



The 17th International Scientific Conference
**“DEFENSE RESOURCES MANAGEMENT
IN THE 21st CENTURY”**
Braşov, October 28th-29th 2021



FAKE NEWS AND THE MILITARY ORGANIZATION

CRĂCEA Cătălin

Ministry of National Defence, România

Abstract:

Fake news is a phenomenon that, along with the speed of mass communication nowadays, has an enormous potential to do harm. Be it propagated consciously or not, this reality is yet to be addressed at a sufficient scale to be minimized and then eventually, ignored. Its range is non-discriminatory as it affects a wide array of domains, from politics and military operations, to high-life and common people's lives. It can influence elections up to the point that can decide the free choice of a countries' leadership or significantly reduce the huge volume of resources invested in a military operation.

Key words: fake news; military; communication; effects.

1. Introduction

Fake news negatively influences the perception, attitudes, actions and support of the people. It undermines authority, creates panic, confusion, lower the morale of own troops and undermine cohesion. It's a double edge sword as this can be used by both own troops and enemies alike. Manipulated photos, false statements, state propaganda and deepfake videos, with actions filmed in other locations and long before the conflict, have already been used on a large scale in the war between Russia and Ukraine and the battle for truth has been fought on many levels, with false claims on both sides.

2. Fake news characteristics

Easy to produce and distribute

The large scale access to the Internet and recent development of social media with all the encapsulating features such as taking pictures, filming and sending messages instantly, coupled with the opportunity to alter them in a convenient way makes the fake news distribution not only an easy task, but also accessible for reading, hearing and seeing to anyone.

Disinformation can be created by different toolsets, of which 'deepfakes' (who have the potential to confuse and deteriorate credibility) can be of a potentially destructive nature.

An increasingly interconnected world, which is providing easy access to technology, offers the ability to deliver real time, audience-tailored communication to report, command, inform, persuade, confuse, coerce, distract or deceive.

False news stories and so-called deepfakes are increasingly sophisticated and making it more difficult for data-driven software to spot. Artificial intelligence imagery has advanced in recent years and is now used by Hollywood, the fashion industry and facial recognition systems. Researchers have shown that these so-called generative adversarial networks, or GANs, can be used to create fake videos. Researchers can already produce convincing fake videos and generate persuasively realistic text.



The 17th International Scientific Conference
**“DEFENSE RESOURCES MANAGEMENT
IN THE 21st CENTURY”**
Braşov, October 28th-29th 2021



First release advantage

The speed and scale by which the information environment may be affected by anyone, on any level, are factors that create threats and/or opportunities to exploit vulnerabilities.

There is an inner temptation, a psychological feature in all of us to believe the first hand information and it takes a lot of time and a lot of facts and counter arguments that could be verified in order to combat the fake news already released and prove the originator wrong.

Sometimes, the willingness or ability of military officials to offer specific evidence associated with a particular event are often very limited. At the very least, this complicates the task of refuting fake evidence of military actions.

Additionally, military release of information is naturally a very deliberate process for operational security reasons to avoid the potential of giving enemy forces an unintended advantage. In an effort to be thorough and accurate, the military is often slower to officially respond to an incident and this often advantages the purveyor of a false narrative.

Multiple ways for orchestrating events

Fake news offers multiple ways to present negative facts and actions that didn't take place to change or affect the opinion or even make people hate or condemn the supposed wrongdoers, or attract the international attention, calling for international action. Some people, groups, organizations end up in being blamed for and accused of something they didn't do or at least to the extent that was presented.

In the ongoing effort to discredit the U.S. involvement in the Syrian conflict the Russian Defense Ministry claimed that the U.S. was in fact providing support to ISIS forces which are opposing President al-Assad and is actively supported by the Russian military.

As evidence of this claim, the Russian Defense Ministry offered purported imagery of an ISIS convoy that it claimed was being over watched by a supporting U.S. AC-130 gunship. Fact checkers eventually determined the image was actually captured from a video game entitled “AC-130 Gunship Simulator: Special Ops Squadron.”

