Target Audiences' Characteristics and Prospective in Countering Information Warfare

Daniel Ionel Andrei Nistor
National Defence University „Carol I", Bucharest, Romania

dan.nistor.rp@gmail.com

Abstract: NATO Defense Education Enhancement Program defines Information Warfare as an operation run to get cognitive assets over the opponents, by controlling one's own information space while disrupting the opponents' one. Not new as a process, continuous technological progress has endowed this phenomenon with speed and instruments to fight cyber and cognitive battles, to attack perceptions, trust, polarise and disrupt societies at large. The all present and undergoing kinetic conflict between Russia and Ukraine doubled by an even stronger cognitive and information war since February 2022 has highlighted even more the need to better understand individuals' behaviour and characteristics when faced with unconventional attacks, irrespective of a passive or active feedback. By identifying and analysing specific public categories, one can establish which are contextual variables that trigger a social reaction, to be able to then design a set of protective or defensive measures. For a full understanding of the way Information Warfare impacts people's thinking and decision-making process, to see how a resilience plan can be designed, one should investigate not only the information war instruments but also their effects over people at large. Not knowing the voice of the hostile authors, it Is still important to understand the domestic audience and their reaction to it, so that protective actions be taken for resilience and protection, through education. The domestic public's identity and its dominant characteristics are brought into attention to understand which is the relation between these and the way Information Warfare can be countered through education, with examples from the Russian's hostile activity. Values, national identity, stereotypes and generalist psychological profiles will be looked at in this paper, to be put in relation to behaviours, attitude change and resistance in front of types of messages, campaigns and types of media-embedded grey zone threats. The present paper is part of a larger PhD research program that focuses on consolidating a society's security culture through better institutional strategic communication, therefore all the findings will be used to this end.

Key words: Information Warfare, Disruptive Process, Behaviour Change, Target Audience

1. Introduction

In order to counter Information Warfare, is It key to anticipate and plan accordingly - because many scenarios are mostly recurrent and repetitive, or is it necessary to change the approach in order to better understand the situation and act to prevent it long before it occurs? It sounds like being a choice of creating awareness and not dealing with consequences. Can growing awareness change or alter the degree in which we are affected by Information Warfare? We will try to provide an answer to these open questions.

In this research paper we will investigate how values, national identity, stereotypes and individuals' psychological profiles can be put in relation to behaviours, attitude change, resistance to propaganda and influencing actions to create structural changes within a specific society.

Yet, the purpose of this article is not to analyse the evolution or the techniques, tactics and procedures of Information Warfare, but rather to forward an approach that focuses on the audience, as countering Information Warfare is not only about doctrine, strategy, techniques, tactics and procedures, but also about audiences and a larger societal context.

Therefore, we need to examine how our audience looks like, what we want to protect, how we can understand the context, and how to use the proper channels to change behaviours, including but not limited to educating the audience and teaching them how to protect themselves and others or be part of the process.

Not more than half a century ago, Information Warfare was an attribute associated predominantly with the military and, to a lesser extent, with the political. The war of public statements was the main instrument that kept political figures on top of audiences' mind. To the same extent, public statements could make an official vanish from the political stage overnight, either following a scandal or by a simple twist of words.

Today, Information Warfare is present everywhere - from social to economic, military or political, and its impact is often difficult to forecast or anticipate. Big data and the massive flow of information have fundamentally changed the way media reports. More than half of the world's population has access to Internet and, in a single day, more than 333 billion emails, 650 million tweets and 41,6 million WhatsApp messages are sent; 150K messages and 147K images are sent and received on Facebook, while Instagram users post around 347K stories

per day. (Bulao 2023) Taking into account that almost 60 percent of the total global population has a social media account, one can easily understand the dimension of this phenomenon (Datareportal, 2022).

