A Practical Guide*, 141.
29. "Telegram: Contact @SBUkr."
30. "Telegram: Contact @SBUkr."
31. "Telegram: Contact @SBUkr."
32. "Telegram: Contact @SBUkr."
33. "Telegram: Contact @SBUkr."
34. "Telegram: Contact @SBUkr."
35. "Telegram: Contact @SBUkr."

36. "Telegram: Contact @SBUkr."
37. "Telegram: Contact @SBUkr."
38. "Telegram: Contact @SBUkr."
39. "Telegram: Contact @SBUkr."
40. "Telegram: Contact @SBUkr."
41. "Makiivka."
42. "The Mobile Network Battlefield in Ukraine – Part 2 | Enea."
43. WarTranslated, "Can We Believe the Russian Phone Calls Intercepted and Published by Ukrainian SBU and GUR?."
44. "Telegram: Contact @SBUkr."
45. "Telegram: Contact @SBUkr."
46. "Telegram: Contact @SBUkr."
47. Kaul, "Ukraine's Current Counterintelligence Capabilities."
48. "Telegram: Contact @SBUkr."
49. "Telegram: Contact @SBUkr."
50. "SSU's Chatbot Helps Destroy Hundreds of Enemy Military Vehicles and Even Several Generals – Ilya Vitiuk."
51. Schrijver, "The Wise Man Will Be Master of the Stars."
52. Ekman and Nilsson, "Ukraine's Information Front", 20.
53. Riemer and Sobelman, "Coercive Disclosure", 20.
54. Magen, "Strategic Communication of Israel's Intelligence Services: Countering New Challenges with Old Methods", 272.
55. Petersen, "Three Concepts of Intelligence Communication", 317.
56. Petersen, 317.
57. Petersen, 320.
58. Petersen, 319.
59. Slick, "2022 Public Attitudes on US Intelligence", 2.
60. Petersen, "Three Concepts of Intelligence Communication", 320.
61. "Le plan Vigipirate."
62. "National Terrorism Advisory System | Homeland Security."
63. Petersen, "Three Concepts of Intelligence Communication", 321.
64. Petersen, 322.
65. "Threat Intelligence | Cyber Threat Intelligence Platform."
66. Petersen, "Three Concepts of Intelligence Communication", 323.
67. Lostri, Lewis, and Wood, "A Shared Responsibility", 3.
68. Schmitt, "Ukraine Symposium – Using Cellphones to Gather and Transmit Military Information, A Postscript."
69. Clark, "The Protection of Intelligence Sources and Methods."
70. "Ukraine's Fusion of Cyber and Kinetic Warfare."
71. Fluri et al., "Intelligence and Security Services Reform and Oversight in Ukraine – An Interim Report", 55.
72. "500 נחקרים, ומיליוני שיחות פינוי ואזהרה."
73. Dylan and Maguire, "Secret Intelligence and Public Diplomacy in the Ukraine War", 34.
74. Clack and Johnson, *The World Information War: Western Resilience, Campaigning, and Cognitive Effects*.

Disclosure statement

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

Notes on contributor

Peter Schrijver is a PhD researcher affiliated with the Netherlands Defence Academy. His academic interests focus on Ukraine's operations in the information environment.

Bibliography

APAN Community. "Integration of the Ukrainian Tech Sector for Civil Defense", TRADOC G-2 - Red Diamond Newsletters - Operational Environment and Threat Analysis Directorate. Accessed March 13, 2023. https://community.apan.org/wg/tradoc-g2/operational-environment-and-threat-analysis-directorate/w/red-diamond-newsletters/38129/06-integration-of-the-ukrainian-tech-sector-for-civil-defense-by-jerry-england-tradoc-g-2/.

BBC News. "Makiivka: Russia Blames Missile Attack on Soldiers' Mobile Phone Use." January 4, 2023. https://www.bbc.com/news/world-europe-64159045.

Braun, V., and V. Clarke. *Thematic Analysis : A Practical Guide*. London: Sage, 2022.

