Intercepted Phone Calls at the Russo-Ukrainian War: Cyberoperation or Propaganda Campaign?

Raimo Tapio Tikkanen

Master’s thesis
May 2024
Master's Degree Programme in Information Technology, Cyber Security

Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Tikkanen, Raimo

Intercepted Phone Calls at the Russo-Ukrainian War: Cyberoperation or Propaganda Campaign?

Jyväskylä: JAMK University of Applied Sciences, May 2024, 121 pages

Master's Degree Programme in Information Technology, Cyber Security. Masters's thesis.

Permission for open access publication: Yes

Language of publication: English

Abstract

Russo-Ukrainian war started in 2014 and escalated on 24.2.2022, when Russia invaded Ukraine. At the moment, the war is still ongoing. The war was fought on multiple fronts, information domain included. The Ukrainian military intelligence, GUR started to publish alleged intercepted cell phone calls between Russian personnel at 28.10.2022 and this activity did deviate greatly from normal publishing activity of official actor of such branch. From this viewpoint it was imperative to research this anomaly as a sample of information warfare conducted by other parties than Russia.

The anomaly was so interesting that it had to be researched from two different viewpoints, Cyber and information. Firstly, the content was allegedly obtained from intercepting and eavesdropping the mobile network communication. It was important to find out if this could have done technically and if Ukrainian national actor had been able to conduct such operation. Secondly, from the viewpoint of information, research was made to examine the content to find out if it was actually propaganda and what was the purpose of this alleged propaganda.

The study was implemented by using qualitative and quantitative methods, and by collecting a dataset of all published tweets between 28.10.2022-1.9.2023. The samples were quantified and analyzed using both statistical and qualitative methods.

It was found that the content was highly likely obtained with the means of cyber operation that was focused on eavesdropping and intercepting communication. The content itself was not found to be propaganda, but it was used as such. It was utilized in publishing operation that was highly organized. The operation itself was considered to support or to undermine both Russian and Ukrainian narrative from the viewpoint of strategic communication.

Keywords/tags (subjects)

Information warfare, propaganda, Russo-Ukrainian war, eavesdropping, mobile communication

Miscellaneous (Confidential information)

n/a

Tikkanen, Raimo

Siepatut puhelut Venäjän ja Ukrainan sodassa: kyberoperaatio vai propagandakampanja?

Jyväskylä: Jyväskylän ammattikorkeakoulu, Toukokuu 2024, 121 sivua

Master's Degree Programme in Information Technology, Cyber Security. Masters’s thesis.

VerkkoJulkaisulupa myönnetty: Kyllä

Julkaisun kieli: Englainti

Tiivistelmä

Venäjän ja Ukrainan välinen sota alkoi vuonna 2014 ja eskaloitui 24.2.2022 Venäjän hyökättyä Ukrainaan. Sotaa käydään edelleen tätä työtä kirjoitettaessa. Sotaa käydään monella rintamalla, informaatioavaruus mukaan luettuna. Ukrainan puolustusministeriön päädirektoraatti, GUR, alkoi julkaisemaan Twitter-tilillään sisältöjä, joiden väitetään olevan kaapattuja venäläisten puhelinkeskusteluja. Tällainen toiminta eroaa merkittävästi tämän tyyppisen toimijan tavan- ja tehtävänmukaisesta toiminnasta. Tämän informaatiovaikuttamisen ilmiön tarkastelu jostakin muusta kuin tavanomaisesta näkökulmasta nähtiin arvokkaaksi.

Ilmiötä tarkasteltiin sekä kyber- että informaatiovaikuttamisen näkökulmasta. Ensimmäiseksi, sisältö on väitetysti viestiliikennettä, jonka Ukraina on saanut haltuunsa kuuntelemalla ja kaappaamalla vastustajan viestiliikennettä. Tutkimuksellisesti oli tärkeää selvittää, onko tällainen toiminta teknisesti mahdollista laajuudessa Ukrainan toimesta siinä laajuudessa, kuin sitä väitetysti on toteutettu. Toisekseen haluttiin selvittää, onko sisältö tarkoituksellista propagandaa ja mitä sillä tavoitellaan Venäjän ja Ukrainan välisessä informaatiosodassa.

Tutkimuksessa hyödynnettiin laadullisia ja määrällisiä tutkimusmenetelmiä ja kerättiin Ukrainan puolustusministeriön tiedustelun päädirektoraatin aikavälillä 28.10.2022-1.9.2023 julkaisemista twiiteista aineistokokoelma, joka analysoitiin käyttäen laadullisia ja tilastollisia menetelmiä.

Tutkimuksen perusteella Ukrainan puolustusministeriön tiedustelun päädirektoraation julkaisema sisältö on aitoa ja on saatu menestyksekkäällä, pitkään jatkuneella mobiiliviestilikenteeseen kohdistuneella kyberoperaatiolla. Sisältö itsessään ei ole tarkoitettu propagandaksi, mutta sitä on hyödynnetty sellaisena. Ukrainan puolustusministeriön tiedustelun päädirektoraatin toteuttamaa pitkäkestoista julkaisuoperaation ei kuitenkaan nähdä olevan itsenäinen propagandakampanja, vaan sen arvioidaan olevan Ukrainan kansallista narratiivia vahvistava ja Venäjän vastaavaa, heikentävä tukitoiminne laajemmassa viitekehyksessä

Avainsanat (asiasanat)

Informaatiosota, propaganda, Venäjän-Ukrainan sota, salakuuntelu, mobiilikommunikaatio

Muut tiedot (Salassapidettävät liitteet)

n/a

Contents

Figures

Tables

LIST OF ABBREVIATIONS

1G	The first generation of mobile networking
2G	The second generation of mobile networking
3G	The third generation of mobile networking
4G	The first generation of mobile networking
5G	The fifth generation of mobile networking
A3	Encryption/authentication protocol
A5	Encryption/authentication protocol
A8	Encryption/authentication protocol
AuC	Authentication Center
BSC	Base Station Controller
BTS	Base Transceiver Station
CIA	Central Intelligence Agency
COMP128	Encryption/authentication algorithm
COMP128-2	Encryption/authentication algorithm
COMP128-3	Encryption/authentication algorithm
DPR	Donetsk People's Republic
EDGE	Enchanted Data Rates for GSM Evolution
EIR	Equipment Identity Register
Gb	Gigabyte
GPRS	General Packet Radio Service
GSM	Global System for Mobile communication
GUR	Main Directorate of Intelligence of the Ministry of Defence of Ukraine; *Головне управління розвідки Міністерства оборони України*
HD	High Definition
HLR	Home Location Register
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Station Identity
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ISIS	Islamic State in Iraq and Syria

Mb	Megabyte
MS	Mobile Station
MSISDN	Mobile Station International ISDN Number
MSRN	Mobile Station Roaming Number
NATO	North Atlantic Treaty Organization
NMT	Nordiska Mobiltelefongruppen, Nordic Mobile telephony network
NSA	National Security Agency
NSS	Network and Switching Subsystem
NYSE	New York Stock Exchange
OMC	Operation and Maintenance Center
OSS	Operation Subsystem
PSYOPS	Psychological Operations
RAT	Remote Access Trojan
RSS	Radio Subsystem
SBU	Security Service of Ukraine, *Служба безпеки України*
SIM	Subscriber Identification Module
SMS	Short Message Service
TMSI	Temporary Mobile Station Identity
VLR	Visitor Location Register
VPN	Virtual Private Network(ing)
WISDOM	Wireless System for Dynamic operating Mega Communications

1 Introduction

> *"Power is in tearing human minds to pieces and putting them together again in new shapes of your own choosing."* (George Orwell, 1984)

The Russo-Ukrainian war 2014-continuing escalated in February 2022, when Russia invaded to Ukraine. Russia has not admitted that there is a war, but its narrative has been that it is conducting a "Special Military Operation" since the 24.2.2022. Social media has been filled with audiovisual content direct from the battlefield and it has been used by both warring parties to promote or undermine the national narratives.

The strategic communication and the narratives that are created are especially important for any country, even in a time of peace. In strategic communication, cyberspace has an increasingly significant role (Lange-Ionatamshvili et al., 2015). At the time of war, national narratives of just cause, heroic actions and sacrifices of the people are the backbone of the work that helps the citizens of the country to support the efforts to win the war. Alternatively, one has to counter, or undermine the narrative of the enemy by proving that their cause is not just, their intentions are malicious, or otherwise illegal, and their narrative is untruthful. The concept of social cyber-attack has emerged and is gaining popularity (Lange-Ionatamshvil et al., 2015).

Social media has become a battlefront in warfare. Information has been weaponized and is utilized to change the "Hearts and minds" of public audience. The Russian invasion in the early 2022 has been monitored in real time over Youtube, Instagram and other significant social media platforms in a way that it could be treated as an alternative battleground. This could raise the question of how much of the content is delivered, produced, approved, and published by the national actor. This would also raise the question of how accurate and genuine a picture of the situation this information gives to the ordinary public. This is one of the main points of interest in this work.

Mobile devices have become an essential part of everyone's life. Even at the front lines of the war the soldier has some sort of mobile communication device with them. This has its advantages and its liabilities. For a soldier, a communication tool that can be used to communicate with loved ones and friends on the home front can have a mental health-improving and stress-reducing effect. On the other hand, a cell phone can also endanger the safety of a number of operations, if it is used irresponsibly or in violation of regulations. This is the second point of interest of this work. Throughout the invasion, allegedly intercepted cell phone conversations have been posted on social media channels, in which a Russian military personnel talk to the people at the home front. In this work, we want to examine whether this is technically possible, whether there are precedents for such activity, and whether this material is used for propaganda purposes. In addition, the research wants to examine whether it is possible to assess the correctness of the content based on empirical data.

This is a case study that examines the content of allegedly intercepted cell phone conversations published on the Twitter account of the Ukrainian military intelligence agency (GUR). From a research point of view, examining and researching the content of the account's publications is relevant because it does not fit the organization's actual mission. The primary purpose of military intelligence is to support the military commanders in the decision-making process (Connable 2012). Usually, the information and its sources are kept strictly confidential and secured tightly. In this case, Ukrainian military intelligence agency is acting against the norms. This raises a question if the scope of the military intelligence agency widened to the field of information warfare? Lange-IonaTamshvili, Svetoka and Geers (2015) have stated that in addition to affecting the communication and information systems of an enemy the cyber domain can be used as a method to conduct the operations to promote nations strategic narrative. The former includes the classical intelligence that is conducted at the cyber domain, and the latter might be the explanation to this case.

In this particular case we want to understand the phenomenon from different viewpoints. Firstly, we need to understand how interception and eavesdropping could be technically implemented. Secondly, we want to know If the actor has been conducting similar activities previously. Thirdly, we want to understand the reasons for the behavior of the actor through the purpose of the content that it is publishing. There is lots of studies, articles and research papers on Russian propaganda, information warfare and cyberoperations, but there is not much research done on the opposing side. The purpose of this study is to have a unique perspective on the usual and common approach to information warfare.

This case is researched goes from details to conclusions. Firstly, the basic technological solutions of mobile networking are presented. This includes the basic understanding of technology, architecture, and cybersecurity issues. Secondly, the study examines cases, events, and situations where cell phone communication has been compromised or the content has been breached. Thirdly, the collected content is analyzed from the perspective of propaganda. Finally, these themes are tied at the end and the conclusions are made from research question's viewpoint.

This study is structured in the following way: In this first chapter background is introduced and the justification and purpose of the study is presented. The methodology, research questions, data collection and ethical questions of the study are documented in the second chapter. The third chapter is dedicated to mobile networking. The basic architectural structure and technological background is presented among the possible attack vectors that could be used to eavesdropping the communication. The fourth chapter discusses the perspectives of strategic communication, information warfare and psychological operations, with the focus on propaganda. The fifth chapter introduces the most important actors from the point of view of the research. The empirical parts of the work are discussed in chapters six and seven. Chapter six examines the reported findings of wiretapping and eavesdropping conducted by Ukraine, and the seventh chapter analyzes the research material collected in the study. Chapter eight presents the answers to the research questions and the conclusions reached based on the research. The research is concluded with a discussion and an examination of the phenomena observed in the research in the ninth chapter.

2 Research methodology

This is a case study that has two separate viewpoints to the phenomenon that is researched. Firstly, the research examines the phenomenon from a technical point of view, where it is assessed whether the phenomenon is technically possible to implement. After this, it is assessed against historical observations whether the actor had the opportunity to produce the phenomenon. Finally, by looking at the content of the phenomenon, we evaluate what its purpose has been and if possible, why the phenomenon has been created.

Firstly, the research questions have to be formed. Those are documented at the first sub-chapter of this chapter. The multi-faceted approach to the researched phenomenon has to be considered while the questions are formed. Secondly, we will decide how we are going to find the answers to the questions we asked. We have to have scientifically sound methods to perform the research and to analyze the information that has been collected. The information and the findings that are deducted from it must lead to reasoned conclusions that lead to answers to research questions. Used methods are described and explained in the second sub-chapter. Thirdly, the scope and form of the dataset that must be planned. The dynamic nature of the data that is collected must be taken account for, while the dataset is planned and structured. The dataset and the collectable content are documented in the third sub-chapter.

Finally, the ethical aspects of this research and the ethics of this study are considered in the fourth sub-chapter. The nature and content of this research might bring us to situations where serious ethical considerations must be made. The last sub-chapter contains the common ethical principles, that every researcher must abide to be respected and qualified member of the scientific community.

2.1 Research questions

The main research question in this study is: "*Is it possible, that the private mobile phone communication published by the Ukrainian Intelligence agency at their twitter account be result of the successful cyberoperation or is it a propaganda campaign*?" The research question has to be approached from information and cyber domain. Firstly, when approaching the phenomenon from the cyberdomain, it is necessary to find out whether it is technically possible to capture and listen to mobile network communication. After this, it is necessary to find out whether the target has previous experience in the activity in question. Secondly, the research of the empirical material aims to find out whether the content can be interpreted as propaganda. In addition to this, by examining the material, we look at whether it is genuine intercepted and eavesdropped material or if it is fabricated or false content.

The first step in the study is to find out whether mobile network technology enables intercepting, decrypting, and eavesdropping of mobile communications. The first sub-research question "*Does mobile networking allow eavesdropping in a way that such content can be obtained.*" Should give an answer to this question. This requires an examination of mobile networking technology and architecture to see if vulnerabilities and opportunities for exploitation exist.

The second sub-research question “Is there evidence of such actions and if so, how have they been implemented ?” is answered by searching and familiarizing previously published cases. The cases in which the perpetrator has been a Ukrainian actor strengthen the assumption that the actor had the ability to conduct call interception and eavesdropping.

If eavesdropping is technically possible and the operator has been identified as having conducted such activities before, we can assess that the published material can be genuine from a technical point of view. When looking at previous cases referring to the phenomenon, it has to be observed how the events in question are timed to the case of the research topic. It is worth assessing that the closer in time the reported previous case is to the research case, the more likely it is that the Ukrainian actor is still capable of such activities.

Third sub-question will point to the actual content that the Ukrainian actor is publishing. If the content has features that are typical to propaganda, then it can be used for propagandistic purposes. This leads to the actual sub-question: “*Does the content have features of propaganda?*” If such features appear in the collected context, it would be concluded as propaganda.

The answer to the main research question requires deductive reasoning that is based on the findings and conclusions on the sub-questions. If the findings in all of those point to conclusions that there is technical method or methods to implement the activity, there is known cases in which such activities have been implemented and the findings in the collected content point to its propagandistic nature, it can be assumed that this case is actually propaganda campaign that is supported by cyberoperation. The structure of this study is visualized in figure 1.

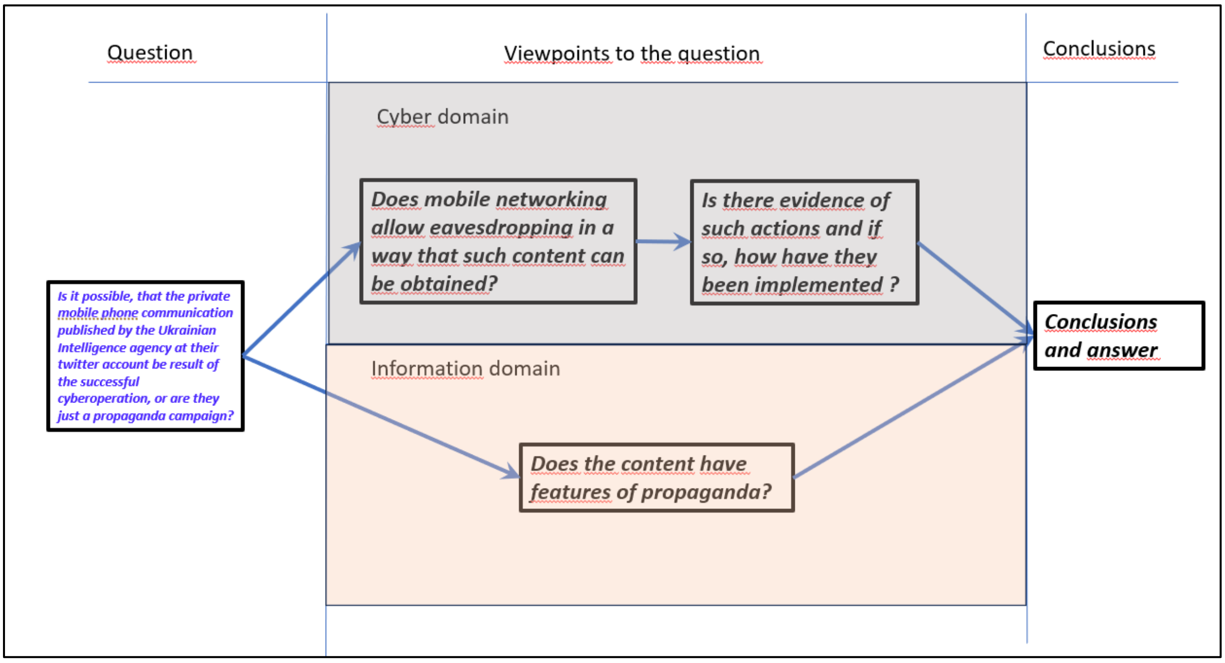

Question
Viewpoints to the question
Conclusions
Cyber domain
Is it possible, that the private mobile phone communication published by the Ukrainian Intelligence agency at their twitter account be result of the successful cyberoperation, or are they just a propaganda campaign?
Does mobile networking allow eavesdropping in a way that such content can be obtained?
Is there evidence of such actions and if so, how have they been implemented ?
Conclusions and answer
Information domain
Does the content have features of propaganda?

Figure 1. Structure of research questions.

2.2 Analysis and research methods

This is a case study. The case study is defined as a method that involves an examination of a specific event or phenomenon to get deeper knowledge and understanding when researched. Gerring (2004) defines case study as an intensive study of a case to understand a larger set of similar cases (p.342). The phenomenon that is researched is a typical target for case study. It has a clear and evident starting point; it has limited samples that are collected, and it is limited to certain actor and certain actions at the certain platform. The phenomenon started on 28.10.2022 and even if it is ongoing, the sampling can be ended at any given time when the dataset size is large enough. There is defined actor, Ukrainian military intelligence agency at its social media account. The actor has a regular action it performs that creates the sample for the dataset and the action is performed at the singular social media platform. For these reasons, this particular phenomenon is an ideal candidate for the selected method of research.

Methodically this thesis uses quantitative and qualitative content analysis. Content analysis in general is a research method that is used to analyze systematically various forms of communication (Krippendorff, 2018). The sub-research questions that need to be answered to conclude the primary question, “Is it possible, that the private mobile phone communication published by the Ukrainian Intelligence agency at their twitter account be result of the successful cyberoperation or is it a propaganda campaign?” need a different contextual approach with the selected method. This study uses both quantitative and qualitative content analysis method, because of the nature and complexity of research subjects.

The qualitative content analysis is used with the first two research sub-questions and the anomalistic samples that are collected when they are found while doing research for the third sub-question. The qualitative content analysis is defined as a category-based method of research in which the categories refer to aspects in the content (Mayring, 2019). According to that the method is suitable for categorizing the content that involves or clarifies the subject. Also, according to Mayring (2019) qualitative content analysis is text analytical driven in which context it answers the questions that were derived from the main research question. The main research question from this research line, the answer is deducted through the sub questions to which the method is applied. This also applies to anomalistic samples, which differ from the rest of the samples of the collected dataset.

The quantitative method of content analysis is used in analyzing the collected dataset for propagandistic elements. Kolbacher (2006) has defined quantitative method of content analysis as a type of evaluation of volume of occurrences in samples per category. The dataset is analyzed through thematic approach. The themes are selected, and variables are created in context of propaganda. The themes have been approached from the point of view of the narratives explained in chapter 4. In order to identify themes from the empirical research material, they have been divided into variables.

All the samples that are collected are quantified and the occurrences of selected variables are recorded. The overall quantitative numerical values that are extracted are analyzed by using planned and selected statistical analysis methods. The anomalistic samples that differ or are otherwise interesting in nature are analyzed with quantitative content analysis. In qualitative content analysis the phenomenon is researched as an independent event or anomaly in the thematic context (Vaismoradi, Turunen & Bondas, 2013).

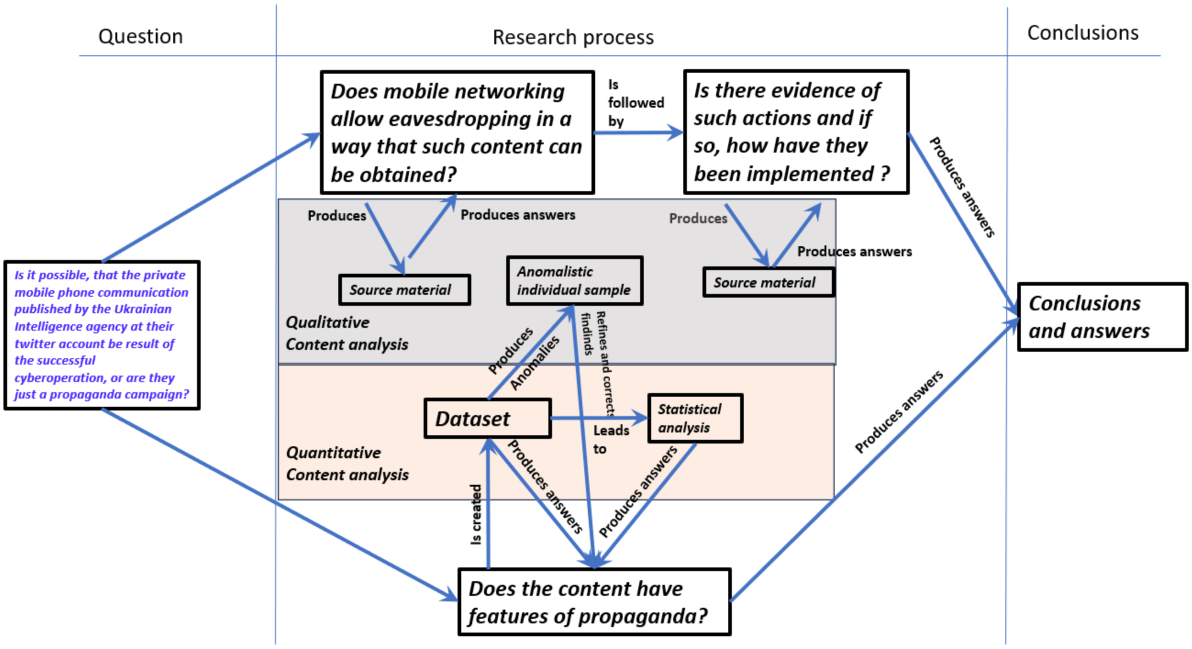

Question
Research process
Conclusions
Is it possible, that the private mobile phone communication published by the Ukrainian Intelligence agency at their twitter account be result of the successful cyberoperation, or are they just a propaganda campaign?
Does mobile networking allow eavesdropping in a way that such content can be obtained?
Is followed by
Is there evidence of such actions and if so, how have they been implemented ?
Produces
Produces answers
Produces
Produces answers
Source material
Anomalistic individual sample
Source material
Qualitative Content analysis
Produces Anomalies
Refines and corrects findinds
Dataset
Leads to
Statistical analysis
Quantitative Content analysis
Produces answers
Produces answers
Is created
Produces answers
Produces answers
Conclusions and answers
Does the content have features of propaganda?

Figure 2. The structure of the research process.

The study approaches the phenomenon from the viewpoint of two different domains. Firstly, the research for the Ukrainian state actor’s capability and means for eavesdropping and intercepting the content over mobile networking is evaluated. If those exists, the possible events in which Ukraine has been utilized such capabilities are searched. Secondly, the content that the actor has published is collected, and it is analyzed.

The research of technical capability begins by collecting information about mobile networking technology and its structure, architecture, and its vulnerabilities. After that use cases where vulnerabilities are exploited are collected and evaluated. In this part, scientific articles and other peer-reviewed material are preferred. The secondary sources are blog postings and other online material from respected and well-known specialists and experts.

After the approach from the viewpoint from cyber domain is completed and the understanding of the underlying technology and its vulnerabilities is built, the first actual subject-related research is conducted. The information about the cases where Ukrainians are reported to eavesdrop, intercept, and utilize the mobile network communication are collected. Collected material is analyzed using qualitative content analysis from the viewpoint of following questions: 1) How does the content describe the usage of the alleged intercepted content? 2) Does the material refer to the source from where the content is obtained? 3) Is there any, if all information of what method is or was used to obtain the alleged intercepted content?

The accuracy and validity of the data may vary significantly. Part of the material that is collected and researched concerning the findings about eavesdropping and intercepting mobile network communication is not from peer-reviewed or otherwise validated sources. After the analysis of the content, the findings are documented, and conclusions are made.

The second research line consists of the research of the allegedly intercepted and published content. The information is collected from the source and quantified by the rules that are set in chapter 2.4. The themes are structured in a way that the quantified content can be analyzed. The quantitative content analysis is used in this because the subjective element must be eliminated. According to Franzosi (2008) quantitative content analysis lacks the reliance on subjective assumptions, and it enables broader examination of content over extended periods. All of these claims apply to the collected data. The collected data in dataset is quantified with the categorized themes that either contradict the Russian or support Ukrainian narrative. After these different values are calculated and evaluated using different statistical methods, and from the results the findings are documented, and conclusions are made. The literal content of the samples in the collected dataset might not be accurate or truthful. The methods which are used to interpret the samples might give faulty or wrong results. In situations where more accurate sources can be used, should be used to validate the results.

2.3 The scope and limitations of the study

This study uses only public information and sources. Because of this, the quality and truthfulness of the information might vary. Only the alleged propaganda of Ukraine is examined, Russian counterpropaganda or response to the published content is not researched.

The technological approach is limited to explaining the basic information and the vulnerabilities and exploits that can permit the activities in scope of research questions. There is no intent to produce a deep technical understanding of mobile networking technologies. The exploitation of vulnerabilities that enable eavesdropping or decrypting intercepted communications are not examined at a deep technical level, but possible documented "proof – of -concept" are presented when possible. This applies also to the events and incidents that work as evidence of Ukraine's capability to apply such activities.

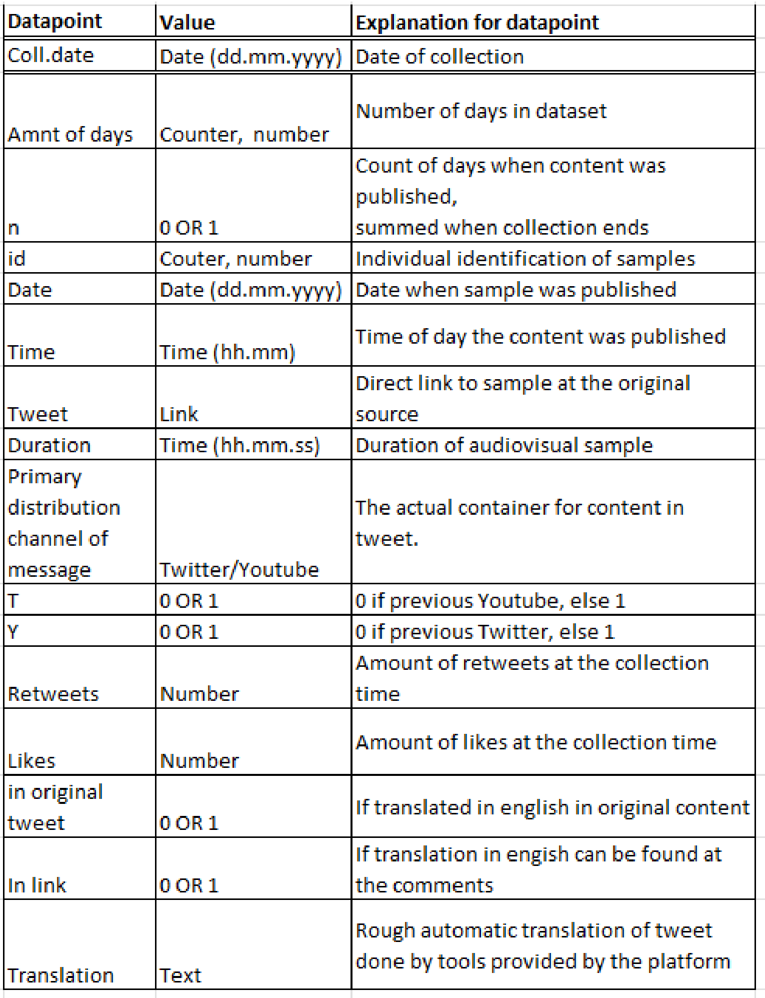
The samples of the dataset are not analyzed using technical methods, such as analyzers or other similar devices. The evaluation of the samples is based on possible phenomena that can be identified based on the content or the conclusions drawn from them. Content does not have any raw data, and it is processed with different methods that could affect the technical analysis. In quality research the samples are not translated with literal accuracy, because of the nature of this study.

The collection time of the dataset is limited to a given timeframe where the starting date is 28.10.2022 and ending day for collecting the data is 1.9.2023. The latter date is not included in the timeframe. No additional samples will be collected for analysis after that time.

2.4 The Dataset and collecting the data

The samples to the dataset are collected from the Twitter account of the Main Directorate of Intelligence of the Ministry of Defense of Ukraine, GUR. The first collected sample is from the 28.10.2022 and data collection ends to the sample or samples at 1.9.2023. The dataset will include all samples that meet the criteria. Sample must include: i) It must be published by the said Twitter account, ii) It must have audiovisual content that can be analyzed, iii) it has to fit to the set timeframe.

The dataset will be collected to the excel spreadsheet. The collected data will be described in figure 3 below.



Datapoint	Value	Explanation for datapoint
Coll.date	Date (dd.mm.yyyy)	Date of collection
Amnt of days	Counter, number	Number of days in dataset
n	0 OR 1	Count of days when content was published, summed when collection ends
id	Couter, number	Individual identification of samples
Date	Date (dd.mm.yyyy)	Date when sample was published
Time	Time (hh.mm)	Time of day the content was published
Tweet	Link	Direct link to sample at the original source
Duration	Time (hh.mm.ss)	Duration of audiovisual sample
Primary distribution channel of message	Twitter/Youtube	The actual container for content in tweet.
T	0 OR 1	0 if previous Youtube, else 1
Y	0 OR 1	0 if previous Twitter, else 1
Retweets	Number	Amount of retweets at the collection time
Likes	Number	Amount of likes at the collection time
in original tweet	0 OR 1	If translated in english in original content
In link	0 OR 1	If translation in engish can be found at the comments
Translation	Text	Rough automatic translation of tweet done by tools provided by the platform

Figure 3. Datapoints in the dataset

The dataset will include following values, that are counted from the actual data: date, when the sample has been collected (Coll.date), Sum of samples at the column (n), sum of samples at the support column (T) for column “Primary distribution channel of message”, sum of samples at the support column (Y) for column “Primary distribution channel of message”, sum of samples at the column “in original tweet”, and sum of samples at the column “in the link”. Other statistical or mathematical methods are not present at the main dataset table. When dataset is analyzed, the content is copied to another table and the modifications and adjustments are applied in these tables.

The audiovisual content is analyzed following the following procedure. The sample is examined individually visually to identify deviations and phenomena. Exceptional samples are marked to the dataset. The audio communication is listened to and transcribed using automatic tools and it is translated using the provided automatic translation tools. In case of translation does not appear to be clear or it can be assumed that the translation is wrong, the content is translated manually. The accuracy of the translation does not have to be literal, accuracy that allows the recognition of variables in translated communication is seen sufficient. Themes, variables, and justifications for their use can be found in chapter 7.

Because of the source the quality and reliability of the material is low. The collected data is dynamic, the value of the variables will be changing over time. The samples are not collected but linked to the dataset. Their dynamic nature causes certain variables to change over time. For these variables, the values have been determined at the time of collection and the aim is to keep their value small in the final analysis. The translations are not literally accurate. After careful consideration of the accuracy of the content it was not seen necessary. It was seen that translation and understanding the content should be done in such precision that the variables of the themes were found from the content. This accuracy would not require literal translation of the content.

It should be noted that the samples that are collected are dynamic in nature. The numerical values that are collected can change over time. The values that are in static dataset picture the situation at the collection time. This should be considered when evaluating the accuracy of the results of the findings and conclusions that are made based on these values.

2.5 Ethical considerations

This work is done by following the ethical guidelines set by the JAMK University of Applied Sciences and guidelines for research integrity set by Research ethics committee of Finland (Tutkimuseettinen neuvottelukunta).

This research is conducted by the author and by the author only. If any other person has helped the author to complete this research, they are mentioned as contributors in this thesis. When the other author’s ideas, texts or other intellectual properties are cited, they are credited, and the citations are made in a way that the reader can separate the cited information from the author’s own texts, ideas, and conclusions.

This research is conducted in a way that the good research practices are applied throughout the whole thesis. The research is conducted and the process through which the results are acquired is made as transparent and dependable as the author has been able to do. The researcher must not let one’s subjective views influence the research process, outcomes, findings, conclusions, or results, but one has to be objective and present them as objective as possible. In this particular study, objectivity has been applied throughout the whole research process with due diligence.