Whether we are talking about sovereign states, state actors, alliances, coalitions or private entities, we must be aware of the fact that the techniques, tactics and procedures have been largely adapted to the environment and context. As a result, any protective strategy (process) should be rethought and refocused from channels to the audience we want to protect. At the same time, we ought to reanalyse if the doctrine should be redone or just readapted, in order to see if protecting the public could be seen as a strictly defensive operation or it can also involve offensive actions. What are the limits of Information Warfare countermeasures? The areas of Information Warfare, its methods and channels have multiplied and diversified, making it more and more important to understand all these developments in the context of understanding the audience.

2. Information Warfare and the Security Ecosystem

According to Sartonen (2022) the concept of "war" is being transformed due to in the inclusion of Information Warfare in the digital environment. The cyber domain and the internet in particular allow global audiences to be reached in battles of influence (all, 2017), pressuring us to seek to understand the "war" in a broader ecosystem. As Severinghaus (2019) underlines, we are operating with seven warfare areas: the first five are the domains traditionally associated with the military (air, sea, land, space, and cyber), while the other two, not explicitly recognised as such, are economic and education warfare. "If one wants to be politically correct, economic and education warfare are characterised simply as "competition". But, in truth, other nations of the world, not just China, are stealthily waging economic and education warfare outside the military, and others are significantly outpacing the United States in educational achievements in many areas with national security implications". (Severinghaus 2019)

NATO Defence Education Enhancement Program defines Information Warfare as an operation ran to get cognitive assets over the opponents by controlling one's own information space and disrupting the opponents'. In a conceptual delineation, Dan Kuehl defined Information Warfare as "the conflict or struggle between two or more groups in the information environment", while professor Stupples sees Information Warfare as "the integration of electronic warfare, cyberwarfare and psychological operations, for both attack and defence". (Stupples, 2015). To understand Information Warfare, we should therefore explain the larger framework of warfare and analyse why it is different today, compared to two decades or a century ago. Western leaders are investing billions to develop capabilities matching those of China and Russia, establishing military commands for attacking, defending and exploiting the vulnerabilities of electronic communications networks. Information Warfare combines electronic warfare, cyberwarfare and psychological operations into a single fighting organisation, and this will be central to all warfare in the future (Stupples, 2015).

The concepts of "security" and "securitization" were largely studied and explained by Buzan (1991) who defines security as "the pursuit of freedom from threat and the ability of states and societies to maintain their independent identities and their functional integrity against forces of change which they see as hostile. The bottom line of security is survival, but it also reasonably includes a substantial range of concerns about the conditions of existence. Quite where this range of concerns ceases to merit the urgency of the "security" label (which identifies threats as significant enough to warrant emergency action and exceptional measures including the use of force) and becomes part of everyday uncertainties of life is one of the difficulties of the concept". (Buzan, 1991)

Influencing audiences and changing behaviours are just a part of Information Warfare. The entity, state or state actor are executing Information Warfare actions on a targeted audience to change perceptions or behaviours in order to achieve a specific objective. The main goal is not to change the behaviour, but to reach an objective. This is the main reason why audiences should be the point of focus when conducting Information Warfare or in countering hostile Information Warfare. Even if we are talking about changing behaviours in order to accept a new political regime, a new social policy, new state borders or significant economic changes, the hearts and minds of the audience are more efficient and enduring than using physical force. Using "supreme excellence in breaking the enemy's resistance without fighting" (Tzu 2011) has always been the most powerful way of achieving an objective.

The struggle to move confrontation from physical to informational, political or economic areas while reducing loss of life as always been constant aim of states, alliances and organisations. Hence, Information Warfare can be construed in relation to two possible approaches: "as a movement from the area of hard power to that of soft power, and as a mutation of the confrontation having the centre of gravity not in the physical domain but

in information domain (using the cyberspace and electromagnetic spectrum)". (Lesenciuc 2016) Information Warfare can be used by states in foreign policy to employ and advantage. (Lewis, 2022)