Byrne, D. "A Worked Example of Braun and Clarke's Approach to Reflexive Thematic Analysis." *Quality & Quantity* 56, no. 3 (June 1, 2022): 1391–1412. doi:10.1007/s11135-021-01182-y.

Campbell, K., E. Orr, P. Durepos, L. Nguyen, L. Li, C. Whitmore, P. Gehrke, L. Graham, and S. Jack. "Reflexive Thematic Analysis for Applied Qualitative Health Research." *The Qualitative Report* (June 20, 2021). doi:10.46743/2160-3715/2021.5010

Clack, T., and R. Johnson. *The World Information War: Western Resilience, Campaigning, and Cognitive Effects*. Abingdon: Routledge, 2021.

Clark, R. "The Protection of Intelligence Sources and Methods", 2016. Accessed 12 December 2023. https://www.afio.com/publications/CLARK%20Robert%20The%20Protection%20of%20Intelligence%20Sources%20and%20Methods%20FINAL%202016Oct15.pdf

Dylan, H., and T. Maguire. "Secret Intelligence and Public Diplomacy in the Ukraine War." *Survival* 64, no.4 Routledge (2023): 33–74. doi:10.1080/00396338.2022.2103257.

Ekman, I., and P. Nilsson. "Ukraine's Information Front Strategic Communication During Russia's Full-Scale Invasion of Ukraine". FOI Sweden, April 2023. https://www.foi.se/en/foi/news-and-pressroom/news/2023-04-21-war-of-words—how-ukraine-uses-strategic-communication-to-beat-russia-on-the-information-front.html

Fluri, P., and L. Polyakov. "Intelligence and Security Services Reform and Oversight in Ukraine – an Interim Report." *Connections: The Quarterly Journal* 20, no. 1 (2021): 51–59. doi:10.11610/Connections.20.1.03.

Ford, M. "Ukraine, Participation and the Smartphone at War." *Political Anthropological Research on International Social Sciences* 1, no. aop (2023): 1–29. doi:10.1163/25903276-bja10048.

gouvernement.fr. "Le plan Vigipirate." Accessed November 21, 2023. https://www.gouvernement.fr/risques/le-plan-vigipirate.

Hauter, J., A. Umland, H. Kuromiya, and Y. Nasadyuk. *Russia's Overlooked Invasion: The Causes of the 2014 Outbreak of War in Ukraine's Donbas*. Berlin: Ibidem Verlag, 2023.

Higgins, E. "MH17 - the Open Source Evidence." Bellingcat, 8 October 2015. https://www.bellingcat.com/news/uk-and-europe/2015/10/08/mh17-the-open-source-evidence/.

Kaul, E. *The Evolution of the Security Services of Ukraine: Institutional Change in the Post-Soviet Security Apparatus*. Kent, Ohio, United States: Kent State University, 2021.

Landon-Murray, M. "Social Media and US Intelligence Agencies: Just Trending or a Real Tool to Engage and Educate?" *Journal of Strategic Security* 8, no. 3 (2015): 67–79. doi:10.5038/1944-0472.8.3S.1476.

Lostri, E., J. Lewis, and G. Wood. "A Shared Responsibility: Public-Private Cooperation for Cybersecurity", 22 March 2022. https://www.csis.org/analysis/shared-responsibility-public-private-cooperation-cybersecurity.

Lowenthal, M. *Intelligence: From Secrets to Policy*. 8th ed. Washington DC: CQ press, 2022.

Luțai, R. "European Intelligence Services Just Signed Up on Social Media. An Analysis of Secret Services and Social Media Platforms." *Studia Universitatis Babes-Bolyai-Studia Europaea* 67, no. 2 (2022): 199–223. doi:10.24193/subbeuropaea.2022.2.08.

Magen, C. "Strategic Communication of Israel's Intelligence Services: Countering New Challenges with Old Methods." *International Journal of Strategic Communication* 11, no. 4 (2017): 269–285. doi:10.1080/1553118X.2017.1334207.