The research does not break any laws, rules, regulations. The research has been conducted in a way that human or civil rights have not been violated. The content of the samples that are collected from the social media platform, can violate the laws of certain countries, including Finland if it was collected by the researcher from the sources that it allegedly been collected. The researcher has not been involved in collecting said information in a way or from illegal sources. The information that has been used to create the dataset for the research is obtained from public sources and they have been in public reach, and they have been published by the third party.

The technical part of this research might point out weaknesses or vulnerabilities in certain technologies or in some products. The researcher will not promote or describe the methods in this work in a way that the reader would be able to exploit said weaknesses or vulnerabilities. The author does not document nor describe in this work any of such means that would allow or help others to utilize or participate in utilizing those.

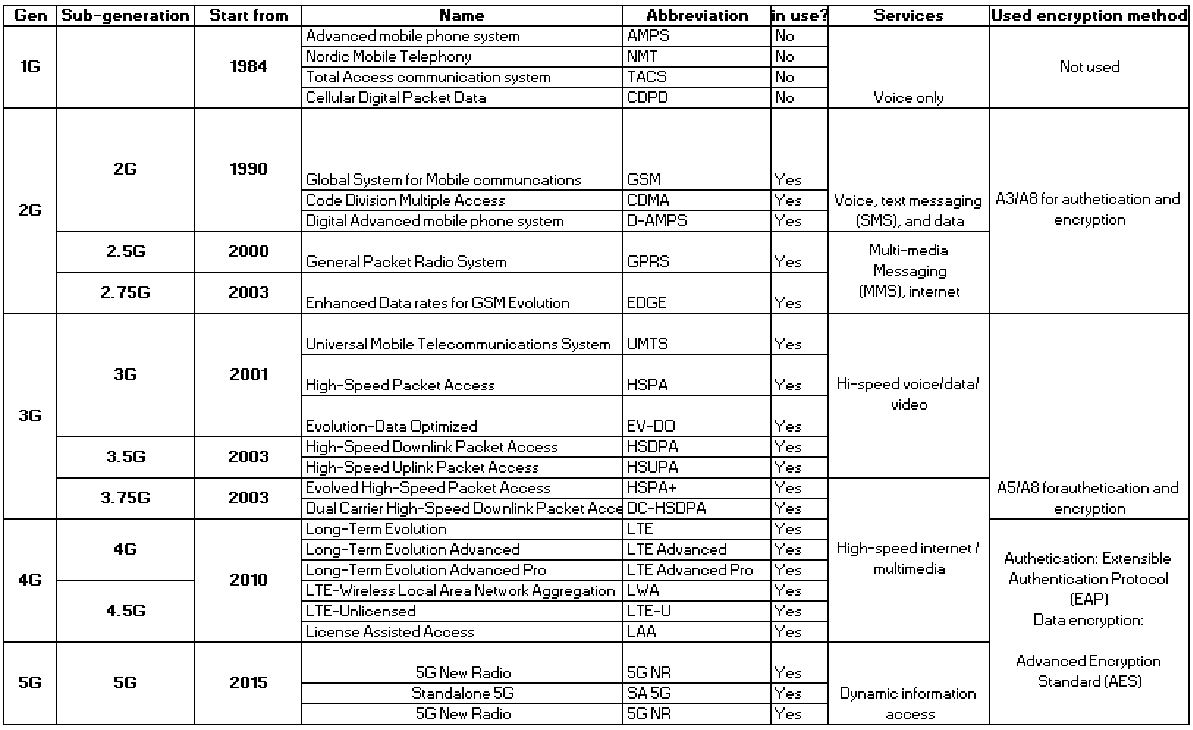
The samples that are collected contain hate speech, racial slurs, offending language, confessions of crimes and other elements that might offend common populace, or certain national groups. The content is processed and documented in such a way that the effect of the problematic content would cause as little harm as possible. The cases where such content has to be used, the usage must be thoroughly and transparently justified. In these cases, the problematic information must be presented in a way that the impact for the impacted audience is minimized.

The empirical information that is collected to this study is overseen in such a way that the content remains unaltered. Any adjustments and corrections are made in a way that they are retraceable, and the reader of this work can evaluate their effect to the actual data. The collected data is and will be available for any other researcher for reviewing, researching, and educational purposes. The author will deliver the information upon request to the other parties.

3 Mobile network communication

The first mobile networks were established and launched in the early 1980’s (Bakare & Bassey, 2021). There have been five major generations during the lifespan of mobile communication. According to Siau and Shen (2003) mobile networking provides the user mobility, reachability, localization, and personalization. Mobility is the most important feature that mobile networking provides. Users can use services, engage in activities, and obtain information from anywhere. Reachability means that the user can be accessible and can access anybody or any service at any time and from anywhere. The user can also limit one’s reachability. With localization, the user can obtain information of one’s location by using the services provided by the mobile device. The user is able to filter or tailor the services and the information in a way that is most suitable for him or her.

The mobile networking generation is defined as a change in technology, service or frequency band that is used with the device and the network (Sharma, 2013). There have been lesser evolutionary steps within major generations, which have been significant, have had enchantments to the basic structure of mobile networking, but have not been significant enough to create major change in generation. According to Dunnewijk and Hultén (2007) every generation has brought increased capacity and richer content to the subscribers. The different generations of mobile networking are presented in table 2 below.



Gen	Sub-generation	Start from	Name	Abbreviation	in use?	Services	Used encryption method
1G		1984	Advanced mobile phone system	AMPS	No	Voice only	Not used
			Nordic Mobile Telephony	NMT	No		
			Total Access communication system	TACS	No		
			Cellular Digital Packet Data	CDPD	No		
2G	2G	1990	Global System for Mobile communcations	GSM	Yes	Voice, text messaging (SMS), and data	A3/A8 for authetication and encryption
			Code Division Multiple Access	CDMA	Yes		
			Digital Advanced mobile phone system	D-AMPS	Yes		
	2.5G	2000	General Packet Radio System	GPRS	Yes	Multi-media Messaging (MMS), internet	
	2.75G	2003	Enhanced Data rates for GSM Evolution	EDGE	Yes		
3G	3G	2001	Universal Mobile Telecommunications System	UMTS	Yes	Hi-speed voice/data/ video	A5/A8 forauthetication and encryption
			High-Speed Packet Access	HSPA	Yes		
			Evolution-Data Optimized	EV-DO	Yes		
	3.5G	2003	High-Speed Downlink Packet Access	HSDPA	Yes		
			High-Speed Uplink Packet Access	HSUPA	Yes		
	3.75G	2003	Evolved High-Speed Packet Access	HSPA+	Yes	High-speed internet / multimedia	
			Dual Carrier High-Speed Downlink Packet Acce	DC-HSDPA	Yes		
4G	4G	2010	Long-Term Evolution	LTE	Yes		Authetication: Extensible Authentication Protocol (EAP) Data encryption: Advanced Encryption Standard (AES)
			Long-Term Evolution Advanced	LTE Advanced	Yes		
			Long-Term Evolution Advanced Pro	LTE Advanced Pro	Yes		
	4.5G		LTE-Wireless Local Area Network Aggregation	LWA	Yes		
			LTE-Unlicensed	LTE-U	Yes		
			License Assisted Access	LAA	Yes		
5G	5G	2015	5G New Radio	5G NR	Yes	Dynamic information access	
			Standalone 5G	SA 5G	Yes		
			5G New Radio	5G NR	Yes		

Sources:
(Kaur, Birla & Ahlawat, 2011)
(Salih, Zeebaree, Abdulraheem, Zebari & Ahmed, 2020).
(Tidke, Uttarwar, Dandwate & Tupe, 2020)
(Chen, Ji, & Zhang, 2013).

Table 1: Different generations of the mobile networking.

3.1 Architecture and structure of the mobile network

The purpose of the mobile network is to enable mobile communication and offer services for the subscriber. Mobile communication systems are divided into three subsystems: Radio subsystem(RSS), Network and Switching Subsystem (NSS), and Operation Subsystem (OSS) (Deuter, 2012). Simplified structure of the mobile communication network is shown in Figure 3 below.

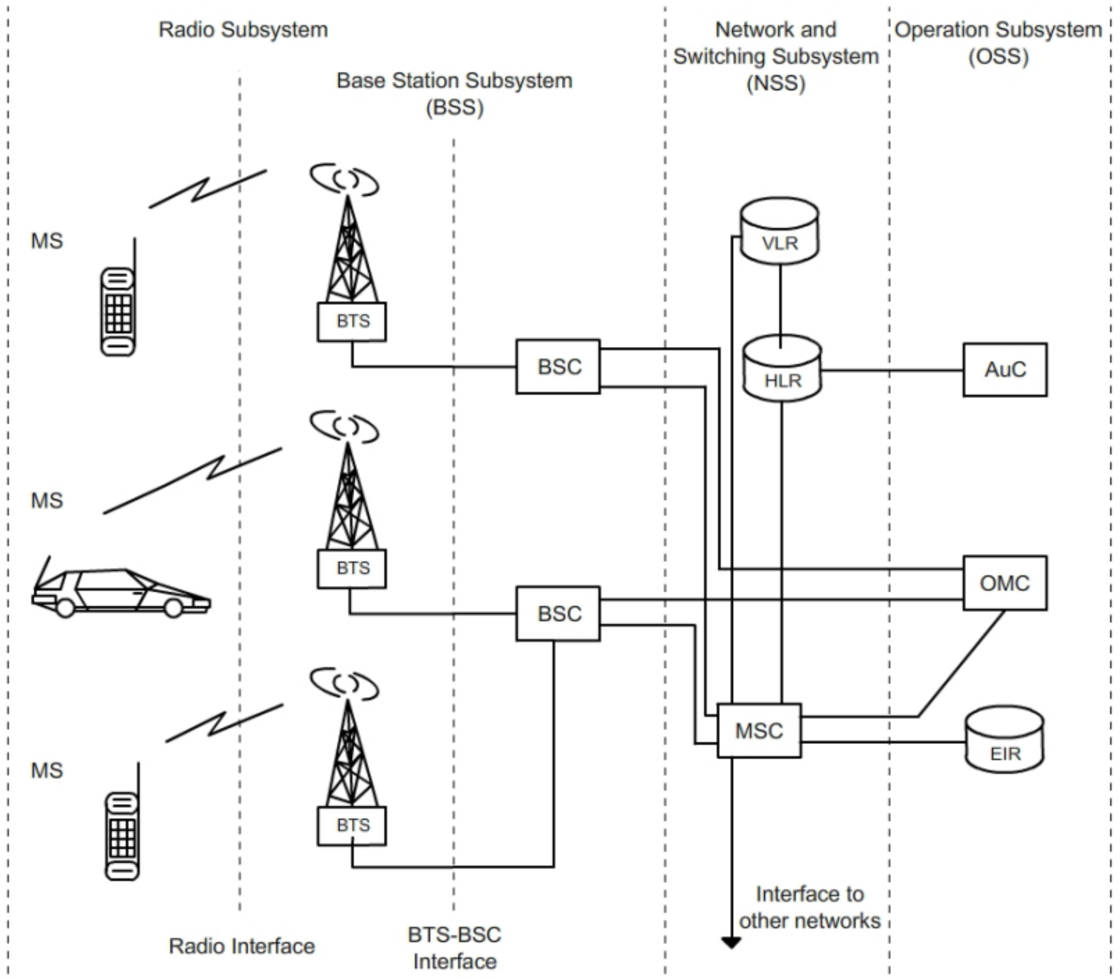

Radio Subsystem
Base Station Subsystem (BSS)
Network and Switching Subsystem (NSS)
Operation Subsystem (OSS)
MS
MS
MS
BTS
BTS
BTS
BSC
BSC
VLR
HLR
MSC
AuC
OMC
EIR
Interface to other networks
Radio Interface
BTS-BSC Interface

Figure 4. structure of mobile communication network (Deuter 2012).

The radio subsystem includes mobile stations and base station subsystem. The mobile station consists of two parts: Radio interface and subscriber identity module (SIM). The device and its software form a radio interface, and the subscriber identity module contains all subscriber-specific information. The radio interface, or users' physical device provides the contact to the mobile network while subscriber identity module serves as a tool for user to authenticate to the subscripted services at the mobile network. IMEI (International Mobile Equipment Identity) identifier is attached to the end user equipment's SIM (Subscriber Identification module) -card slot. IMEI-code is unique, and it is used to identify the device. While the mobile device is connected and operational at the mobile network, the following unique identifiers or numbers are assigned to it:

- International Mobile Station Identity (IMSI)
- Temporary Mobile Station Identity (TMSI)
- Mobile Station International ISDN Number (MSISDN)
- Mobile Station Roaming Number (MSRN)
- International Mobile Equipment identification number (IMEI)

International mobile station identity (IMSI) is unique 15-digit long number, which is provisioned to the users SIM-card, or in case of 4/5G mobile network, universal subscriber identity module (USIM). Temporary mobile station identity (TMSI) is used instead of IMSI to secure user's information's confidentiality and is periodically changed (Deuter 2012). TMSI is assigned to the mobile user by the current visitor location register (VLR) to witch the user is registered. Usage of TMSI is implemented to prevent the allocation of the particular mobile subscriber for potential eavesdroppers.

Mobile station international ISDN number (MSISDN) is user's known telephone number. It consists of country code, national destination code and subscriber number (Rahnema, 1993). Mobile station roaming number (MSRN) is obtained from the home location registry (HLR) and its composition follows the structure of the MSISDN (Rahnema, 1993). MSRN is used to route the call to the subscriber by the visitor location register to which said subscriber is currently assigned (Rao, Oliver, Holtmanns & Aura. 2016). The MSRN is sent to the user's home location registry (HLR) either on location update or on a call basis. International Mobile equipment identification number

(IMEI) identifies used mobile device (Singh, Bhargava, & Kain, 2007). IMEI is used to validate the access rights for the device connected to the mobile network.

Base station subsystem (BSS) of the radio station subsystem includes base transceiver station(s) (BTS) and base station controller (BSC). BTS is an element in the subsystem responsible for transmitting and receiving the transmission and processing the signal (Deuter, 2012). The connection between user equipment and mobile network is established after the user and the device that is used are identified. This validity is frequently checked by the mobile network.

Validity of subscription is implemented, and the connection is maintained with the TMSI or IMSI identifier. IMSI is used if the mobile network loses the TMSI for some reason (Rao et al., 2023; Norrman, Näslund & Dubrova, 2016). The communication between the user equipment and BTS is encrypted since the second generation of GSM mobile communication.

BSC controls and manages the radio interface. It oversees reservation and disengaging of radio channels and user's handover to another BSC (Deuter 2012). The handover takes place when the call must be moved from one mobile network cell to another. The BSC ensures that this happens without interruptions to the call (Deuter, 2012). One BSC can manage several base transceiver stations simultaneously.

Network and Switching Subsystem (NSS) produces to the mobile network its transition network (Deuter, 2012). It consists of a mobile service switching center (MSC), the home location register (HLR), and visitor location register (VLR).

MSC is a digital switching center, and it performs switching and management operations to the network. MSC also connects the mobile network to the regular wired network and coordinates subscriber's handover between base station subsystems (Rahmani, 1993). In addition, it offers different services to the mobile subscribers, for example call forwarding, call barring, teleconferences and charging the subscribers.

Home location registry (HLR) is a database, where all information of the mobile subscriber is stored (Deuter, 2012). It contains permanent data, for example the subscribers phone number

(MSISDN) and temporary data, for example the information for the subscriber’s current location (MSRN). Visitor location registry (VLR) contains a copy of the necessary information of the contents of the HLR. VLR is used as a storage of the information about the mobile subscribers that are located within the service responsibility area of the mobile service switching center to which the VLR is connected (Deuter, 2012). In addition, VLR controls the roaming numbers. Roaming numbers are the subscribers that are not at the area of their home location registry (HLR) but at the area of the said VLR.

Operation Subsystem (OSS) oversees and manages the subscriber administration (Deuter, 2012). OSS functions that provide monitoring, control, and intervention options for the network operator. The operation and maintenance center (OMC) is a controlling element for other network elements in the other subsystems of the structure. It collects and calculates statistics of the status and utilization of the elements of the subsystems.

The authentication center (AuC) contains all the information which serves the protection of subscriber identity (Deuter, 2012). AuC provides an authentication service to the radio interface to prevent eavesdropping. The authentication algorithm and encryption key that are used to authenticate the subscriber, are stored at the AuC. The equipment identity register (EIR) functions as a central database for device identification information. It stores the International mobile equipment identities (IMEI) that are unique identifiers for the user equipment (Deuter 2012). The IMEI’s are sorted to three different lists: White, gray, and black. Whitelist contains the IMEI identifiers of the valid user equipment, grey list contains IMEI’s for equipment that are not eligible to utilize all available services and blacklist contains all the IMEI’s for equipment that are stolen or otherwise blocked to use the mobile network.

3.2 The mobile network generations and the elements of security

While the basic structure of the mobile networks has stayed fairly stable and unchanged over time, security features, technology, and service portfolio that is provided to the user have been evolving greatly. This has been affecting used bandwidth, data transfer speeds and the variety of services that are provided.

1G, the first-generation mobile communications standard was used at the first analogue cell phone networks and there were no encryption methods used. First commercial 1G network was established and launched in Tokyo, Japan (Bakare & Bassey, 2021). The first-generation mobile networking presented call handover and roaming capabilities, but the cellular networks did not offer calling services between countries. The 1G technology is obsolete, and it is no longer used.

2G is the second generation of mobile communication. The first commercial, GSM-standards based network was launched in Finland in 1991 (Bakare & Bassey, 2021). The network offered low-bit-rate data services among the speech services. Main difference to the 1G networking that the 2G was circuit-switched and fully digital system (Pereira & Sousa, 2004). Another significant difference compared to former generation was that the communication between user and the base transceiver station was encrypted. Two encryption protocols, A3, and A8 were defined and presented at second generation mobile networking (Toorani & Beheshti, 2008). This enabled encrypted communication and safe user authentication when using 2G mobile communication. The protocols were based on COMP128 algorithms.

Subscriber identity module (SIM) was presented at second generation mobile networking (Deuter, 2012). The module is installed to the mobile device at its identified slot, and it manages the identification of the subscriber when the device is powered up and it connects to the network. SIM card stores and contains all needed information for user to connect to the network (Deuter, 2012).

2.5G was the minor generation change of the mobile communication network. The difference between standards was the used network technology. The 2.5G used General Packet Radio Service (GPRS) and Enchanted Data Rates for GSM Evolution (EDGE) technologies instead of legacy, second generation GSM-networks (Toorani & Besheti, 2008; Deuter 2012). Encryption technology remained the same as in second generation products, but the algorithms were developed to use enhanced versions of COMP128 (COMP128-2 and COMP128-3) algorithms.

2.75G was the minor update to major 2G generation. The security features remained unchanged from the previous version. Main difference to the 2.5G version of mobile networking was the enhanced transmission capacity to EDGE-technology (Lamba, Yadav & Devi, 2012).

3G was presented in the year 2000 and it enhanced the reliability and the data transfer speed of mobile networking. Its transmission system and protocols supported data transmission rates up to 2Mbs (Salih, Zeebaree, Abdulraheem, Zebari, Sadeeq & Ahmed, 2020). The wider bandwidth enabled the usage of web-based applications, streaming multimedia, and video conferencing. 3G brought the BTS authentication to the mobile networking (Eshelman, 2020). At the second generation of mobile networking, only the mobile subscriber authenticated the network and trusted that the BTS was authentic base station, which belonged to the actual mobile network. From the 3G on, the BTS was to authenticate itself to the subscriber and to the network and this enhanced the overall security of the mobile networking.

Subscribe identification module was replaced by universal subscriber identity module (USIM). It enhanced the security of confidentiality of user identity and user data, enabled mutual authentication, and provided integrity of user data (Kim, 2007). A3 protocol was replaced with A5 protocol, which provided enhanced security to mobile networking (Toorani & Beheshti, 2008).

With 3.5G, the data transfer speed with 3G connections increased to 14Mt/sec (Lamaba, Yadav & Devi, 2012). This made it possible to use internet, TV and video calls on a mobile device. 3.75G of mobile networking enhanced transmission speeds even further but brought no other essential upgrades.

4G did enhance the transmission rates even further, up to 100Mbs (Salim et. al., 2020). The wider bandwidth and high-speed internet access enabled gaming, HD recording, both video and audio and High-quality video conferencing. Most important enhancement with the 4G mobile network was the transition to use IP-core networking, which allowed the usage of IP-based protocols (Ahmadpanah, Chashmi & Yadollahi, 2016). Previous generations were using closed systems and mobile network dedicated protocols and standards, which made entering mobile network business challenging.

5G did enhance the transmission speeds even further, to 25Mbs with the bandwidth of 1Gbs (Salim et. al., 2020). Also, other enhancements were reduced latency, the support for massive number of simultaneous devices and reduced energy consumption. Fifth generation networks utilize 4G networks and the “Wireless System for Dynamic operating Mega Communications (WISDOM)”- conceptual networking (Salim et. al., 2020). Enhancement for the security is that 5G allows virtual private networking, VPN, usage.

3.3 Known weaknesses in mobile networking

The encryption and key generation algorithms are weak and can be cracked at the 2nd and 3rd generation mobile networks. The vulnerabilities of the A3/A5/A8 algorithms are based on the weaknesses that are found from the COMP128 algorithm. A3 is used to authenticate the device to the network, A5 is used to generate the random key and A8 encrypts the transmission (Ali, Roble, Shire & Mahamud, 2016). COMP128 algorithm was secretly by GSM association (Strobel, 2007; Toorani & Behesti, 2008). There are documented methods to crack the older encryption and key generation algorithms A3, A5 and A8 efficiently. The weaknesses in the algorithms might allow the attacker to reveal the user’s individual authentication key which is stored at the user’s SIM-card and at the users home networks authentication center (Toorani & Behesti, 2008).

The unilateral authentication was used in 2G (Deuter, 2012). Every user authenticated to the network, but the BTS was not authenticated to user. This allows the attacker conduct “man-in-the-middle” attack and eavesdrop the communication. Since the third generation, bilateral authentication has been implemented in the mobile network, where authentication is also required from the base station.

The communication is encrypted between the mobile device and the base transceiver station by default (Strobel, 2007; Toorani & Besheti, 2008; Deuter 2012). The transmission from there on to the receiver encryption is optional and service provider dependent. This can be used if the attacker has access to other parts of the network that are behind the BTS.

The architecture to every generation is backwards compatible to the second-generation level. This means, that all generation devices have to be able to connect with previous architecture, and therefore the vulnerabilities from the previous generations are available even to newest devices for attacker to exploit. For example, attacker can use different denial of service- attacks to prevent user to access 4/5G network thus forcing the connection to less secure 2/3G network (Shaik, Borgaonkar, Asokan, Niemi, & Seilfert, 2015). Method for such attack was presented in HITB2016AMS conference in 2016 (Huang, 2016).

3.4 The attack vectors of eavesdropping against mobile networks

Dayyani (2016) states, that eavesdropping is illegal listening to conversations and even recording them (p. 30). Eavesdropping and intercepting communication can be lawful or illegal, depending on the purpose and the actor that is conducting such activities. Some governments use eavesdropping as a way of surveillance (Curran, Breslin, McLaughlin & Tracey, 2007). Eavesdropping is legal in multiple countries even without the consent of the party that is eavesdropped and whose communication is intercepted. In most countries eavesdropping is illegal if it is performed without the court order or if it is performed by an unauthorized actor without the consent of the target of the activity. The national security actor can implement legal interception and eavesdropping if it is needed for national security or in criminal investigation (Han, Yeun & Kim, 2009).

There are four vectors that can allow the third party to eavesdrop and to intercept communications. Firstly, the mobile devices of one or both users are infected by malware, and a third party is thereby able to listen and record their communication. Secondly, the transmission can be intercepted between the mobile station and base transceiver station. Thirdly, the hostile actor may have taken control of base station subsystem or parts of it and is able to perform eavesdropping. Lastly, communication can be intercepted and eavesdropped on at the core- or backbone-network.

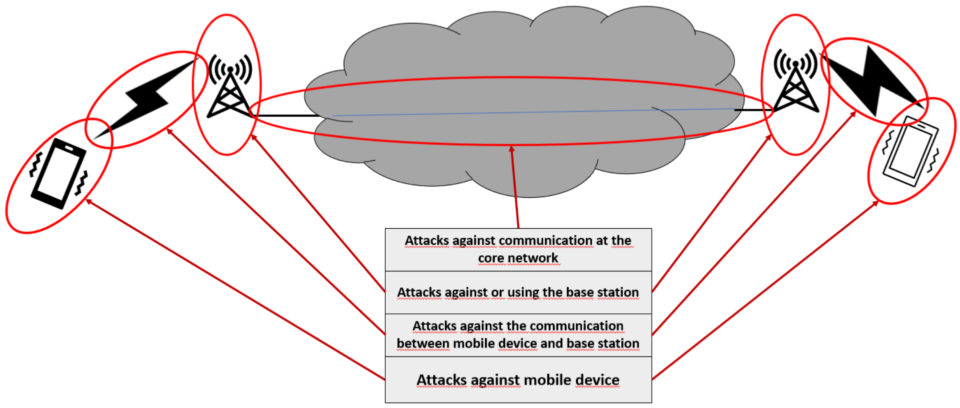

Attacks against communication at the core network
Attacks against or using the base station
Attacks against the communication between mobile device and base station
Attacks against mobile device

Figure 5. Attack vectors for eavesdropping and intercepting communication

Attacks against mobile device

Mobile device can be infected with malicious software, which enables eavesdropping. Malware can be installed to the victim’s mobile device and that can be used to eavesdrop and record victim’s calls. For example, remote access trojan (RAT) is such tool for eavesdropping the communication. RAT is a) is malware an attacker uses to gain full administrative privileges and remote control of a target device (Yasar, 2022). RAT is often downloaded from the malicious website or is sent as an attachment to the phishing e-mail.

RAT can also be delivered to the target device as a payload using different worms or exploit kits, which use exploit that utilizes vulnerabilities at the target device. Well known sample of usage of such malware is Pegasus, which is product of Israel- based company, NSO-group. It is known to been utilized in both legitimate and criminal purposes. Marczak and others (2018) listed forty-five documented instances where the malware was used. Also, they presented three cases, where national actors had utilized several remote access trojans to obtain personal information of their own citizens.

User's SIM – card is vulnerable for different attacks if it falls into the hands of malicious actor. It can be cloned, and the content of it could be used by malicious actor to use it as it was the original SIM – card (He & Paar, 2007). This method of attack requires the attacker to have physical access to the SIM card. This attack method is mitigated on the later generations of mobile networking from 3G and beyond. USIM mitigates the weaknesses of the previous subscriber identification module, but it is not completely immune to identity attacks (Singh, Ruhl & Lindskog, 2013).

Attacks against the communication between mobile device and base station

The communication between the mobile device and the BTS is encrypted by default at the mobile networking technology, with the exception of the first-generation mobile networks. This, on the other hand, does not prevent it from getting intercepted. As it was explained earlier, the encryption methods at the 2nd and 3rd generation mobile networking are insecure, and there are documented methods to decrypt them. The interception can be divided into two different methods, active and passive (Sustek, Oplustil, Tomasek, & Urdenicek, 2016). In passive method the attacker listens to the traffic at the certain mobile networking cell and intercepts the communication between the mobile device and the BTS. Passive method is difficult to notice by the network, or by the subscriber, because the monitoring gives no indication for either of them. Communication interdiction and eavesdropping requires the capability to decrypt the traffic. This is a feasible method for the older 2G and 3G technologies.

The encryption and key generation algorithms are weak and can be cracked at the 2nd and 3rd generation mobile networks. There are documented methods to crack the older encryption and key generation algorithms A3, A5 and A8 efficiently. Toorani and Behesti (2008) described a method in which the algorithm became 1024 times weaker than and vulnerable for attacks against the system. Dunkelman, Keller, and Shamir (2010) documented and described a practical attack against A3/A5 cryptosystem. It allows the attacker to solve the encryption key in 50% of test cases that they applied. The attack does not directly crack the key, but it reduces the complexity of the encryption key from the 276 to more manageable 232 combinations of the used key. Cattaneo, De Maio & Petrillo (2013) presented five passive attacks that can be used against the A5/1 algorithms and are able to extract the key from the connection and to encrypt the communication in real-time.

Singh, Bhargava, and Kain (2007) described numerous examples of successful methods of bypassing and cracking mentioned algorithms. The A8 algorithm, which generates the encryption key was found to be deliberately weakened (Singh et al., 2007). They also claimed that the communication that was encrypted using A3 algorithm could be deciphered in milliseconds. The vulnerability was caused by the encryption algorithm COMP128 to which the A3 and A8 were based on.

For example, the National Security Agency, NSA is known to intercept the signal from the mobile device and use it, at least to locate high value targets for operations (Scahill & Greenwald, 2014). Horváth (2016) claimed that France and Italy practiced signal intelligence against Russian cell phones and combat net radio traffic in 2014 from the Black Sea area during the occupation of Crimea. The equipment used to intercept radio frequency traffic is not limited to military usage. According to Weinbaum, Berner and McClintock (2017) such equipment can be acquired legally from the open market.

Attacks against the base transceiver station (BTS)

Base transceiver station creates the interface for the mobile device to the mobile network. This can be used in eavesdropping or intercepting user’s communication. As stated before, the communication between mobile device and BTS is encrypted, but the encryption at the BTS and beyond that is optional (Strobel, 2007).

BTS can be faked, and the mobile device can be lured to connect to it. The man- in-the-middle attack can be performed by impersonating BTS to the victim and victim to the network at the same time (Meyer & Wetzel, 2004; Eshelman, 2020). This can be applied by using specific equipment. IMSI-catchers can be used in “Man in the middle” – attacks against mobile network users. IMSI catcher is used to imitate Base transceiver station (BTS). In pre- 3G mobile networking architecture it exploits one-side authentication and masquerades itself to mobile station as a base station (Strobel, 2007). In 4G and 5G mobile networking architectures IMSI-catchers can be used at least to obtain mobile subscribers International Mobile Subscriber Identity and the location information of the mobile subscriber(Mjølsnes & Olimid, 2017).

Attacks against the core network

The IPX networks that use signaling system no. 7 (SS7) protocol stack are prone to certain kind of SS7 message application part attacks (Holtman & Singh, 2018). This allows attacker to track location of mobile device, to eavesdrop, to intercept users SMS-messages, to apply denial-of-service attack, to hijack data session, to unblock stolen phone, to apply password theft and with that take over users accounts in numerous services. Göker (2022) suggests that intelligence agencies prefer to use such method to gather intelligence, including eavesdropping the communication and intercepting SMS-messages where other means are not eligible to obtain such information. The weaknesses of the protocol were used against the clients of Spanish teleoperator O2 and because of this, the hackers got their credentials for their bank accounts (Thomson 2017).

National security officials can legally intercept and eavesdrop the communication in the national communication networks. The level and difficulty of these actions varies according to national legislation and situation, in which the nation is, for example, the network operators are enforced to allow the national security officials to decrypt and intercept the telecommunication and internet traffic by certain people or groups if they endanger the national security or pose a terroristic threat and use the network data to locate possible criminals if court gives the permission to do so. According to Dempsey (1997) law in United States of America allows wiretapping and eavesdropping without informing the target of surveillance if the target is suspected to work for foreign nation or is suspected to be a foreign agent.

4 Propaganda

Propaganda is communication that is aimed to influence the attitudes, opinions, and behavior of the target audience. Propaganda aims to strengthen one’s own and to weaken the opposing viewpoint by exploiting fears, hopes and expectations (Bearnays, 1928). Different channels of communication are used in propaganda to evoke the wanted reaction from the target audience. Propaganda is not solely used as a tool of war, but also within politics, economics and commercially to influence the population’s attitudes, opinions, or behavior.

The modern viewpoint to propaganda was defined and presented by Edvard Bearnays (1928) and Walter Lippman (1922). Bearnays (1928) defined propaganda as a purposeful means of strategic communication. He saw it as a neutral tool that could be used to achieve either positive or negative objectives. The purpose of the propaganda is to influence people’s opinions and their behavior to achieve the preferred goals of the propagandist. Propaganda is used to manipulate feelings, to create different associations between objects, objectives, or other items by using expertise and networks (Bearnays, 1928).

Lippman (1922) saw that propaganda involves spreading information and its influence on common opinion. According to him, propaganda tries purposefully to guide people to think and behave in favor to preferred viewpoint or agenda. Propaganda is using different methods of communication, including selected and manipulated information, rhetorical means, and strong emotional messages (Lippman 1922). Main difference between the approaches of Bearnays (1928) and Lippman (1922) is that while Bearnays visioned the propaganda as a tool for reaching both positive and negative results, Lippman (1922) saw propaganda as a malevolent method of influencing the common population.

Ross (2002) has defined propaganda as a model that has four components: The propaganda has a message, has intention to persuade, has a significant target audience and is applied by the or behalf of a political institution, organization, or cause. According to her, message is manipulative in nature, appeals to target’s emotions and in most cases, is based on lies. The propaganda's purpose is to make the target audience have strong emotions and emotional response towards the cause the sender targets.

Laskin (2019) claims that people are constantly targeted with propaganda messages. According to him, propaganda is an essential component of building nations, communities, and business enterprises. From the psychological viewpoint Laskin (2019) sees propaganda as a tool to dissolve individuality and to unite the people into unified, similarly thinking groups. From this we can conclude that the propaganda aims to create a reason for a person to perform actions or have an opinion that is not directly benefiting oneself. Propaganda must wake both positive and negative emotions to be successful (Laskin, 2019).

Onuh (2010) suggested that propaganda was systematic style of spreading information, idea, or belief to manipulate people's opinions or attitudes for general or selfish interest. The purpose of the propaganda is to manipulate, instead of influencing the target audience. This viewpoint does not have focus on communication but in the contents of the communication.

Taylor (2013) has been studying propaganda from the viewpoint of warfighting and conflict between the nation states. According to him, propaganda is defined as something that is a deliberate attempt to persuade people to think and behave in a desired way (p. 6). Communication is used to spread the idea or opinion to the public to affect them in a way that it favors the propagandist. From the viewpoint of conflict, propaganda is used to enhance and support the people's will to fight and the efforts of war.