Besides, Information Warfare is not a new phenomenon, yet it contains innovative elements such as technological development effects, resulting in information being disseminated faster and on a larger scale. Ullman highlights a series of factors that can change the world order by simply influencing audiences: "*failed or unperformed governance, climate change, cyberspace, social networks, drones, terrorism and state debt.* Seen as a new doctrine that marks the transition *from a Cold War doctrine based on nuclear weapons only, we are now witnessing the creation of a new doctrine that has the same mechanism of action as a virus: no physical border or internal or external state policy, known as transition from MAD (Mutual Assured Distraction) to newMAD (Massive Attack Disruption)".* These are all disturbing and disruptive factors for the world order, acting independently or simultaneously, charged with huge potential for disruption or destruction (Ullman, 2021). Each of those factors can become either a channel or an influencing factor that, attuned to the right massage, can reach and influence the targeted audience in order to achieve the Information Warfare objectives.

Information Warfare and propaganda have always been outstanding instruments for Russia. The Kremlin used its powerful narrative in most of the Baltic, former Communist or Soviet states, including Czech Republic, Slovakia, Poland, Hungary, Ukraine, Bulgaria, Georgia, Moldova and Romania. Before the Russian invasion in Ukraine, the authorities were scarce in creating coherent strategic plans or in joining efforts to counter Kremlin's influence, being mostly concerned with domestic political issues or worse, being completely unaware of the imminent risk. Russian Information Warfare in Black Sea Region was present long before the attack on Ukraine, in February 2022. The Kremlin has been playing strong since the annexation of Crimea in 2014. (Lucas, 2014). The "green man's" presence in Eastern Ukraine was just the tip of the spear; Moscow targeted the Russian-speaking minority and conducted military exercises in the Black and Baltic Seas to project the image of a military superpower. Thousands of cyberattacks have been executed, severely affecting critical infrastructure. The Ukrainian electricity grid was targeted in 2015, leaving more than two thousand people with no power, followed by an attack on Kyiv in 2016 that generated a major blackout. (Scutaru, 2022)

To counter Russian Information Warfare, NATO, the EU and Ukraine developed programs in all domains - from political to military, economic and social. They imposed diplomatic and economic sanctions, closed and banned Russian media outlets, protected their own cyberspace and physical borders. The rules of conducting propaganda activities on social networks have been also updated, becoming more restrictive, educating and promoting awareness. NATO readjusted its Strategic Concept, strengthened his Eastern and Northern flanks, deployed the Battle Groups at NATO's borders and in the countries neighbouring Russia, and increased military cooperation with Ukraine, Georgia and Moldova by conducting military excises and training missions. Western governments pressed social media firms to remove pro-Russia propaganda after the war in Ukraine began, and outlets like RT (Russia Today TV station) have been wiped from popular platforms. That may create an impression in much of the world that related disinformation is on the decline. (Letzing, 2022)

3. The Role of Audience in Information Warfare

In order to protect the audience and counter Information Warfare, we need to understand the actors, the environment and how the "game" is be played. The effectiveness of our actions depends on understanding audiences, the context, instruments and adversary objectives, while all of those measures are executed from the defensive strategy, aiming to prevent malign influence and protect domestic audiences. At the same time, another way of countering Information Warfare is by offensive actions, targeting the adversary in order to diminish, reduce or even annihilate his capability of action.

In Informational Warfare, the logical scheme is defined by the relation between two actors, where actor A has a clear mission and Actor B has the objective of not letting Actor A fulfil its mission. In this relationship, the public is not a target *per se.* Yet, protecting its people is the most powerful way through which Actor A can fight against the mission of actor B, not allowing him to accomplish its objective. Developing further on this scheme, Actor A targets Actros's B audience to change its behaviour in order to accomplish its objectives. Actor B, at the same time, needs to protect its own audience from Actor A's malign influence. In protecting its audience, Actor B can execute defensive actions as pre-emptive actions, protective actions or offensive operations. In today's world, we face a multitude of potential influencing factors that both actors A and B can make use of to influence audiences in Information Warfare. A psychological operation has largely three major steps: (1) establish the objectives and define target audiences (TA); (2) produce, approve and deliver to the TA the influence messages; (3) assess the effectiveness; (FM3-05.302, 2005). To maximize the results, it is important to disseminate the

influencing messages and proper evaluate their effectiveness to the same extent as it is key to focus the message on behavioural change and execute all the required actions.

