DIGITAL LITERACY AND RESILIENCE AGAINST DISINFORMATION AMONG NATO MILITARY PERSONNEL

Colonel Associate Professor Petko DIMOV, PhD

Director of the Distance Learning, Language Training, and Qualification Department, Rakovski National Defence College, Sofia, Bulgaria

Colonel Associate Professor Georgi MARINOV, PhD

Department of Logistics, Rakovski National Defence College, Sofia, Bulgaria

DOI: 10.55535/RMT.2024.4.25

This article examines the digital literacy and resilience to disinformation among NATO military personnel, with a particular focus on the emerging challenges related to social media and search engine platforms. By analysing data collected in 2019 and comparing it to findings from a 2023 survey, the research identifies key trends in social media engagement, the capacity to recognize disinformation, and the strategies used to evaluate the credibility of online content. The results demonstrate that while a substantial proportion of military personnel actively use social media, there remains a significant deficiency in their ability to critically assess and verify the authenticity of the information they encounter. The study underscores the ongoing risks that disinformation poses to NATO's information security framework and stresses the urgent need for comprehensive digital literacy training programmes. The recommendations suggest implementing mandatory training to enhance critical thinking and analytical skills regarding information, alongside the development of specialized teams within NATO military structures dedicated to monitoring and combating disinformation.

Keywords: digital literacy; disinformation; military personnel; NATO; social media;

INTRODUCTION

The phenomenon of disinformation has increasingly become a focal point of academic research, particularly considering the rapid evolution of digital technologies and Artificial Intelligence. These advancements have substantially facilitated the creation and dissemination of false information, posing significant risks to information security and societal stability (Bradshaw, Howard, 2021). Military personnel, due to their pivotal societal roles, are often the targets of disinformation campaigns aimed at eroding morale and operational efficiency within military units (NATO Strategic Communications Centre of Excellence, 2022).

According to Martínez-Bravo et al. (2022), digital literacy encompasses a broad range of competencies that are crucial for successful functioning in the modern information society, including information literacy, technological literacy, cybersecurity, digital communication, content creation, critical thinking, digital financial literacy, and ethics and responsibility in the digital environment. (Martínez-Bravo et al., ib.)

Considering the already documented relationship between digital literacy and efforts to mitigate the effects of disinformation, this study aims to explore in greater depth the interconnection between digital skills, technological competence, and the ability of military personnel not only to recognize but also to critically evaluate and respond to disinformation. Specifically, the research emphasizes the hypothesis that service members with higher digital literacy and superior skills in Internet technologies are more capable of identifying disinformation in social media and search engines compared to those with lower digital literacy and weaker technological skills.

The benefits of this research extend beyond the military, contributing to a deeper understanding of the factors that influence resilience to disinformation and aiding in the development of more effective strategies to enhance this resilience. Such outcomes are valuable not only for the Armed Forces but also for society at large, as they contribute to greater security and stability within the digital environment.

This study employs a mixed-method approach, drawing on data from a 2019 NATO Command post exercise conducted in Poland. A survey comprising both closed and open-ended questions was administered to a sample of 5,844 respondents

– participants from various countries involved in the exercise[1]. The aim of this survey was to better understand the preferences, practices, and motivations of these participants in focusing on their duties rather than on unregulated news from the surrounding media environment. Military personnel represent a unique group of news consumers who can significantly impact national security during crises.

Building on this foundation, the present study focuses on how military personnel acquire, evaluate, and critically engage with news on social media and the role these activities play in their lives. It is crucial to investigate how these service members locate, verify, and ultimately trust news, as well as their ability to distinguish between *"fake news"* and *"real news".*

The research addresses the following three questions:

❖ *How do military personnel conceptualize what constitutes "news" and its implications?*

❖ *How do military personnel interact with and experience news on social media platforms?*

❖ *How do military personnel assess the credibility of online content?*

METHODOLOGY

The current research is based on data collected in 2019 during the largest International Logistics Command post exercise in NATO, *"Capable Logistician 19"*, in Poland (3-13 June 2019), as we have mentioned (NATO, 2019). These data were subsequently compared with a more recent survey conducted by the European Defence Agency (EDA) in 2023, covering 1,200 military personnel from 27 EU member states (EDA, 2023). The first sample includes responses from 360 military personnel from 23 countries who completed an anonymous online survey with English-language questions conducted by us. The survey contained 48 questions, and only 16 of them were used for the current research. 3,450 military personnel participated in this exercise, and to determine the size of the representative sample, the study authors used the non-returnable small population formula (Atanasov, Kaloyanov, 2020).