Propagandistic message can be white, black, or gray. According to Rusu and Herman (2018) white propaganda comes from the source that is known, when in black propaganda the source is unknown and in grey propaganda the source can be partly either. Also, according to them, the message can be based on truth in white propaganda or can be untruthful in black and in gray it can or may not be based on truth.

4.1 Propaganda and psychological operations (PSYOPS)

Psychological dimension and psychological aspect are present in every conflict (Narula, 2004). The decisions that leadership is making are based on all information that is available ,and on the point of view through which the information is interpreted. Psychological operations use information to affect enemy reasoning process, and through this, to its decision-making process (Narula, 2004). Rumors, misinformation, information manipulation, and stereotyping are used in psychological operations (Saran, 2016). The attacker conducts psychological operation to affect the audiences attitudes and opinions with suitable information and propaganda. The message is spread through different channels to receivers determinately and continuously until the wanted outcome has been reached.

Wallenius and Nilsson (2019) define psychological operations (PSYOPS) as an attempt to influence public opinion in the issue whereas the operation is targeted. The purpose of PSYOP is to influence people's perceptions, attitudes, emotions, motives, objective reasoning, behavior, and decisions in a way that is favorable to the one that is conducting the operation.

Propaganda can be seen as a fundamental tool of psychological operations. If psychological operations are examined from the viewpoint of Wallenius and Nilsson (2019) and is compared to Taylor's (2013) definition of propaganda, propaganda perfectly supports the aims of psychological operations. Propaganda, in general by its different definitions, is a tool to influence people's opinions, viewpoints, and decisions psychologically in a way that they meet the goals of the propagandist.

4.2 Strategic communication, narratives, and propaganda

Strategic communication can be understood as strategic narrative (Schmitt, 2018). In this interpretation the narrative describes the actor to the surrounding audience. The strategic communication, or strategic narrative attends to legitimate the actions of the actor to the audience and to gain their support (Aspiriadis, 2023). According to Eder (2007), strategic communication means massing information among all agents of public information at a critical time and place to accomplish a specific objective. The purpose of this is to prevent destructive effect of conflicting information and otherwise mixed messages.

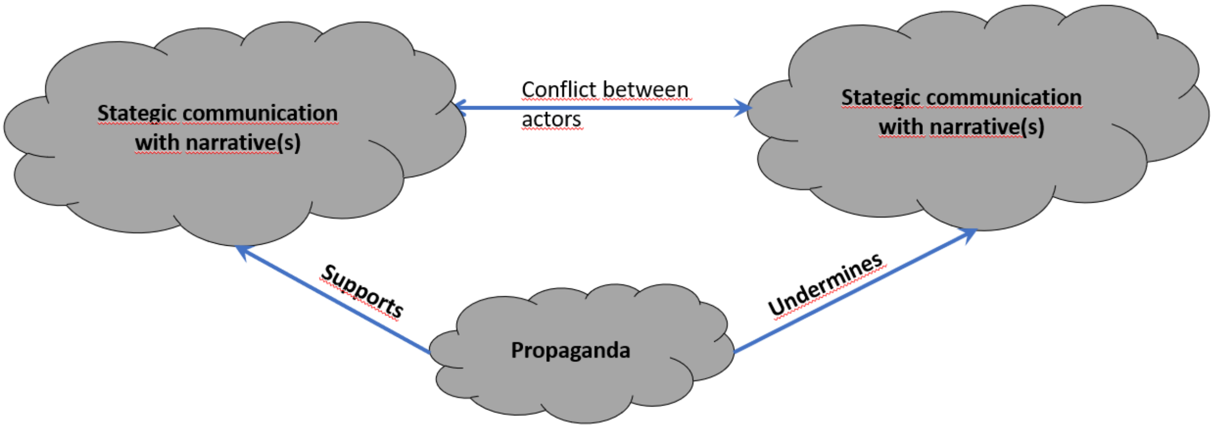

Stategic communication with narrative(s)
Conflict between actors
Stategic communication with narrative(s)
Supports
Undermines
Propaganda

Figure 6. Relationship between strategic communication and propaganda

The propaganda can be used in strategic communication to support the favorable narrative or to undermine the advisory's narrative. As an example of this, Russia used propaganda as a tool to strengthen its narrative to justify the occupation of Crimea and to mitigate the reaction of the western world at 2014 (Schmitt, 2018). In this particular case the propaganda was used to support the national narrative and to confuse others. The clash of narratives that is supported by propaganda can be recognized at the Russo-Ukrainian war, where Russian anti-Ukrainian narrative is countered by the Ukrainian anti-Russian narrative (Szostek, 2017).

Successful usage of propaganda is to transform and change strategic communication in a way that the narrative can change completely to different path. Before year 2014 and Euromaidan protests the Russian opinion towards Ukraine were mostly positive. After the protests after which the pro-western government got into power, the Russian narrative of Ukraine changed from fraternal relations to anti-Russian rhetoric (Khaldarova, 2021). The incidents without any evidence were published and communicated by and in Russian media platforms. The refugees who escaped fighting at the Donetsk-region to Russia were described as escapee's from Ukrainian nazi-regime (Khaldarova, 2021). The pro-Ukrainian habitants that participated in fighting against unlawful leadership of so-called "Donetsk Peoples Republic, DPR" were portrayed as "rebels" by the Russian national news channels. According to Khaldarova (2021) the narrative that was describing Ukrainians as "little brothers" before 2014, was successfully changed to portray Ukraine as "enemy of Russia".

The narrative of "denazifying" and "demilitarization" of Ukrainian state to prevent the atrocities that Ukrainian Nazis have conducted to the Russian minority in Ukraine narrative was used by Russian leadership when Russia invaded Ukraine in 24.2.2022 (Treissman, 2022). Also, term "war" was not used, but it was marketed as a "special military operation" to make the invasion to seem less intimidating for common citizen of Russia. Other pro-Russia narratives that Russia has used are Ukraine has staged the war, discrediting Ukrainian leadership, NATO's involvement in the fighting, and the Russian army is winning at Ukraine (Kienneman, 2023). The Russian army is winning the war narrative is supported by the "Second army in the world"-narrative that has been distributed by the official Russian channels (Topalskyi & Ivanenko, 2020). In this narrative Russian regime has instrumentalized the historic role of Red army and it has begun its narrative of illegitimate and neo-Nazist Ukrainian government in 2014 (Kranz, 2023).

Ukraine's narrative has had following elements: Ukrainian army's and nation's resistance, Russian army's criminal actions in war and Russian leader's weakness (Kienneman, 2023). According to Xu and Tao (2023) the national unity against the unlawful war and aggression of Russian invaders has been narrated since 24.2.2022.

Both warring parties have been using heavily different social media platforms to spread their narratives. This is because if one needs to influence a mass audience, the narrative has to reach the individuals through the media (Szostek, 2018). The mass audience is more easily reached through social media platforms than with the classic forms of distribution, for example television or radio. Also, the reliability of the distribution channel must be high (Szostek, 2018). The global social media platforms present a robust and resilient platform for the narratives.

4.3 Information warfare and propaganda

Information is a message that has meaning, implication, or input, and comes from current communication or historical sources (Liew,2014). The context of information is used in situations where it helps the actor to choose the right action or make the right decision. Misinformation is a subset of information, which is false by definition. According to Guess and Lyons (2020) if information cannot be verified to be truthful or has reasonable consensus among the appropriate experts of authorities, it is deemed misinformation. Disinformation is misinformation that is deliberately distributed. The disinformation is meant to deceive the common audience (Guess & Lyons, 2020). The distinction between mis- and disinformation according to this definition would be difficult because it is difficult to show one's intent to distribute false information.

Information manipulation is a part of information operations and -warfare. Information manipulation can be defined as altering the information to deceive the audience or influence their opinions (McCornack, Levine, Solowczuk, Torres, & Campbell, D., 1992). Both propaganda and information manipulation involve using information to influence the perception of the target audience, and they might utilize common methods and tactics.

The term "information warfare," as is implied in the term "warfare," treats information and activities with it as weapons used for achieving political or military goals at the expense of the interests of other individuals, social groups, and nations. Liptak (2009) sees information warfare as a complex concept, but the focus of it is on information. According to her, information warfare is a series of offensive and defensive operations, where information is both weapon and target. More precisely, in information warfare information is weaponized to achieve the goals at the expense of others (Berzina, 2018). Taddeo (2012) defines Information warfare as a fight in the information domain. Definition describes information warfare similar to any other conflict that if fought in any other domain. This means that one defends one's own assets, particularly information, and attempts to disrupt and destroy those of advisory's.

Libicki (1995) did not see information warfare as a separate technique of war, but as a larger concept that is formed from seven different forms of warfare: Command-and-control, intelligence-based, electronic-, psychological-, hacker-, economic-information-, and cyberwarfare. This definition bonded different warfare types under the single structure. In this context propaganda could be utilized as a valuable tool in the context of information warfare.

Di Pietro, Raponi, Caprolu and Cresci (2021) defined information warfare as manipulation of information that is trusted by a target without its awareness, so the target makes decisions against their best interests, but in the interests of the one that is conducting the information warfare. In this interpretation does not take account of the countermeasures, with what the target could defend itself against the hostile information actions but does oversee the information warfare as single sided operation to cause effect on unprepared target.

According to different definitions, the newest definition gives a role to propaganda as a tool for information warfare. As it was defined before, the purpose of propaganda is to persuade the audience to behave in a desired way (Taylor, 2013) and the purpose of information warfare is to make adversary make decisions in favor to the party that is conducting the information warfare (di Pietro et. al., 2021).

Through these definitions, propaganda can be seen as a tool in information warfare, and strategic communication and can be used as a tool to defense and in offence. Propaganda can be used to leverage the national narrative, defend it against the adversaries' undermining narrative, or be offensive tool to undermine adversaries narrative. Propaganda can tell the truth when it is beneficial to the propagandist, it can contain truth and lies mixed in a way that it suits the needs for the narrative or it can be based on lies, if the need be. Overall, propaganda can be used as a tool to manipulate the information space in a way that is favorable to the one that is utilizing propaganda.

5 Involved actors

5.1 The Main Directorate of intelligence of the Ministry of Defense of Ukraine

GUR (or HUR depending on abbreviation) stands for The Main Directorate of Intelligence of Ukraine (Головне управління розвідки Міністерства оборони України, Holovne upravlinnja rozvidky Ministerstva obrony Ukrajny). It is an agency of the ministry of defense of Ukraine. The agency was formed in 1992 from the different organizational parts of the former Soviet intelligence agencies and organizations that were situated to area of Ukraine (Defense intelligence of Ukraine, n.d).

Its mission and the responsibilities are to obtain and analyze information and provision it to authorities, and to ensure the realization of national interests and security of Ukraine (Prokopiv, 2019). GUR is responsible for collecting, analyzing, and disseminating intelligence related to potential military threats to Ukraine's national security, particularly those of a military nature. Its primary focus is to monitor and assess activities on neighboring countries that that might have impact on security of Ukraine.

GUR is an organization that has military and civilian dimensions. The organizational structure of is seen to be built in a following way: five directorates, Strategic Intelligence, Armed Forces General Staff Intelligence Support, Information Support, Personnel Policy, and Logistic directorate and five departments, Internal Security, Planning, Automation and Communication, Economic and Finance and finally, Information and State Secret Protection departments (Smith, 2023).

The armed branch of GUR consists of various military units and formations. According to Smith (2023) the fourth Special Intelligence Service that consist of 3rd Separate Special Forces Regiment, 8th Separate Special Forces Regiment, 10th Separate Special Purpose Unit, 54th Separate Reconnaissance Battalion, Regional Electronic Intelligence Center South, and Regional Electronic Intelligence Center West. There is no exact and validated public information about its position in the organizational structure of GUR. It is possible that it is an independent branch among the directorates and departments.

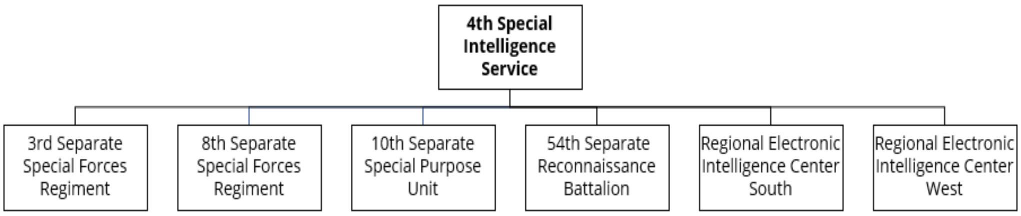
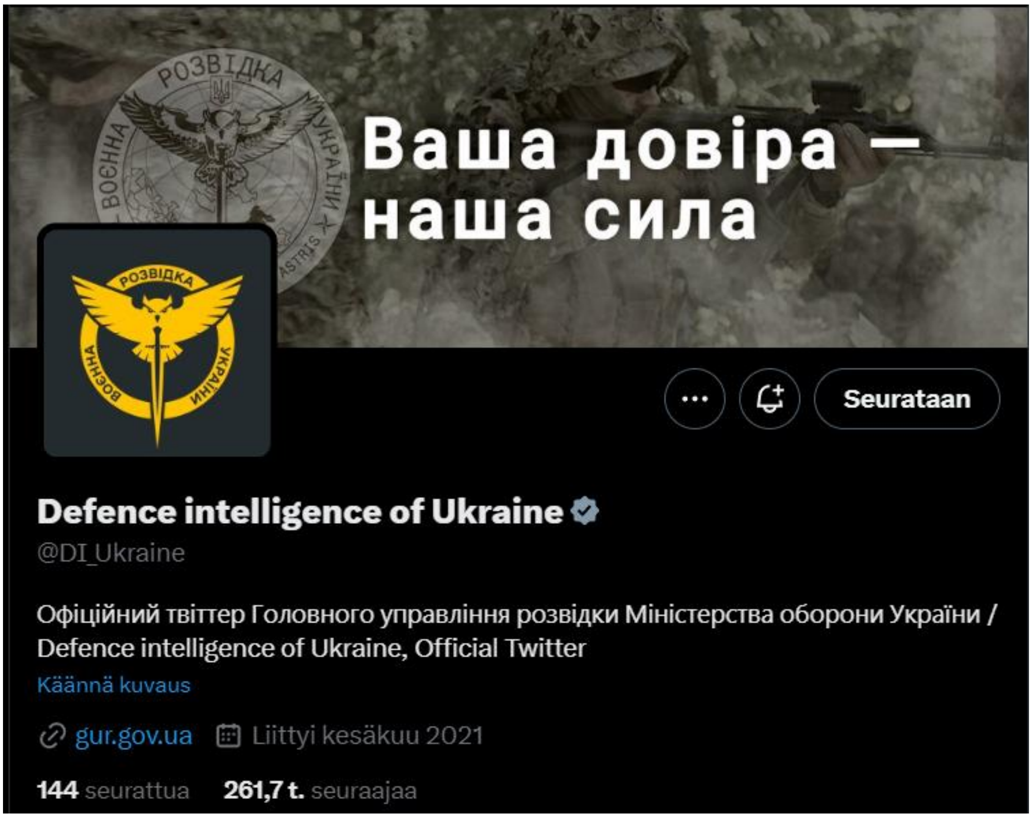

4th Special Intelligence Service
3rd Separate Special Forces Regiment
8th Separate Special Forces Regiment
10th Separate Special Purpose Unit
54th Separate Reconnaissance Battalion
Regional Electronic Intelligence Center South
Regional Electronic Intelligence Center West

Figure 7. The strucure of the armed branch of GUR (Smith, 2023)

Information and State Secret Protection department is the organization within the GUR that is responsible for Cyber and information security issues. It is working closely with the Security Service of Ukraine (Служба безпеки України, Služba bezpeky Ukrajiny, SBU). GUR is said to have been conducting collaboration with its western counterparts and other intelligence services. Central Intelligence Agency (CIA) is told to been helping GUR to procure material that would help it to conduct eavesdropping during the Russo-Ukrainian war (Miller & Khurshudyan, 2023). According to Soesanto (2022) IT Army of Ukraine has been conducting information collecting operations with GUR against various energy operations in Russia (p.24). Unfortunately, the validity of the information about these operations cannot be validated from independent and more reliable sources.

The actor joined Twitter in 2021 and has over 261 thousand followers. GUR is also active in other social media platforms, for example Youtube, Instagram and Telegram. It uses same handle (@DI_Ukraine) in different platforms. GUR's outlook and social media image is well maintained and branded as it can see in figures , social media image is well maintained and branded, see figures 8, 9, and 10.



Defence intelligence of Ukraine

@DI_Ukraine

Офіційний твіттер Головного управління розвідки Міністерства оборони України / Defence intelligence of Ukraine, Official Twitter

Käännä kuvaus

gur.gov.ua Liittyi kesäkuu 2021

144 seurattua 261,7 t. seuraajaa

Figure 8. GUR at Twitter (Twitter, nd)

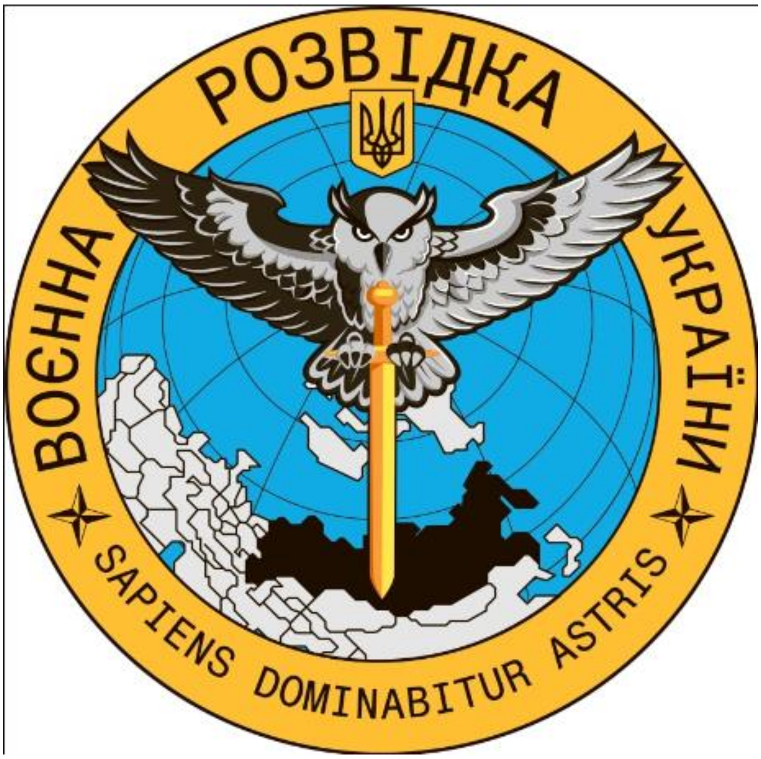


Figure 9. Emblem of The Main Directorate of Intelligence of Ukraine, GUR 2015-2023 (Smith, 2023)

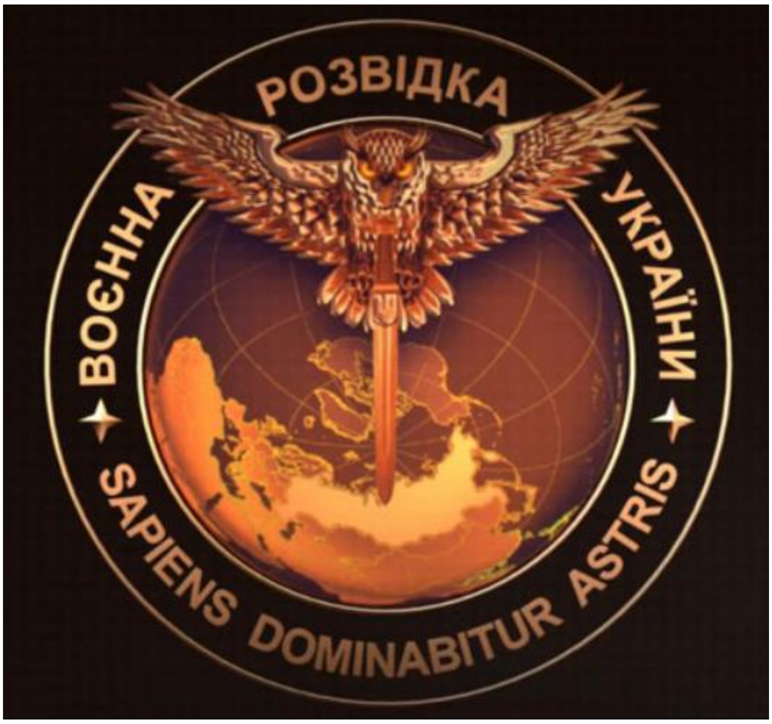


Figure 10. Emblem of the Main Directorate of Intelligence of the Ministry of Defense of Ukraine from 2023- present (Defence intelligence of Ukraine, nd)

5.2 X, formerly known as Twitter

The company was established in 2006 in San Francisco, in the United States of America by Jack Dorsey, Evan Williams and Noah Glass. Twitter is a social media and microblog service, in which the users can publish short “tweets” . The company was listed on the New York Stock Exchange (NYSE) in 2013 and was removed from there when becoming a private company after purchase in 2022. The company is best known for its iconic logo in figure 11 below.

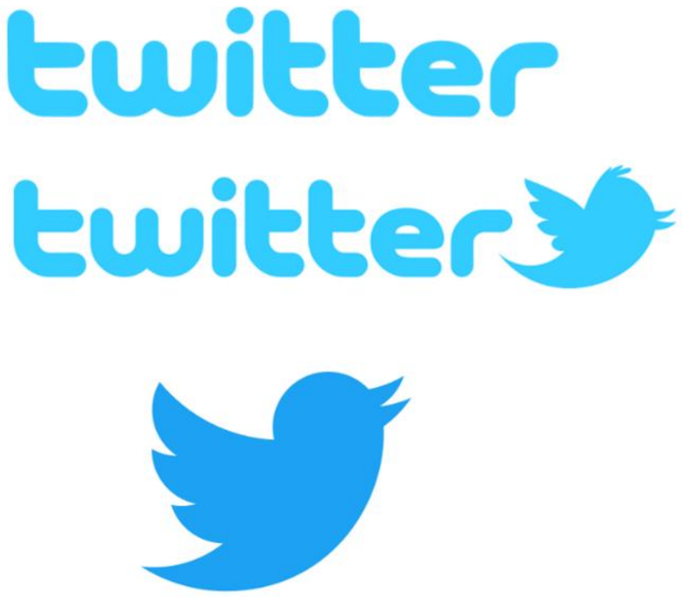


Figure 11. Logos of Twitter from the 2006-2023 (creativefreedom.com, nd)

South-African born, American billionaire Elon Musk bought Twitter in 2022 and changed the name of the company to “X”. This, among other things, led to a change of the name of the company and the overall outlook and public profile of the company. The purpose of this change is seen as Elon Musk’s vision of creating the versatile and universal app, the X (Shah&Martin, 2023). The famous logo was changed soon after the takeover to stylized X presented in figure 12 below.

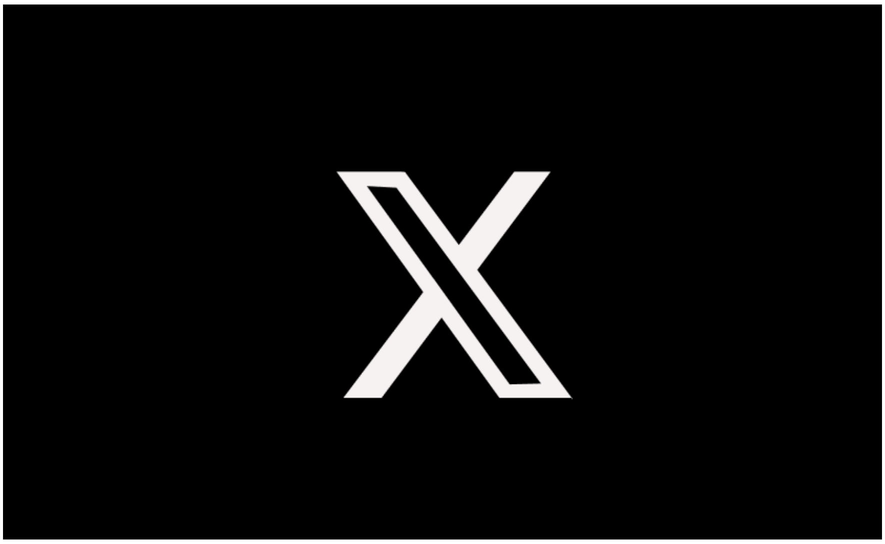


Figure 12. Twitter /X logo 2023-> (Twitter, nd)

Ravaonorohanta and Sayumwe (2020) have researched different social media platforms, and they suggest that Twitter, or X among other popular platforms, is an efficient channel for companies to promote openness and to mitigate the agency problems that affect the company's public image. On the other hand, Twitter has been seen as a prominent platform for spreading misinformation, fake news, and propaganda. In his study, Jones (2019) that the number of twitter-bots increased significantly during the crisis in the middle east in 2017, and they did spread negative information and propaganda against Quatar. He also noticed that the bots also manipulated the trends to make more visibility to anti-Quatar information.

Islamic state terrorist network ISIS has found to utilize Twitter to spread their propagandistic message. Chatfield, Reddick, & Brajawidagda, (2015) found out in their study, that the networks by different actors within Twitter were a significant part of ISIS's communication strategy and its targets. They came to this conclusion by using network-, trend-, and content analysis in their study, which analyzed empirically 3039 tweets that were sent from the Twitter account named @shamiwitness.

Golovchenko, Buntain, Eady, Brown, & Tucker, (2020) came to conclusion that Russia did use Twitter as a channel in operation where it tried to influence the presidential election in USA in 2016. According to them, the networks in Twitter and in other social media platforms are dynamic, complex, and the influencing efforts are not connected to the ideological and political viewpoints of the accounts that are used in influencing campaigns.

Pierri, Luceri, Jindal, & Ferrara (2023) suggested in their research, that Russia did use Twitter for distribution channel of propaganda before the escalation of the Russo-Ukrainian war in 2022, but the volume of it did decrease after the invasion. Also, they found out that Twitter and Facebook did remove a significant amount of the said propagandistic content from their platforms but did not succeed perfectly. According to them, about 8-12 per cent of the malicious content did persist (Pierri et al., 2023).

6 The history of cases of eavesdropping and intercepting communication implemented by Ukraine

The research to find reports, articles, events, or other kind of facts of eavesdropping implemented by Ukraine was conducted by using public sources. The literature review was implemented by using different databases and news blogs on the internet. At this work we utilized search engines provided by Google. Main sources were the news platforms, defense and intelligence blogs and Google scholar. The earlier studies and peer reviewed articles were used where applicable, but the latest information had to be accessed through different non-peer-reviewed sources. From the perspective of time, it was noted that the indications of mobile networking surveillance and eavesdropping actions of both sides of the war did significantly increase after the invasion of Russian forces against Ukraine in February 2022. There were fewer articles or information in public sources about mobile network eavesdropping, with the exception of a few, that mostly connected to Euromaidan riots and the war in Donbass e.g., Horbyk, (2022).

6.1 Findings before the Russian invasion on 24th February 2022

Kramer (2014) suggested in his article at the New York Times, that the governmental officials had sent text messages to the participants of the Euromaidan protests and solved the identities and locations of the individuals by using the BTS data. According to him, the local mobile network operators did deny this, and he suggested that there was some kind of false base station, which would have given that information to officials.

In his article, Rash (2017) wrote about a campaign where various user devices were infected with malware that recorded sounds and discussions that were heard around the device's microphone. The sound files were sent to Dropbox from where they could have been used by the malicious attacker.

At their article Shklovski and Wulf (2018) claim that the Russians attacked against Ukrainian GSM network and re-routed the traffic through their own network operator's network shortly after the occupation and annexation of the Crimea in 2014. The operation was implemented by using signaling level attack against the Ukrainian network. This re-routing operation allowed Russians to intercept and eavesdrop all the traffic made by those who were making phone calls while the communication was re-routed through Russian operator's infrastructure.

Palmer (2018) describes in his article the usage of different remote access trojans in Ukraine. The attacks were conducted against the officials of the Ukrainian government but made by the unknown actor. The used remote access trojans were able to enable the microphones of the infected mobile devices and to eavesdrop the communication nearby or the calls made with the said device. The operation was believed to have begun in 2015 and lasted until 2018.

Hornbyk (2022) authored an article about the war in Donbass, in which he interviewed various people that served at the front. According to those interviews, soldiers from both sides knew that both sides had means to intercept and to eavesdrop the communication over mobile communication. Ukrainian intelligence was known to intercept and to eavesdrop communication of both sides, the enemies, and the own soldiers. According to the article, more harmful result of mobile network surveillance was locating the caller, than to eavesdrop the communication.

6.2 Findings from 24th February 2022 to present

According to Varris (2022) Ukrainian military used volunteers to follow Russian soldiers calls and conducted attacks using that information. This information indicates that Ukrainians have or had access to the huge mass of data or to the source that produces high amount of information that has to be processed manually. Detsch and Mackinnon (2022) also refer to the enormous number of intercepted calls by the intelligence service of Ukraine has obtained, but they do not specify in their writing, which of the national intelligence services has had that material.

Devine (2023) wrote in his article, that both parties did heavily exploited mobile networks at the warzone in both eavesdropping and in locating enemy troops. In his article he published the instructions of Ukrainian armed forces in which the troops were warned of dangers of eavesdropping and geo-locating the mobile devices that were used carelessly. Furthermore, in the article the most common methods and means that were used at Ukraine by both parties were presented.

Orlova (2023) had interviewed an intelligence operator, whose task was to listen and analyze the calls of Russian soldiers. According to the interviewed intelligence person, the content of the calls did contain evidence of war crimes and various atrocities that the Russian military personnel had committed. The intelligence operator said that she had been working with the material for over one and a half years. On general, one should be aware, that the interview was published in the Ukrainian press, so the validity of the interviewee should be evaluated with caution. According to the article, the operator did not work with the GUR, but with another Ukrainian state law enforcement actor.

McDaid (2022) described the actions of Ukrainian mobile network operators. According to her, all the operators disabled the roaming service from subscribers, who had subscription from the Belarussian or Russian service operators. This action was conducted at the night between 24th and 25th of February and this disabled the usage of Russian or Belarussian origin mobile telephone connections. The operators did not disable the calls from Ukraine to neighboring countries (McDaid, 2022). This made it possible and easy for Ukrainian national officials to intercept and to eavesdrop the communication (McDaid, 2022; Aviv and Ferri,2023).

According to Oh (2023) the Ukrainian military was able to eavesdrop the communication of Russian commanders if they had devices that connect to their command networks over the Ukrainian mobile networks. The observations were published at the white hat conference in Seoul by a cyber expert Kim Yongdae. Detsch & Mackinnon (2022) on the other hand wrote, that the usage of insecure, civilian cell phones occurred because the leadership of the Russian forces was so far from behind, so the more secure communication method forced the troops to use insecure communication devices. This led to the situation, where the civilian mobile devices and the Ukrainian mobile network operators had to be used. As it has to be remembered, that the roaming services for Belorussian and Russian subscription was disabled from the 25th of February (McDaid, 2022).

The information about troops and their activity is monitored by the handshake activity of their cell phones at the certain cell phone calls by both warring parties (Yujas, Gibbons-Neff & Al-Hlou, 2023). The location and the approximate number of the troops give out valuable information about formation and the intention of the advisory and its intentions. This information can be extracted even without the admittance to the content of the communication itself. The capabilities of electronic warfare are well equipped with this kind of operation, so the method or the attack vector that was used cannot be confirmed with this information.

At the ninth of July 2023 Politico, a European news site, published article of that Ukrainian intelligence service SBU had intercepted phone call in which two Russians discussed and admitted the attack against Nova Kakhovka dam (Melkozerova, 2023). The Ukrainian officials claim that the information was obtained by wiretapping the communication between two Russian operatives, who were discussing the matter over the phone. No further evidence of the means or methods of how the interception was implemented was described in the article.

7 The analysis of the collected dataset

The research was conducted in a methodical manner as was described earlier in Chapter two. The dataset was quantified with the numerical data that was inducted from the collected content. The dataset was altered by removing the days when there were no samples collected. This was implemented to another table in the spreadsheet. Both tables were used in analysis. The dataset was collected from the Tweets that were published by the @DI_Ukraine, which is verified account for The Main Directorate of Intelligence of the Ministry of Defense of Ukraine. The collection was conducted between 28.11.2022 and 31.8.2023, both days included. The collection time was 276 days, and 261 samples (n=261) were collected over the given time period.

The audio content was mostly (n=260) spoken Russian, and only one (n=1) was Ukrainian. Visual and written content was with no exception written in Ukraine (n=261). The translation was made applying the following process: the audio was listened to in order to find different anomalies. While listening, the audio was transcribed automatically with the tools provided by the social media platform (Youtube). The transcription was translated with automated tools by the social media platform (Youtube) and also with the GPT for educational and learning purposes. The results were confirmed with Google translate occasionally for quality control purposes or in cases where the results were not reasonably understandable.

The results were then cross-checked and evaluated for the quality. The automatic translation was cross-checked with the content that had subtitles (n=97). The purpose of this was to validate the results given by automatic translation methods. As it was defined in the chapter 2.4, exact translation was not considered necessary, because the themes could be detected even in an inaccurate translation.

7.1 Themes and variables used in dataset.

The themes were selected according to their effect to the efficiency to the Russian military. When selecting themes, the evidence for either support for the narrative for Ukraine or undermining effect for Russian narrative would be found. The structure of selection of themes and their variables is presented in figure 13.