Individuals tend to focus more on values, certain people, objects, phenomena, and situations that can usually satisfy their needs, being highly influenced by previous experience, tradition and cultural characteristics. Yet, in order to determine an individual's behavioural patterns, we must therefore consider first how the *interest, values, social norms and social sanctions* are adopted through the process of socialisation (AJP-3.10.1(A) Allied Joint Doctrine for Psychological Operation 2009). Groups act different than individuals, and are largely characterized by "impulsivity, mobility and irascibilities of the masses, animated and manipulated by leaders who understand the power of suggestion and the gullibility of the masses." (LeBon, 2022)

4. Instruments and Research Methods

When analysing the "Romanian case", we used observation and comparative analyses as research methods. For comparative insight, we turned to Hofstede's 6D cross-cultural model, showing the effects of a society's culture on the values of its members, and how these values specifically relate to behaviour. Hofstede's study covers 70 countries and has been last updated last in 2010 (Hofstede, 2006)**.** In addition to Hofstede's study, we used David's research (2015) "Psihologia poporului roman" (The Psychology of the Romanian People), a comprehensive cultural study forwarding the psychological profile of the Romanian people from a cognitive-experimental perspective. One of the central points of David's study is the comparative analysis of how Romanian's see themselves, how they are seen by others, and how they actually are. (David, 2015)

For clarity and scientific relevance, we have followed up Hofstede's and David's studies, which provide a revealing information about the Romanian society from a psycho-social point of view, with two security barometers, realized by the Strategic Thinking Group, entitled "Public distrust: West vs. East, the Rise of Nationalism in the Disinformation Era, and the Fake News Phenomenon", (StrategicThinking, 2022) and respectively with a barometer called "The Security of the Future" realized by the Romanian National Institute of Statistics". These two barometers shed some light on the feelings and perceptions of Romanians regarding their trust in the military and political European and Euro Atlantic alliances.

And last but not least, for the particular investigation on how Romanians responded to fake news and disinformation immediately after the start of the conflict in Ukraine we referred to a study called "Propaganda Without Borders, A study of pro-Kremlin propaganda among far-right and radical voices in Hungary, Poland, Romania and Serbia" carried out by Global Focus, an NGO specialised in analysing pro-Russian propaganda in Romania and Eastern Europe. (GlobalFocus, 2022)

To end with, the observational dimension of this paper is supported by a number of narratives retrieved from various Romanian media outlets in 2022, in the context of the Ukrainian conflict, aiming at emphasising the relation between the characteristics of the Romanian audience and their reaction to hostile narratives.

5. The Romanian Case

To illustrate how values, national identity, stereotypes and psychological profiles can be put in relation with behaviours, attitude change and resistance to messages, campaigns and various types of media-embedded grey zone threads, in the larger contexts of Information Warfare, we shall conduct an analysis on Romanian audiences.

The first four narratives that took shape in the immediate aftermath of Russia's invasion of Ukraine in Romania are: (1) related to the food crisis, a scenario in which s*hops are running out of basic goods, such as sunflower oil, flour and sugar, because Ukraine was one of the biggest producers in the world; food will increasingly become more and more expensive; therefore, we need to make supplies;* (Antena3, 2022) (2) The rising price of petrol - *the price will dramatically increase (with 50% or more); gas stations become crowded overnight with drivers willing to purchase gallons of fuel before prices spiked.* (EuropaLibera, 2022) (3) Chaotic purchase and unsound administration of iodine pills under the immediate threat of Russia employing nuclear assets (Munteanu, 2022). And last but not least (4), *inflation*, *cash shortage or lack of money in ATMs; for fear of not losing money due to raising inflation, people need to withdraw cash immediately*. (RomaniaLibera, 2022). The response of Romanian citizens was purely emotional, creating chaos and extra demand that temporarily resulted in increasing the price of various goods. People created huge queues at gas stations and ATMs to make supplies and safeguard their savings. The state institutions promptly responded and managed the situation reassuring Romanian people and conveying clear messages to counter fake news.