When confronted with external evidence of the unauthenticity of the photo, the Russian Defense Ministry admitted that the photo was false and claimed the release was the result of a mistake by a low level employee.

Exaggeration is sometimes a successful and workable method, for example, as it contains or might have as starting point some true elements. Ukrainian forces pretended that they were able to kill a large number of high ranking Russians officials and even if the number might not have been the real one, at least some of them were admitted by Russian military spokesperson to have being killed in the battle and this in turn left room for credibility even if the figures were not always accurate.

Relationship with reality

Fake news must not be too far away from truth, otherwise it will not be credible, or at least, not for a long time. Facts should be distorted in a credible way.

A recent example was a story, about an Ukrainian pilot, that was officially debunked. “Hero of Ukraine Stepan Tarabalka is NOT “Ghost of Kyiv” and he did NOT hit 40 planes.” This is one of the most interesting statements included in an official statement shared on social networks by the General Staff of the Armed Forces of Ukraine. The post, was published in the afternoon European time on Apr. 30, 2022, and appears to be a response to the reports that started to circulate on [British media outlets](#) on Apr. 29. The legend of the “Ghost of Kyiv” is almost certainly an example of bizarre distortions and manipulations of fact or near-fact that are amplified during the chaos of war, especially a new war during the opening hours.



The 17th International Scientific Conference
**“DEFENSE RESOURCES MANAGEMENT
IN THE 21st CENTURY”**
Braşov, October 28th-29th 2021



These legends sometimes have at least some basis in fact, but as they travel through language barriers and across borders at the speed of light via social media, they become embellished, retransmitted and retweeted as “news”. There may have been Ukrainian air-to-air victories in the opening day of the war. There may have even been six total, or some other number. But the likelihood that six of these alleged aerial victories belongs to a singular, gallant “ace-in-a-day” is very remote.

3. Impact of fake news on the military

Disappointment, discouragement, speculation

Fake news is wreaking havoc on the battlefield and unfulfilled expectations, losing face, losing hope, instilled fear, panic and confusion are obvious effects of carefully conceived and released fake news.

Disinformation is often designed to trigger an emotional response. The audience have to be cautious of the content that uses emotional language to elicit a strong reaction. Fear and anger are big drivers that allow disinformation to thrive.

It cannot be excluded also the fact that sometimes fake news could lead to a real war, or make states be on the verge of it as a result of falsified or manufactured pretexts. Sometimes operations under a false flag might be conducted in an effort by outsiders to trigger a conflict between states. The attack on oil tankers of Oman in 2019 raised a question mark regarding the authors, making the world wonder whether it was Iran or Saudi Arabia or Israel or a combination of all three.

Also, following a recent incident that took place in Zaporizhzhya province in Ukraine where Russians accidentally wiped out own troops with flame throwers, there were claims from the Ukrainian side that demoralized Russian troops have vandalized their own vehicles so that they cannot be sent into battle.

Gaining or losing support

Pretending unrealistic success over the enemy, multiplying the figures related to their losses, with the aim of encouraging own and friendly forces and make the stand-by or neutral actors decide on which side they are or make them understand that is not such a high risk as anticipated if trying to help. Amid Russia-Ukraine war it was mentioned that the Russian soldiers had fuel, ammunition and food left for a few days only and even if the reality was not like that, it raised morale and hope of both Ukrainian fighters and neutral actors.

Research indicates that people are much less likely to identify disinformation if it aligns with their own beliefs or preferences and for many times the content is shared not just because people know it’s true but because they agree with it. Saying what people would like to hear, or hope to happen, even if not true, sometimes is widely accepted by the audience.

A photo of Kyiv Mayor, Vitali Klitschko, for example, went viral in the first days of the war, suggesting he was defending his country on the front line, and it was a very effective encouragement tool, but a quick reverse-image search, as described [by the Deutsche Welle fact-checking video](#), reveals that the image was from 2021 and it was posted on Instagram by Klitschko himself and shows him exercising with Ukrainian reservists.