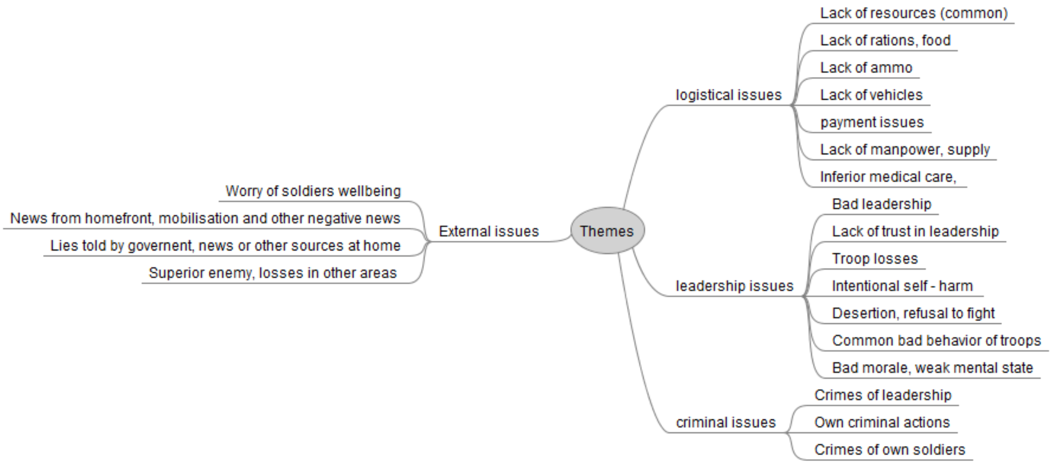
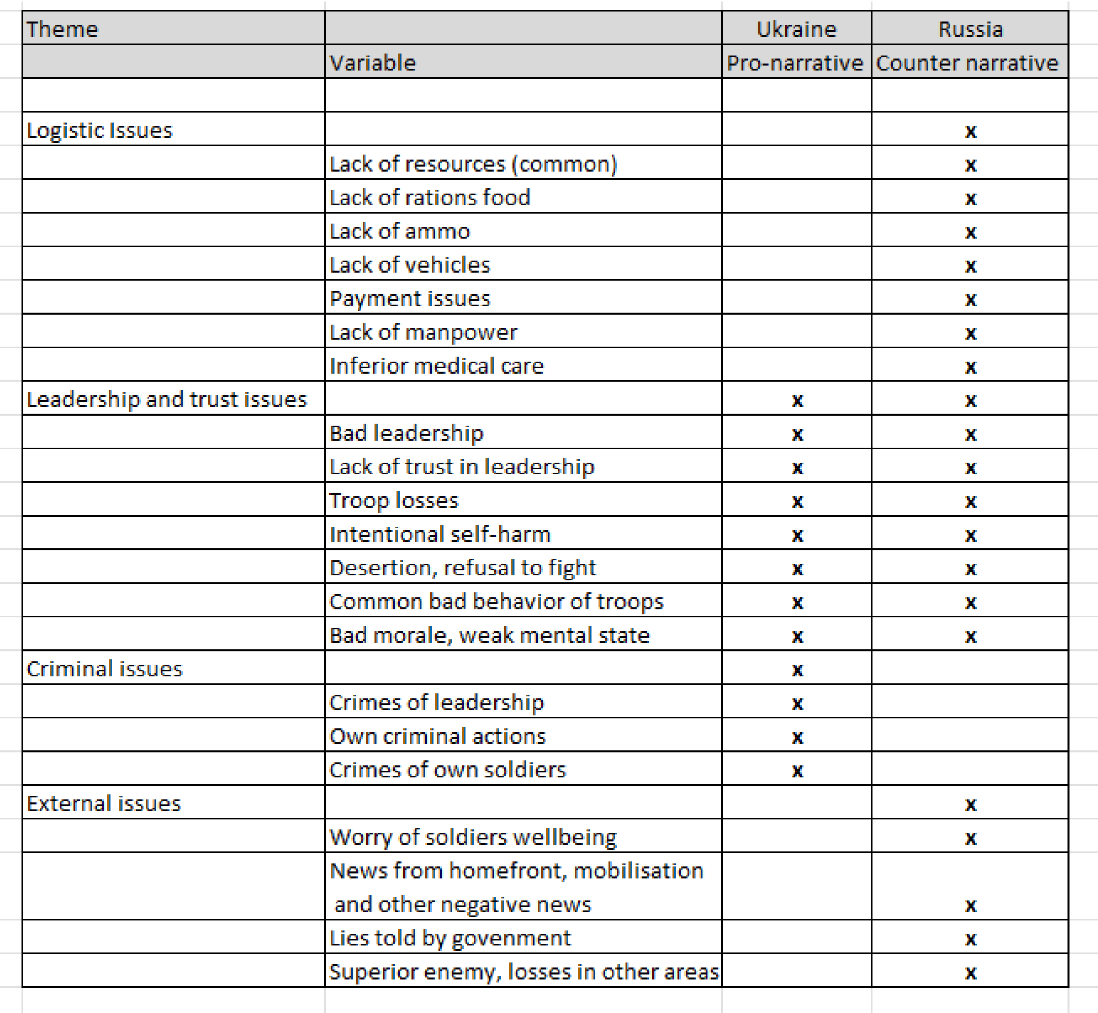

Themes
External issues
Worry of soldiers wellbeing
News from homefront, mobilisation and other negative news
Lies told by governent, news or other sources at home
Superior enemy, losses in other areas
logistical issues
Lack of resources (common)
Lack of rations, food
Lack of ammo
Lack of vehicles
payment issues
Lack of manpower, supply
Inferior medical care,
leadership issues
Bad leadership
Lack of trust in leadership
Troop losses
Intentional self - harm
Desertion, refusal to fight
Common bad behavior of troops
Bad morale, weak mental state
criminal issues
Crimes of leadership
Own criminal actions
Crimes of own soldiers

Figure 13. Themes and variables used in evaluation of the dataset

Selected themes and their variables were evaluated from two viewpoints. Firstly, the message was undermining the Russian narrative of victorious army of Russia over Ukraine (Kienneman, 2023), poor leadership of Ukraine (Kienneman, 2023), or if it were discrediting the efficiency of Russian army, in which case it would counter the narrative of “Second army in the world” (Topalskyi & Ivanenko, 2020). Secondly, the message would be supporting Ukrainian narrative, if the content contained findings of criminal actions of the Russian army, or the superior capability of Ukraine (Kienneman, 2023).

The conflict between narratives and themes is described in table 2. It was evaluated, that “logistical and external issues” undermine Russian and supporting Ukrainian narrative. “Criminal issues”-theme and its variables were seen to support Ukrainian narrative, but it was not seen any connection to Russian narrative. Lastly, “leadership and trust issues”-theme was seen to support Ukrainian and undermining Russian narrative.



Theme		Ukraine	Russia
	Variable	Pro-narrative	Counter narrative
Logistic Issues			x
	Lack of resources (common)		x
	Lack of rations food		x
	Lack of ammo		x
	Lack of vehicles		x
	Payment issues		x
	Lack of manpower		x
	Inferior medical care		x
Leadership and trust issues		x	x
	Bad leadership	x	x
	Lack of trust in leadership	x	x
	Troop losses	x	x
	Intentional self-harm	x	x
	Desertion, refusal to fight	x	x
	Common bad behavior of troops	x	x
	Bad morale, weak mental state	x	x
Criminal issues		x	
	Crimes of leadership	x	
	Own criminal actions	x	
	Crimes of own soldiers	x	
External issues			x
	Worry of soldiers wellbeing		x
	News from homefront, mobilisation and other negative news		x
	Lies told by govenment		x
	Superior enemy, losses in other areas		x

Table 2. Perceived effect of themes and variables on Ukrainian and Russian narratives

<u>Logistical issues and its variables</u>

A logistical issues-theme was selected because the logistical challenges cause difficulties for military force to execute operations, either defensive or offensive. Jalowiec and Grala (2020) have listed basic supply, stockpile and sourcing the supplies as crucial aspects of logistical elements. The indications that there is a lack of capabilities in items listed above would message that the invading Russian army in Ukraine would not be as efficient as it is told to be. Therefore, the logistical issues would seem to counter the Russian narrative of "the second army of the world" (Topalskyi & Ivanenko, 2020) and the victorious army of Russia (Kienneman, 2023).

First variable, "lack of resources" would indicate general lack of logistical services. The second variable would indicate the lack or absence of food. This would be indicative if there was an indication of hunger or the need to acquire food from locals. Third variable, "lack of ammo" means, that the Russian troops did not have enough ordnance for their weapons systems. Fourth variable "lack of vehicles" is indicated at the content through the stories of long distances that had to be crossed by foot, because there was no transportation, or by the stories of commandeering civilian vehicles, which would also be noticed in "Criminal issues"-theme. Fifth variable, "payment issues" is indicated in the content with stories of absence of payment, lack of promised pay, or in lies that were told about the compensation for service in the Russian army. Sixth variable "lack of manpower" is indicated in the content in stories, that the organizations are not manned fully, the reinforcements are not trained or are not able to fight or operate efficiently, or the losses are mounting, or the rotation of troops has not been made. Seventh variable, "inferior medical care" is indicated in the content with stories of illnesses or wounds that have not been treated or are treated badly. Also, the perceived problems and difficulties to get to medical care are indicative to this variable.

Leadership and trust issues

In general, negative, or bad leadership undermines followers will, initiative potential, destroys military units morale, subordinates motivation, and commitment (Shufelt & Longenecker, 2017). This reflects negatively on trust in leadership and to the quality of the work. Bad, or destructive leadership leads to negative attitude and unwillingness to execute given orders, and weak performance for those who perceive bad leadership from their superiors (Schyns & Schilling, 2013). Trust is weakened through the sub-par quality of leadership. Dirks & Skarlici (2004) have suggested that trust has significant effects on individual, team, and organizational performance.

Thematic findings of variables of this theme measure the quality of the leadership, or the lack thereof. The leadership and trust issues would seem to promote Ukrainian narrative of weak leadership of Russia (Kienneman, 2023) and counter the Russian narrative of Russian narrative of “the second army of the world” (Topalskyi & Ivanenko, 2020) and the victorious army of Russia (Kienneman, 2023).

The first selected variable was “Bad leadership”. The variable would manifest absence of leadership, poor decisions that lead to catastrophic losses or are seen by the narrator as unprofessional or simply wrong. Also, the indifference and other low-quality elements of leadership capabilities, which were presented in the content would indicate the presence of the variable at the content.

The second selected variable was “Lack of trust to leadership”. This would be indicated by questioning the capability of the leadership to lead their troops, questioning the given orders, or just in general, refusing to fulfill the given order, when it was believed that the orders would cause catastrophic consequences.

The third variable, “Troop losses” was indicated at the content by narrator with stories of operations or strikes of Ukrainian armed forces that caused loss or losses. Assumption with this variable is, that it has, or it should have a causal connection with the “troop losses”-variable. Either troop losses are caused by bad leadership, or it has led to the lack of trust to leadership when catastrophic losses have taken place.

The fourth variable “intentional self-harm” is indicated in content, when narrator has been or is going to harm oneself to get away from the front lines or from the warzone. Also, this could be preferred as perceived behavior of others or if the narrator has been told that some other or others have been conducting such behavior.

The fifth variable “Desertion, refusal to fight” is indicated in content when the party, which is operating at the front or at the warzone informs one’s intention to become deserter or describes one’s intention to not to participate in operation that is ordered for him/her or has already refused to obey the command to participate. Also, the variable is indicated, if the participant of conversation in content has heard or is informed about such actions of some other individual or unit.

The sixth variable “the common bad behavior of troops” is indicated in content when other party describes different actions that are not suitable behavior of well-trained or professional military personnel or -unit. This includes but is not limited to getting drunk in service, bad behavior towards civilians or fellow service members, theft, or another element of behavior that is not suitable for military service member. This variable is indicated if the person has witnessed such behavior by oneself or has heard such from other sources that have witnessed such conduct in other units or in other areas.

The seventh variable “Bad morale, weak mental state” is indicated in context if person describes one’s suspicions or feelings in a way, that they indicate one’s willingness to fight to be weak or very weak. Also, if a person describes elements that affect a person or person’s service unit’s feelings, mental state, or morale to be so low, that it affects their efficiency negatively, the indication of this variable exists. This also includes the perceived incidents and stories of other people or units that are affected by such elements.

Criminal issues

The criminal issues were selected to this study because the crimes made by the Russian troops has been a persistent theme of Ukrainian narrative from the beginning of the invasion at 24.2.2023 (e.g., see Kinetz, 2022; Mak, 2022; Biesecker, 2022). If the content would contain findings of confessions of committed crimes by the caller, their peers, or their leaders, this would strengthen Ukrainian narrative of criminal actions of Russian troops (Kienneman, 2023).

Crimes of leadership are indicated if such actions, which are seen illegal or can be considered as such are discussed in content. This includes the actions and situations where a leader either has attended in such action or has given an order to anyone to conduct such behavior. Also, variable is noted also if the narrator has heard someone talking about such incident.

Own crimes-variable is marked if the narrator admits such action or behavior that can be overseen as a criminal activity. This applies to crimes against Ukrainian or other civilian population, the crimes that are seen as misconduct against own leadership are marked to variables “Desertion, refusal to fight”, “Common bad behavior of troops”, or “Bad morale, weak mental state”-variables in “Leadership and trust issues”-theme depending on context at which the variable is noticed.

Crimes of own troops- variable is marked, if the narrator has been witnessing or has heard and is telling another party about crimes that have been conducted by own troops against Ukrainian or other civilian population. The indication of crimes against other members of military or leadership are marked to variables “Common bad behavior of troops”, or “Bad morale, weak mental state”-variables in “Leadership and trust issues”-theme depending on context at which the variable is noticed.

External issues

External issues were selected mostly to examine the sentiment and signals that come from the home front to the front line. This also investigated the situation where the information from the home front was refuted or rejected by the information from the person, who was serving or supposedly had more concrete information that was learned from own personal perspective.

The external issues would seem to counter the Russian narrative of Russian narrative of “the second army of the world” (Topalskyi & Ivanenko, 2020), the victorious army of Russia (Kienneman, 2023), and when focusing to variable “superior enemy, losses from the other fronts” promote Ukrainian narrative of national unity against aggressive invader (Xu & Tao, 2023).

“Worry of soldiers wellbeing”-variable is marked when the other person indicates her or his worry on the person that is supposedly under the mortal threat at the war zone. The variable is noted in situations, if the indication comes from typical communication that can be expected in casual conversation.

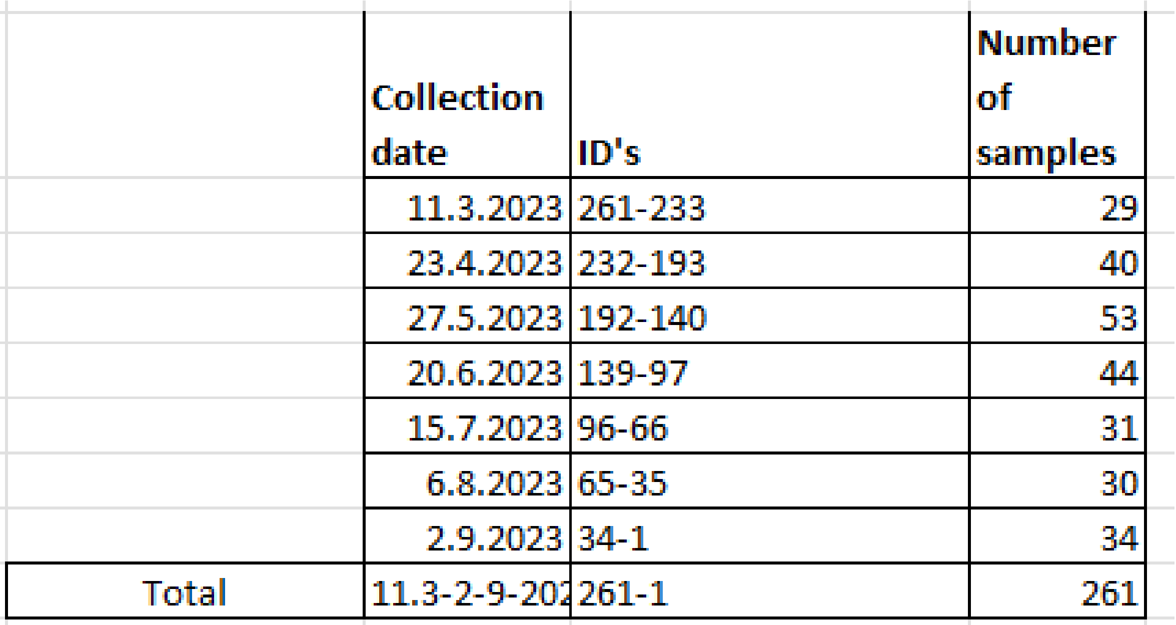
“News from the home front”- variable is marked, when the main focus of the communication is with the different stories that has taken place somewhere else. The emphasis is on negative news, which is told to one that is supposedly at the front. The news that is presented to a person that is allegedly at the frontlines and is debunked by the person to be lies, are marked to the “Lies told by government”-variable.

“Lies told by government”- variable is marked when the party that is supposedly at home front or at the frontlines tells the official statement or story told by government that is debunked by another party of the communication based on their own experiences. The border with previous variable is decided according to context in which the statement is given.

“Superior enemy, losses in other area”-variable are marked if the communication involves stories or information of enemy successes in areas that are other, where the person that is supposed to be. Also, stories of successes of enemy that are told at the home front and is not debunked by the person that is allegedly at the front line are marked to this variable. The context is used to decide between this variable and “news from the Homefront”.

7.2 General findings

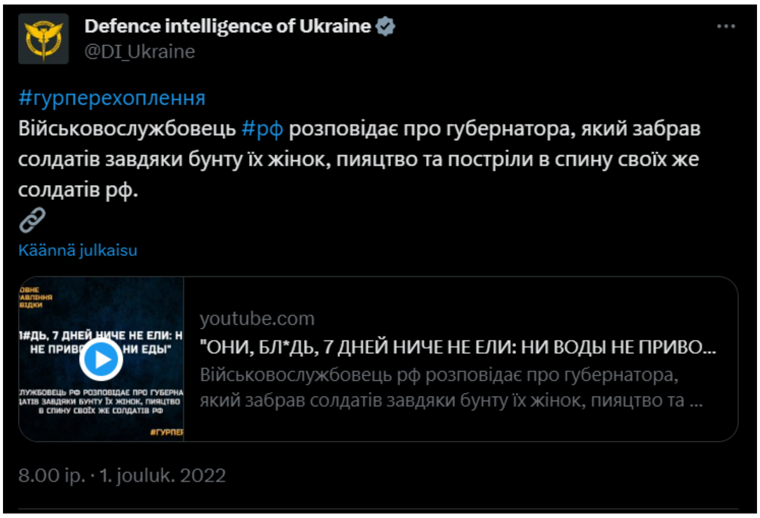
The dataset was collected between 11.2.2023 and 2.9.2023. The collection of the dataset was performed in 7 different instances. The instances, the collection dates, number of samples and their ID's are shown in Table 4. The results of the numerical values are from the exact date when they were collected. Those values might differ from the values if they are viewed now. Earlier values were not changed later even if those had been seen changed in later collection date. Also, The number of samples and their collection dates is shown at the table 3 below:



	Collection date	ID's	Number of samples
	11.3.2023	261-233	29
	23.4.2023	232-193	40
	27.5.2023	192-140	53
	20.6.2023	139-97	44
	15.7.2023	96-66	31
	6.8.2023	65-35	30
	2.9.2023	34-1	34
Total	11.3-2-9-202	261-1	261

Table 3. Dataset collection timeframe

All the samples (n=261) have uniform structure. All (n=261) samples share the following elements, some of which are not present in the other content that the said account has been publishing. The example of the common structure of the tweet is shown in figure 14 below.



Defence intelligence of Ukraine
@DI_Ukraine

#гурперехоплення
Військовослужбовець #рф розповідає про губернатора, який забрав солдатів завдяки бунту їх жінок, пияцтво та постріли в спину своїх же солдатів рф.

Käännä julkaisu

youtube.com
"ОНИ, БЛ*ДЬ, 7 ДНЕЙ НИЧЕ НЕ ЕЛИ: НИ ВОДЫ НЕ ПРИВО...
Військовослужбовець рф розповідає про губернатора, який забрав солдатів завдяки бунту їх жінок, пияцтво та ...

8.00 ip. · 1. jouluk. 2022

ОВНЕ
АВЛЕННЯ
ВІДКИ
1#ДЬ, 7 ДНЕЙ НИЧЕ НЕ ЕЛИ: Н
НЕ ПРИВ НИ ЕДЫ"
ЛУЖБОВЕЦЬ РФ РОЗПОВІДАЄ ПРО ГУБЕРНА
ДАТІВ ЗАВДЯКИ БУНТУ ЇХ ЖІНОК, ПИЯЦТВО
В СПИНУ СВОЇХ ЖЕ СОЛДАТІВ РФ
#ГУРПЕ

Figure 14. Screenshot of the tweet from the @DI_Ukraine (Twitter, nd)

All the samples have common handle, #гурперехоплення (#gurintercepted in English). With this handle one can find all the content that said account has published. No other content published by this account is tagged with this particular handle. No other handles are used in any of the samples in the collected dataset (n=261). This suggests that the handle is reserved for this kind of content, so it would be easy to find it. The handle itself gives credit to the assumed organization (GUR) has obtained the information that is published.

All the samples have the same structural context. The Tweet begins with the hashtag, and after that there is a text in Ukrainian that describes the message that the audiovisual content is offering. The link to external content is offered in cases where the content is at the different platform (n=236, 90,4% of cases) or the embedded media player is showing the content (n=25, 8,6% of cases).

The audiovisual content always has the same general structure and visual image. The content starts with the logo of GUR revealing from the background mist. This takes exactly 8 seconds. Example is shown at the figure 15 below.

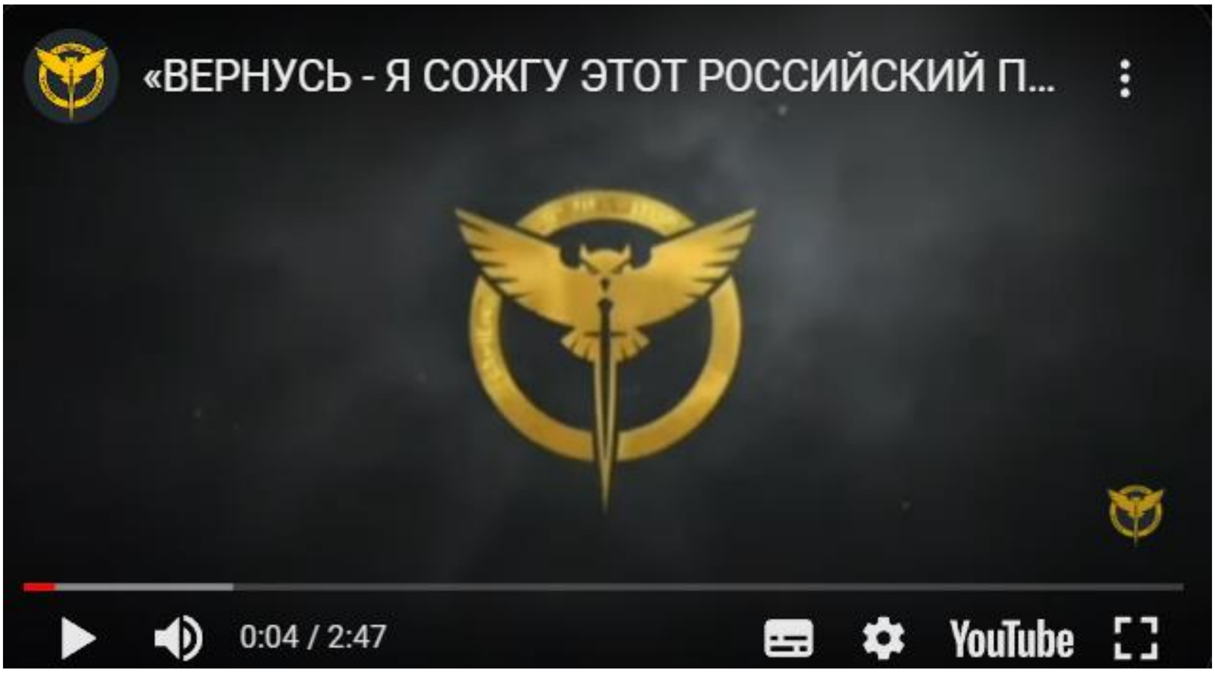
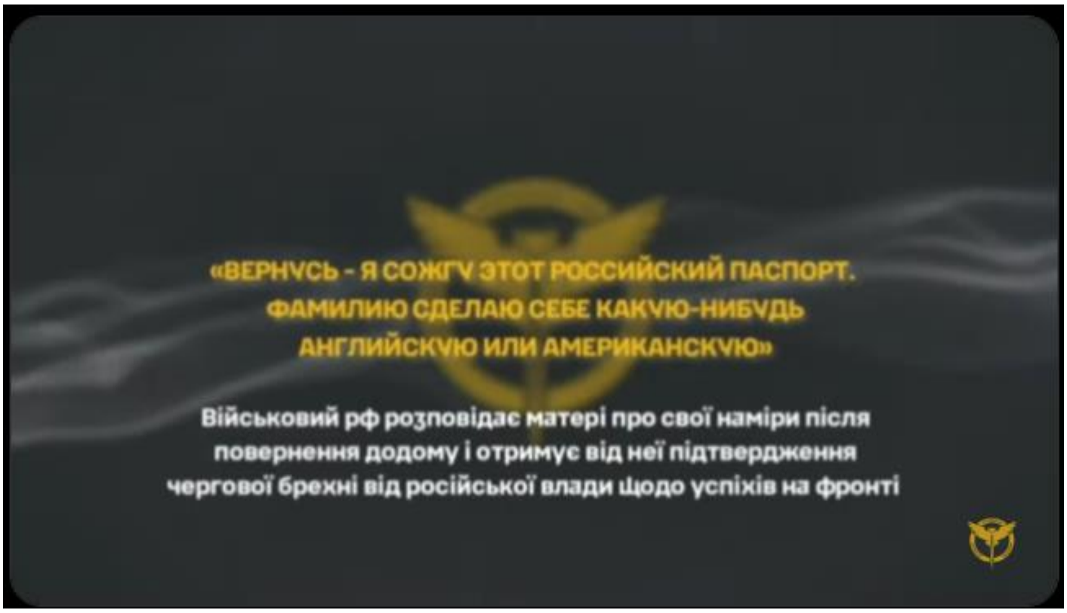


Figure 15. Starting screen of content (Twitter, nd)

After this text, content that was readable in Twitter appears on screen, letter by letter. Time, this process takes varies between cases and is dependent on the length of the text. The content is written in Ukraine. Example is shown at the figure 16 below.

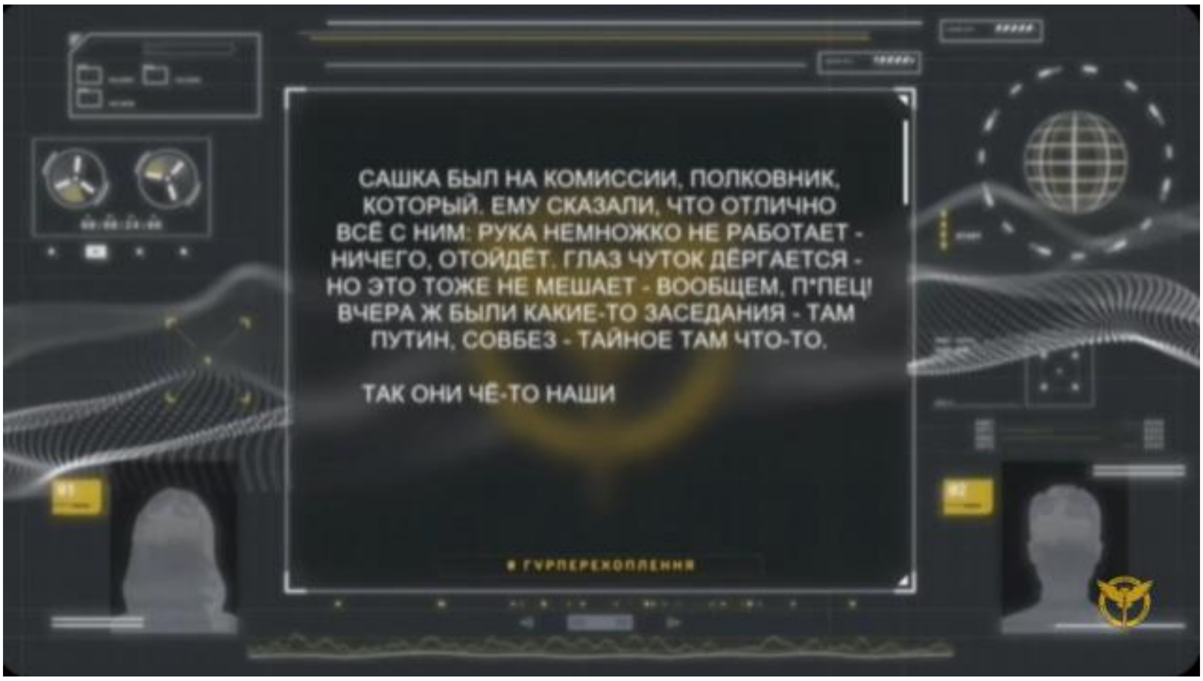


«ВЕРНУСЬ - Я СОЖГУ ЭТОТ РОССИЙСКИЙ ПАСПОРТ.
ФАМИЛИЮ СДЕЛАЮ СЕБЕ КАКУЮ-НИБУДЬ
АНГЛИЙСКУЮ ИЛИ АМЕРИКАНСКУЮ»

Військовий рф розповідає матері про свої наміри після
повернення додому і отримує від неї підтвердження
чергової брехні від російської влади щодо успіхів на фронті

Figure 16. Summary of the audiovisual content before the actual audio is started (Twitter, nd)

After the initialization, the actual audio content starts playing. The content, which is Russian, has been translated into Ukrainian as a text that can be played on the screen in real time. Harsh language has been edited away. This suggests that the content has been listened to and its language has been checked and cleaned. Content with harsh language can be flagged as inappropriate by social media platforms, and editing the content might refer to the intention to keep it appropriate to all to listen. Example of typical visual outlook of the content is shown at figure 17 below.

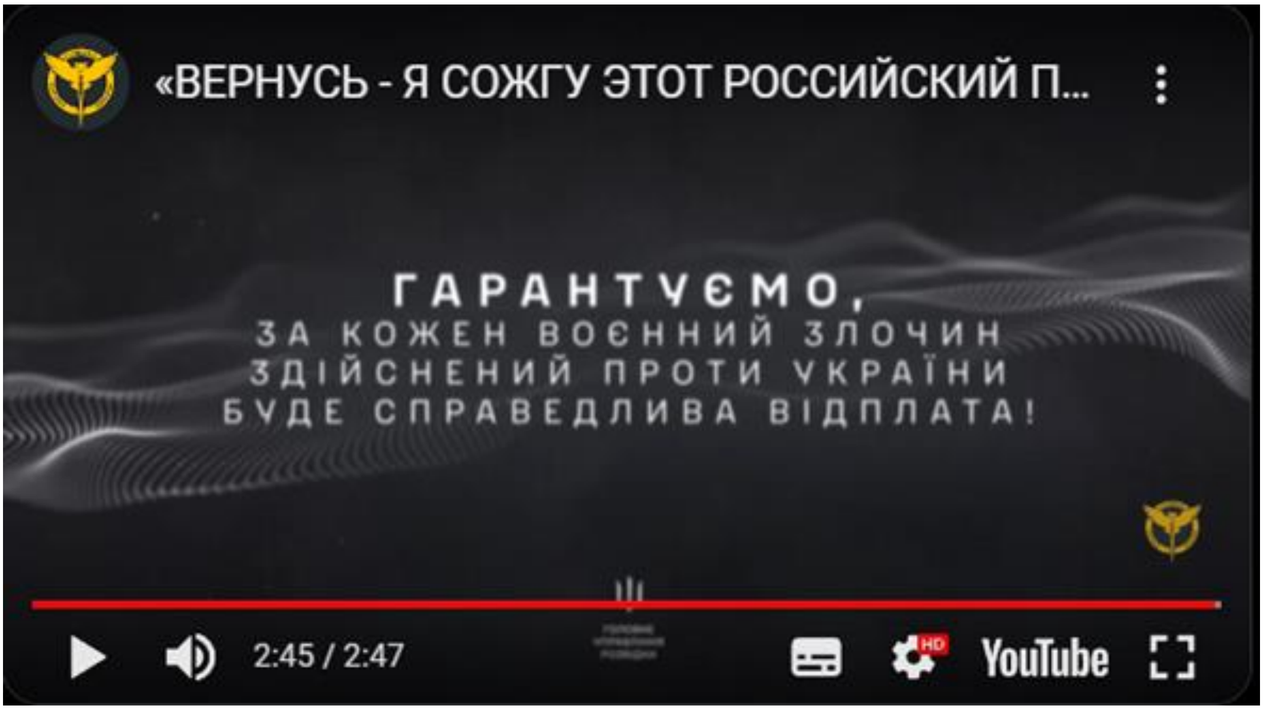


САШКА БЫЛ НА КОМИССИИ, ПОЛКОВНИК, КОТОРЫЙ. ЕМУ СКАЗАЛИ, ЧТО ОТЛИЧНО ВСЁ С НИМ: РУКА НЕМНОЖКО НЕ РАБОТАЕТ - НИЧЕГО, ОТОЙДЁТ. ГЛАЗ ЧУТОК ДЁРГАЕТСЯ - НО ЭТО ТОЖЕ НЕ МЕШАЕТ - ВООБЩЕМ, П*ПЕЦ! ВЧЕРА Ж БЫЛИ КАКИЕ-ТО ЗАСЕДАНИЯ - ТАМ ПУТИН, СОВБЕЗ - ТАЙНОЕ ТАМ ЧТО-ТО.

ТАК ОНИ ЧЁ-ТО НАШИ

Figure 17. Example of visual outlook of the content while the audio content is played (Twitter, nd)

The audiovisual content ends to the screen that says, “ We guarantee, that every war crime against Ukraine will be avenged”. This text is shown five second at the screen to the end of the content. Example is shown at figure 18 below.



