Marijana Opašinova Šundovska*

Security Implications of Fake News and Disinformation in Nato Member and Partner Countries

Abstract

Misuse of digital platforms for the dissemination of fake news and disinformation online is becoming an increasingly serious problem both for individual states and multilateral organizations. Alternative facts presented under the veil of awakening critical thinking, or false and purported information placed in the social media environment by state and non-state actors for their own purposes, have been disturbing the credibility of traditional fact-checking media outlets to present actual information to the public. Grasping the notion of parrhesia as part of the democratic free expression in a liberal society via social networks is now seriously questioning the common objective standards of truth. Deliberate interference with fake news and disinformation in contemporary democracies, especially during election campaigns, the use of anti-NATO narrative, particularly in countries with former communist regimes, and recent promotion of a false sense of security or insecurity about the Covid-19 pandemic, became an issue of major concern for the entire Alliance and its field work. Although in essence being a military organization with the aim to secure peace and stability in its wider area and promote its values globally, what the NATO has witnessed in the last decade is that peace and security in the traditional sense cannot be taken for granted. The emergence of modern non-military tactics by adversaries to destabilize member and partner countries require specific methods and approaches for deterrence and defense. This paper will analyze how these alternative facts affect both state and overall Alliance stability, possible implications on the diminishing public trust in state institutions, and actions needed to mitigate their effects.

Key words: fake news, disinformation, state stability, elections, pandemic.

* Marijana Opašinova Šundovska, PhD, University American College Skopje, North Macedonia, mopasinova@gmail.com
Introduction

Although in essence its establishment has been linked to the security of the North Atlantic area in a military context, the NATO has changed in the face of emerging challenges over the past decades. Declared the most successful alliance in history, it has been promoting the fundamental values of pluralist societies and has assisted its members in reinforcing their mutual trust and preventing future conflicts on their territories. With the world changing and new conflicts emerging, the NATO, according to Article 5 of the Washington Treaty, or under UN mandate, has been undertaking military actions to prevent conflicts from reaching disastrous proportions with unforeseeable consequences. The modern world has on the other hand shown that there are new challenges far more dangerous and with longer lasting consequences on our societies, posing a direct threat to the resilience of our democracies. Rapid development of the internet, despite it being an essentially positive innovation intended to make our lives easier and to save time, proved to be multi-faceted, and fertile soil for state (in)stability. Fake news, disinformation and propaganda during election campaigns, the Covid-19 pandemic, as well as continuous hybrid threats and terrorist attacks against states in general by both individual non-state and state actors, are becoming an increasingly serious concern to individual NATO member and partner countries, and to the organization itself. Their effects demonstrated, depending on the levels of sophistication, their grave influence on state operations. Internet platforms and social networks are filled with information about alleged steps taken by government officials or political candidates in their election campaigns, prominent healthcare experts showing concern over vaccines and their detrimental effects on human health, and offering alternative solutions that will save the society from this virus, some even claiming the virus did not exist. Both state and non-state actors have been strategically working in individual Alliance members and its partner countries to destabilize citizens’ trust in their state institutions and governments, and shift it toward them. Having seen that, the NATO recognized the need to take action, widening its operation perimeter to combat these challenges whenever they occurred. This research paper will examine how the post-truth phenomenon relates to contemporary malign information in the NATO wider area and how it affects state (in)stability in terms of political decision-making, citizens’ opinions and decisions, sources of information distributed to reach such effects, and try to offer solutions as a safeguard to those threats.
Theoretical approach to truth and contemporary post-truth phenomenon

Mark Twain once said that “a lie can travel halfway around the world while the truth is still putting on its shoes.” In recent times, traditional international lies have been defined as fake news – false information used to influence, affect, convince and manipulate recipients; disinformation – misleading information as a form of deception to end users (Fallis, 2009). Such terms are historically rooted as well, in the term propaganda, which was initially used by the Roman Catholic Church to disseminate religious beliefs and reinvigorate the people’s faith in Christianity (Jowett and O’Donnell, 2018). From Themistocles in ancient Athens, who spread fake news to defeat Xerxes, and Julius Caesar, who mastered propaganda instead of using force and weapons, to the US founding fathers who performed political propaganda for the adoption of the federal Constitution (Manning and Romerstein, 2004), or the Black Nazi Propaganda during the Second World War used to impose a new world order or a new system of government, psychological warfare has been used to feed people particular beliefs for political purposes, truths deemed necessary in order to achieve certain political objectives. The problem is, all of them were convinced that taking such steps would make the world a better place, and managed to animate masses of people to support them and implement their cause. Aristotle considered that the truth lied in calling things what they were or were not, i.e. in their original form. The great Austrian philosopher Ludwig Wittgenstein claimed that structures have spatial locations and could be easily detected or seen in their original form, unlike facts which could take the form of those presenting them. He believed that danger comes from hidden meaning and the construction of words or sentences, or the narrative created behind the surface (Wittgenstein, 1921). Russel and Moore on the other hand considered that many equally coherent, but incompatible truths could co-exist; however, only one could contain the truth (Moore, 1899; Russel, 1912). Unlike them, Joachim considered that truth was the character of a significant whole that excluded individual judgement or beliefs, rather a system of common judgements (Joachim, 1906). This approach was argued by Blanshard, who posited that such systems of coherence containing sets of beliefs actually corresponded to objective facts (Blanshard, 1939).