Failure or success misinterpretation

Denying, saying nothing, or admitting that failure was caused largely due to unusual circumstances and not because of the enemy superiority so that the news can be less exploited and the moral of own troops be maintained, even if at lower level. Not mentioning anything about own



The 17th International Scientific Conference
**“DEFENSE RESOURCES MANAGEMENT
IN THE 21st CENTURY”**
Braşov, October 28th-29th 2021



losses such as number of casualties, highest ranks and type of equipment is a recommended tactic. During Russia-Ukrainian war there were only presented figures, that couldn't be instantly checked, on damages inflicted to Russian troops both to military equipment and personnel, and for the majority of times there was no news related to Ukrainian losses, which cast a doubt on the ability of the invaders to achieve their goal even if this was close to reality or not and even if the war took a heavy toll on the Ukrainian forces also. A good example of claiming victory in battle is one debunked by Deutsche Welle (DW), a jubilant video of Ukrainian military success over Russia that was posted on an unofficial Twitter page with more than 450,000 followers, containing also incidents filmed in Syria before 2022.

Losing cohesion

Duplicating a high ranking official social media profile and writing something he didn't say in connection with the conflict, such as measures that must be taken or data regarding future actions, future plans especially those related to multinational commitments or obligations will lose cohesion.

In May 2017, for example, ahead of a big exercise in Poland called Defender Europe, hackers cracked into real European news outlets' websites. They posted a fake interview in which Army Europe's new German chief of staff disparaged his Polish allies. Taking a more recent example, a Hungarian politician said that a BBC reporter tried to propagate the "fake news" by which Hungary does not support Ukraine's right to defend itself from Russian attacks militarily.

In this respect, information activities represents an effective tool whose aim is to influence an adversary's will and undermine cohesion. For example, by questioning the legitimacy of leadership and cause, information activities may undermine their moral power base, separating leadership from supporters, political, military and public, thus weakening their desire to continue and affecting their actions.

On the other hand, adversary attempts to influence NATO's will should be countered, in order to isolate the enemy, maintain coalition cohesion and enhance our freedom of action.

3.Counteracting fake news

Continuous monitoring

Continuous monitoring and permanent evaluation of all the news on the military delivered on all the information channels is a basic tool that apart from providing a collection of all the fake news it will also contribute to creating subsequent measures for reaction to them.

Identifying and flagging common sources of disinformation, such as certain websites or authors will make it harder for such sources to succeed in promoting new pieces of disinformation.

One of the biggest challenges is the volume as there are nearly three billion monthly active users on Facebook alone, each one capable of posting something inflammatory online. Twitter has over 350 million active users, including prominent individuals, popular opinion leaders, and clever and resourceful influencers.

Usually, though we cannot exclude biases and collective interests, real news is covered by more than one source. If mainstream media are not picking up the story, there's a good chance it can't be confirmed. By running a search, one might find that independent fact-checkers have already debunked the story. Fact-checking sites, such as BBC Reality Check and AFP Fact Check, allow us to check the accuracy of stories. By increasing the number of algorithm checks, the military research agencies hope they can spot fake news with malicious intent before going viral.

Romanian Ministry of Defence, for example, monitor all the military related news delivered on all national and main international television channels and printed media through Media Monitoring Centre and social media through Facebook Office, all the collected data being further analyzed from quantitative point of view, frequency, delivery time, attention paid to by the media



The 17th International Scientific Conference
**“DEFENSE RESOURCES MANAGEMENT
IN THE 21st CENTURY”**
Braşov, October 28th-29th 2021



and depending on the circumstances the leadership and public affairs personnel take all the necessary measures for counteracting them.

Anticipation of fake themes/key messages

Anticipation of fake themes, topics and messages during the planning processes and making available to the public, in a controlled manner, some information related to future activities such as movement of military convoys and live fire exercises will minimize the chance of exploiting the information in a negative way.

Comprehensively understanding the information environment, specifically disinformation, is crucial to enable a credible response.

Focusing more on checking emotions and less on checking facts is a well working method. Artificial intelligence-based sentiment analysis represents an entirely different approach to mitigating disinformation by training computers to identify messages and posts containing elements of surprise, disgust, and other emotional predictors. These are more likely to be associated with false information and to inflame the passions of social media users.