The *distribution and acceptance of power and authority* and a high preference for avoiding uncertainty (Hofstede, 2006) are the psychological traits that pushed Romanian people to respond to messages that highlighted a potential, urgent threat, also explaining the chaotic, emotional response. Romanians are still fighting a cultural trauma related to lack of food, fuel and closed borders, dating back to the Communist era. At the same time, Romania is considered to be a collectivistic society (Hofstede, 2006), characterised by "*long-term commitment* to the member groups", which could be the family or extended relationships. Loyalty is also highly important, as well as the relation between employee and employers. The West (meaning the European Union, United States or NATO) is where Romania should be heading politically, economically and military is what 77% of the respondents answered, while only 10.4% believe that Romania should head towards the East (nr. Russia, China). An important 12.6 percent of the interviewees chose not to respond**.** (StrategicThinking, 2022). *The long-term orientation* (Hofstede, 2006) maintains an equilibrium between tradition and the modern way of preparing for the future; the resistance to change is somehow moderate, closing the gap between the radical changes that took place after the fall of the Communist regime.

Romanian people are also extroverts, scoring high on amiability. The psychological threats related to family and community care (David, 2015) generated solidarity with the Ukrainian people in terms of providing safe passage, shelters and food for more than 3.3 million refugees (as retrieved on 12th of January 2023) and assisting with transportation of cereals and materials from Ukraine to Europe (Government, 2023). This relates to Information Warfare by proving that the Romanian people's embedded values are stronger than nationalist propaganda messages, backing the "toxic pacifist" idea that Romanian should step aside and support peace by not getting involved in any way (GlobalFocus, 2023). At the beginning of the war, Romanians strongly backed Ukraine, aside from the supply of military aid. According to a March 2022 national poll, 81% of respondents supported receiving refugees and 79% supported sending humanitarian aid (GlobalFocus, 2023). Romanian citizens' continuous efforts to support Ukrainian refuges are consistent with David and Hofstede findings about family care. Romanians provided not only food and shelter, but also access to education Ukrainian and the possibility for Ukrainian adult population to be employed. These attitudes are once again supported by David's study, according to which "minorities are better integrated in Romania, in comparison with Serbia, Slovakia or Ukraine (David, 2015). Censorship, propaganda, diminishing or restricting freedom of opinion and speech narrative (Global Focus Report 2022) match Romanians' uncertainty avoidance, individualism and power distance (Hofstede, 2006). Like a double-edged dagger, the public asks Government officials to take cautionary measures and counter propaganda, while also accusing public institutions of manipulation and censorship. L*eadership is transactional* (David, 2015) and the "people" will always feel the need to criticise, request urgent solutions and try to preserve the sentiments of freedom and democracy. The freedom of speech is one of the most important rights for Romanian people, as important as family and propriety. Reinstating the mandatory military service in the context of war (G4Media, 2022) was also a narrative easy to debunk. The conscription service has been suspended in peacetime since 2007, and as per David's findings, *Romanian's have a strong sentiment for fighting for defending the country, thus being in a strong opposition with 31 modern cultures* (David, 2015). The official position of the Minister of Defence was prompt and properly pushed on traditional channels, new media and social media. (i.e. there is a designated Ministry of National Defence website for fake news debunking called inforadar.) (Inforadar, 2023). Regarding their exposure to fake news and disinformation 54,7% of Romanian appreciated that they were highly exposed, while 41,8% consider their exposure low exposure or none. (StrategicThinking, 2022)

Another idea backed by nationalist groups is that of Romania being drawn into the conflict, risking a direct attack from Russia. Yet, as the low score on individualism and trusting the Western alliances diminished the impact of this right-wing propaganda, that failed to create a pro-East, anti-West cleavage within the Romanian society. Good governmental communication and protective measures helped keep this narrative at bay. The same explanation also applies to the "it's the refugees' fault" narrative, also pushed by nationalist propaganda to support the idea of rising prices for basic goods and medication, and failing of Romanian government to support the disadvantaged.