Pragmatists developed a position that truth may involve a certain level of correspondence only if possibility is provided to verify that truth (Haack, 1976). Contemporary information warfare related to the right, or true, belief, which was used mostly locally in the past due to limited tools and media of dissemination, is being undermined by abuse of modern information technology, confusing people about what truth is and how this concept can be most objectively delivered in this modern society of post-truth. Placing an emphasis on non-military and non-lethal means of achieving
its objectives, this kind of unconventional “fight” demonstrated the ability to instigate conflict, destabilize and weaken our modern democracies at a lower cost than standard warfare. Such continuation of political war by other means against adversaries (Clausewitz, 1984), combined with ideology, communication and use of media (Lord, 1989), is what we witness every day. Frank Hoffmann (2014) considered that the world faced the so called “hybrid warfare” as a new phenomenon of war, which included both conventional and unconventional means, i.e. kinetic and non-kinetic, a tailored mix of military means, terrorism, criminal behavior, cyberwarfare, fake news and foreign election influence for obtaining a political objective.

Nowadays, traditional international lies are defined as fake news – false information used to influence, affect, convince and manipulate its recipients, whereas disinformation is characterized as misleading information, a form of deception of its end users. Woolley and Howard consider that the use of human-software hybrids by state and non-state actors, and the discriminatory nature of the algorithms, are now threatening to undermine world political potential and manipulate end users (Woolley and Howard, 2016). The term was rightfully named Word of the Year in 2016 – post-truth – as post-truth politics of putting aside factual evidence in political discourse and putting emotions before the truth (Oxford Dictionary, Word of the Year, 2016).

The philosopher Rini defined fake news stories as such that take event in the real world mimicked by rules of traditional media reporting to deceive an audience as wide as possible (Rini, 2017). The English journalist Mathew d’Ancona wrote in 2017 about a trend of declining value of truth, following humanity as currently dwelling in a political era of emotional narratives that dominate over factual arguments. This is not due to the fact that politicians lie more than they did in the past, but the problem is the response of the public, even in developed democracies (d’Ancona, 2017). Today, non-events in a form of news construction, fabrication and dissemination are considered typology of fake news, accompanied by carefully chosen language and terminology. The motivation for their publication comes generally from political, economic and social reasons – political in the form of disinformation or propaganda aimed at influencing public opinion; economic attempting to bring financial benefits to the creators; and social related to status in society, as well as identity and acceptance in community (Kalsnes, 2018).

Recently, Nobel Peace Prize winner Maria Ressa accused Facebook of being a threat to democracy, showing bias against facts as the largest online news distributor, and such processes, she believes, happen with a purpose – targeted and used like weapons (Ressa, 2021). Search engines, as well as social networks’ personalized algorithms, selectively present news based on user preferences and internet histories in filter bubbles, a powerful tool in the hands of fake news creators to direct users toward comfortable, cocooned cognitive spaces (Badouard, 2017) where they can read, discuss and confirm their beliefs and perceptions, their truths, with other like-minded users.
**Post-truth and state fragility**

The impact of state and non-state actors in political warfare is neither new nor unknown to the world. What is becoming gravely concerning is the power accumulated in these actors to influence the international system, unseen before in diplomatic, economic, information, or military terms. Liberal democracies, founded upon the principles of sacred trinity of democracy, the rule of law and fundamental rights, became challenged for a possible disturbance in their interdependent implementation. The right of each individual to freedom of expression and access to information for an increased participation in democratic processes is a test of government legitimacy in deliberate democracies, while the consultation process and the access to information, critical thinking and facts available to individuals remain essential to the validity of those processes.

Modern warfare provides diverse opportunities for undermining state stability through attack and disbelief at state institutions and critical infrastructure, making them functionally fragile, especially in terms of their legitimacy. Both state and non-state actors have understood that diminishing legitimacy as the main pillar of authority and governance inevitably leads to the loss of public trust, and opens up space for turning to other sources of power; in this case, to their own benefit and interest. Fake news and disinformation focused on governments and citizens is carefully networked to disturb the political balance of states and to convince their citizens of the authenticity of such information. State legitimacy presupposes high percentages of confidence among citizens in elected governments as supreme political authority, as well as in the information provided by official media sources, which also implies establishment of a solid and functional legal framework that secures proper functioning of such media in the media market. The extent of influence and the penetration into the society by external actors determine the strength of state legitimacy.