«ВЕРНУСЬ - Я СОЖГУ ЭТОТ РОССИЙСКИЙ П...

ГАРАНТУЄМО,
ЗА КОЖЕН ВОЄННИЙ ЗЛОЧИН
ЗДІЙСНЕНИЙ ПРОТИ УКРАЇНИ
БУДЕ СПРАВЕДЛИВА ВІДПЛАТА!

Figure 18. Eexample of the ending of the content (Twitter, nd)

All the samples (n=261) follow the previously described pattern and audiovisual structure. It is as highly structured and uniform as the content in actual tweet. This suggests that the visual and artistic appearance is the result of careful and calculated planning. Using uniform graphical design has a crucial role in branding and marketing. It makes communication to the audience visually appealing and consistent (Evalina, Angeline & Mariani, 2014).

Inappropriate language is edited from the content. This indicates that the content is listened to, selected, and edited to meet the purpose. This also suggests that there is intention to avoid the content to be flagged as "inappropriate content". The language that is used in the content is usually very rude and popular, no samples with clean, literary language were found. This was found while automatic translations were used, because the popular expressions would be translated differently from what they in practice means. This caused the need to interpret and evaluate the translation in various samples and to evaluate what the content actually meant. This would indicate and suggest, that the language is either well prepared and acted, if the content is fabricated or it actually is genuine content from actual transmission. Secondly this would suggest that the target group for this content is actually Russian speaking audience, which would fluently understand spoken language without the need for translation programs or similar methods.

The audiovisual content had translation to English in ninety-seven tweets (37.1% of tweets). Only four of those were actual translations that were contributed by the publisher, other parties contributed the rest. Third parties contributed all of the translations. This suggests that the target audience for the content were either able to understand Ukrainian language or are native Ukrainians.

The published content was retweeted on average forty-five and liked 172 times. One should be cautious when analyzing these values, because as mentioned, these will vary over time, because the content is dynamic. The value can change because the likes and retweets can be removed. These values or other numerical results might be different over time and should be considered to be indicative values, which were accurate when the dataset was collected.

The actual audiovisual content was viewed approximately 23115 times on Twitter and 26852 times on Youtube. The number of samples differs in this from the total amount of samples (n=261), because the earliest Tweets (n=18) did not contain the information of views. This is the status in the time when the dataset was collected because the dynamic nature of the volume of the datapoints can differ from the calculated values.

7.3 Statistical analysis

The dataset was analyzed through the quantitative variables that were collected with the actual content. Collection date was marked, as amount of “likes,” “retweets” and “views” are dynamic. The values mentioned can change over time, and those that are collected to this dataset are the snapshot at the time that the sample is collected. Every sample was given a unique identifier, which would make it easier to refer to individual sample. The timeline of the dataset was marked as days, and every sample got attached to a certain day. The datapoints and their definitions are presented in chapter 2.

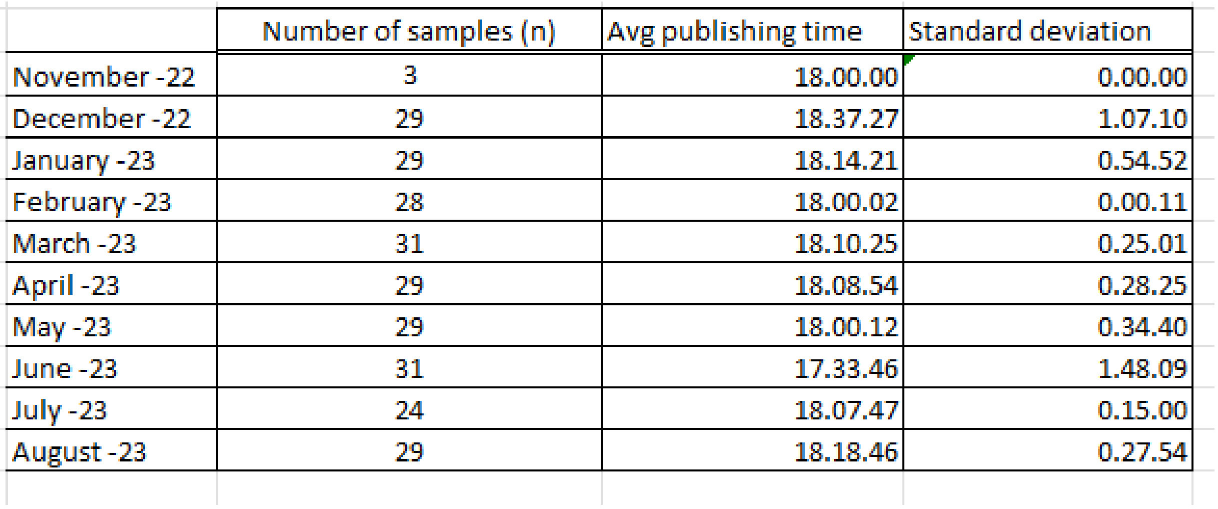
The primary distribution channel for audiovisual content was Youtube (n=185). The primary distribution channel was determined if the Tweet did have a link to the content in the Youtube and did not have automatic play-function or it did redirect to the Youtube if the media player in Twitter was allowed. In case that either of those options were true, the primary distribution channel was marked as Twitter. Only 25 Tweets that did not have content that was linked to Youtube were found. This suggests that Twitter is a secondary distribution channel for the content.

The average number of views of the content in Twitter was 23115. In comparison, the audiovisual content that was shared in tweets was viewed 26825 times on average at Youtube. The content was retweeted 45 times and liked 172 times on average. With these values, one should be aware of the dynamic nature of these values.

Average publishing time for selected samples was 18:07:42 with standard deviation of 0:53:50. The greatest deviation in samples can be found from December 2022 (1:07:10, Figure 8) and in June 2023 (1:48:09) when compared to the average monthly publishing time. This would suggest that there is a certain schedule according to which the content is to be published.

Results from November 2022 were not taken account for, because of the small sample size. The structure of results of the average publishing times suggests that there is a content publishing schedule that is mostly followed. Monthly deviation suggests that there are individual samples in which the publishing time differs from the actual scheduled time. This, on the other hand, suggests that the publishing is not automated, but is conducted by a person or by persons.

When the data is researched statistically on a monthly basis, the assumption of standard publishing process will have support. When the samples are examined on a monthly basis by estimating the average publication time and by taking account the standard deviation, it can be observed that their publication coincides with significant accuracy at 18:00. Every segment that was collected suggests that the publishing is done after 18:00. Exception for this is June 2023, where the average publishing time was almost half an hour earlier. The results are shown in table 4 below.



	Number of samples (n)	Avg publishing time	Standard deviation
November -22	3	18.00.00	0.00.00
December -22	29	18.37.27	1.07.10
January -23	29	18.14.21	0.54.52
February -23	28	18.00.02	0.00.11
March -23	31	18.10.25	0.25.01
April -23	29	18.08.54	0.28.25
May -23	29	18.00.12	0.34.40
June -23	31	17.33.46	1.48.09
July -23	24	18.07.47	0.15.00
August -23	29	18.18.46	0.27.54

Table 4. Average publishing time with standard deviation

Visualization of the anomaly can be seen in the chart below. The samples are figured in a way that the newest samples are at the left side of the chart, the oldest are at the right. The pattern suggests that the publishing process has a publishing schedule, at around 18:00 daily. The pattern is visually verifiable from figure 19 below. There is anomalistic and erratic period in July 2023, that cannot be completely explained, but when comparing this anomaly to the perceived missing samples, this could be explained by the holiday season, and the lack of people that are dedicated to this task.

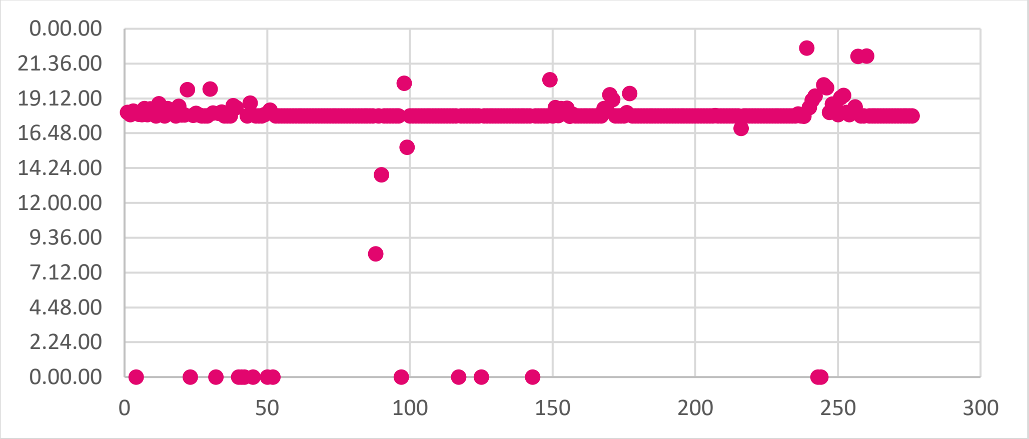
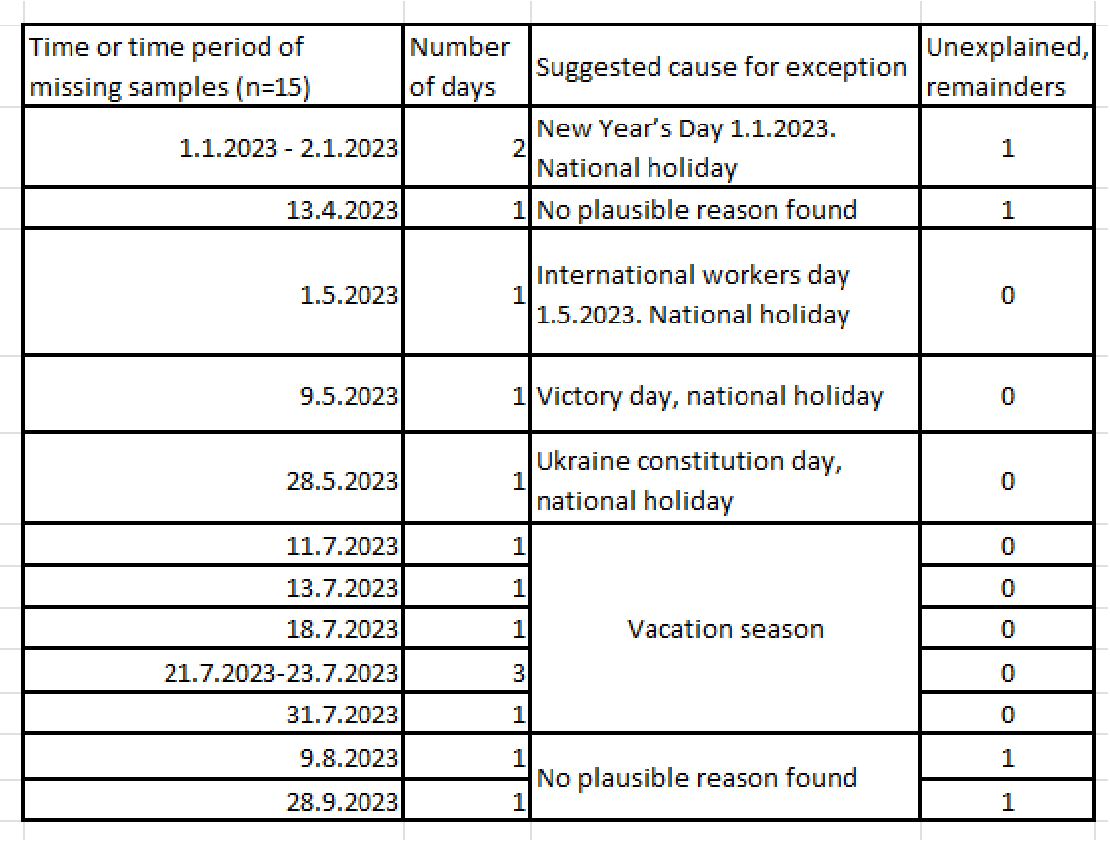


Figure 19. Visualization of the suggested publishing schedule.

When the dataset was collected it was found that there were 15 days when the content was not published. The days when the content was not published were collected and evaluated are listed in the table 5 below.



Time or time period of missing samples (n=15)	Number of days	Suggested cause for exception	Unexplained, remainders
1.1.2023 - 2.1.2023	2	New Year's Day 1.1.2023. National holiday	1
13.4.2023	1	No plausible reason found	1
1.5.2023	1	International workers day 1.5.2023. National holiday	0
9.5.2023	1	Victory day, national holiday	0
28.5.2023	1	Ukraine constitution day, national holiday	0
11.7.2023	1	Vacation season	0
13.7.2023	1		0
18.7.2023	1		0
21.7.2023-23.7.2023	3		0
31.7.2023	1		0
9.8.2023	1	No plausible reason found	1
28.9.2023	1		1

Table 5. Missing samples and explanations

An explanation for the absent samples was searched. 4 (26,7%) of missing samples can be explained with the national holidays (Onix, nd). According to Wonders holidays (nd), the July among the May and June are most popular months in Ukraine to spent holiday. If this is found to be a plausible explanation, seven out of 15 (47%) missing published tweets could be explained. These two reasons combined would explain eleven out of 15 or 67% of missing samples. No apparent or plausible explanation was found for the rest of the missing samples. This finding supports the suggestion that there is a certain schedule, and the publishing is conducted by a person or by persons manually.

When the actual content in the audiovisual material was examined, the following findings were made. Average length of a telephone conversation in Russia in 2022 was 4 minutes (Howarth, 2023). The average duration of the conversation over the samples (n=261) was 0.01.50 with standard deviation of 0.00.53. Also, it was found that statistically, the length of the audio content was reducing over time. This anomaly is shown in figure 20 below.

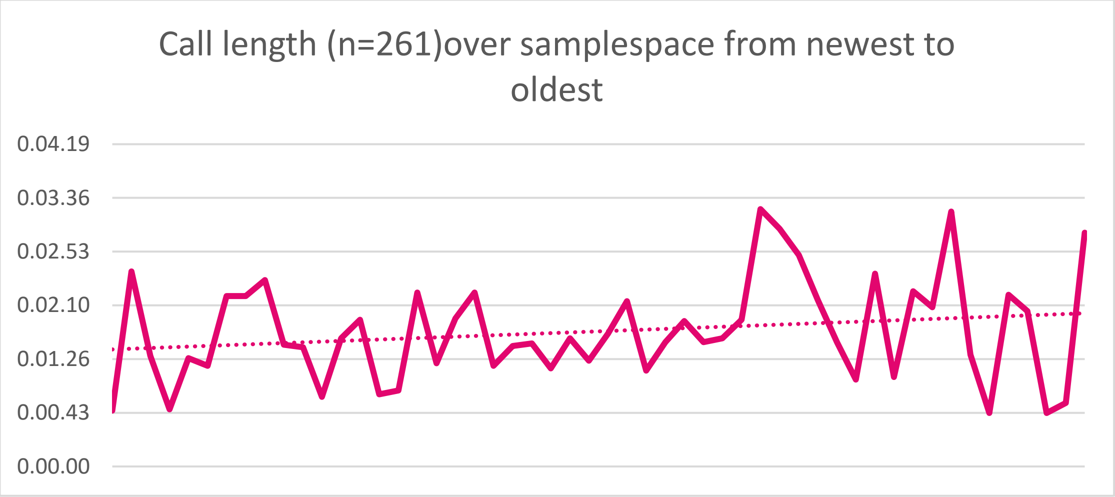


Figure 20. Call length evolution from newest to oldest sample (n=261).

Figure 21 below shows that the variability of the content decreases and its overall monthly duration stabilizes. This development suggests that the content has evolved in a more efficient direction. The message that is delivered to the public has either been more efficiently edited to contain only the content that is wanted to be released, the original phone calls are more edited or the actual phone calls have become shorter.

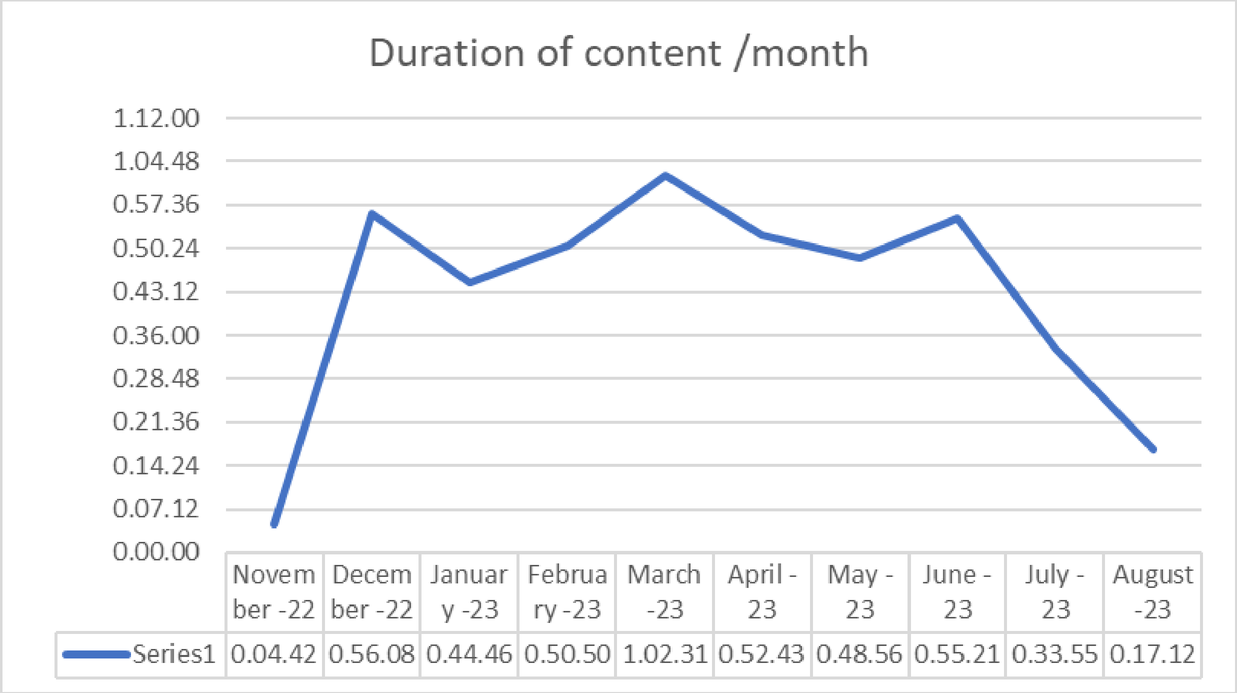


Figure 21. The average duration of content per month

The monthly average duration of actual content was examined. It was noted that the duration of the calls did not have much variance, with the exception of November 2022, in which the sample size was exceedingly small and in the August 2023. The duration of the calls in the content did differ significantly from the average length of usual Russian call duration. This suggests that either the content has been edited and only the purposeful content has been published, or some unidentified causes have been affecting the length of the published calls. If the natural causes would have been affecting the length, there should be more variation in length of individual calls. This would prefer the option that suggests that the content has been edited.

7.4 Analysis by themes

The thematic study was conducted by using pre-determined themes. All samples in the dataset had at least one (min=1) variable presented, while maximum was 5 (max=5). Distribution of the themes on the dataset is presented below in the figures 22 and 23.

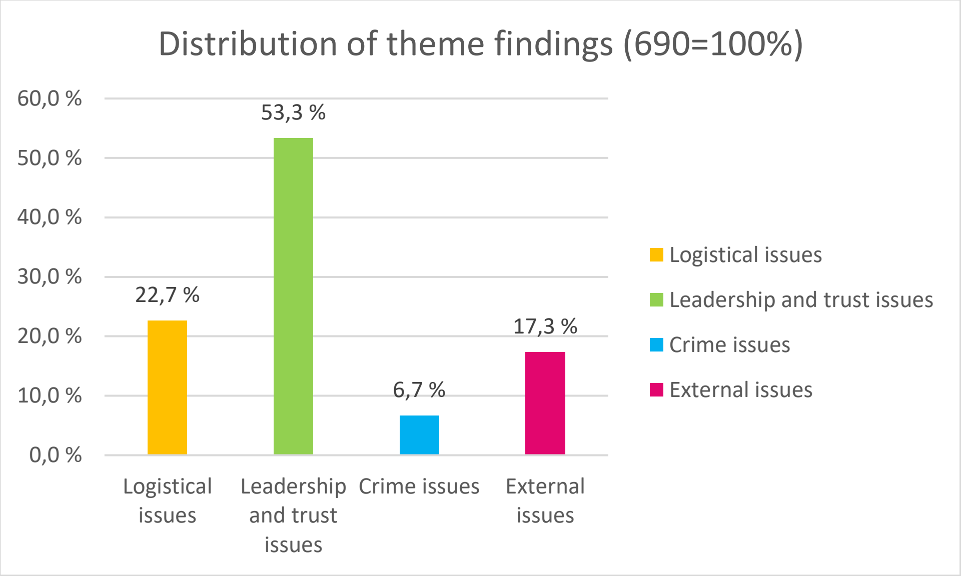


Figure 22. Distribution of themes (%)

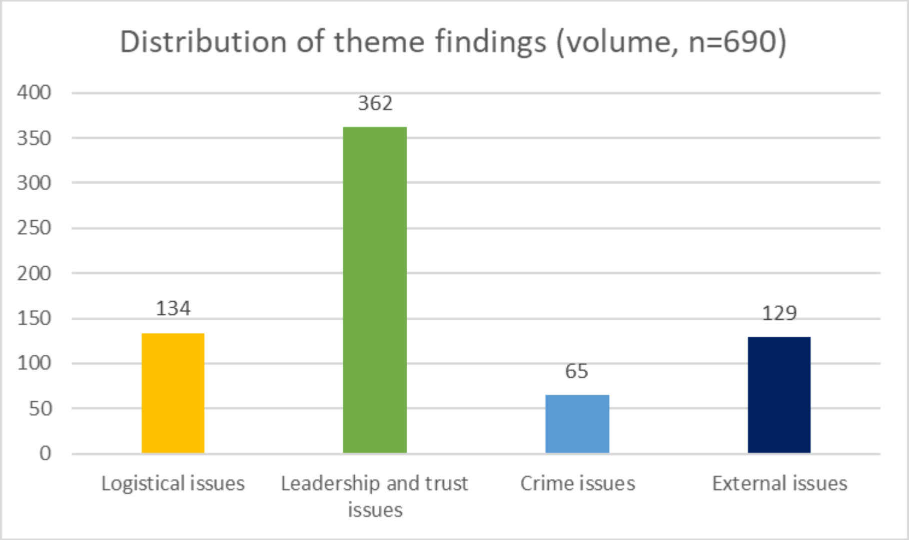
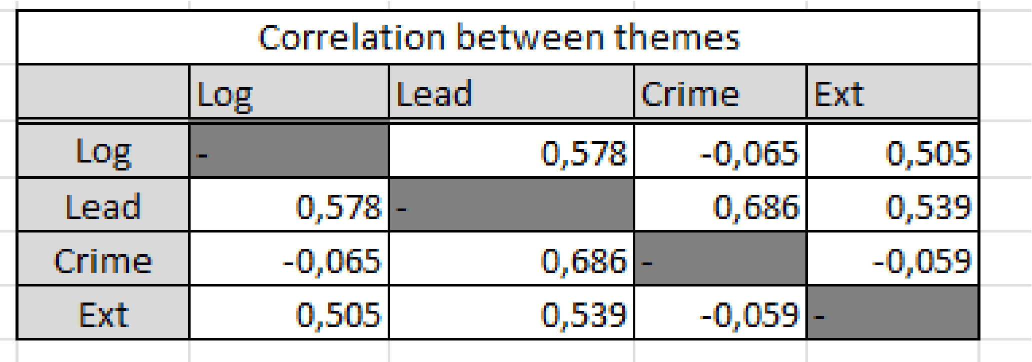


Figure 23. Volume based distribution of themes.

The “leadership and trust issues” was the most presented theme in the samples of the dataset (53,7%, n=362). The variables of “Crime issues” were least presented when the content was analyzed. This would suggest that the content does not support the narrative of “crimes of Russian forces. This finding with “logistical issues” and “External issues” would counter the for “Second army of the world” and “Russia is winning” narratives (Topalskyi & Ivanenko, 2020) Variables of “Crime issues”-theme were least presented items. This suggests that the main purpose of this content is to counter the Russian narrative and only secondarily support the Ukrainian own narrative.

Correlations between themes were evaluated. This was conducted using Excel- function “CORREL (array1;array2)”. The correlation is evaluated in scale of -1-1, where -1 means perfect negative correlation and 1 means perfect correlation between the variables. The value that is near 0 means that no correlation between variables is found. The values near I 0,5 I show reasonable correlation. It was found that there were few reasonable correlations between themes. “Leadership and trust issues”- and “Crime issues”-themes did have the strongest correlation, while “Criminal issues”- and “external issues”-themes did not have a correlation at all. This would suggest that the themes did occur evenly over the dataset. The strong correlation between “Leadership and trust issues”- and “Crime issues” was expected, because bad leadership does weaken the ethics of the subordinates (Schafer, 2010). The results of this are presented in table 6 below.



Correlation between themes				
	Log	Lead	Crime	Ext
Log	-	0,578	-0,065	0,505
Lead	0,578	-	0,686	0,539
Crime	-0,065	0,686	-	-0,059
Ext	0,505	0,539	-0,059	-

Table 6. Correlation between themes

The themes did occur in the dataset evenly, the variation between the themes did not change drastically over the time. The prevalence of the theme “Crime issues” in the material increased more strongly than other themes at the samples from July 2023 to August 2023, with no apparent explanation.

The overall number of themes, with exception of “logistical issues” -theme did have a significant drop in July 2023. Monthly distribution is presented in figure 24.

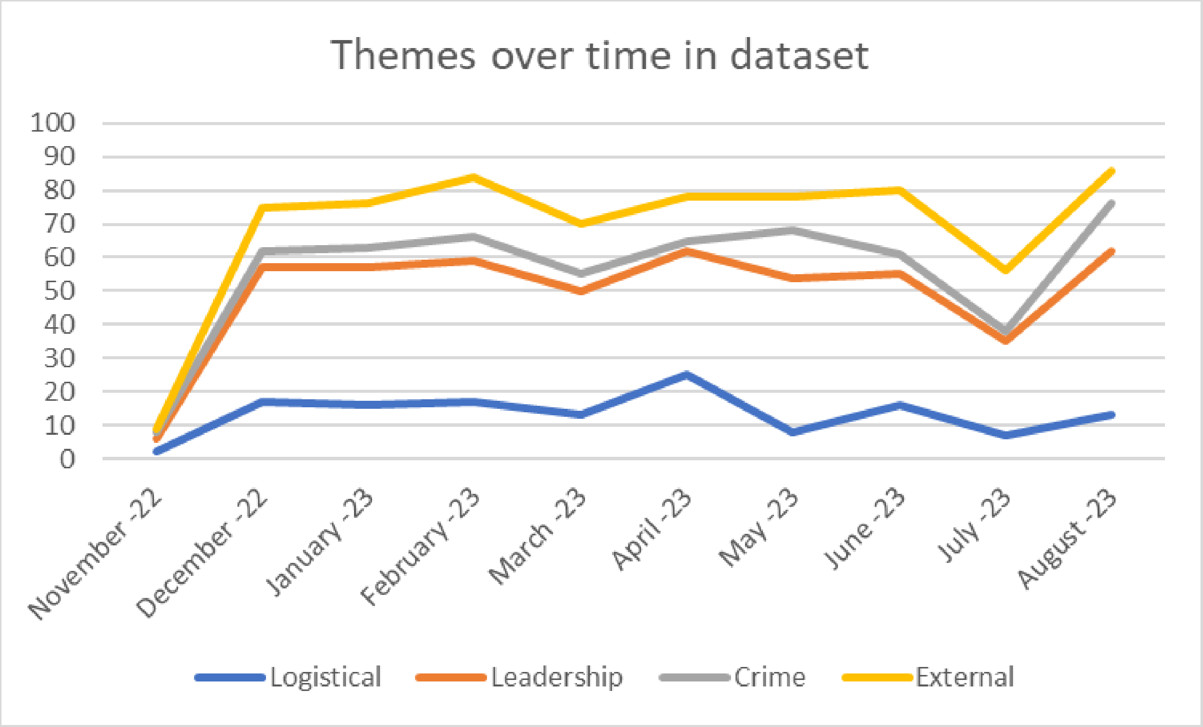


Figure 24. Monthly distribution of occurrences of the themes.

The selected variables were examined separately and the appearance in the dataset was analyzed. The dependencies and correlations were not analyzed statistically. In the instances where the logical reasoning would suggest such, the possible suggestion was reasoned by comparing the variable to another logical variable. There was a significant drop in all themes except in "logistical issues"-theme in July 2023. This could indicate a weakened evaluation or inspection process during that month. The relative distribution of variables is presented in the figure 25.

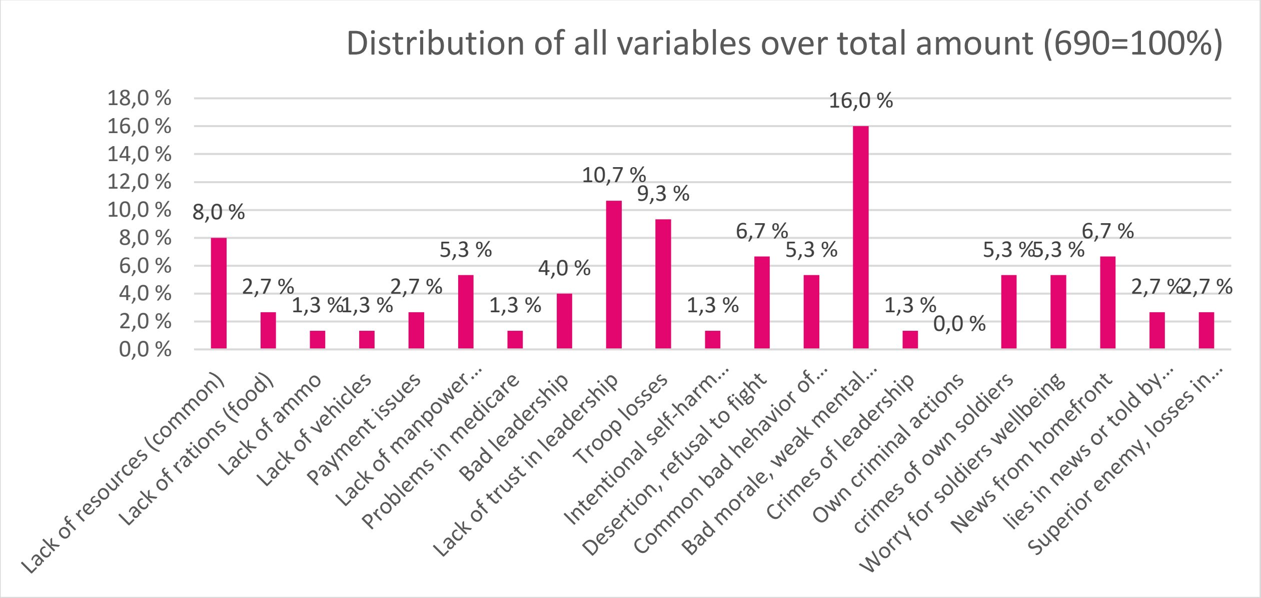


Figure 25. Distribution of variables over the dataset

When the content of the dataset is seen from the viewpoint of all of the variables, the variable "Bad morale, weak mental state" is found to be the most common variable (16,0%). Variable "own criminal actions" variable is least to appear in the content. The presence of variable "Bad morale, weak mental state" could be explained by the soldier's need to express the outcome of various difficulties through the personal effects that they inflict.

The personal need for preservation would explain the absence of the variable "own criminal actions". It would be hard for a person to self-criminate oneself, even to the significant one, to another family member, or to the friend. This would be held as evidence for the claim that the content is actual and intercepted and eavesdropped by Ukrainian intelligence actors. If the content were falsified, it would be reasonable to expect more content, that would include stories about crimes that oneself has been committing.

“Logistical issues”- theme was least presented over the time in the dataset. The logistical issues theme did appear regularly over time during the collection time. The trend was very stable, as can see in figure 26 below. The instances did peak in April 2023, when the number of instances went to 25, while the lowest value was on July 2023 (n=7). The issues of logistical process of the Russian armed forces have been a constant theme in media from the start of the invasion, so it is very logical that it would be a common theme in the published content.

A particularly good, published example of Russian logistical issues was the 64 kilometers long halted convoy at the start of the invasion (BBC, 2022). Other issues, which have been out in the public are the weak condition of Russian transport capacity (Lendon, 2022), ability to supplement personnel losses (Osborn, 2022), and salary payment issues (Lyall, 2022). Distribution of themes over time is presented in figure 26.

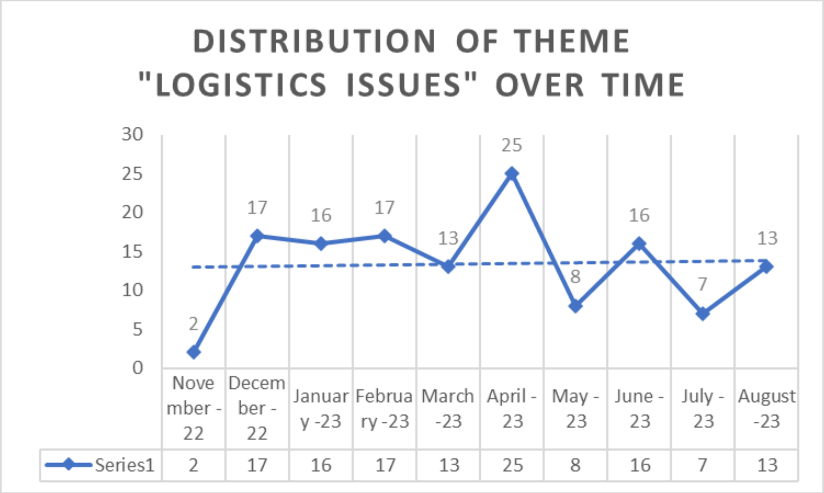


Figure 26. Distribution of the theme "Logistic issues" over time.