[1] The questionnaire is part of a larger research project. Because of the scope and confidentiality of the study, the authors cannot provide detailed information (A.N.).

$$n = \frac{Z^2 N * p(1-p)}{\Delta^2 N + Z^2 p(1-p)} = \frac{1{,}96^2 3450 * 0.25(1-0.25)}{\Delta 0{,}05^2 1100 + 1{,}96^2 0{,}25(1-0{,}25)} = 174{,}74, \quad (1)$$

where "z" is the guarantee multiplier corresponding to the chosen confidence level. In the general case, with a guaranteed probability of 95%, 1.96 is assumed (Gatev, 1995);

"p" is the relative proportion of units expected to have violations and is assumed to be 0.25;

"Δ" is the maximum stochastic error for the study assumed to be 0.05;

"N" – general population of all military personnel registered in the exercise, which are 3,450 people from 30 countries.

From the calculations, the 360 received responses to the questionnaires are significantly more than the required 174.74 to be a representative sample with a guaranteed probability of 95% and a confidence interval of 5%, which is quite sufficient for the needs of the present study.

In addition, the validity of the results is ensured by the fact that the survey was anonymous and military personnel from 23 countries out of 30 participated in it: Bulgaria, Bosnia and Herzegovina, Great Britain, Canada, Denmark, Czech Republic, Georgia, Hungary, Germany, Spain, Estonia, Finland, France, Italy, Lithuania, Latvia, Poland, Romania, Serbia, Slovakia, Sweden, Ukraine and Croatia. The second sample is significantly larger and serves to validate the obtained results.

RESULTS

To determine the level of social media usage among military personnel in 2019, respondents were asked whether they had accounts on any social media platforms and to specify which ones. Out of 360 military personnel, 306 (85%) confirmed having an account on a social network, while 54 (15%) did not. Among those with social media accounts, 220 (72%) used Facebook, 70 (23%) used Instagram, 8 (3%) used Snapchat, 7 (2%) used Twitter, 2 (1%) used VKontakte, 19 (6%) used Viber, 23 (7%) used WhatsApp, 8 (3%) used LinkedIn, and 3 (1%) used Messenger *(figure 1)*.

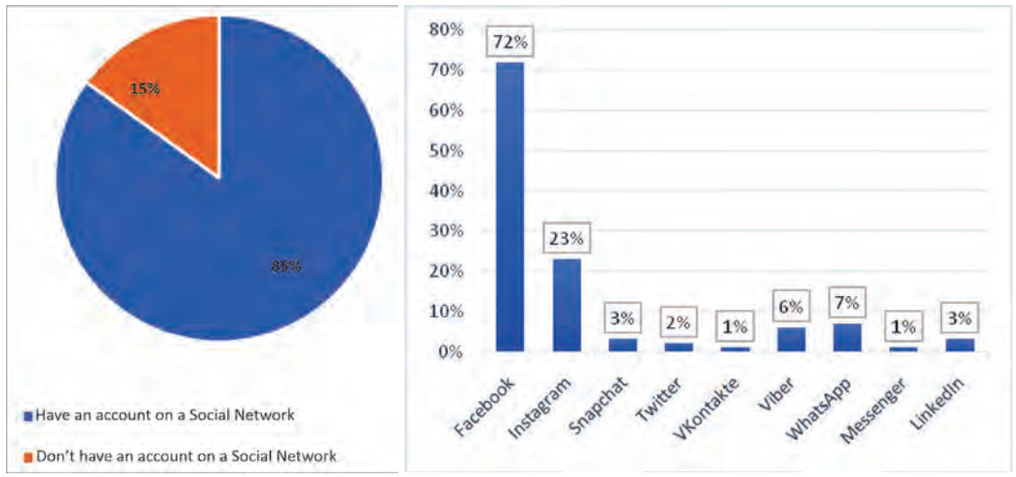

Figure 1: Distribution of military personnel with social media accounts: on the left, overall distribution; on the right, by type of social media (authors' design)

The EDA study from 2023 reported an increase in this percentage to 92%, with growing popularity of platforms such as TikTok (18%) and LinkedIn (15%) among military personnel (European Defence Agency, 2023). This indicates that social media is becoming a primary channel for receiving information or disinformation. While Facebook and Instagram remain the dominant platforms, a particularly concerning 1% of military personnel obtain information from the Russian social network VKontakte.

To assess the level of disinformation recognition, respondents were next asked whether they had ever encountered misleading or false information on social media. In 2019, 319 (89%) reported having encountered such information, while 41 (11%) said they had not or were unaware of it *(figure 2)*. It suggests that military personnel are aware of the risks of disinformation on social media. The 2023 data showed a slight increase to 93%, which may be attributed to heightened awareness or the growing amount of disinformation online (European Defence Agency, 2023).