Globalization and changes in the contemporary international system make nation states more prone to losing their monopoly of power over external actors, who manage to organize themselves in multi-organizational networks, both domestically and abroad, by means of the most sophisticated form of psychological warfare – effectiveness of fake news rhetoric and disinformation in reshaping our understanding of democracy, peace or war in the international system (Snyder, 2017). The post-truth landscape has drastically changed the traditional perception of security and the historical theory of warfare by use of military means for achievement of political goals. The traditional guardrails of democracy that keep accountable leaders in power and prevent citizens from epistemological manipulation do not demonstrate effectiveness in our modern liberal democracies (Ziblatt and Levitsky, 2018). It comes closer to the notion that war is nothing more than the continuation of politics by other means (Clausewitz, 1940) of modern technology, a range of possibilities to a new matrix of destabilization.
Questioned legitimacy of election processes

The 21st century changed the relationship between the individual and the state by making it more decentralized and thus more prone to external control or oversight by other entities. Provision of truth by multiple sources in order to prevent government monopoly or censorship is endangered by the emergence of artificial intelligence, as well as social media regulation gaps. Freedom House, in its Freedom on the Net 2017 annual report, stated that online manipulation and disinformation tactics played a vital role in general elections of 18 countries, including the US (FH Report, 2017). A myriad of pre-election processes in the last decade were colored by fake news at the expense of political opponents, with the use of tools such as sensationalist photos or headlines, fake opinions, factual information shared in false contexts, or misleading information where opinions were presented as truth or facts. Such exaggerated, deceptive stories intended to convince the user/reader in the “right” option and to influence their opinion. They have been present in almost all NATO member and partner countries. Different actors used these online possibilities to decrease the political support of candidates in elections, bearing in mind the increased use of the internet and the millions of users of social networks available to them. Targeted at the human psychological reaction to threat, as well as at cultural tradition and education of citizens in particular countries, such activities weakened democratic systems and made countries more vulnerable to external influences. In campaigning, both external actors and politicians benefited from the language of emotion, fear or concern, a well-known psychological tool of persuasion, to obtain political points and to convince voters of their post-truth stories. Highly sophisticated technologies helped them learn and group user choices based on their search practices, which in turn enabled perfect environments for propaganda and threats to human rights and democratic values placed in a political context (O’Neil, 2016). The process, initiated by politically motivated bots with concealed identities, started sending information to identified preference groups, which then went viral due to constant sharing and liking, enabled via the information cascade option in those groups, i.e., close contacts’ information sharing without fact-checking. Use of provocative terminology and language were often applied to convince even the most traditional media users. Dr. Aaltola, director of the Finnish Institute of International Affairs, when analyzing US, German and French elections, defined five stages of the election interference paradigm that may predict the level of influence on candidates in election campaigns: using disinformation to amplify suspicions and divisions; stealing sensitive leachable data; leaking stolen data via supposed “hacktivists”; whitewashing leaked data through professional media; and secret colluding (Figure 1) in order to synchronize election efforts. He also believed proper channe-
ling of such data to the “right voters” and proper timing of the release to be crucial to producing the final effect (Aaltola, 2017).

**Figure 1.** Five Stages of Election Meddling (Aaltola, 2017)

---

Disinformation was used to amplify divisions regarding data about political candidates’ personal lives, as such data usually spurs large interest among voters, and sometimes determines their final voting decisions. Fabrication of such disinformation against political opponents has been multi-faceted, well-chosen and bolstered with knowledge of the composition of society, voters’ preferences, their personal beliefs and even prejudice. It was during 2008 US presidential campaign, where the birth certificate of one candidate, Mr Obama, was among the most debated issues online. Despite the published birth certificate, fake “newsers” or “birthers,” as they were called in the US, claimed the document was forged and that the actual birthplace of Mr Obama was Kenya or Indonesia, as well as that he was Muslim by religion. This was clearly aimed at stirring voters’ racist attitudes as he was an African American candidate for US presidency. The outcome was that at least 20% of adult Americans doubted his place of birth (Washington Poll, 2011) and 72% of the registered Republican votes still doubted his citizenship on his re-election. To check whether this applies to all types of Republicans, the poll organizers asked the respondents three factual questions about politics, and came to the conclusion that there were no differences between low-knowledge and high-knowledge Republicans regarding their beliefs on Obama’s citizenship (NBC News Survey,
The issues about poor health conditions of Ms Clinton and Pope Francis’ fake endorsement of Mr Trump’s candidacy ranked very high among the disinformation that attracted a significant number of voters during the 2016 US elections. Similarly motivated fake news occurred during the 2016 French elections, when Sputnik news agency qualified Mr Macron as homosexual, backed by the powerful gay lobby (Sputnik, 2017), in an attempt to dissuade the traditional French public and convince them to vote for Ms Le Pen.