When the theme was researched by variables, it was found that there were 134 instances of variables of theme over the time at the dataset. “Lack of manpower (reinforcement)” – variable did exist the most, while “lack of vehicles” and “payment issues” were least presented. The variation of variables is presented in figure 26 below.

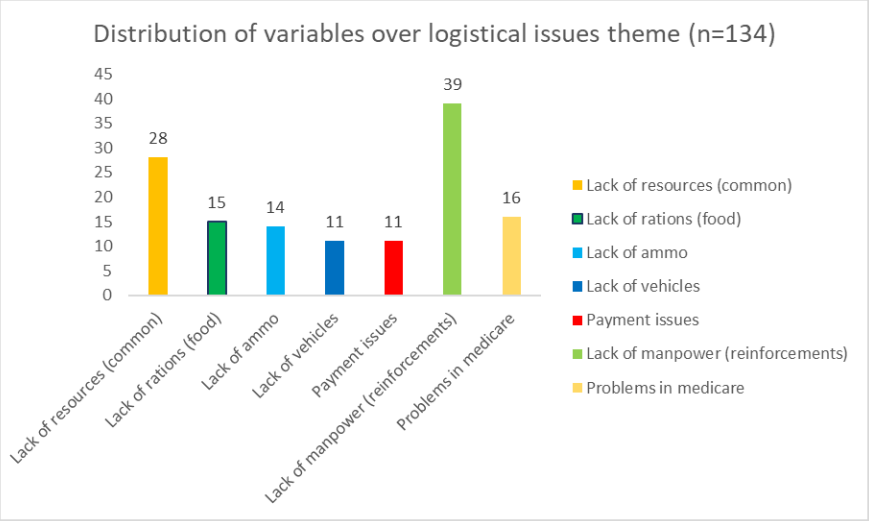


Figure 27. Distribution of variables of the "logistical issues"-theme.

“Lack of resources (common)”-variable was on downward trend over the time in the collected content. The number of appearances in the samples became almost non-existent at the newer samples. This would suggest that the samples were selected to be more accurate in describing the shortage of different resources. This can be validated from the trend from the other variables, in which the trend is either horizontal or rising. The trend and the variation of variable is shown in the figure 28.

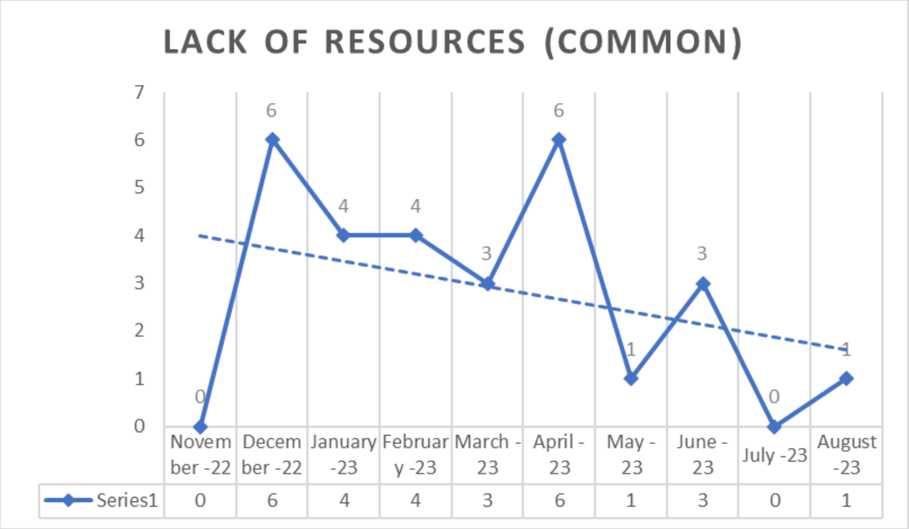


Figure 28. Presence and trend of variable "Lack of resources (common)" over the time.

Variable “lack of rations (food)” did have remarkably high variation over time. The appearance of the variable did peak in April 2023, but it did not exist at all in February and July 2023. The amount of number of variables in total is noticeably big, so the variance can be explained with this. The trend declined over the time. The trend and the presence of variable “lack of rations (food)” is shown at the figure 29.

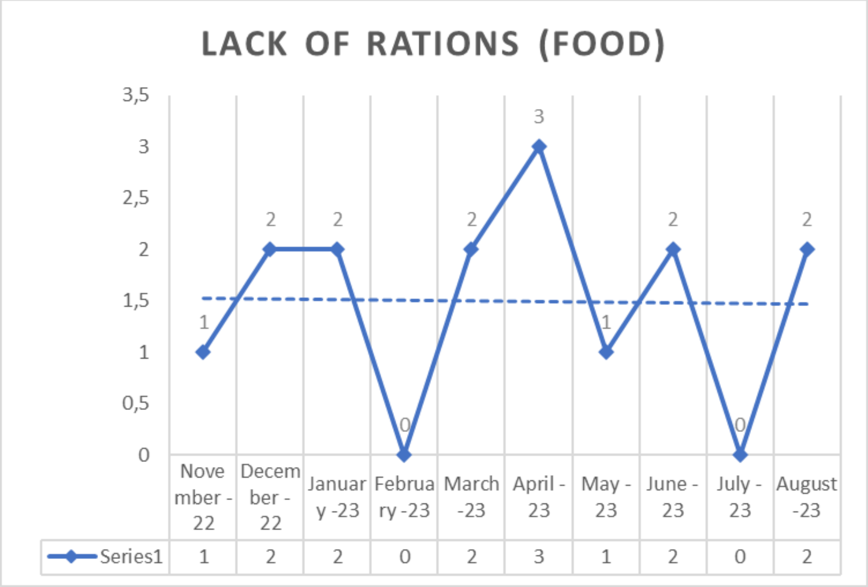
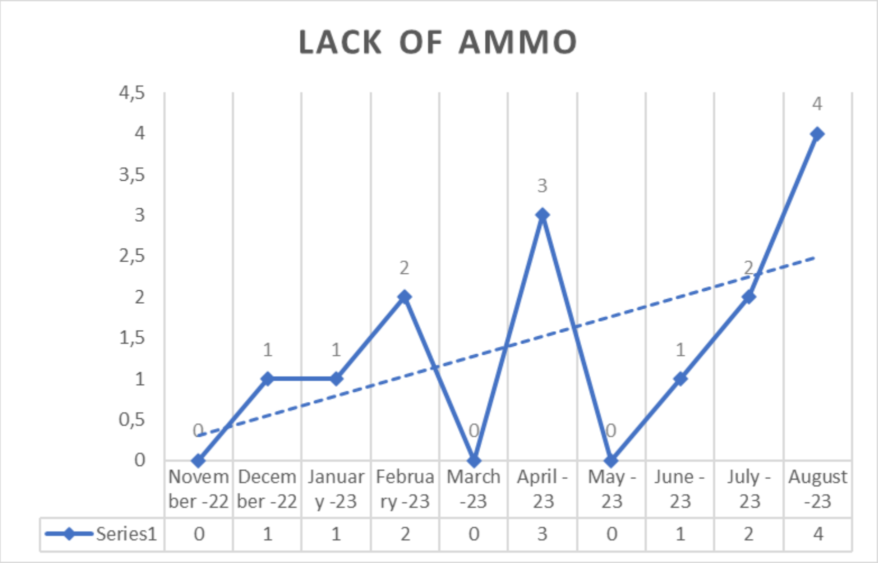


Figure 29. Presence and trend of variable "Lack of rations (food)" over the time.

The trend of variable “lack of ammo”-variable did vary very much but it had very tight upwards trend because of the variable began to appear more often in the content. This suggests that this variable either did appear on the material that the publishing process did get had more occurrences of variable or it was deliberately selected to appear on the content. The lack of ammunition theme did occur in the public media more often in the fall of 2023. For example, Russia had to purchase ammunition from North Korea, because of inability to produce enough artillery shells for the army (Inocensio, Redman & Reals, 2023).



	November -22	December -22	January -23	February -23	March -23	April - 23	May - 23	June - 23	July - 23	August -23
Series1	0	1	1	2	0	3	0	1	2	4

Figure 30. Presence and trend of variable "Lack of ammo" – variable.

Appearance of variable “lack of vehicles” varies over time and the amount of the instances and the amount of the instances, where variable appears, is scarce. This is quite surprising, because the material losses, especially vehicles, is a very persistent theme in different medias (for example, see Hall, 2022). On the other hand, the upwards trend is apparent over the timeline. The presence and trend of variable “lack of vehicles” is shown in figure 31.

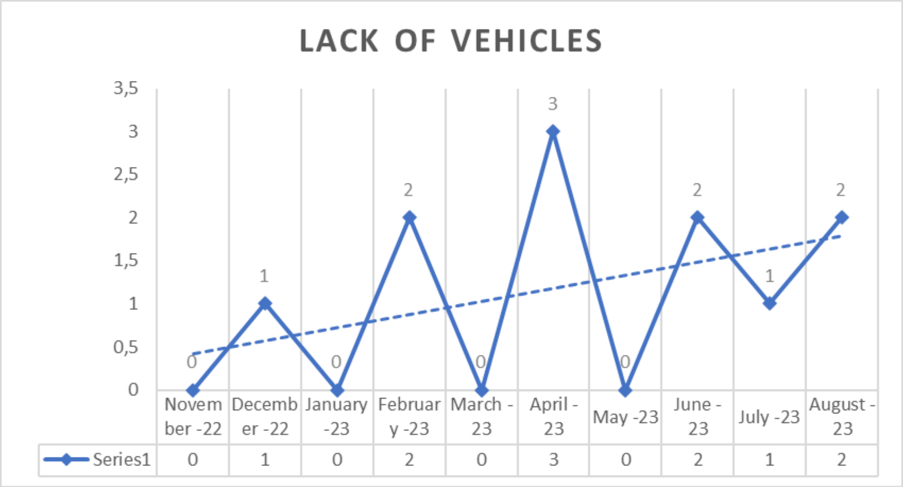


Figure 31. Presence and trend of variable “Lack of vehicles” over the time.

Payment issues – variable does not appear very regularly in the dataset. The peak of presence is in May 2023. This might contribute evidence to narrative, which did appear shortly in western media in April 2023 (e.g., Peck (2023); Artyushenko (2023)). This would suggest that the content with certain theme or variable is selected to support the most prominent narrative. The presence and trend of variable "payment issues" is shown in the figure 32.

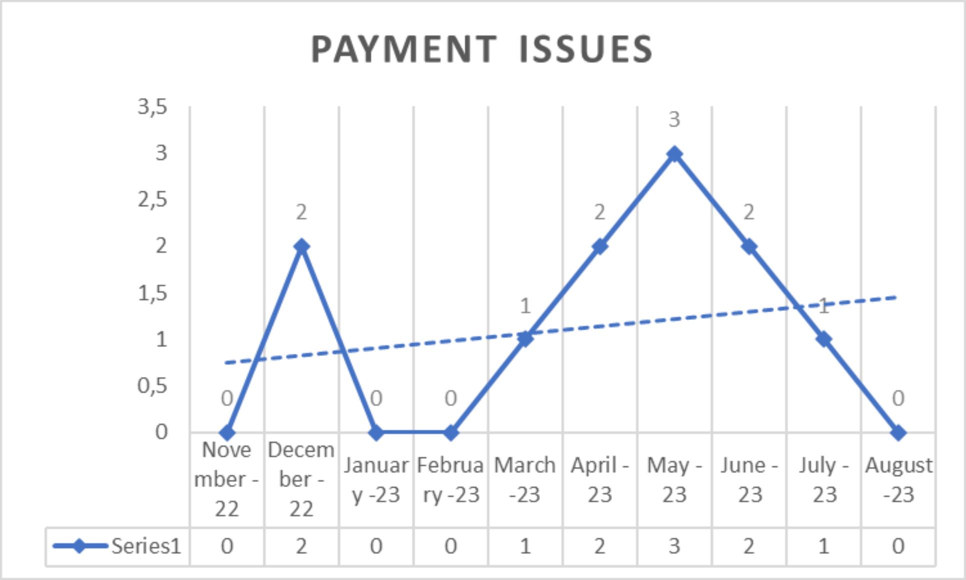


Figure 32. Presence and trend of variable "Payment issues" over the time.

Variable “lack of manpower (reinforcement)” did have small variance but a declining trend. The finding of the decreasing trend in the variable was surprising because the “loss of troops”-variable in the “leadership and trust issues”- theme was very often presented in the dataset over the time. This would suggest, that either the persons that whose conversations were eavesdropped did not find this to be an issue, they were used to the scarcity of manpower, or they just did not want to discuss about the issue. Other viewpoint would suggest that this was not an issue that was seen as an efficient variable to be published. If the latter viewpoint is considered to be the reason, there would be some form of selection process of what kind of message the publishing content contains. The presence of “lack of manpower (reinforcement)” variable and trend is shown in the figure 33.

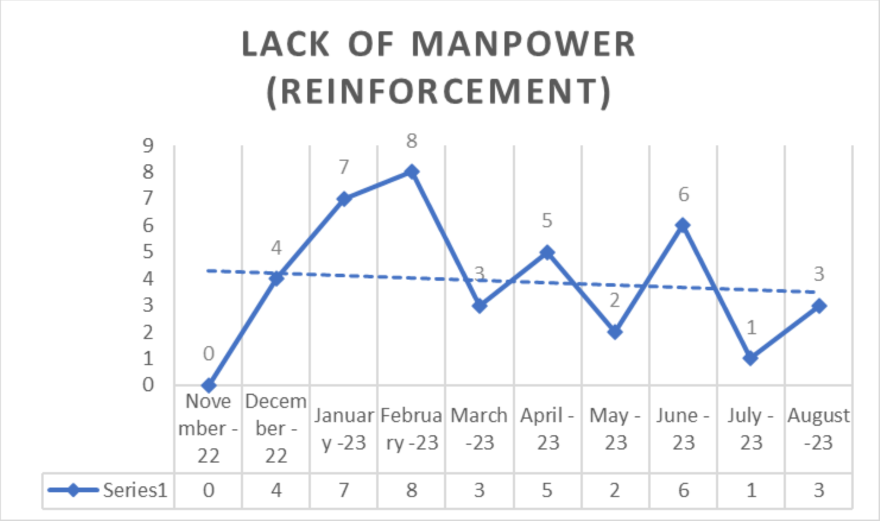


Figure 33. Presence and trend of variable "Lack of manpower (reinforcement)" over the time.

The trend in variable “problems in Medicare” is decreasing slightly over time. The variance in the appearance of the variable is high, the peak is in March 2023, and the variable does not appear in the content at all in June 2023. As expected, the most popular issue was overcrowded hospitals, and the under resourced medical care. This was not a surprise, because it would be in line with “troop losses”-variable in “leadership and trust issues”-theme. The presence and trend of variable “problems in Medicare” is shown in the figure 34.

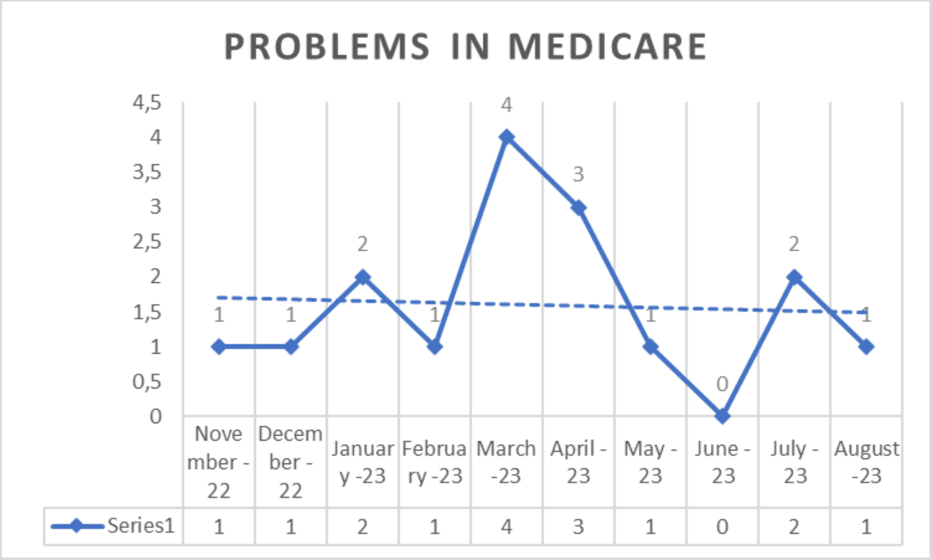


Figure 34. Presence and trend of variable "Problems in Medicare" over the time.

Theme “leadership and trust issues” has low variance over the collection time of the dataset. The trend that can be seen in Figure 36 appears to be rising over time. This could suggest that the trust to the ability of the leadership is diminishing, and the material that Ukrainian intelligence actors collect contains more of such content. The occurrence of this theme suggests that the content is undermining the narrative of “second army of the world” (Topalskyi & Ivanenko, 2020).

The most commonly perceived variable is “Bad morale, weak mental state, which presents 28,2% of all findings. The variable “intentional self-harm intentions” was the least presented variable (1,1% of all findings). “Bad morale, weak mental state”- variables presence in the dataset would mirror the effect of other negative variables. The low morale variable has been a persistent theme from the beginning of the invasion phase of the war (see e.g., Osborne (2022); Lyall (2033)). The distribution of variables is presented in the figure 35.

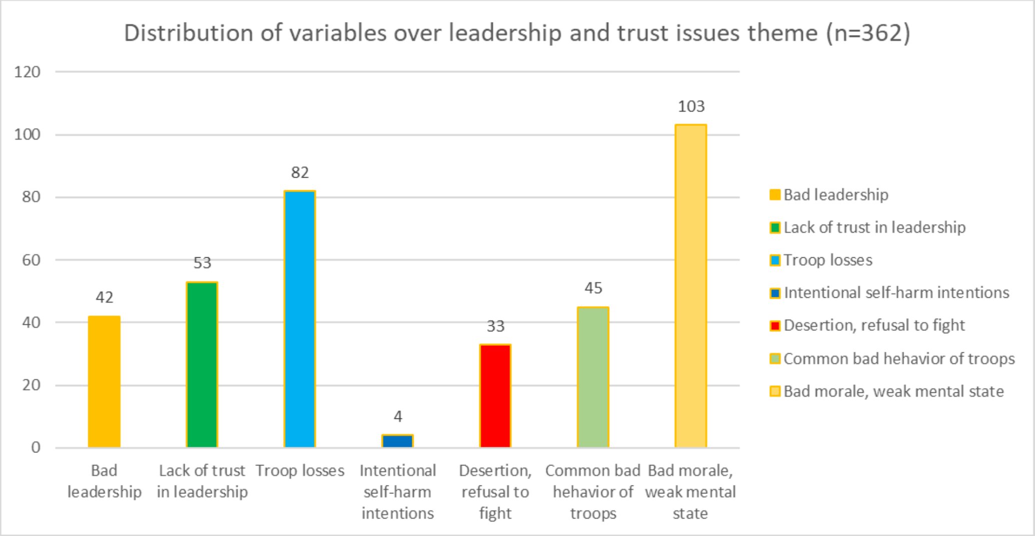


Figure 35. Distribution of variables of the "leadership and trust issues"-theme.

The low occurrence of variable “intentional self-harm intentions” is a surprising find. The narrative of self-sabotaging Russian troops was at the public media. Among other things, the self-harming was also an issue with the Russian armed forces (Akhbar, 2022). This suggests, that either the material that was obtained by the Ukrainian intelligence services did not include such material, or it was not seen important subject to publish.

Bad leadership is the most common variable found in the samples that present “leadership and trust issues”-theme. It might be understandable, when another party of communication can perceive the quality of the leadership in the battlefield. If the nature of the communication is to be negative in nature, mistakes and problems with leadership are easy topic. This suggests that the content is selected, because the dataset does not present any samples that would have anything positive about the leaders or would raise positive topics about leadership. From the statistical viewpoint the trend at this variable is rising over time. The presence and the trend of variable is shown in figure 36.

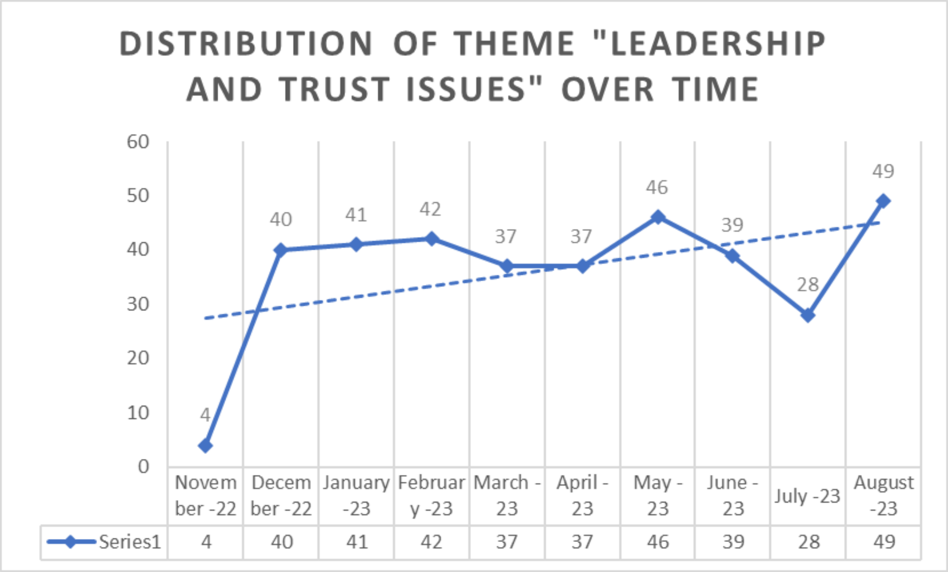
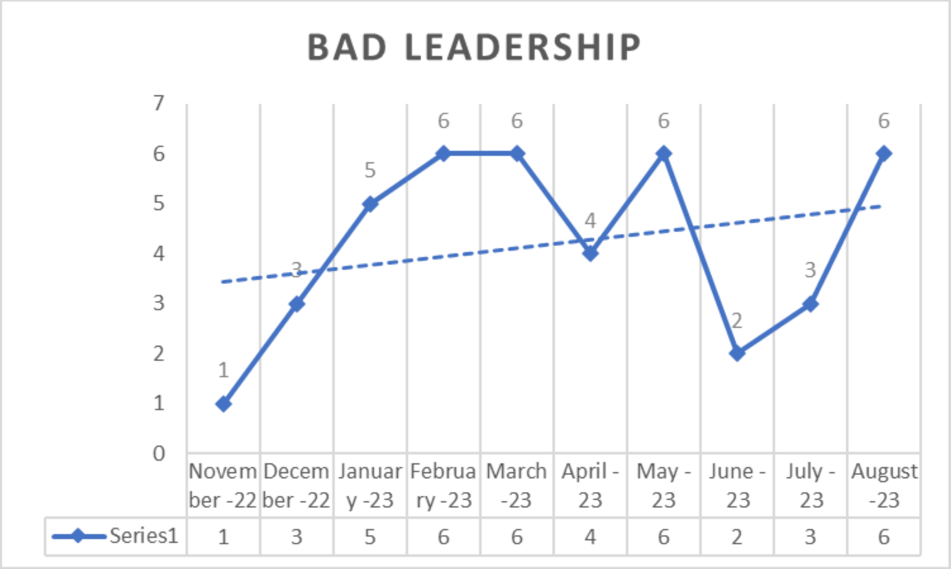


Figure 36. Distribution of the variables of the theme "Leadership and trust issues" over time.

Bad leadership can be seen as a default topic when the inability of leadership is discussed. This variable has a rising trend over time. Variable has a significant drop in June 2023, and it returns to normal and expected level in August 2023. The eccentric drop in June can be seen in other variables too and suggests that the content selection process is not as precise as in other time periods. This might be explained by the absence of a person or personnel that has been running the process at other times. The presence and trend of variable is shown in figure 38.



	Novem ber -22	Decem ber -22	Januar y -23	Februa ry -23	March -23	April - 23	May - 23	June - 23	July - 23	August -23
Series1	1	3	5	6	6	4	6	2	3	6

Figure 37. Presence and trend of variable "Bad leadership" over the time.

The “lack of trust in leadership”- variable has an upwards trend over time. The appearance of the variable is constant over the sample space with a minor notch in July 2023. Trust in the leadership can be seen as a determining factor to the efficiency of the organization or the personnel (Mineo, 2014).

This variable could be seen as determining factor among the bad leadership-variable to all other variables in “leadership and trust issues”-theme. The presence and trend of variable is shown in figure 38.

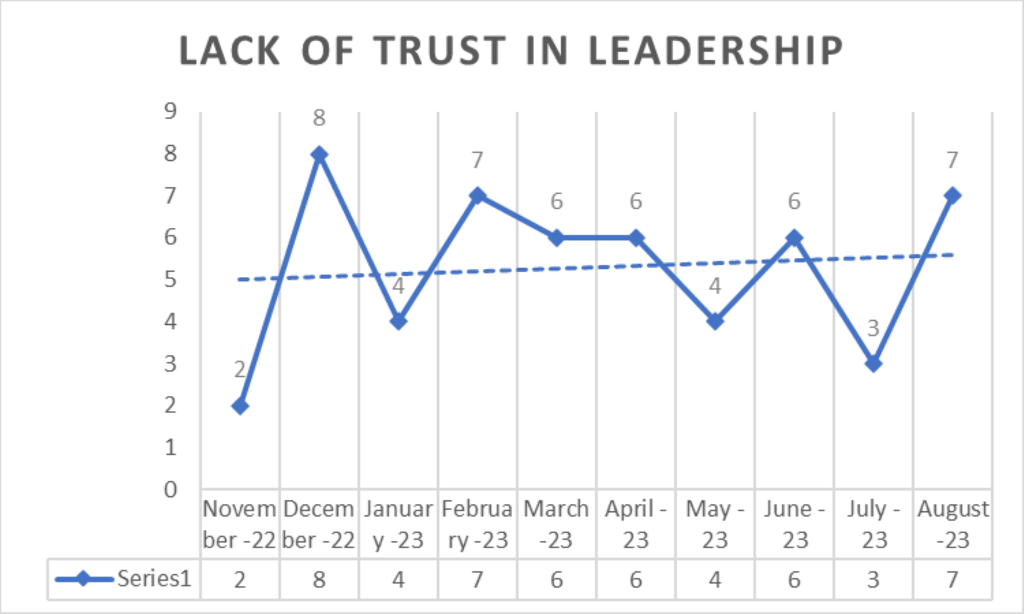


Figure 38. Presence and trend of variable "Lack of trust in leadership" over the time.

Figure 39 shows that the volume of the observations of variable “Troop losses” has been constant, but the trend is upwards. The variable “troop losses” was the third most common variable among all variables. The variance in presence of instances over the time with the variable is low. The variable has a very rapid rise from November 2022 to February 2023 following sharp decline to March 2023. . The presence and trend of variable is shown in figure 39.

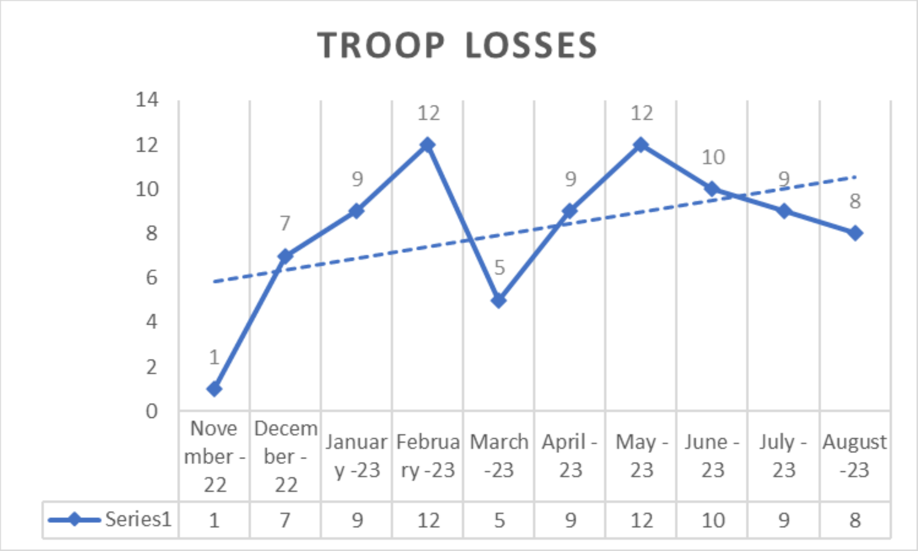


Figure 39. Presence and trend of variable "Troop losses" over the time.

The lack of presence of “intentional self-harm intentions”-variable in the dataset was a surprise when it was compared to the other variables in “leadership and trust issues”-theme. According to Daniel and Metcalf (2015) poor-quality leadership can lead even to intentional self-harming behavior.

The number of “bad morale, weak mental state”-variable instances would suggest that this variable should be more presented in the dataset over time. Another surprising finding in this variable is that the trend is horizontal despite other indicative variables, whose trend was rising. The presence and trend of the variable is shown in figure 40.

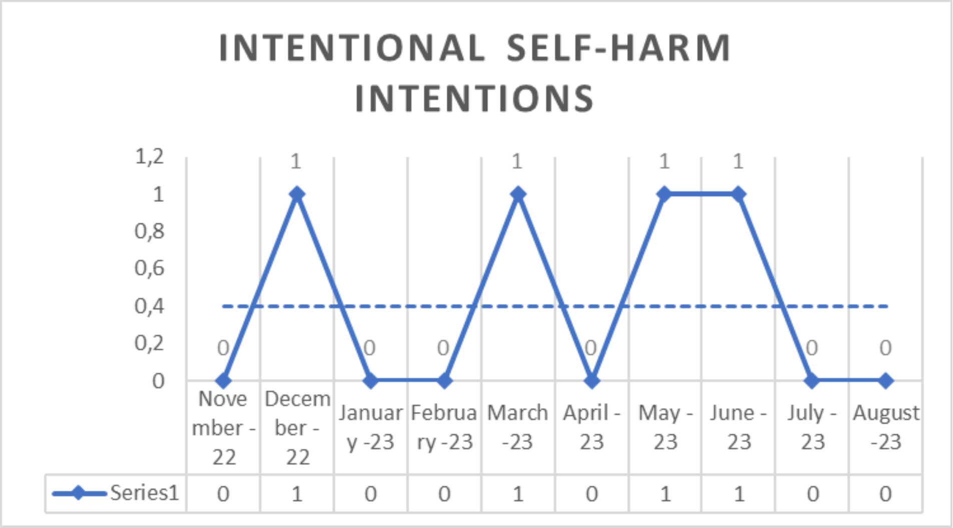


Figure 40. Presence and trend of variable "Intentional self-harm intentions" over the time.

The trend of variable “Desertion, refusal to fight” was rising over time. While comparing this to “Bad morale, weak mental state” this was expected development. The variation of appearance of the variable was low and it did not have any sharp declines, and it did reach its highest value at the end of timeline. The presence and trend of variable is shown in figure 41.

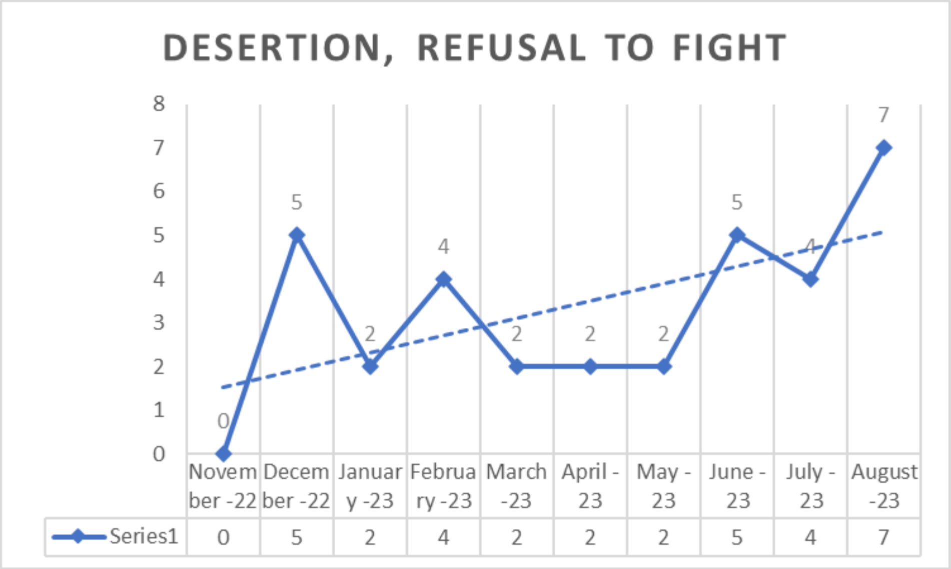


Figure 41. Presence and trend of variable "Desertion, refusal to fight" over time

The trend in variable “Common bad behavior of troops” is rising over time. The lack of presence of variable in the June 2023 is unexpected, because the volume had exceptionally low variance over the previous months. The variable can be seen to support the narrative of Russian army war crimes (Kienneman, 2023). The presence and trend of variable is shown in figure 42.

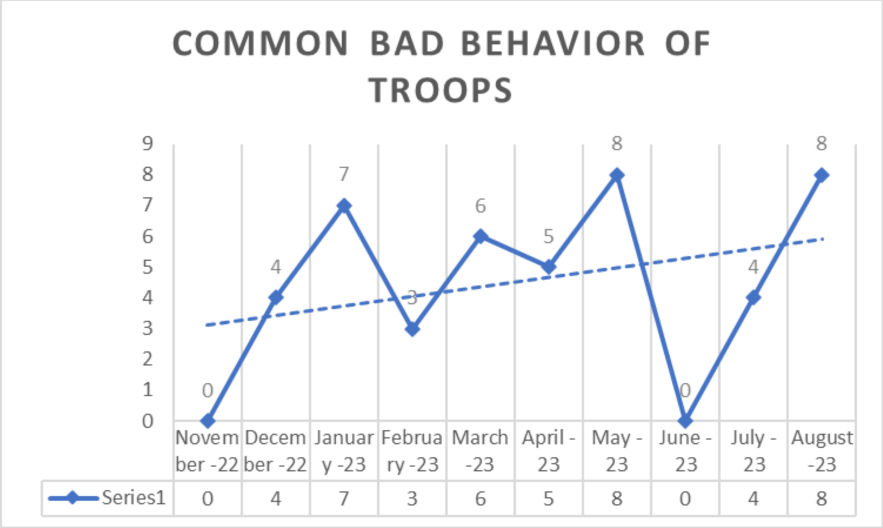


Figure 42. Presence and trend of variable "Common bad behavior of troops" over the time.