To explore the frequency of information verification, respondents in the 2019 NATO Command post exercise in Poland were asked how often they verify the information they see on social media before sharing it. Only 54 (15%) of the military personnel confirmed that they verified information, while a significant 306 (85%) did not! *(figure 3).*

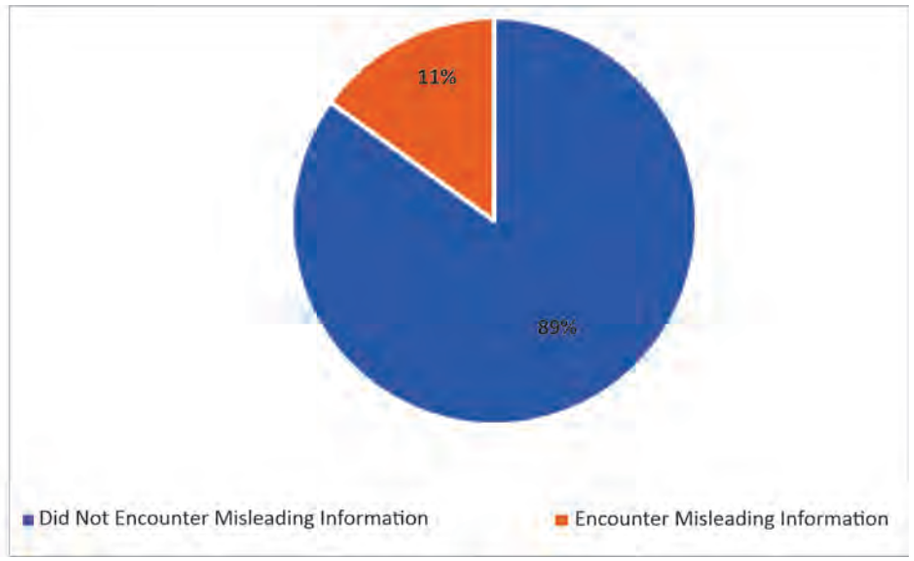

Figure 2: Percentage of those who have encountered disinformation online (authors' design)

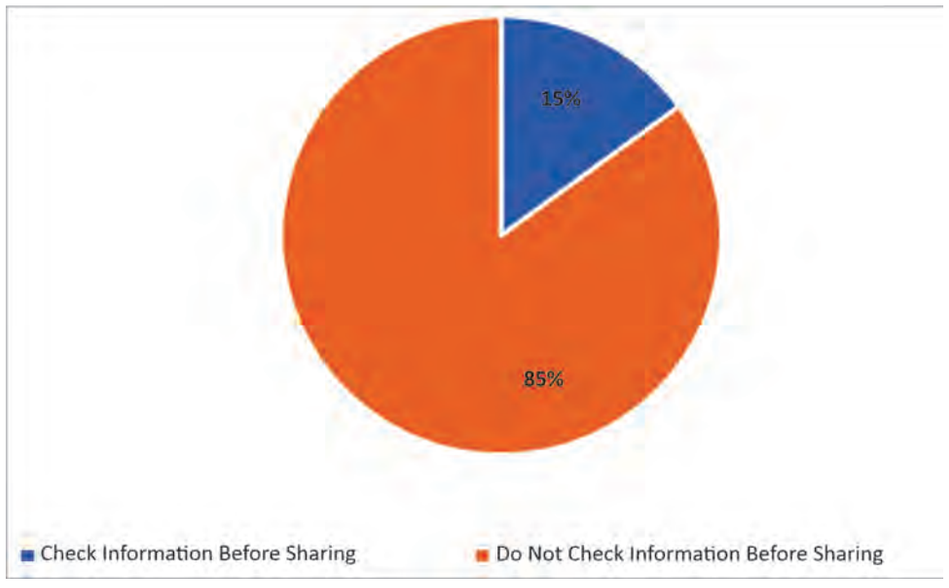

Figure 3: Percentage of military personnel who verify information before sharing it on social media (authors' design)

Despite being aware of the risks of disinformation and encountering it on social media, a very small percentage of military personnel verify the information they see before sharing it.

One of the most concerning aspects of the 2019 study is that only 15% of military personnel verify information before sharing it on social media. Data from 2023 shows some improvement, with 28% of respondents confirming that they regularly verify information before sharing it (European Defence Agency, 2023). However, this percentage remains unacceptably low given the importance of information security in the military context.