An important role is played, for example, by the PsyOps specialists who comprise analysis, advice, prevention and crisis management throughout the continuum of competition to mitigate and counteract the use of adversary hostile information activities and develop Allied options and opportunities for employment of their own PsyOps. Identified themes in adversary's hostile information activities can be countered by information and communication activities through coordination by J10-StratCom, as required. It remains the responsibility of Allies and their entitled bodies to decide how and if they counter/respond to hostile information activities in their respective countries.

Collaboration with media, other National Security structures and NATO

Maintaining a close and continuous relationship with media, facilitating dialogue and close cooperation with them as well as with the other institutions from the National Defence System and NATO will improve shared understanding and create conditions to correct the wrong information in a timely manner.

There is no single solution to disinformation and nations and NATO cannot act alone. From international organisations and national and local governments, to private companies, civil society and a free and independent media, all actors – including NATO – have a part to play.

In Romania, specialists from Ministry of Defence, Governmental Communication System, Romanian Intelligence Service, Ministry of Interior, Ministry of Communications and Information Society work in an integrated manner to mitigate the risks associated with fake news and disinformation.

As a collaborative effort is needed, computer hackers and propaganda specialists working in the British Army were placed in a single division, as part of a reorganisation designed to reflect a belief that the boundary between peace and war has become increasingly blurred. The cyber and intelligence experts were consolidated into a reborn 6th Division – one of three in the army with a strength of 14,500 – which also contain ground troops who can be used in secret, special forces-type operations.

As technology advances with quick steps, generals hope that it will be possible to further retrain soldiers keen to work or improve their skills as hackers or information specialists to enhance the capabilities needed to battle disinformation.

Official statements and press releases

Some of the fake news are counteracted by coming up with additional specifications, explanations, usually in the form of press releases. People are encouraged to inform themselves only



The 17th International Scientific Conference
**“DEFENSE RESOURCES MANAGEMENT
IN THE 21st CENTURY”**
Braşov, October 28th-29th 2021



from official sources. The information is cross-checked before acting, by asking confirmation from another source that is part of the loop or the information chain.

Depending on the circumstances, sometimes it's more effective for authoritative figures to present accurate facts early and routinely, instead of trying to rebut every piece of disinformation after-the-fact. This becomes more effective when knowledge gaps are identified and addressed in order to reduce our audience susceptibility to disinformation.

Romanian Ministry of Defence webpage, for example, contains a special subpage/index called InfoRadar where all the fake news are promptly presented and additional explanations added, with the aim of increasing awareness over the current fake news and make the people disregard them. Since the start of the Ukrainian war, there were attempts to influence the public opinion by fake news such as starting the recruitment and mobilization processes, an existing Romanian–Ukrainian agreement, the location of Allied forces and their further deployment from Romania to Ukraine and fake news on the NATO led special operations forces exercise that takes place every year.

Access interdiction

Blocking the sensitive military related information, especially facts and figures that show a clear defeat, tightening the operation security (OPSEC) regulations, denying access to social media platforms such as Facebook, Twitter and control the radio, television and printed media, especially the private ones. Censorship it's not something new for the communist countries and it is still applicable wherever vital information has to be preserved for the success of the overall mission. A recent example from the ongoing war in Ukraine is that of Russia's parliament passing, in the month of April 2022, a law imposing a jail term of up to 15 years for spreading intentionally "fake" news about the *military*. Some other countries use a parallel IT system, especially for social media. A good example is China, where Facebook, Yahoo, Google Maps are very difficult to access or not accessible at all, but some other applications that allows sharing information such as WeChat are used instead, and unlike civilians, military personnel are forbidden access to some of the world wide web applications.

Truth denial

Admit the truth but not entirely, say that indeed losses occurred but too a much lower extent, losing of ground was in fact a planned retreat, a regrouping for a more successful counteroffensive. Following the sinking of Moskva warship in the Black Sea, by a Ukrainian missile, the Russian Ministry of Defence, stated that the sinking was not related to the ship being struck by a missile but by a fire that broke out on that day and in turn created an explosion.