Criminal issues theme was divided to three variables, which would indicate either perceived crimes that were conducted by leadership, one's own conducted criminal actions, and perceived or heard unlawful actions of other fellow soldiers. The variables of criminal issues theme would strengthen the Ukrainian narrative of crimes conducted by Russian army. The presence and trend of trend is shown in figure 43.

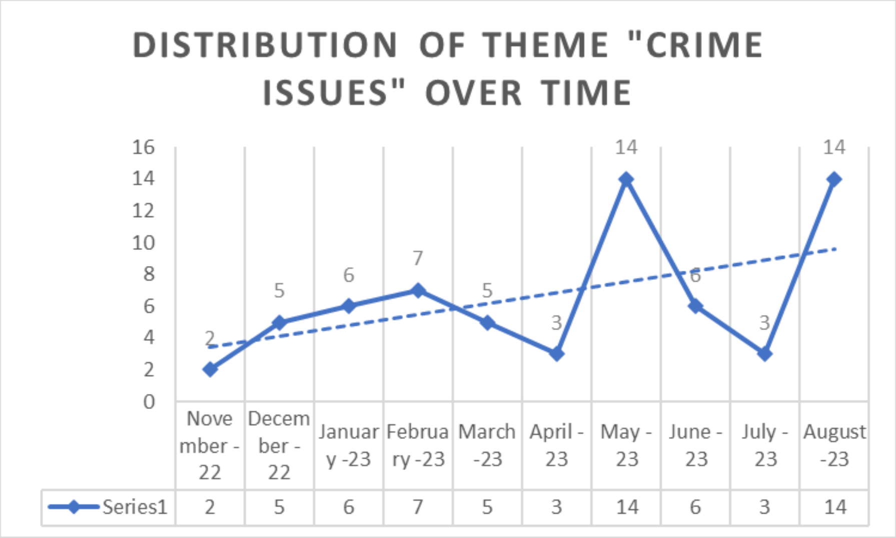


Figure 43. Distribution of the variables of the theme "Crime issues" over time.

The instances of variables of “Criminal issues” – theme did have upwards trend over the time. The peaks of the instances did occur in May 2023 and in August 2023, indicating that the volume would be rising even higher. Most of the instances of the variables of “crime issues”-theme were from “Crimes of leadership” and “Crimes of own soldiers”-variables. “Own Crimes”- variable occurred only occasionally. The total count of variables and their numerical distribution of occurrences is presented in figure 44.

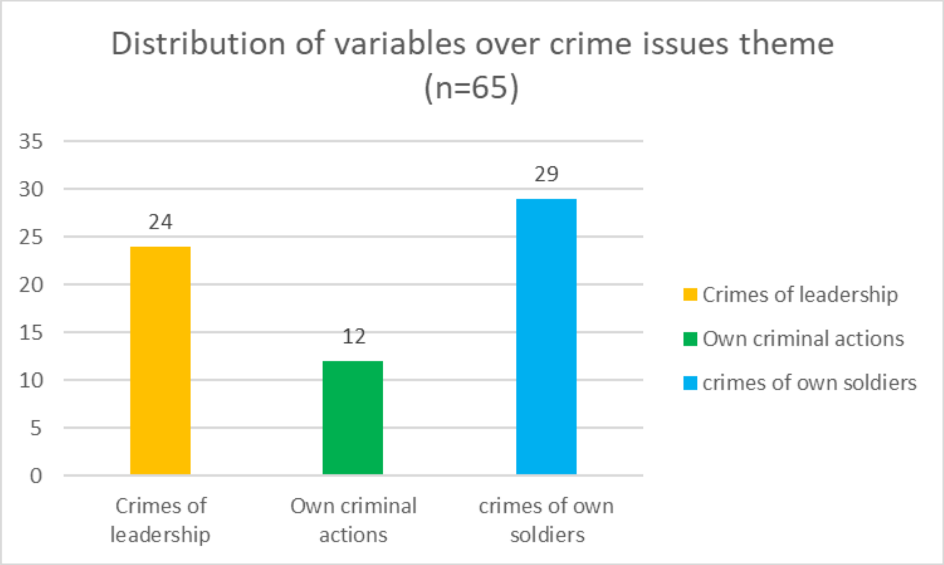


Figure 44. Distribution of variables of the "crime issues"-theme.

The appearance of variable “crimes of leadership” did spike at the spring-summer 2023. The correlation between the themes “Crime issues” and “leadership and trust issues” would have effect on this phenomenon, or it could be an explanative element to the said statistical correlation. The trend can be seen rising over time. If this is examined from the viewpoint of Schafer (2010) and if the correlation between the “leadership and trust issues”- and “Crime issues”- theme is investigated, the trend could be explained through the long-term issues with bad leadership. This would suggest that the material from which the content is extracted contains increased indications of acts of crimes that leadership is participating.

This would be a result of the decaying trust in the leadership, not just an increase of crimes that leadership committing. This suggestion would be supported by the effect of trust to leadership by Mineo (2014). The trust in leadership affects people's efficiency and morals, and if this trust is weak, the people are more prominent to perceive unlawful behavior of leadership (Mineo, 2014). The presence and trend of variable is shown in figure 45.

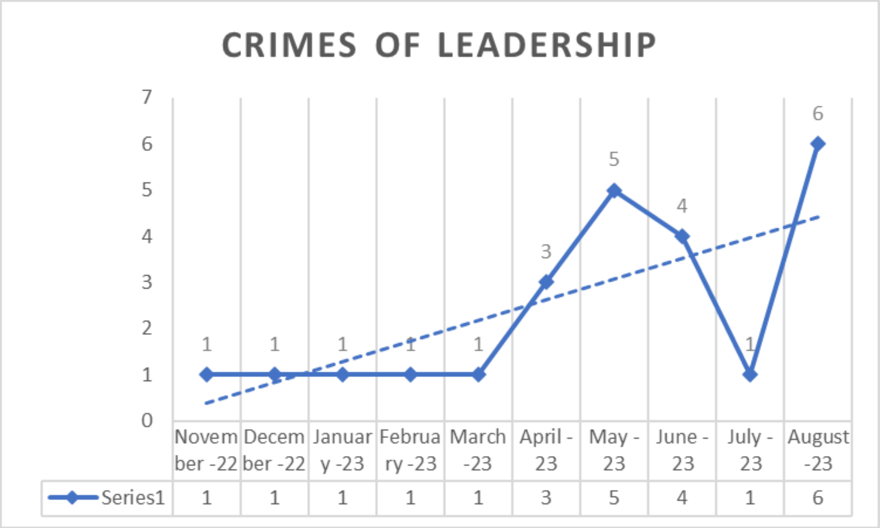
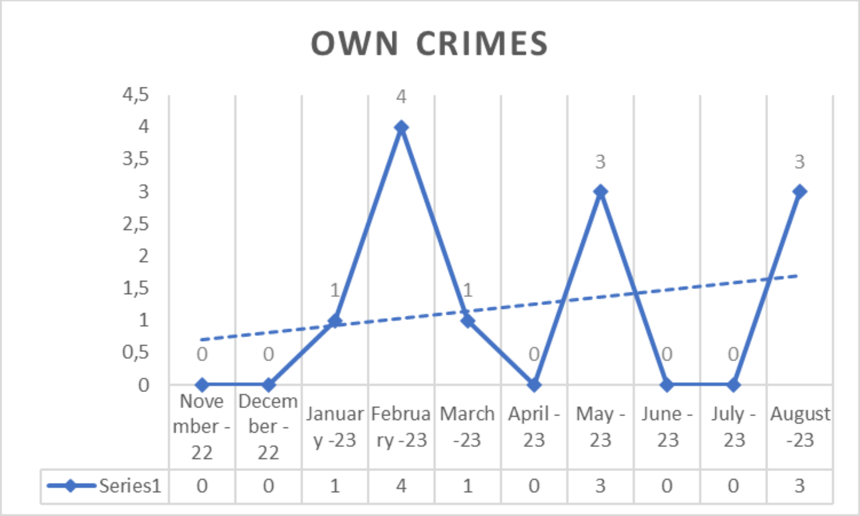


Figure 45. Presence and trend of variable "Crimes of leadership" over the time.

The appearance of "own crimes" – variable was polarized. It could be hypothesized that self-preservation would hinder the conversation of own crimes, so the material that consisted confessions of own criminal actions would be scarce. The appearance of "own crimes"-variable did peak at February 2023. An upwards trend was found, but the number of instances and the variance over time would not support the validity of the finding. The presence and trend of variable is shown in figure 46.



	November -22	December -22	January -23	February -23	March -23	April -23	May -23	June -23	July -23	August -23
Series1	0	0	1	4	1	0	3	0	0	3

Figure 46. Presence and trend of variable "Own crimes" over the time.

The trend of "crimes of own soldiers" was slightly rising over time. The variance was mostly small, but it did decline in April 2023. A reasonable explanation for the phenomenon could not be found.

This variable, like the two other variables did not occur very often, which would support the authenticity of the content. If the content were fabricated, it would be intuitive to expect more occurrences of this variable in the dataset. The presence and trend of variable is shown in figure 47.

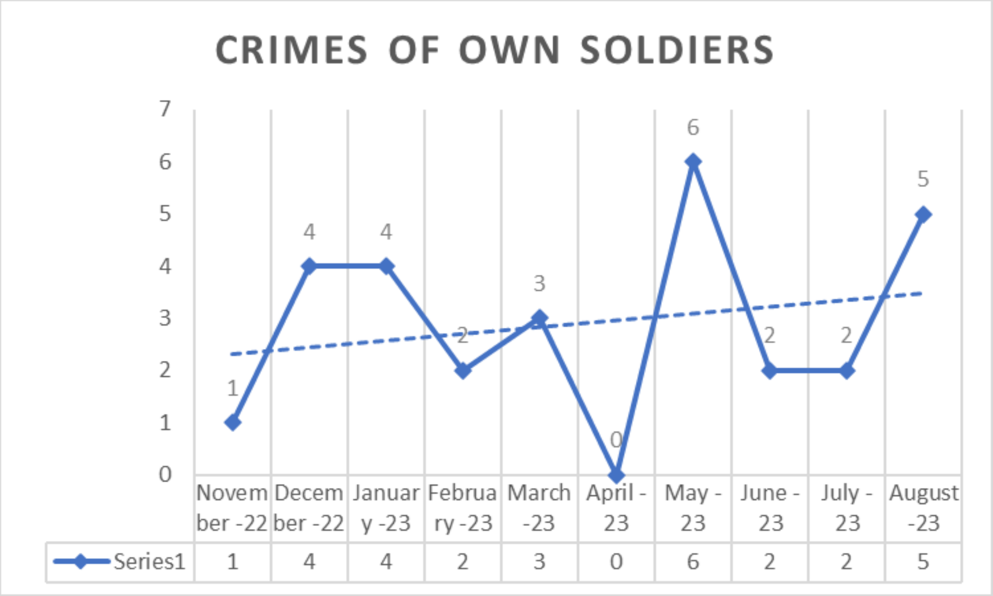
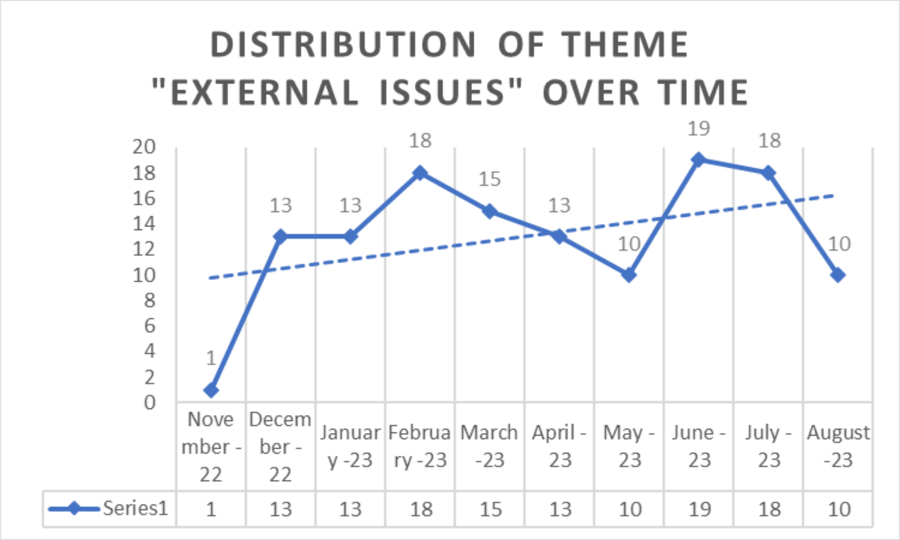


Figure 47. Presence and trend of variable "Crimes of own soldiers" over the time.

External issues consisted of items and incidents, that mostly would happen when the person or party that is not at the warzone, would be the active party at the conversation, either presenting worry for the party at the frontlines or at conflict area, or would present a statement that either is negative or would be debunked as a lie by the party at the frontline. This would suggest that the feelings of the party that is not at the warzone are conflicting the narrative of quick victory (Kienneman, 2022), narrative of mighty army of Russia (Topalskyi & Ivanenko, 2020). On the other hand, the narrative of victories or successes of Ukrainian armed forces by the parties would present content, which would undermine the Russian narrative of victorious war (Kienneman, 2022).

The upwards trend was noticed over the timeline. The variance was low but the number of instances of this theme seemed to be declining at the end of the collection. The overall number of instanced did peak at February 2023 and June 2023 when the number of instances did sharply return from the lowest value. The sharp decline would correlate with the finding of erratic behavior in the publishing process that was seen in statistical analysis. The presence and trend of the theme is shown in figure 48.



	November -22	December -22	January -23	February -23	March -23	April -23	May -23	June -23	July -23	August -23
Series1	1	13	13	18	15	13	10	19	18	10

Figure 48. Distribution of the variables of the theme "External issues" over time

Most common variable at the “external issues” theme was news from the home front. In this variable, the content did have information from the Homefront to the person that was at the frontlines. The variable consisted of information about possible actions of government, including news about possible mobilization, incidents from other fronts that were then discussed.

The main focus in this theme is that the individual at the home front is a bearer of the information, and the main outcome is one of three of the following: The individual at the front lines is a target of the worry, the individual confirms the news or debunks possible information. The total count of variables and their numerical distribution of occurrences is presented in figure 49.

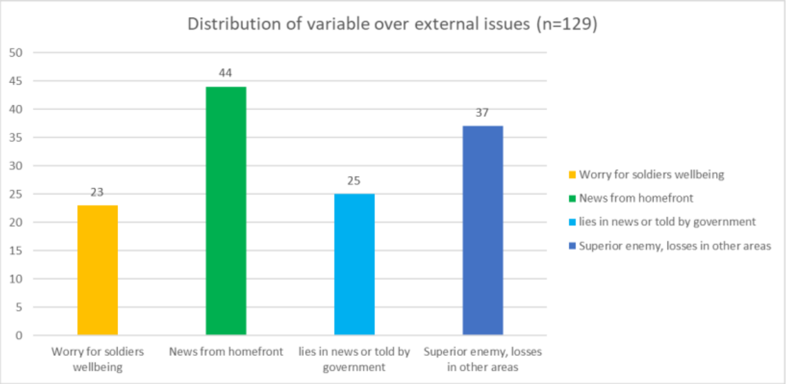
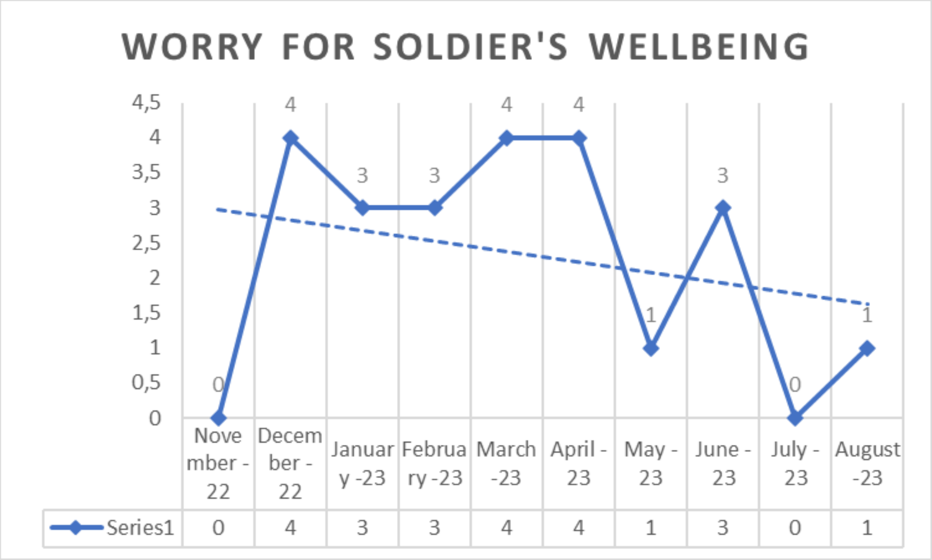


Figure 49. Distribution of variables of the "external issues"-theme.

“Worry for soldier’s wellbeing”- variable did decline very sharply from April 2023 to August 2023. No reasonable explanation could be found for this phenomenon. The appearance of the variable was extremely high with exceptionally low variation to said April 2023, but it did sharply decrease after that. The explanation could not be found for this anomaly. Another explanation is that the publisher does not see this as an important topic in the theme. The presence and trend of variable is shown in figure 50.



	November - 22	December - 22	January -23	February -23	March -23	April - 23	May - 23	June - 23	July - 23	August -23
Series1	0	4	3	3	4	4	1	3	0	1

Figure 50. Presence and trend of variable "Worry for soldier's wellbeing" over the time

“News from the home front”- variable had a stable trend, the appearance of variable did drop sharply at April 2023, but returned at June 2023. The peaks fit to the remarkable events identified in this study, Makiivka incident in January, and mutiny of PMC-Wagner in June. This would suggest that this variable was correlated with noteworthy events, but it did not handle those particular events. The presence and trend of variable is shown in figure 51.

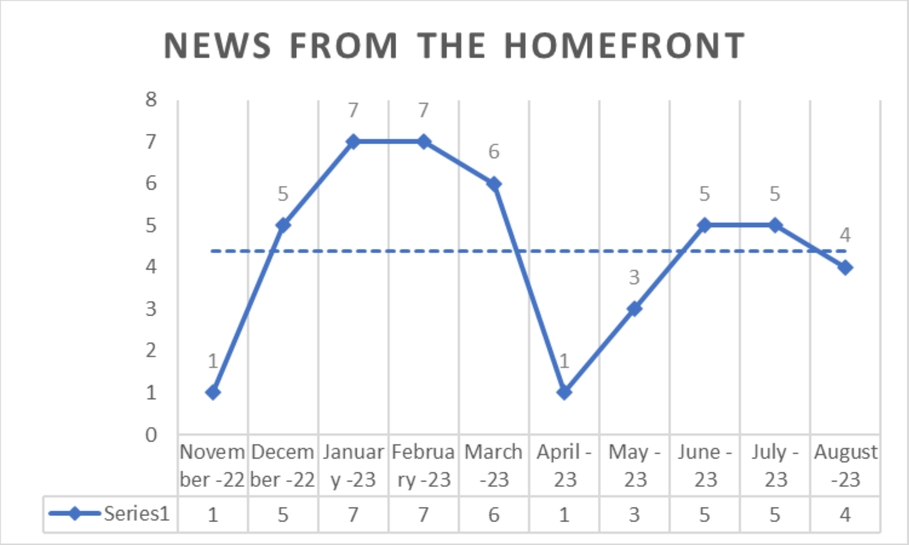


Figure 51. Presence and trend of variable "News from the homefront" over the time

The increase of appearance of “Lies in news told by government”- variable was evident over the time. The number of appearances did peak at July 2023 with the exception of total absence at March 2023, when not a single instance was found from the samples. The August 2023 variable had a sharp decline, but no reasonable explanation could be found for this anomaly.

The rising trend would suggest that there is either a rise of amount of topic at the material or it is wanted to be a trending topic within theme. The presence and trend of variable is shown in figure 51.

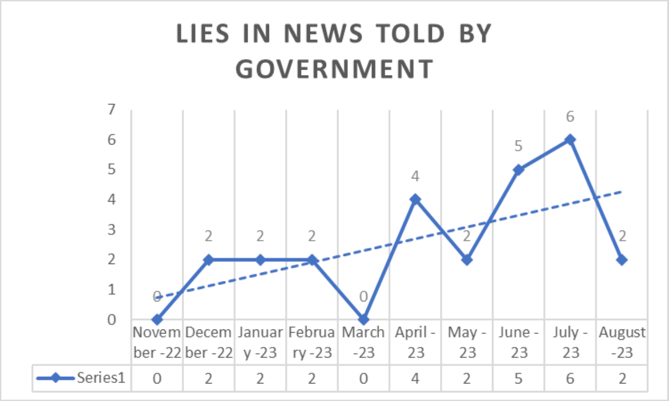


Figure 52. Presence and trend of variable "Lies in news told by government" over the time

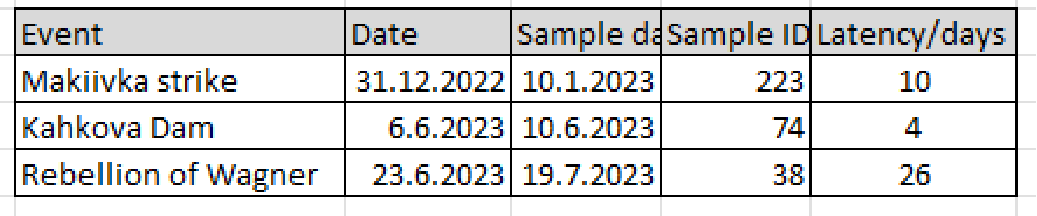
7.5 Analysis for individual anomalies

The remarkable events that did happen during the dataset collection time did appear also in the dataset in singular samples. This was unexpected, because of the magnitude of events they could have been more useful from the viewpoint of propaganda. For example, the sample where two persons discuss the consequences for destruction of the Kakhovka dam, the discussion handles what the troops did after the destruction, not to that who was to blame. From the viewpoint of propaganda, this would have been a great chance to blame Russian leadership for such action that also put the troops to harm’s way.

The Makiivka strike that allegedly did cause significant losses for Russian forces was interesting from the viewpoint of this study. It was most certainly focused for the audience as evidence to witness even more serious loss for Russian forces than it was reported by either side. It also had almost five times views on Twitter than the average sample from the dataset that was collected (average views at Twitter 23115, sample id74 105300). The said sample did not have link to Youtube content, and it has English subtitles embedded to the content, which is extraordinary for any content in this dataset. These details suggest that this content was deliberately focused on the foreign twitter audience that was using Twitter as a source of information of the events of the war.

A short-lived PMC Wagner's rebellion did occur on 23.6.2023. The content did not handle the actual rebellion or march of the PMC Wagner toward Moskva, but speculated the possible fate of Prigotzin, the founder and the leader of PMC Wagner. The sample (ID 38, table 7) was published on 19.7, almost a month after the actual event.

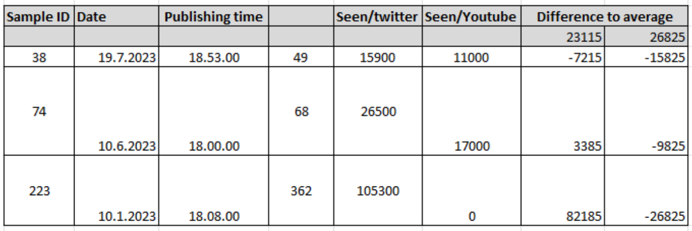
The delay between the actual event and the sample that contained information about it had no pattern or schedule. Because of the small number of events and samples (n=3) no conclusions can be made. From the viewpoint of this study, these individual events suggest that remarkable events are present in the content. The delay in the publishing of individual events is presented in table 7.



Event	Date	Sample da	Sample ID	Latency/days
Makiivka strike	31.12.2022	10.1.2023	223	10
Kahkova Dam	6.6.2023	10.6.2023	74	4
Rebellion of Wagner	23.6.2023	19.7.2023	38	26

Table 7. Delay between the event and the content publication

Only sample that had significantly higher number of views comparing to average views was sample 223, that contained conversation over Makiivka incident. Other samples over other remarkable events did not have any significant effects on the views at the Twitter. Views to samples at the original source did have less than average number of views in all of selected and found individual anomalies. The number of views and statistical analysis is shown in the table 8.



Sample ID	Date	Publishing time		Seen/twitter	Seen/Youtube	Difference to average	
						23115	26825
38	19.7.2023	18.53.00	49	15900	11000	-7215	-15825
74	10.6.2023	18.00.00	68	26500	17000	3385	-9825
223	10.1.2023	18.08.00	362	105300	0	82185	-26825

Table 8. The number of views of individual samples and their relation to average

7.6 Summary of findings

The general findings made from the empirical material suggest that the published content is highly professional and uniform. Every item at the dataset has uniform structure and the quality of the content is high. The level of the graphical layout and design is high, and the content, from the production point of view, is high quality. This finding suggests that the published content has been pre-planned and professionally produced . Published material is professionally made to be presented at the selected platform.

When examining the material, it could be observed that a reasonably accurate schedule was followed in the publication of the content. This suggests that the publishing activity is planned and organized professionally. Only a few deviations were identified in the publishing routine, most of which can be explained with national holidays and holiday seasons. The volume of themes did have a significant drop in the July 2023, which would suggest that the quality of the analysis of the content process had shortage of capable personnel. This would support the hypothesis that there is a person or persons that are responsible for publishing operation.

The content is edited. Harsh language has been censored, so the content would not be labelled to be inappropriate. The length of the content does not correlate to the average duration of phone calls. This suggests that the content has been edited and shortened so that it contains only the part that is wanted to be presented without unnecessary material that increases the length of the content.

The appearance of themes varies over time, but the themes appear in the content persistently. The “leadership and trust issues”-theme is the most popular of themes, while the criminal issues-theme does not appear so often. Overall, published content has some elements of some of the themes that were selected. This suggests that the content is selected in a way that it contains elements that are favorable to Ukraine. No neutral or positive samples that would support Russian narrative were found.

The variables of the themes have variance but appear in the material evenly. No apparent raise during the events that would support or undermine narratives were found. This would suggest that the content is not fabricated but selected from pre-existing material. Also, the individual interesting content that has mentions of events of interest does appear without any apparent frequency. This would also support the hypothesis that the content is authentic and is published when it was found from the collection of the content. From a quantitative point of view, the amount of content about interesting events was exceedingly small. This does also support the hypothesis of genuine content because the opportunity to exploit such major events could have been utilized more effectively if the content were fabricated.

The selection of themes and their variables seemed to suit well to the study. Themes and their seemed to have some correlations, but this was not mathematically verified. A few variables did not appear in a way that was expected. Especially variable “intentional self-harm intentions” did not occur in a way it should have. Either the selection process did not prefer the content that would contain the variable, or the content that had more preferrable and more “selling” content was selected. This would suggest that the content is not produced but is selected from a larger collection of material. This suggestion is supported by the articles of Varris (2022) and Detsch and Mackinnon (2022).

Most of the content is published on Youtube, and only in a few instances the only publishing channel is Twitter itself. This suggests that Twitter is not a primary provider for the content, but a channel to reach to it. The average amount of views to the content in the twitter (23115) compared to that in Youtube (26825) does not differ much. Either Twitter is the main channel to the content in Youtube or views to the content in twitter do not lead to watch or listen the content in Youtube.

8 Conclusions

The research question was set at the chapter 2, in sub-chapter 2.1 was " ***Is it possible, that the private mobile phone communication published by the Ukrainian Intelligence agency at their twitter account be result of the successful cyberoperation or is it a propaganda campaign***?". On the basis of the research of this case, it is estimated to be a cyber operation, the product of which the information obtained has been used for propaganda purposes. However, it has not been an independent propaganda campaign, but a sub-operation of a campaign that supports the national narrative and weakens the enemy's narrative.

The answer has to be approached from two separate domains: cyber and information. Firstly, from a technical viewpoint the first and second sub-research questions have to be given a reasoned answer. Secondly, the third sub-research question has to be answered. Finally, the answers to these questions have to be combined and a reasoned conclusion has to be made.

The first sub-research question was " *Does mobile networking allow eavesdropping in a way that such content can be obtained?"* The answer Is yes. Mobile networking has various exploitable weaknesses that can be utilized. Technical possibilities and opportunities enable eavesdropping and wiretapping. In case of advanced actor, what Ukraine can be assessed as in this field this can be utilized in technical sense and to the extent required of the operator in this case study.

The second sub-research question was: "*Is there evidence of such actions and if so, how have they been implemented ?*" Again, the answer is yes with reservations. In this work we focused on cases in which Ukraine was allegedly implementing such actions and various such cases were found. Such cases were found when the literacy study was conducted. Although only circumstantial evidence was found through public sources, their credibility is sufficient to assess that Ukraine has sufficient capabilities, motive, and will goal to carry out information acquisition by eavesdropping on mobile network traffic in various ways. The articles (Orlova, 2023; Varris, 2022) even suggested that Ukraine had problems in processing the material that they had obtained. Hornbyk (2022) had conducted a very credible study and suggested that even the common soldiers knew that their calls were eavesdropped on by both warring parties.

According to findings that were made in Chapter 3, about the history and motivation of Ukrainian intelligence actors, it is highly likely, almost sure, that Ukrainian intelligence actors have been able to intercept and decipher the communication that is made over mobile networks. There is enough circumstantial cases and evidence, that Ukrainian officials have conducted such actions before. The operations, which were conducted at the beginning of the invasion, especially disabling the roaming service in the mobile networks that were maintained by Ukrainian teleoperators refer that it was possible for Ukrainian intelligence officials to capture and record the Russian communication. Also, the evidence that was found (see: Horbyk, 2022, Orlova, 2022; McDaid, 2022) suggests, that the material was analyzed, gathered, and processed. This would suggest that the material would be authentic, but this cannot be validated from the public official sources.

However, there were no definitive and absolute evidence which could verify that the activity was conducted by Ukraine. The variety of possible attack vectors that allow eavesdropping and wiretapping make it hard to find the actual method that was used, so technically it would have been impossible in this time frame to conduct a study that would give a definitive answer to this question. But in practical sense, the amount of circumstantial evidence would let us assume, that even without definitive proof, the eavesdropping and intercepting has been conducted by Ukrainian state actor.

The findings that were made in the analysis of the collected dataset do not give any additional information for either of the first sub-research question. Because of the scope and limitations of the study, which were set for practical reasons, the technical analysis was not conducted on the samples that were collected. Statistical content analysis did point out certain anomalies that the content had when it was compared to statistically to an average regular caller's cell phone communication, but this does not give any added value to these questions.

Third sub-research question was "*Does the content have features of propaganda.*" . The answer is yes again. If this sub-research question is evaluated against the definitions that were given in the chapter 4, the usage of the content defines the content as propaganda. The actual content is not meant to be propagandistic message due to its confidential nature, but usage and utilization of it weaponizes it to propagandistic message. This conclusion is supported also by the methods, means and process of how it is delivered to the public.

From the viewpoint of content itself it is evident that its message is used as propaganda. It is used as a weapon in the information domain (Berzina, 2018; Taddeo, 2012). The content itself is not meant to be propaganda, but in this particular case it has been weaponized and used in a way that fulfills definitions of propaganda. According to Ross (2002) the propaganda has a message, it persuades, has a significant target audience, and is applied by behalf of organization. The content that was collected and researched in this study, all these elements were found. The message was persistent and continuously delivered to the public audience.

We can argue if this case in itself is an independent propaganda campaign. According to Aspiriadis (2023) strategic communication in the form of strategic narrative attends to legitimize the actions of the author and tries to gain their support for the cause. In this particular case the content itself does not have a clear autonomous message or purpose, but it either supports or undermines different narratives that are told by Ukraine and Russia. The content contradicts the definition of Laskin (2019), because as of campaign, this content does not try to dissolve individuality of the audience and it does not attempt to unite people think similar. In this case, the examined phenomenon can rather be described as a support function that manipulates the strategic narrative.

Instead of “propaganda campaign” The content collected in this case study could better be considered a psychological or information operation. As it was previously defined, psychological operations attempt to influence people’s perceptions, attitudes, and emotions (Wallenius & Nilsson, 2019). This is required when one is trying to support or undermine the narratives that are announced and communicated publicly by both parties. From the viewpoint of information warfare and -operations the content is weaponized information in a way that Berzina (2018) defined, it is distributed solely in information domain, as it was defined by Taddeo (2012) and focuses purely on information, like Liptak (2009) suggested. Deviant behavior of the source publishing the content contrary to its defined mission could indicate an improvement in the credibility of the content.

Looking at the matter as a whole, the research material leads to the conclusion that the content in the case is used as propaganda, which through a psychological and information operation supports the strategic communication of the state actor by supporting the state's own and undermining the opponent's narrative. In this conclusion, the assumption of a “propaganda campaign” would be false. The research findings strongly suggest that the publishing activities have been well organized and professional. Deviations observed in the process could be explained to a significant extent by, for example, resource shortages due to vacations.

Among the official conclusions, it would be justified to ask if the content is obtained from the cyber operation, which was deemed plausible, or if it was a fabrication and made by Ukrainian officials. The research found no evidence that the content was artificially made, fabricated, or produced. On the other hand, the need to edit the content supports the claim that the content would be genuine because there would not be needed to edit scripted and acted material. Also, the findings of research on individual samples support the originality of the content. If the content were scripted and acted, it would be intuitive to think that there was no absence of content that would exploit remarkable events. In this case, the lack of such content supports the authenticity of the content. Again, without actual technical analysis, the conclusion is made through observation and is supported by circumstantial evidence. The confirmation cannot be obtained through public sources, and the ongoing war prevents Ukrainian officials from revealing details of this. For the sake of argument, it can also be asked if this even matters.