To sum up, understanding the friendly, tolerant, emotional, religious nature of of Romanian people, their positive, but sceptical personalities and rather undisciplined behaviour (David, 2015) proves to be highly relevant in understanding what type of messaging Romanian audiences can successfully be targeted with, in the larger context of Information Warfare, also offering strong insights for how to effectively respond, counter and educate.

6. The Social Media Impact

Media plays a crucial part in Information Warfare, providing the channels for both influencing through hostile propaganda or malign information and counter influencing through informing, educating and debunking. **Information Warfare is the battle to** "persuade and induce the sympathy of potential allies; and simultaneously spread confusion, uncertainty and distrust in the enemy's population". (Pelletier, 2022)

Social media expansion facilitates interconnectedness and access to information, thus amplifying social risks and vulnerabilities. Social media creates bubbles, and "what's in your filter bubble depends on who you are, and it depends on what you do. But the thing is that you don't decide what gets in. And more importantly, you don't actually see what gets edited out" (Gould 2019). By using social media, we can easily convert an audience. Sending messages is cheap and the distance between the message and the audience is reachable within a click. On social networks we can create groups and communities, support social causes and sell products or services, and more importantly, we can polarise, segment and split different categories, according to our interest. For example, in two weeks, the leader of the Romanian extremist party, AUR (The Alliance of the Union of Romanians), George Simion, generated over half million intersections (almost double than mainstream online media overall) on the topic of Romania's Schengen acceptance. (GlobalFocus, 2023)

Meta platform counts "5.3 billion global Internet users", while 3.71 billion people use at least one Meta app - Facebook, Instagram, Messenger, or WhatsApp every month. This means that "70% of all Internet users are active on at least one Meta app", but the truth is that many use more than one. Yet, the impact in not only measured in the large number of users, but also in the massive spread of data, with over "1 billion stories posted every day across Facebook and a potential advertising reach of 2.08 billion people" (Newberry, 2023). Now, imagine the targeting process in terms of speed, respectively how fast you can reach a larger audience using short message. If a malign actor passed on a message in large private groups and the message is then redistributed in even larger public groups and pages, it becomes almost impossible to identify the original source, let alone to map the spreading. As a result, any attempt the correct the messaging and address the disinformation becomes, to say the least, chimerical. If you are not in the "right" bubble, you don't stand a chance to locate the source of the deception.

"Social media is used to create accounts and develop groups that, **collaborated** with the algorithms behind social networks and other programming mechanisms developed using artificial intelligence such as bot networks or the construction of non-existent human profiles, ensure their transmission and support of messages, which, if necessary, can be used in the command and control of Information Warfare." (Preda, 2021) "*The Facebook data breach wasn't a hack. It was a wake-up call"* is one conclusion related to the Cambridge Analytica scandal, one of the first massive scale use of users' data without consent, aiming at manipulating the socio-political system, influencing decision and changing social behaviour. 87 million Facebook user had their data exposed and used by a political consulting firm engaged in an electoral campaign, using an application build in tool. (Romano 2018)

Social media has become a powerful instrument that can be easily used by any actor who aims at creating beliefs and changing behaviours. Is can be used offensively in Information Warfare to directly address the audiences with malign intentions, and defensively with purpose of educating and protecting.