When asked which search engine they use most frequently, 334 (93%) of military personnel cited Google, 9 (2%) mentioned Qwant, and the rest were distributed among Seznam, Yahoo, Startpage, Safari, Yandex, and Netscape, each receiving less than 1%. This underscores Google as the main channel for receiving information or disinformation on the Internet. Search engines do not directly create disinformation, but their algorithms can inadvertently amplify it, as their ranking systems prioritize content based on engagement, popularity, and relevance, which can favour sensational or misleading information. Disinformation spreaders exploit search engine optimization (SEO) to rank higher in results. Additionally, search engines index vast amounts of unverified user-generated content, making it easy for false information to spread. Monetization strategies also encourage clickbait, which boosts disinformation further due to high traffic.

In a follow-up question on whether they had ever encountered misleading or false information in search engine results, 292 (81%) of military personnel confirmed they had, while 68 (19%) said they had not. These results are similar to those seen in social media interactions.

Respondents indicated that in Lithuania, false news predominantly concerns their history or historical figures, particularly partisans. Political leaders are the second most common target, especially in Eastern European countries. A persistent theme is the claim that NATO cannot protect them. In the United Kingdom, there are issues with influencers citing Russian propaganda sites such as Sputnik.ru. Americans primarily encounter disinformation related to Trump, while in Canada, respondents were generally unaware of false news.

When asked if they use cloud storage services such as Google Drive, iCloud, OneDrive, or others, 245 (68%) of military personnel confirmed they do, while 115 (32%) do not. Of those using cloud storage, 81 (33%) use iCloud most frequently,

93 (38%) use OneDrive, 180 (73%) use Google Drive, and 6 (2%) use Dropbox. These results suggest that digital literacy may influence the ability to recognize disinformation in social media and search engine results.

Google remains the dominant search engine, both in 2019 (93%) and in 2023 (89%), despite a slight decline in favour of privacy-focused alternatives (EDA, 2023). The use of cloud storage services increased from 68% in 2019 to 79% in 2023, with a greater variety of platforms being utilized.

Respondents were asked to determine how disinformation is detected, *"How do you assess the credibility of the information you share on your profiles?".* It was found that 73% verify the source of the news, 61% compare the news across multiple sources, 54% read the entire article before making a decision, 34% check the URL, 27% monitor comments, 23% consider the number of likes, and 41% conduct reverse image searches. The percentages exceeded 100% because respondents used multiple methods of verification. This indicates a certain level of digital literacy and knowledge of available tools *(table 1)*.

Table 1: How do you assess the credibility of the information you share on your profiles?
(authors' design)

Answers	Respondents %
I check who posted or tweeted the news	73
I read the whole news from beginning to end and then decide	54
I compare the news from several sources	61
I track the URL, date, or hashtag	34
I read the comments below the post	27
I observe how many times the news has been liked	23
I do a reverse Google search on the image used	41

The comparison between 2019 and 2023 data shows a positive trend in using more sophisticated methods to assess the credibility of information. For example, the percentage of military personnel conducting reverse image searches increased from 41% in 2019 to 58% in 2023 (Ib.).

DISCUSSION

The primary objective of this study was to examine the level of digital literacy among military personnel and whether it impacts their ability to recognize disinformation on social media and web search engines. The results indicate that the majority of military personnel have social media accounts, with Facebook being the most frequently used platform. Most respondents understand the risks of disinformation on these platforms; however, only a small percentage verify the information they see on social media before sharing it. This behaviour may indicate a lack of digital literacy.

The comparative analysis reveals both positive trends and ongoing challenges in the realm of digital literacy and resilience to disinformation among NATO military personnel. The increased use of social media and cloud services highlights the need for continuous updates to cybersecurity policies and digital literacy training.

Despite observed improvements in the methods used to assess the credibility of information, there remains a significant gap between recognizing disinformation and taking active steps to prevent its spread. This discrepancy underscores the need for more targeted educational programmes focused on critical thinking and media literacy in the digital age.

One of the key findings of the study is that Google is the most widely used search engine among military personnel. It aligns with other research showing Google as the most popular search engine globally (Stat Counter Global Stats). However, the majority of military personnel reported encountering misleading or false information in search engine results, indicating that additional security measures should be considered when presenting information on websites.

In line with the study's goal to investigate the relationship between digital skills and the ability of military personnel to critically evaluate and respond to disinformation, the use of cloud storage technology by military personnel, particularly Google Drive, plays a crucial role in enhancing operational efficiency and collaboration. However, while this reliance on digital tools reflects a positive development in terms of technological competence, it also introduces potential vulnerabilities. These cloud services, if not properly secured, may expose sensitive data to cyberattacks, which can be exploited as part of broader disinformation campaigns. Therefore, strengthening cybersecurity measures is essential to ensure that the use of such technologies does not undermine efforts to counter disinformation.