On the other hand, the need to edit the content supports the claim that the content would be genuine because there would not be needed to edit scripted and acted material. Also, the findings of research on individual samples support the originality of the content. If the content were scripted and acted, it would be intuitive to think that there was no absence of content that would exploit remarkable events. In this case, the lack of such content supports the authenticity of the content. Again, without actual technical analysis, the conclusion is made through observation and is supported by circumstantial evidence. The confirmation cannot be obtained through public

sources, and the ongoing war prevents Ukrainian officials from revealing details of this. For the sake of argument, it can also be asked if this even matters.

9 Discussion and propositions for the further studies

"In war, truth is the first casualty."— Aeschylus.

In this work, we were able to show with a high probability that Ukraine has been able to eavesdrop on Russians' mobile network communications using just public sources. Does this have any value for anything? The calls and communication can be intercepted and eavesdropped on. A common lesson to everyone is that one should not trust the confidentiality of cell phones. One should be careful and think very carefully what information is shared in mobile communication.

First finding outside the range of this study is that this case can be considered a textbook example of this type of information operation. The communication in the content is not in any ways intended to be propaganda, has been utilized as such. As Liptak (2009) and Berzina (2018) suggested. This could be studied further by looking for similar cases and by comparing them using a similar approach that is used in this study.

Russian propaganda and information warfare has been exceedingly popular field of study. The counterpropaganda or the information against Russians has had lesser interest and has been seen less important. But as everyone who has ever watched sports or knows anything about military strategy knows, no event has ever won by just defending. Victories can be achieved with offensive operations. Research for, not just counterstrategies, but offensive methods against the Russian information domain should be carefully studied. Ukrainian offensive operations in information space after 24.2.2022 have been very efficient and successful.

What makes this particular case interesting is the actor whose content was used as empirical material for the study. When looking at the official task described in the fifth chapter of GUR, this type of publishing activity is, to say the least, special. The mission of the military intelligence services without exception is to produce information to support decision-making, and the goal is to keep the information received by the intelligence secret. In this particular case, however, the intelligence agency is publicly sharing information that is allegedly obtained using methods and tools of cyber. So, it must be asked why exactly GUR was the actor that systematically started the publication of the information in question and by no means some other national authority whose task is especially to share the national narrative.

One should also understand how the information can be exploited. As it was concluded, the content was not meant as propaganda but was used as such in this particular case. All information can be taken out of context and used as tool against the advesary if presented in different framework. One should decide what one communicates and in which communication channels to prevent weaponization of one's information.

Last, but not least, the author likes to raise a question about the context of cyberwarfare and its purpose. During this work, the importance of information and its usage raised a lingering question in the writer's mind. Is the technical aspect even remotely important when the value does lie in information? What is the worth and value of offensive cyberoperation in this case? It is evident that this operation was cyberoperation in every sense, but if we are honest, there was no actual need to conduct the eavesdropping or interception of communication in the first place to produce the content that was in focus of this study. Could such an operation be conducted in a way, that adversary "trusts" that the content is obtained by offensive cyberoperation, and acts according to it? Would it be as efficient to manipulate the opinion of the general public and to guide the decisions and actions of adversary similarly without even having to spend resources in difficult and complex operation. To this, the writer has no answer, but for a further study, this would be an interesting point of view.

References

Ali, A. H., Roble, A. A., Shire, A. A. A., & Mahamud, I. M. SECURING MOBILE COMMUNICATION AGAINST MAN-IN THE MIDDLE ATTACK. *JOURNAL OF ENGINEERING &SCIENCE*, 21.

Akhbar, S. (2022, March 31). Russian Troops Are Self-Sabotaging In Ukraine, Says British Intelligence Chief. *Huffpost*. https://news.yahoo.com/russian-troops-self-sabotaging-ukraine-000200176.html?guccounter=1. Accessed 12.1.2024.

Ahmadpanah, S. H., Chashmi, A. J., & Yadollahi, M. (2016). 4G Mobile Communication Systems: Key Technology and Evolution. *arXiv preprint arXiv:1606.05477*.

Artyushenko, O (2023, April 1). Empty Promises': Wives Of Russian Soldiers Fighting In Ukraine Say Pay Is Not What Was Promised*. RadioFreeEurope/RadioLiberty*. https://www.rferl.org/a/russia-soldiers-salaries-unpaid-ukraine-invasion/32345161.html. Accessed 10.1.2024.

Aspriadis, N. (2023). Preparing for War: Strategic Narratives and Disinformation in Leadership Rhetoric during Ukraine War. *ESSACHESS–Journal for Communication Studies*, 16(1 (31)), 21-41.

Aviv, I., & Ferri, U. (2023). Russian-Ukraine armed conflict: Lessons learned on the digital ecosystem. *International Journal of Critical Infrastructure Protection*, 43, 100637.

Bakare, I., & Bassey, E. (2021). A Comparative Study of the Evolution of Wireless Communication Technologies from the First Generation (1G) to the Fourth Generation (4G). 12 73-84.

BBC. (2022, March 3). Ukraine: Why has Russia's 64km convoy near Kyiv stopped moving? *BBC News*. https://www.bbc.com/news/world-europe-60596629. Accessed 10.10.2023.

Bergh, A. (2019). Social network centric warfare–understanding influence operations in social media.

Bernays, E. (1928). Propaganda. Ig Publishing. *E-book*. Google.books.com

Berzina, I. (2018). The narrative of "information warfare against Russia" in Russian academic discourse. *Journal of Political Marketing*, 17(2), 161-175.

Biescker, M. (2022, December 30). Evidence of Russian war crimes mounts as invasion of Ukraine drags on. *PBS News Hour*. https://www.pbs.org/newshour/world/evidence-of-russian-war-crimes-mounts-as-invasion-of-ukraine-drags-on . Accessed 3.6.2023.

Blake, S. & Morton, E. (2023, May 25). Wagner's leader says private army withdrawing from Bakhmut, handing control to Moscow. *PBS*. https://www.pbs.org/newshour/world/wagners-leader-says-private-army-withdrawing-from-bakhmut-handing-control-to-moscow . Accessed 4.1.2024.

Brillouin, L. (2013). Science and information theory. Courier Corporation. *E-book*. Google.books.com

Butcher, E. (2022, May 16). War of Narratives: Russia and Ukraine. *RUSI*. https://www.rusi.org/explore-our-research/publications/commentary/war-narratives-russia-and-ukraine/. Accessed 28.12.2023.

Cattaneo, G., De Maio, G., & Petrillo, U. F. (2013). Security Issues and Attacks on the GSM Standard: a Review. *J. Univers. Comput. Sci*., 19(16), 2437-2452.

Chatfield, A. T., Reddick, C. G., & Brajawidagda, U. (2015, May). Tweeting propaganda, radicalization and recruitment: Islamic state supporters multi-sided twitter networks. *In Proceedings of the 16th annual international conference on digital government research* (pp. 239-249).

Chen, J., & Xu, Y. (2017). Information manipulation and reform in authoritarian regimes. *Political Science Research and Methods*, 5(1), 163-178.

Coalson, R. (2022, March 17). Special Operation Z: Moscow's Pro-War Symbol Conquers Russia -- And Sets Alarm Bells Ringing. *Radio Free Europe*. https://www.rferl.org/a/russia-ukraine-letter-z-fascist-symbol/31758267.html . Accessed 10.5.2023.

Connable, B. (2012). Military intelligence fusion for complex operations: A new paradigm. Arlington, VA: Rand Corporation.

Connell, M., & Vogler, S. (2016). Russia's approach to cyber warfare. CENTER FOR NAVAL ANALYSES ALEXANDRIA VA ALEXANDRIA United States.

Creativefreedom.com (n.d.). https://www.creativefreedom.co.uk/icon-designers-blog/twitter-logo-history/ . Accessed 5.12.2023.

Curran, K., Breslin, P., McLaughlin, K., & Tracey, G. (2007). Hacking and eavesdropping. *Cyber Warfare and Cyber Terrorism*, 307-317.

Daniel, T. A., & Metcalf, G. S. (2015). Crossing the line: An examination of toxic leadership in the US Army. *The Leadership Quarterly*, 32(1), 118-227.

Dayyani, A. (2016). Electronic Data & Information Espionage: Civil or Criminal Liability. *JL Pol'y & Globalization*, 47 (27).

Defence intelligence of Ukraine (n.d). History of the Defence Intelligence of Ukraine. https://gur.gov.ua/en/content/creation.html. Accessed 10.1.2022.

Dempsey, J. (1997). COMMUNICATIONS PRIVACY IN THE DIGITAL AGE: REVITALIZING THE FEDERAL WIRETAP LAWS TO ENHANCE PRIVACY. *Albany Law Journal of Science & Technology*, 8(1), Detsch, J. & Mackinnon, A. (2022, March 22). 'The Ukrainians Are Listening': Russia's Military Radios Are Getting Owned. *Foreign Policy*. Accessed 8.12.2023.

Deuter, D. (2012). GSM/3G/4G/DECT Security. *Institute of Media Informatics Ulm University*, 17.

Devine, K (2023, January 4). Ukraine war: Mobile networks being weaponized to target troops on both sides of conflict. *Sky News*. https://news.sky.com/story/ukraine-war-mobile-networks-being-weaponised-to-target-troops-on-both-sides-of-conflict-12577595. Accessed 23.5.2023.

Di Pietro, R., Raponi, S., Caprolu, M. & Cresci, S. (2021). *New dimensions of information warfare* (pp. 1-4). Springer International Publishing.

Dirks, K. T., & Skarlicki, D. P. (2004). Trust in leaders: Existing research and emerging issues. Trust and distrust in organizations: *Dilemmas and approaches*, 7, 21-40.

Duncan, G., (2023, June 6). Nova Kakhovka dam collapse: Ukraine orders evacuations after blaming Russia. *N-world*. https://www.thenationalnews.com/world/2023/06/06/nova-kakhova-dam-collapse/?utm_medium=Social&utm_source=Twitter#Echobox=1686031025 . Accessed 6.12.2023.

Dunkelman, O., Keller, N., & Shamir, A. (2010). A practical-time attack on the A5/3 cryptosystem used in third generation GSM telephony. *Cryptology ePrint Archive*.

Dunnewijk, T., & Hultén, S. (2007). A brief history of mobile communication in Europe. *Telematics and Informatics*, 24(3), 164-179.

Eder, M. K. (2007). Toward strategic communication. *Military Review*, 87(4), 61.

Eshelman, E. (2020). Can You Hear Me Now? The Vulnerability of Cellular and Smartphone Use on the Battlefield. *Doctoral dissertation.* Naval Postgraduate School.

Evelina, L., Angeline, M., & Mariani, V. (2014). Topic: Performance Excellence in Business IMHA 2014 UNIFORMS AND PERCEPTION OF PROFESSIONALISM.

Figma.com (n.d.). https://www.figma.com/community/file/1266471630484921505/new-twitter-logo-now-x. Accessed 16.12.2023.

Franke, U. (2015). War by non-military means: Understanding Russian information warfare.

Franzosi, R. (2008). Content analysis: Objective, systematic, and quantitative description of content. *Content analysis*, 1(1), 21-49.

Gerring, J. (2004). What is a case study and what is it good for? *American political science review*, 98(2), 341–354.

Glanz, J., Santora, M., Robles, P., Willis, H., Leatherby, L., Koetti, C. & Khavin, D. (2023, June 16). Why the Evidence Suggests Russia Blew Up the Kakhovka Dam. *The New York Times*.

https://www.nytimes.com/interactive/2023/06/16/world/europe/ukraine-kakhovka-dam-collapse.html . Accessed 6.12.2023.

Golovchenko, Y., Buntain, C., Eady, G., Brown, M. A., & Tucker, J. A. (2020). Cross-platform state propaganda: Russian trolls on twitter and YouTube during the 2016 US Presidential Election. *The International Journal of Press/Politics*, 25(3), 357-389

Guess, A. M., & Lyons, B. A. (2020). Misinformation, disinformation, and online propaganda. Social media and democracy: *The state of the field, prospects for reform*, 10.

Göker, A. (2022, April 28). SS7 ATTACK. *Medium.com*. https://lockpin010.medium.com/ss7-attack-a068f45ef83f .Accessed 5.7.2023.

Hall, R. (2022, April 22). 'I can't keep up': Russia is losing so much military equipment in Ukraine that weapons monitors are overwhelmed. *The Independent*. https://www.independent.co.uk/news/world/europe/russia-ukraine-military-equipment-losses-b2049613.html. Accessed 12.11.2022.

Han, K., Yeun, C. Y., & Kim, K. (2009, January). New key escrow model for the lawful interception in 3GPP. *In 2009 Digest of Technical Papers International Conference on Consumer Electronics* 1-2. IEEE.

Harris, S., DeYoung, K., Kurshudyan, I., Parker, A. & Sly, L. (2022 August 16). Road to war: U.S. struggled to convince allies, and Zelensky, of risk of invasion. The Washington Post. https://www.washingtonpost.com/national-security/interactive/2022/ukraine-road-to-war/. Accessed 10.4.2023.

He, S., & Paar, I. C. (2007, July). SIM card security. *In Seminar Work, Ruhr-University of Bochu*m.

Holtmanns, S., & Singh, I. (2018). New attack vectors for mobile core networks.

Horbyk, R. (2022). "The war phone": mobile communication on the frontline in Eastern Ukraine. *Digital War*, 3(1-3), 9-24.

Horváth, L. (2016). "THE BATTLE OF WIZARDS": THE FUTURE OF ELECTRONIC WARFARE. *Defense*, 171.

Howarth, J. (2023, January 9). Time Spent Using Smartphones (2023 Statistics). *EXPLODING TOPICS. https://explodingtopics.com/blog/smartphone-usage-stats.* Accessed 30.9.2023.

Huang, L. (2016, May 26). Forcing a Targeted LTE Cellphone into an Eavesdropping Network. *HITBSecConf. Conference proceedings*. https://archive.conference.hitb.org/hitbsecconf2016ams/sessions/forcing-a-targeted-lte-cellphone-into-an-eavesdropping-network/. Accessed 10.9.2023.

Inocencio, R., Redman, J. & Reals, T. (2023, October 23). North Korea provides Russia artillery for the Ukraine war as U.S. hands Kyiv ammunition seized from Iran. *CBS News*. *https://www.cbsnews.com/news/ukraine-war-russia-north-korea-artillery-us-gives-kyiv-siezed-iran-ammunition/*. Accessed 14.1.2024.

Jałowiec, T., & Grala, D. (2020, April). The Effectiveness of Logistic Processes in Military Supply Chains. *In Proceedings of the 35th International Business Information Management Association Conference (IBIMA)* 1-2.

Jesson, J. K., & Lacey, F. M. (2006). How to do (or not to do) a critical literature review. *Pharmacy education*, 6(2), 139-148.

Jones, M. (2019). The gulf information war| propaganda, fake news, and fake trends: The weaponization of twitter bots in the gulf crisis. *International journal of communication*, 13, 27.

Kapantai, E., Christopoulou, A., Berberidis, C., & Peristeras, V. (2021). A systematic literature review on disinformation: Toward a unified taxonomical framework. *New media & society*, 23(5), 1301–1326.

Kara, İ., & Aydos, M. (2019). The ghost in the system: technical analysis of remote access trojan*. International Journal on Information Technologies & Security*, 11(1), 73-84.

Khaldarova, I. (2021). Brother or 'Other'? Transformation of strategic narratives in Russian television news during the Ukrainian crisis. *Media, war & conflict*, 14(1), 3-20.

Khaldarova, I., & Pantti, M. (2020). Fake news: The narrative battle over the Ukrainian conflict. In *The Future of Journalism: Risks, Threats and Opportunities* (pp. 228-238). Routledge.

Kim, C. (2007). Design and Implementation of USIM Security Module for the Wireless Network Interworking. *Journal of the Korea Institute of Information Security & Cryptology*, 17(2), 41-49.

Kim, I., & Kuljis, J. (2010). Applying content analysis to web-based content. *Journal of Computing and Information Technology*, *18*(4), 369-375.

Kinetz, E. (2022, July 26). Ukraine pushes to try alleged war crimes as fighting rages. *AP news*. https://apnews.com/article/russia-ukraine-kyiv-war-crimes-4cb96a5e0ac1550d9ea38b29fdcf7e70 . Accessed 3.6.2023.

Kienneman, L. (2023, February 23). How one year of disinformation has shaped the narrative of the Ukraine war online? The Observers/24 France. https://observers.france24.com/en/europe/20230223-ukraine-russia-war-debunked-one-year-of-disinformation. Accessed 14.3.2023.

Kirby, P. (2023, January 3). Makiivka: Russia points fingers after deadliest Ukraine attack. *BBC News*. https://www.bbc.com/news/world-europe-64155859 . Accessed 30.12.2023.

Kohlbacher, F. (2006). The use of qualitative content analysis in case study research. *In Forum Qualitative Sozialforschung/Forum: Qualitative Social Research* (Vol. 7, No. 1, pp. 1-30). Institut fur Klinische Sychologie and Gemeindesychologie.

Krantz, M. (2023). Past, Present and Future: History, Memory, Politics and the Russo-Ukrainian War in Official Russian Discourse 2021-2023.

Krippendorff, K. (2018). Content analysis: An introduction to its methodology. Sage publications.

Laskin, A. V. (2019). Defining propaganda: A psychoanalytic perspective. *Communication and the Public*, *4*(4), 305-314.

Lamba, A., Yadav, J., & Devi, G. U. (2012). Analysis of technologies in 3g and 3.5 g mobile networks. *In 2012 International Conference on Communication Systems and Network Technologies* (pp. 330-333). IEEE.

Lange-Ionatamishvili, E., Svetoka, S., & Geers, K. (2015). Strategic communications and social media in the Russia Ukraine conflict. *Cyber war in perspective: Russian aggression against Ukraine*, 103-111.

Lendon, B. (2022, April 14). What images of Russian trucks say about its military's struggles in Ukraine. *CNN World*. https://edition.cnn.com/2022/04/14/europe/ukraine-war-russia-trucks-logistics-intl-hnk-ml/index.html. Accessed 15.12.2023.

Libicki, M. (1995). What is information warfare*?* *Center for Advanced Concepts and Technology, Institute for National Strategic Studies*, National Defense University.

Liew, A. (2013). DIKIW: Data, information, knowledge, intelligence, wisdom, and their interrelationships. *Business Management Dynamics*, 2(10), 49.

Lippman, W. (1922). Weapons of Democracy: Propaganda, Progressivism, and American Public Opinion. *E-book*. Amazon. Com

Liptak, D. A. (2009). Information Warfare. *Searcher (1070-4795)*, 17(9), 20–31. https://search-ebscohost-com.ezproxy.jamk.fi:2443/login.aspx?direct=true&db=bsh&AN=44499773&site=ehost-live.

Luna, N., Vredenbregt, L. & Pereira, I. (2023, August 23). What is the Wagner Group? The 'brutal' Russian military unit in Ukraine. *ABC News*. https://abcnews.go.com/International/International/wagner-group-brutal-russian-military-group-fighting-ukraine/story?id=96665326. Accessed 3.1.2024.

Lyall, J. (2022, January 3). It is hard for Russia to invade Ukraine, when its soldiers don't want to be there. *Forbes*. https://www.forbes.com/sites/craighooper/2022/03/01/shaken-russian-army-conscripts-make-perfect-targets-for-morale-crushing-operations/. Accessed 14.12.2023.

Mak, T. (2022, December 10). There have been 50,000 alleged war crimes in Ukraine. We worked to solve one. NPR. https://www.npr.org/2022/12/10/1138710652/russian-war-crimes-ukraine-investigation . Accessed 3.6.2023.

Marczak, W. R., Scott-Railton, J., Marquis-Boire, M., & Paxson, V. (2014). When governments hack opponents: A look at actors and technology. *In 23rd USENIX Security Symposium (USENIX Security 14)* (pp. 511-525).

Marczak, B., Scott-Railton, J., McKune, S., Abdul Razzak, B., & Deibert, R. (2018). Hide and seek: Tracking NSO group's Pegasus spyware to operations in 45 countries.

Matishak, M. (2022, March 10). NSA chief trumpets intelligence sharing with Ukraine, American public. *The Record*. https://therecord.media/nsa-chief-trumpets-intelligence-sharing-with-ukraine-american-public. Accessed 28.1.2023.

Mayring, P. (2019, September). Qualitative content analysis: Demarcation, varieties, developments. *In Forum: Qualitative Social Research* (Vol. 20, No. 3). Freie Universität Berlin.

McDaid, D. (2022, March 29). The Mobile Network Battlefield in Ukraine – Part 1. *Blog post*. https://www.enea.com/insights/the-mobile-network-battlefield-in-ukraine-part-1/ . Accessed 6.8.2023.

McCornack, S. A., Levine, T. R., Solowczuk, K. A., Torres, H. I., & Campbell, D. M. (1992). When the alteration of information is viewed as deception: An empirical test of information manipulation theory. *Communication monographs*, 59(1), 17-29.

Melkozerova, V. (2023, June 9). Ukraine says it intercepted call, in which Russians admit they blew up dam. Politico. https://www.politico.eu/article/ukraine-says-russia-admits-blowing-up-nova-kakhovka-dam-call-intercepted/. Accessed 15.7.2023.

Meyer, U., & Wetzel, S. (2004, September). On the impact of GSM encryption and man-in-the-middle attacks on the security of interoperating GSM/UMTS networks. In 2004 IEEE 15th International Symposium on Personal, Indoor and Mobile Radio Communications (IEEE Cat. No. 04TH8754) (Vol. 4, pp. 2876-2883). IEEE.

Miller, G. & Khurshudyan, I. (2023, October 23). Ukrainian spies with deep ties to CIA wage shadow war against Russia. *The Washington Post*. https://www.washingtonpost.com/world/2023/10/23/ukraine-cia-shadow-war-russia/ . Accessed 21.12.2023.

Mineo, D. L. (2014). The importance of trust in leadership. *Research Management Review*, 20(1), n1.

Mjølsnes, S. & Olimid, R. (2017). Easy 4G/LTE IMSI catchers for non-programmers*. In Computer Network Security: 7th International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security, MMM-ACNS 2017*, Warsaw, Poland, August 28-30, 2017, Proceedings 7 (pp. 235-246). Springer International Publishing.

Myre, G. (2022, April 26). How does Ukraine keep intercepting Russian military communications? *www.wamu.org*. https://wamu.org/story/22/04/26/how-does-ukraine-keep-intercepting-russian-military-communications/. Accessed 1.3.2023.

Narula, S. (2004). Psychological operations (PSYOPs): A conceptual overview. *Strategic Analysis*, *28*(1), 177-192.

Nichiporuk, B. (2002). US Military opportunities: Information-warfare concepts of operation. *RAND-PUBLICATIONS-MR-ALL SERIES-*, 187–219.

Norrman, K., Näslund, M., & Dubrova, E. (2016, June). Protecting IMSI and user privacy in 5G networks. *In Proceedings of the 9th EAI international conference on mobile multimedia communications* 159-166.

Onix (nd). National holidays in Ukraine 2023. *Website*. https://onix-systems.com/national-holidays-in-ukraine/2023. Accessed 25.9.2023.

Oh, D. (2022, November 29). Lessons learned from Russia-Ukraine War: Cell network security. *The Readable*. https://thereadable.co/lessons-learned-from-russia-ukraine-war/. Accessed 15.12.2023.

Onuh, M. (2010). Propaganda usage in modern day journalism. *Journal of Communication and Culture: International Perspective* Vol.1 No.3.

Orlova, A. (2023, October 25). The ‘Horrifying’ Job of Listening to Intercepted Russian Soldier Phone Calls .K*yiv Post*. https://www.kyivpost.com/post/23244 Accessed 10.12.2023.

Osborn, K. (2022, September 3). What's Behind the Russian Military's Morale Problems? *National Interest*. https://nationalinterest.org/blog/buzz/whats-behind-russian-militarys-morale-problems-201088. Aaccessed 15.12.2023.

Palmer, D.(2018, July 18). Password-stealing, eavesdropping malware targets Ukrainian government. *ZDNet.com*. https://www.zdnet.com/article/password-stealing-eavesdropping-malware-targets-ukrainian-government/. Accessed 1.12.2023.

Patton, E., & Appelbaum, S. H. (2003). The case for case studies in management research. *Management research news*, 26(5), 60-71.

Peck, M. (2023, April 19). Moscow's promise of big payments to its troops is creating a new headache for the Russian military. *Business Insider*. https://www.businessinsider.com/higher-troop-pay-promises-may-cause-problems-for-russian-military-2023-4?r=US&IR=T. Accessed 10.1.2024.

Pereira, V., & Sousa, T. (2004). Evolution of Mobile Communications: from 1G to 4G. *Department of Informatics Engineering of the University of Coimbra, Portugal*, *4*, 20-0.

Pierri, F., Luceri, L., Jindal, N., & Ferrara, E. (2023, April). Propaganda and Misinformation on Facebook and Twitter during the Russian Invasion of Ukraine. *In Proceedings of the 15th ACM Web Science Conference 2023* (pp. 65-74).

Prokopiv, M. (2019). SYSTEM OF INTELLIGENCE AND SPECIAL SERVICES OF UKRAINE: FEATURES OF INTERACTIONS AND IMPACT ON FOREIGN POLICY.

Rahnema, M. (1993). Overview of the GSM system and protocol architecture. *IEEE Communications magazine*, 31(4), 92-100.

Rao, P., Chen, H. & Aura, T. (2023). Threat modelling framework for mobile communication system. *Computers & Security*, 125. Elsevier.

Rao, P., Oliver, I., Holtmanns, S., & Aura, T. (2016, May). We know where you are! *In 2016 8th International Conference on Cyber Conflict (CyCon)* (pp. 277-293). IEEE.

Rash, W. (2017, February 17). Eavesdropping Malware Discovered Gathering Audio Data in Ukraine. *eWeek*. https://www.eweek.com/security/eavesdropping-malware-discovered-gathering-audio-data-in-ukraine/. Accessed 16.10.2023.

Ravaonorohanta, N., & Sayumwe, M. (2020). Social media presence and organizational performance: An empirical study on companies' presence on Twitter. Contemporary Management Research, 16(2), 123-144.

Ross, S. T. (2002). Understanding propaganda: The epistemic merit model and its application to art. Journal of Aesthetic Education, 36(1), 16-30.

Rusu, M. L., & Herman, R. (2018). The implications of propaganda as a social influence strategy. *Scientific Bulletin-Nicolae Balcescu Land Forces Academy*, *23*(2), 118-125.

Salih, A. A., Zeebaree, S. R., Abdulraheem, A. S., Zebari, R. R., Sadeeq, M. A., & Ahmed, O. M. (2020). Evolution of mobile wireless communication to 5G revolution. *Technology Reports of Kansai University*, *62*(5), 2139-2151.

Şaran, V. (2016). Media manipulation and psychological war in Ukraine and the Republic of Moldova. *CES Working Papers*, 8(4), 738-752.

Scahill, J., & Greenwald, G. (2014). The NSA's secret role in the US assassination program. *The intercept*, 10, 2014.

Schafer, J. A. (2010). The ineffective police leader: Acts of commission and omission. *Journal of Criminal Justice*, 38(4), 737-746.

Schmitt, O. (2018). When are strategic narratives effective? The shaping of political discourse through the interaction between political myths and strategic narratives. *Contemporary Security Policy*, 39(4), 487-511.

Schyns, B., & Schilling, J. (2013). How bad are the effects of bad leaders? A meta-analysis of destructive leadership and its outcomes. *The Leadership Quarterly*, 24(1), 138-158.

Shah, S. & Martin, A. (2023, August 22). Why is Twitter now called X? The big rebranding explained. The Standard. https://www.standard.co.uk/news/tech/x-twitter-logo-rebrand-why-elon-musk-b1096363.html. Accessed 20.11.2023.

Shaik, A., Borgaonkar, R., Asokan, N., Niemi, V., & Seifert, J. (2015). Practical attacks against privacy and availability in 4G/LTE mobile communication systems. *arXiv preprint* arXiv:1510.07563.

Sharma, P. (2013). Evolution of mobile wireless communication networks-1G to 5G as well as future prospective of next generation communication network. *International Journal of Computer Science and Mobile Computing*, 2(8), 47-53.

Shklovski, I., & Wulf, V. (2018). The use of private mobile phones at war: Accounts from the Donbas conflict. *In Proceedings of the 2018 CHI conference on human factors in computing systems* (pp. 1-13).

Shufelt, J., & Longenecker, C. (2017). Practical lessons learned for dealing with toxic leaders and bad bosses. *Military Revie*w, 2, 2-10.

Siau, K., & Shen, Z. (2003). Mobile communications and mobile services. *International Journal of Mobile Communications*, 1(1-2), 3-14.

Singh, J., Ruhl, R., & Lindskog, D. (2013, September). GSM OTA SIM cloning attack and cloning resistance in EAP-SIM and USIM. *In 2013 International Conference on Social Computing* (pp. 1005-1010). IEEE.

Singh, R., Bhargava, P., & Kain, S. (2007). Cell phone cloning: a perspective on gsm security. *Ubiquity*, 2007(July), 1-8.

Smith, J. (2023, October 12). Defence Intelligence of Ukraine (GUR): Rulers of the Stars. *Graydynamics.com*. https://greydynamics.com/defence-intelligence-of-ukraine-gur-rulers-of-the-stars/ Accessed 20.12.2023.

Soesanto, S. (2022). The IT army of Ukraine: structure, tasking, and eco-system. *CSS Cyberdefense Reports.*

Stemler, S. (2000). An overview of content analysis. *Practical assessment, research, and evaluation*, 7(1), 17.

Straub, J. (2019). Mutual assured destruction in information, influence, and cyber warfare: Comparing, contrasting, and combining relevant scenarios. *Technology in Society*, 59, 101177.

Strobel, D. (2007). IMSI catcher. *Chair for Communication Security, Ruhr-Universität Bochum*, 14.

Sustek, M., Marcanik, M., Oplustil, M., Tomasek, P., & Urednicek, Z. (2016). Interception Methods and GSM. *SECURWARE 2016 : The Tenth International Conference on Emerging Security Information, Systems and Technologies.* ISBN: 978-1-61208-493-0

Szostek, J. (2017). The power and limits of Russia's strategic narrative in Ukraine: The role of linkage. *Perspectives on Politics*, 15(2), 379-395.

Szostek, J. (2018). Nothing is true? The credibility of news and conflicting narratives during "Information War" in Ukraine. *The international journal of press/politics*, 23(1), 116-135.

Taddeo, M. (2012). Information warfare: A philosophical perspective. *Philosophy & Technology*, 25, 105-120.

Taylor, P. M. (2013). Munitions of the mind: A history of propaganda. Third edition. Manchester University Press. ISBN 0 7190 6767 7. Paperback. 350 pages.

Thomson, (2017, May 17). After years of warnings, mobile network hackers exploit SS7 flaws to drain bank accounts. *The Register*. https://www.theregister.com/2017/05/03/hackers_fire_up_ss7_flaw/ Accessed 1.3.2022.

Toorani, M., & Beheshti, A. (2008, September). Solutions to the GSM security weaknesses. *In 2008 The Second International Conference on Next Generation Mobile Applications, Services, and Technologies* (pp. 576-581). IEEE.

Topalskyi, V., & Ivanenko, S. (2020). NARRATIVE" GREAT MILITARY WAR" IN RUSSIAN ANTI-UKRAINIAN PROPAGANDA. *CURRENT ISSUES OF MILITARY SPECIALISTS TRAINING IN THE SECURITY AND DEFENCE SECTOR UNDER CONDITIONS OF HYBRID THREATS*, 210. ISBN 978-83-66676-10-7

Treissman, R. (2022, March 1). Putin's claim of fighting against Ukraine 'neo-Nazis' distorts history, scholars say. www.NPR.com. Accessed 10.5.2022.

Vaismoradi, M., Turunen, H., & Bondas, T. (2013). Content analysis and thematic analysis: Implications for conducting a qualitative descriptive study. *Nursing & health sciences*, *15*(3), 398-405.

Varris, K (2022, December 22) Ukrainian forces used Russian soldiers 'panicked' cell phone calls to pinpoint their locations and pick them off, report says. *Business Insider*. https://www.businessinsider.com/ukraine-used-russian-soldiers-panicked-cell-phone-calls-locate-them-2022-12?r=US&IR=T. Accessed 2.3.2023.

Wallenius, C., & Nilsson, S. (2019). A lack of effect studies and of effects: The use of strategic communication in the Military domain. *International Journal of Strategic Communication*, 13(5), 404-417.

Watling, J. (2023, June 26). Wagner's March on Moscow Left Unresolved Challenges in its Wake. *RUSI*. https://www.rusi.org/explore-our-research/publications/commentary/wagners-march-moscow-left-unresolved-challenges-its-wake Accessed 4.1.2024.

Weinbaum, C., Berner, S., & McClintock, B. (2017). Sigint for anyone: the growing availability of signals intelligence in the public domain (p. 0011). RAND Corporation.

Xu, B., & Tao, Y. (2023). National Identity in Media Discourses from Russia and Ukraine: Amid the 2022 Russo-Ukrainian War. *Zeitschrift für Slawistik*, 68(3), 419-439.

Yasan, K. (2022, October). RAT (Remote Access Trojan). TechTarget. Blog post. https://www.techtarget.com/searchsecurity/definition/RAT-remote-access-Trojan . Accessed 1.8.2023.

Yuhas, A., Gibbons-Neff, T. & Al-Hlou, Y.(2023, January 4). For Russian Troops, Cellphone Use Is a Persistent, Lethal Danger. *New York Times*. https://www.nytimes.com/2023/01/04/world/europe/ukraine-russia-cellphones.html. Accessed 7.3.2023.

Zegart, A. (2023). Open Secrets: Ukraine and the Next Intelligence Revolution. *Foreign Aff.*, 102, 54.