7. Conclusions

In this paper, we analysed the relation between the psychological profiles, behaviours, attitudes, values, national identities and stereotypes of Romanian audiences, and the main disinformation narratives employed by malign actors, domestic and foreign, with the goal of influencing and disrupting the Romanian socio-politic environment, in the larger context the Russian-Ukrainian conflict. How Romanians reacted to these disruptive narratives correlates with their psychological and cultural traits, proving why knowing the audience remains a key element in Information Warfare. Success or failure is dictated by the degree in which the coercive message matches the cultural values, psychological profile and social norms of the targeted audiences. To the same extent, the degree in which social and state actors succeed in tailoring their protective measures and further educating their national audiences determines who gains the competitive advantage in influencing and changing behaviour.

The disinformation narratives could be also found in neighbouring countries, such as Bulgaria, Czech Republic, Poland, Serbia and Hungary, and even if the public response was somewhat similar to that to Romanians', the differences stem from the deep embedded cultural straits. For instance, if we examine the growing extremist-nationalist current in all the above-mentioned countries, we can observe that the affiliation is lower in Romania,

mainly due to the strong collectivism factor (70), uncertainty avoidance (90) and power distance (90), compared to Hungary, a country scoring lower on the collectivism (20), uncertainty avoidance (82) and power distance (46).

Of course, using this analysis we cannot predict behaviour, but we can anticipate action by mapping the activities, attitude changes and eventually put them into context. We can, however, set up alternative courses of action and reduce the number of scenarios based on behaviour changes. At the same time, we must own the fact that the malign actors have the same knowledge and understanding, and we must learn how to think and act "out of the box" to be one step ahead protecting our audience and countering the malign influence.

Social media, used as Information Warfare channel, remain one of the most cost efficient and effective tools for influencing and protecting the audiences. There are more than 5.3 billion active social media accounts in the world, expanding with an average rate of six new users being created every single second. It's a sharp tool used by Information Warfare actors in malign operations to target beliefs, polarise societies and change behaviours with potential social, political and economic repercussions. In order to effectively counter Information Warfare, it's therefore crucial to learn how to effectively amplify the protective messages, and convey communication according to the values, beliefs and interests of the audience.

Having that said, social media and digital tools and technologies should become strategically analysed and used by state institutions in their efforts to educate and protect their citizens in the larger context of the ever-present Information Warfare. It remains debatable *how* can states become more effective in protecting audiences using media literacy and education, starting from a younger age, involving not only state institutions, but also social actors. We will investigate these open questions further on, in a larger PhD research paper that focuses on consolidating a society's security culture through better institutional strategic communication.

References

Bulao, J., 2023. *How much data is created in 2023.* [Online] Available at: https://techjury.net/blog/how-much-data-is-created-every-day/#gref [Accessed 12 January 2023].

Datareportal, 2022. *Global Social Media Statistics.* [Online] Available at: https://datareportal.com/social-media-users [Accessed 22 December 2022].

Romano, A., 2018. *The Facebook data breach wasn't a hack. It was a wake-up call.* [Online] Available at: https://www.vox.com/2018/3/20/17138756/facebook-data-breach-cambridge-analytica-explained [Accessed 14 January 2023].

Tzu, S., 2011. The art of war. In: s.l.:HarperCollins Publishers.

Bailyn, B., 1992. *The Ideological Origins of the American Revolution.* [Online] Available at: https://military-history.fandom.com/wiki/Winning_hearts_and_minds [Accessed 15 january 2023].

Bao P., H. U., 2020. *An analytical model for the strategy of winning hearts and minds.* [Online] Available at: https://cradpdf.drdc-rddc.gc.ca/PDFS/unc346/p812125_A1b.pdf

Stupples, D., 2015. *What is Information Warfare?.* [Online] Available at: https://www.weforum.org/agenda/2015/12/what-is-information-warfare/ [Accessed 19 December 2022].

Severinghaus, R., 2019. *Seven-Domain Warfare: What Would Mahan Think?.* [Online] Available at: https://blog.usni.org/posts/2019/06/25/seven-domain-warfare-what-would-mahan-think [Accessed 17 January 2023].