Mandiant. "The IO Offensive: Information Operations Surrounding the Russian Invasion of Ukraine." Accessed 24 October 2023. https://www.mandiant.com/resources/blog/information-operations-surrounding-ukraine.

Mandiant. "Threat Intelligence | Cyber Threat Intelligence Platform." Accessed 24 November 2023. https://www.mandiant.com/advantage/threat-intelligence.

McLoughlin, L., S. Ward, and D. Lomas. "Hello, World: GCHQ, Twitter and Social Media Engagement." *Intelligence & National Security* 35, no. 2 (2020): 233–251. doi:10.1080/02684527.2020.1713434.

"The Mobile Network Battlefield in Ukraine - Part 2 | Enea." Accessed 30 August 2023. https://www.enea.com/insights/the-mobile-network-battlefield-in-ukraine-part-2/.

"National Terrorism Advisory System | Homeland Security." Accessed 29 November 2023. https://www.dhs.gov/national-terrorism-advisory-system.

Omand, D. "Social Media Intelligence (SOCMINT)." In *The Palgrave Handbook of Security, Risk and Intelligence*, edited by R. Dover, H. Dylan, and M. Goodman. London: Palgrave Macmillan UK, 2017. doi:10.1057/978-1-137-53675-4_20.

Omand, D., J. Bartlett, and C. Miller. "Introducing Social Media Intelligence (SOCMINT)." *Intelligence & National Security* 27, no. 6 December 1 (2012): 801–823. doi:10.1080/02684527.2012.716965.

Petersen, K. "Three Concepts of Intelligence Communication: Awareness, Advice or Co-Production?" *Intelligence & National Security* 34, no. 3 April 16 (2019): 317–328. doi:10.1080/02684527.2019.1553371.

PONARS Eurasia. "Ukraine's Current Counterintelligence Capabilities", 1 March 2023. https://www.ponarseurasia.org/ukraines-current-counterintelligence-capabilities/

Riemer, O., and D. Sobelman. "Coercive Disclosure: The Weaponization of Public Intelligence Revelation in International Relations." *Contemporary Security Policy* 44, no. 2 April 3 (2023): 276–307. doi:10.1080/13523260.2022.2164122.

SBU. “SSU’s Chatbot Helps Destroy Hundreds of Enemy Military Vehicles and Even Several Generals - Ilya Vitiuk.” Accessed 30 November 2023. https://ssu.gov.ua/en/novyny/zavdiaky-chatbotu-sbu-znyshcheno-sotni-odynyts-vorozhoi-tekhniky-i-navit-dekilkokh-heneraliv-illia-vitiuk.

”SBU_Telegram_Feb22-Oct23.Xlsx - Google Spreadsheets.” Accessed 29 January 2024. https://docs.google.com/spreadsheets/d/1tqIMHEU45eWXskWUp1hLGvDOIHkopAOS/edit#gid=216706666.

Schmitt, M., “Ukraine Symposium – Using Cell Phones to Gather and Transmit Military Information, a Postscript.” Lieber Institute West Point, 4 November 2022. https://lieber.westpoint.edu/civilians-using-cellphones-gather-transmit-military-information-postscript/.

Schrijver, P. “The Wise Man Will Be Master of the Stars: The Use of Twitter by the Ukrainian Military Intelligence Service.” Irregular Warfare Initiative, 27 June 2023. https://irregularwarfare.org/articles/the-wise-man-will-be-master-of-the-stars-the-use-of-twitter-by-the-ukrainian-military-intelligence-service/.

Slick, S., J. Busby, and K. Nguyen. “2022 Public Attitudes on US Intelligence.” The Chicago Council on Global Affairs, 29 August 2023. https://globalaffairs.org/research/public-opinion-survey/2022-public-attitudes-us-intelligence.

Statista. “Telegram Global MAU 2022.” Accessed 4 December 2023. https://www.statista.com/statistics/234038/telegram-messenger-mau-users/.