Reducing the importance of an issue and dismissing it as trivial, or keeping silent are widely used techniques and it was observed that by saying nothing about what happened, the issue was for many times forgotten.

On the other hand, not admitting one's own actions, such as war crimes, is a common tool that can be used by the enemy. Hitler's minister of propaganda had a motto: 'Accuse somebody else of something you have done.'

A well known example is the official statement of [Maria Zakharova, the spokesperson for Russia's Foreign Ministry, who said](#) that Russia was not bombing cities in Ukraine and alleged that pictures showing the attacks were manipulated videos from NATO countries.

Counter-hostile information and disinformation, also known as countering propaganda, is a multi-discipline effort. In NATO it is directed by J10-StratCom and coordinated by the information operations (Info Ops) staff to deliver agility and proactiveness within the information environment. The continuous Information Environment Assessment (IEA) conducted by J-10 StratCom-led Info Ops IEA cell is complemented by military public affairs (Mil PA) and psychological operations



The 17th International Scientific Conference
**“DEFENSE RESOURCES MANAGEMENT
IN THE 21st CENTURY”**
Braşov, October 28th-29th 2021



(PsyOps) specialists. The latter takes a lead role in the analysis of hostile information and disinformation and plans and supervises the execution of counter-hostile information activities as part of the StratCom-directed coordinated communications campaign. They focus specifically on analysis of adversary information activities, their source, content, intended audience, media selection and effectiveness.

4. Using fake news for own benefit

Deception

Deliberately disclose partial information on current status and future intentions in order to make enemy concentrate their main effort on other direction and in other window time, helping own troops achieve surprise by making the opposition forces vulnerable where and when it was planned. By causing a military formation to believe what is not true, deception seeks to mislead adversary decision makers by manipulating their perception of reality.

Causing ambiguity, confusion, or misunderstanding in adversary perceptions of friendly critical information, causing him to misallocate personnel, fiscal, and material resources in ways that are advantageous to the friendly force, or to reveal strengths, dispositions, or making making him to waste combat power with inappropriate or delayed actions, it will definitely contribute to the accomplishment of friendly mission.

However, no matter how the information is passed, in order to be successful, the deception story must be believable, verifiable, consistent and executable so that the deception target believe that his enemy has the capability to execute the operations that are being portrayed by the deception story.

The deliberate exposure to the enemy of false information that causes the enemy to reach an incorrect conclusion about friendly intentions and capabilities, is not new and in modern times, the militaries of several nations have evolved deception tactics, techniques and procedures into fully fledged doctrine.

A well known example is the creation of the fictional Major William Martin ("The Man Who Never Was") as a British officer carrying important [World War II](#) battle plans. As part of the Operation Mincemeat deception that concealed the location of the planned Allied invasion of [Sicily](#), the Allies intended for the Nazis to acquire the false documents, which indicated a planned Allied invasion of [Greece](#) and the [Balkans](#), and then incorrectly allocate troops and materiel.

Audience profile analysis

Analyze the profile of the ones who can exploit the information or amplify the effect of it, such as decision makers, opinion shapers or key leaders and ensure that the intended information reach them. This will pave the way for future Key Leaders Engagements, and it will also serve as an initial guidance for message development and communication channels to be used. An organization must amplify and contextualize its actions to audiences if there is a risk that others will also do so in their own way for their own ends.

All of our actions, images and words will be observed, interpreted, packaged, redistributed and acted upon by different audiences, according to their perspective and desired objectives.

Having detailed knowledge of key leaders' personalities, leadership styles, ambitions, motivations, objectives (short and long term), current stances, dependencies, psychological profiles and personal histories will be essential to provide the context to plan appropriate information activities. A vital component in all plans will be to recognise the complex, adaptive relationships and dependencies that exist between actors.

Insulating people from outside influences, pre-conditioning or indoctrination ensures that the audience will automatically dismiss messages from a particular source.