Lesenciuc, A., 2016. Razboiul informational. In: Brașov: "Henri Coanda" Air Force Academy Publishing House, p. 98.

Lewis, B. C., 2022. *Information Warfare.* [Online] Available at: https://irp.fas.org/eprint/snyder/infowarfare.htm [Accessed 13 December 2022].

Ullman, H., 2021. *Al cincilea cavaler al apocalipsei și noul MAD.* Bucharest: Ed Militară.

Lucas, E., 2014. *The New Cold War.* London: Bloomsbury.

Scutaru, G., 2022. *Russian Policy in the Black Sea region Report,* Bucharest: New Strategy Center.

Letzing, J., 2022. *John Letzing.* [Online] Available at: https://www.weforum.org/agenda/2022/04/what-is-information-warfare-and-how-pervasive-is-it/ [Accessed 5 January 2023].

LeBon, G., 2022. *Psihologia multimilor,.* Bucharest: Librex,.

Hofstede, G., 2006. *What about Romania.* [Online] Available at: https://www.hofstede-insights.com/country/romania/ [Accessed 13 December 2022].

David, D., 2015. *Psihologia poporului roman.* Bucuresti: Polirom.

Antena3, 2022. *Antena 3.* [Online] Available at: https://www.antena3.ro/emisiuni/news-hour-with-cnn/romania-criza-ulei-floarea-soarelui-ministrul-agriculturii-638177.html [Accessed 22 December 2022].

EuropaLibera, 2022. *EuropaLibera.* [Online] Available at: https://romania.europalibera.org/a/de-unde-a-pornit-panica-cresterii-preturilor-la-benzina-si-motorina/31745801.html [Accessed 20 December 2022].

Munteanu, D., 2022. *Barometrul rezilientei societale,* Bucuresti: Centrul de rezilienta Euroatlantica.

RomaniaLibera, 2022. *Romania Libera.* [Online] Available at: https://evz.ro/romanii-isi-retrag-masiv-banii-de-pe-card-se-intampla-in-plin-razboi-la-granita-romaniei-anuntul-bancilor.html [Accessed 20 December 2022].

Government, R., 2023. *Romania's response to the Ukrainian refugee crisis,* Bucufresti: Guvernul Romaniei.

GlobalFocus, 2023. *Disinformation in a regional context during the War in Ukraine. A comparison between Hungary, Poland, Romania and Serbia,* Bucuresti: Global Focus.

G4Media, 2022. *G4 Media.* [Online] Available at: https://www.g4media.ro/mapn-atentioneaza-asupra-fake-news-urilor-privind-ordine-de-inrolare-in-armata-si-introducerea-serviciului-militar-obligatoriu-va-rugam-sa-va-informati-doar-din-sursele-oficiale.html [Accessed 28 December 2022].

Inforadar, R., 2023. *Inforadar.* [Online] Available at: https://inforadar.mapn.ro/tema28/index.php [Accessed 13 January 2023].

Pelletier, J., 2022. Intelligence, Information Warfare, cyber warfare, electronic warfare – what they are and how Russia is using them in Ukraine. *The Conversation : Science + Technology; Boston* , 1 March.

GlobalFocus, 2023. *Global Focus.* [Online] Available at: https://www.global-focus.eu/2023/01/monitoring-report-on-the-evolution-of-the-main-pro-kremlin-voices-on-facebook-early-warning/ [Accessed 14 January 2023].

Preda, A., 2021. *Social media in Information Warfare. Assault weapon with high recoil.* [Online] Available at: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiGkPTvxs_8AhVJgosKHRZJBd0QFnoECCAQAQ&url=https://revista.unap.ro/index.php/XXI_FSA/article/d [Accessed 7 January 2023].

FM3-05.30, n.d.

FM3-05.302, 2005. *Tactical Psychological Operations Tactics, Techniques, and Procedures.* Washington: US Departament of Army.

FM3-05.302, 2005. s.l.:s.n.