This study contributes to the field by demonstrating the relationship between digital literacy and the ability to recognize disinformation among military personnel. The findings can be used to develop effective digital literacy training programmes for military personnel, as well as to inform security policies that reduce the risk of disinformation when using social media, search engines, and cloud storage technologies. Moreover, future research should consider other factors that may influence the ability to recognize disinformation, such as educational background and professional experience.

RECOMMENDATIONS

The key conclusions of this study are that the majority of military personnel have social media accounts and frequently use them, yet only a small percentage verify the information they see before sharing it, despite being aware of the risk of disinformation. It suggests that digital literacy among military personnel is insufficient, and measures need to be taken to improve it.

On the other hand, most military personnel have encountered misleading or false information on social media and in search engine results, indicating that disinformation is widespread and poses a serious threat to NATO's Information Security in conducting Command post exercises.

A comparison with more recent studies confirms that disinformation continues to be a significant threat to the information security of NATO military structures. Despite observed improvements in some aspects of digital literacy, there are still significant gaps that need to be addressed.

This aspect underscores the need for a comprehensive digital literacy training programme tailored for military personnel, aimed at enhancing their ability to recognize and combat disinformation. Some countries, such as Lithuania, Latvia, and Estonia, have developed programmes in this area, though not to their full extent. Special attention should be given to improving their skills in navigating and critically evaluating content on social media platforms and in search engine results. This programme should be mandatory for all military personnel and conducted before major exercises to ensure that the staff is aware of the latest trends and disinformation techniques. The programme should not only cover technical skills but also foster critical thinking and the ability to analyse information in the digital environment.

Another recommendation is to promote the use of reliable information sources and provide military personnel with access to such sources. It will allow them to receive accurate and up-to-date information, enabling them to make more informed decisions.

Additionally, it is recommended that specialized teams within the military structures should be established to monitor and counter disinformation and enhance cooperation among NATO member states in the field of information security.

In conclusion, disinformation remains a serious threat to security, and digital literacy is essential to prevent its spread. The study shows that the majority of military personnel lack sufficient digital literacy, and measures need to be taken to improve it. The recommendations proposed in this study will help the Armed Forces address disinformation and ensure allied security.

CONCLUSIONS

The most important finding of this study is that military personnel's news consumption is both multimodal and multi-social; they receive news from their colleagues just as much as from social media platforms.

While most military personnel recognize that a free press is essential to democracy and contributes to the resilience of the European Union and NATO, deep political polarization makes them suspicious of certain news sources. A significant number of them even question the spread of *"fast news"* and the fragmented coverage often found on social media platforms.

These aspects underscore the complexity of their media environment and the need for enhanced digital literacy to navigate it effectively.

BIBLIOGRAPHICAL REFERENCES:

1. Atanasov, A., Kaloyanov, T. (2020). *Metodologichnipodhodinaizvadkoviteizsledv ania za izvarshvanenaproverkinabenefitsientitena* (Metodologiq hniподходина извадковите изследван*ия за извършване напроверкинабенефициентитена).* OP RChR 2014-2020. Nauchnitrudovena UNSS, 42-58. Sofia: UNSS, http://unwe-research-papers.org/uploads/ResearchPapers/02_Atanas%20Atanasov,%20Todor%20Kaloyanov.pdf [in Bulgarian], retrieved on 27 July 2024.
2. Bradshaw, S., Howard, P.N. (2021). *The Global Disinformation Order: 2021 Global Inventory of Organised Social Media Manipulation*. Oxford: Oxford Internet Institute.
3. European Defence Agency/EDA (2023). *Digital Literacy and Disinformation Resilience Among Military Personnel in EU Member States*. Brussels, retrieved on 27 July 2024.

4. Gatev, K. (1995). *Vavedenie v statistikata*. Sofia, Lia.
5. NATO. (2019). *NATO Exercise Cyber Coalition 2019*. Brussels: NATO, https://www.nato.int/cps/en/natohq/news_166827.htm?selectedLocale=en, retrieved on 27 July 2024.
6. NATO Strategic Communications Centre of Excellence. (2022). *Countering Information Influence Activities: A handbook for communicators*. Riga: NATO StratCom COE.
7. *Search engine market share worldwide.* Stat Counter Global Stats. (n.d.), https://gs.statcounter.com/search-engine-market-share, retrieved on 17 October 2024.