The 17th International Scientific Conference
**“DEFENSE RESOURCES MANAGEMENT
IN THE 21st CENTURY”**
Braşov, October 28th-29th 2021



It is also important to analyze what the audience can do for us, taking into account their qualifications and even if what they have on their own hand is just a mobile phone, redistribution, further altering the media content and convincing and adding followers in an exponential number, will definitely contribute to resistance and activism.

Creation, approval and transmission of news/messages

Based on the analysis of the combat events and information environment various working groups that include representatives from PSYOPS, EW, IO, Public Affairs, Legal, and Intelligence look at how the target audience on the adversary side can be influenced, manipulated and audio, printed or video materials and communication channels, methods of delivery are discussed and submitted for approval in order to synchronize the non-lethal and lethal actions so that they can achieve the maximum effects.

It is important to note that PA and Info Ops have different audiences and delivery channels, coordination of the message and delivery timing is necessary and appropriate. Effective PA provides a commander freedom of action and supports Info Ops in countering adversary propaganda with the truth about operational activities, while protecting OPSEC.

The credibility of PA spokespersons as sources of timely and truthful information must not be jeopardised. To avoid giving the false impression that the media are being manipulated in any way, a clear distinction must be maintained between Info Ops and PA.

PA and Info Ops are separate, but related functions. They directly support military objectives, counter adversary disinformation and deter adversary actions. However, the efforts of PA and Info Ops differ with respect to audience, scope and intent. Therefore, coordination between PA and Info Ops must be assured at all times and at all levels to ensure consistency in the message released by the military to outside audiences and to promote overall effectiveness and credibility of the campaign.

In order to increase the psychological effect of our own troops combat power, to undermine confidence in the adversary leadership, PSYOPS can be used to shape the battle space prior to the conduct of operations, particularly special operations. Special operations are typically highly compartmentalised, with a great and necessary emphasis on security and when such operations are planned, PSYOPS should also be considered to address expected consequences and mitigate potential negative effects. In order to achieve maximum effectiveness, all the planned actions are analyzed and approved, following the Battle Rhythm, in working groups and boards such as Information Activities Working Groups, Key Leader Engagement Working Group, Targeting and Synchronization Activities Board.

5. Conclusions

Fake news is a phenomenon that, along with the speed of mass communication nowadays, has an enormous potential to do harm. Be it propagated consciously or not, this reality is yet to be addressed at a sufficient scale to be minimized and then eventually, ignored. Its range is non-discriminatory as it affects a wide array of domains, from politics and military operations, to high-life and common people's lives. It can influence elections up to the point that can decide the free choice of a countries' leadership or significantly reduce the huge volume of resources invested in a military operation.

Disinformation, propaganda and misinformation have been a challenge for decades, but are especially dangerous during crisis or in war times. Disinformation from both state and non-state actors attempts to divide Allies, undermine trust in democratic institutions and present authoritarian regimes as better at dealing with crises.



The 17th International Scientific Conference
**“DEFENSE RESOURCES MANAGEMENT
IN THE 21st CENTURY”**
Braşov, October 28th-29th 2021



Mankind has come to learn that it is not as easy to control information and spread disinformation in the age of social media compared to the 1990s, for example, when in Lithuania all that Gorbachev’s army needed was to take over the radio and TV towers.

Ukraine, for example, offered lessons not only about disinformation dangers but opportunities for resistance and activism. Focussing solely on these negative attributes can ignore how effective digital environments and online communities have been for Ukraine. Ukrainians have fully used the power of social media and one only has to look to how Ukrainian officials have used digital tools to amass large-scale support for their country.

The good news is that people became more and more aware of the truthfulness of the news they’re consuming and tools and mechanisms to check the facts versus opinions are emerging but the society needs to have these instruments clearly defined, regulated and supported up to the point the fake news phenomenon becomes marginal and limited.

References:

- [1] *AJP-10 Allied Joint Doctrine for Strategic Communications*, Allied Joint Publications, 2021, 113 pages
- [2] NATO Policy on Public Affairs MC 0628, 2017, 38 pages
- [3] NATO Policy for Information Operations MC 0422/6, 2018, 15 pages
- [4] www.mapn.ro
- [5] www.facebook.com