”Telegram: Contact @SBUkr.” Accessed 26 October 2023. https://t.me/SBUkr/3707.

”Telegram: Contact @SBUkr.” Accessed 22 November 2023. https://t.me/SBUkr/10059.

”Telegram: Contact @SBUkr.” Accessed 22 November 2023. https://t.me/SBUkr/9322.

”Telegram: Contact @SBUkr.” Accessed 14 December 2023. https://t.me/SBUkr/9945 .

”Telegram: Contact @SBUkr.” Accessed 22 November 2023. https://t.me/SBUkr/10005.

”Telegram: Contact @SBUkr.” Accessed 14 December 2023. https://t.me/SBUkr/8902 .

”Telegram: Contact @SBUkr.” Accessed 23 November 2023. https://t.me/SBUkr/9351.

”Telegram: Contact @SBUkr.” Accessed 22 November 2023. https://t.me/SBUkr/4789.

”Telegram: Contact @SBUkr.” Accessed 22 November 2023. https://t.me/SBUkr/8069.

”Telegram: Contact @SBUkr.” Accessed 14 December 2023. https://t.me/SBUkr/8896 .

”Telegram: Contact @SBUkr.” Accessed 22 November 2023. https://t.me/SBUkr/3882.

”Telegram: Contact @SBUkr.” Accessed 23 November 2023. https://t.me/SBUkr/3802.

”Telegram: Contact @SBUkr.” Accessed 4 December 2023. https://t.me/SBUkr/4352.

”Telegram: Contact @SBUkr.” Accessed 22 November 2023. https://t.me/SBUkr/8107.

”Telegram: Contact @SBUkr.” Accessed 22 November 2023. https://t.me/SBUkr/6496.

”Telegram: Contact @SBUkr.” Accessed 29 November 2023. https://t.me/SBUkr/4326.

”Telegram: Contact @SBUkr.” Accessed 22 November 2023. https://t.me/SBUkr/3762.

”Telegram: Contact @SBUkr.” Accessed 23 November 2023. https://t.me/SBUkr/5757.

Thomas, L., and S. Bhat. “A Comprehensive Overview of Telegram Services-A Case Study.” *International Journal of Case Studies in Business, IT, and Education* 6, no. 1 (2022): 288–301. doi:10.47992/IJCSBE.2581.6942.0165.

Treyger, E., J. Cheravitch, and R. Cohen. *Russian Disinformation Efforts on Social Media*. Santa Monica: RAND Corporation, 2022. doi:10.7249/RR4373.2.

”Ukraine’s Fusion of Cyber and Kinetic Warfare: Illia Vitiuk’s Stand Against Russian Cyber Operations | AFCEA International”, 15 September 2023. https://www.afcea.org/signal-media/test-signal-landing-page-format/ukraines-fusion-cyber-and-kinetic-warfare-illia.

Veiligheid, Ministerie van Justitie en. “Onderzoek naar telecommunicatie - MH17 vliegramp - Openbaar Ministerie” [Investigation.telecommunication – MH17 flight disaster]. Ministerie van Justitie en Veiligheid, 8 June 2020. https://www.om.nl/onderwerpen/mh17-vliegramp/vervolging-en-rechtszaak/zittingen-juni-2020/onderzoek-naar-telecommunicatie.

WarTranslated. “Can We Believe the Russian Phone Calls Intercepted and Published by Ukrainian SBU and GUR? • WarTranslated.” WarTranslated, 6 June 2022. https://wartranslated.com/can-we-believe-the-russian-phone-calls-intercepted-and-published-by-ukrainian-sbu-and-gur/.

את’צ. ‘פעילות יחידה 504 בלחימה [Unit 504 activity in combat]. Accessed 1 December 2023. https://www.idf.il/אתרי-יחידות/יומן-המלחמה/כל-הכתבות/הפצות/יחידה-504-אמן-אגף-המודיעין-חוקרים-לוחמים-עזה-רצועת-מלחמה-מחבלים-חקירות/.