Information taken out of context, or completely invented news, also occurred during election campaigns. The 2016 US elections were inundated with fake news and disinformation spread online, with more than 100 active US political websites run from a town in North Macedonia, with thousands of followers. During the 2016 French presidential elections, Mr Macron was severely attacked by disinformation as an alleged US agent supported by Saudi Arabia in another attempt to play on the sentiment of French citizens by showing that he was not a true French politician, one who loved his country and did not “sell” himself to the foreigners. Fake news was also used by his opponent, Ms Le Pen, during the campaign, including just hours before the final debate, about his alleged secret offshore account. The news was massively retweeted by approximately 7,000 accounts and was used in the debate as an argument against Mr Macron (France 24 Observers, 2017).

There were cases of fake news and disinformation created to sensitive questions like migration, military missions abroad, or government public policies targeted to undermine state stability and make citizens lose trust in their institutions or international organizations. Deep fakes with superficial accusations towards political candidates or political opponents were observed for example in almost all NATO members and in many partner countries. Ms Clinton’s alleged plans for the approval of weapons sales to Islamic jihadists, “including ISIS,” were among the most consumed fake news during her election campaign. In Germany, prevalence of migration issues, topical at that time across the federal states, and the negative effects of migrants’ behavior (Meister, 2016), contributed to a more vigorous debate between political candidates during the 2017 elections, which enabled fake news actors to use such sensitive topics to their advantage. A study conducted by the Neue Verantwortung foundation revealed that fake news was mostly spread by right and extreme-right populist groups, especially by the extreme-right Alternative Party of Germany (AfD), noted as no. 7 out of 10 fake news spreaders who gained momentum of the popular sentiment of dissatisfaction with Chancellor Merkel’s migration policy, combined with unintentional statements by government officials, to reach as many users as possible. They also drew support of an extreme-right application channel by use of military language and manipulative content intended for “patriots” and aimed against AfD’s political opponents (Gensing and Kampf, 2020). Migrant issues, as well as the difficult economic situation in the
entire country, were also abused by populist and far-right parties at the 2018 elections in Italy.

Another observed method was the theft of sensitive and confidential documents. It happened, for example, in the USA, France, the United Kingdom, Albania, Turkey, and Israel. In France, the culmination point was reached two days before the run-off election, with hacked emails from Mr Macron’s campaign team, labeled operation “Macron Leaks” by the same team behind the Macron’s offshore account. The first spread was re-tweeted 47,000 times in just a couple of hours (Nimmo et al., 2017). There were other smaller documents and news spread online at the same time, but they did not reach the same magnitude. The 2017 German federal elections put the German authorities on full alert, following the US and French experience. It targeted leading politicians’ offices, including Chancellor Angela Merkel’s. This event was attributed to Russian intelligence interference.

Information warfare through cyberattacks of government institutions occurred often in the past decade in Germany, Estonia (McGuiness, 2017), Lithuania (Coble, 2020), Latvia (Viksnins, 2020), Georgia, Ukraine (Corera, 2020) and Poland (Rajca, 2021), affecting private mailboxes of prominent politicians, data storages and sensitive information. Furthermore, the attacks were intended to disseminate disinformation promoting anti-NATO agenda (Bahgat, 2021) in an attempt to undermine the member countries’ sovereignty and create mistrust among the general public in the efficiency of their state institutions. The intensity, frequency and complexity of the attacks have increased significantly in recent years. Although there was no conclusive information about the center of their origin, there is one thing they have in common – they all came from Russian locations.

Popular vote on referendums has also been under the influence of foreign actors, being able to create a division in Europe. The 2016 vote in the UK showed how difficult it was to distinguish between true and untrue facts, and to make people understand later on that the processes might bear serious consequences and few benefits (Viner, 2016). The outcome of a major vote in the post-truth era came unexpectedly, inflicting serious damage to European unity. The 2017 crisis in Spain regarding the self-determination of Catalonia had been preceded by a timely and targeted fake news campaign accusing the Spanish government and police forces of using repression to make the citizens vote against the independence of Catalonia, and claiming that the country was on the brink of civil war. Others published news aimed to undermine cohesion by claiming that the European Union would recognize the independence of Catalonia as long as it went through the process of accession, and once the European Parliament approved the right of the citizens of Catalonia to determine their future in a democratic way (Alandete, 2017). The main problem here was that the campaign
influenced not only the voters’ opinions, but also their ability to receive objective facts and information necessary to reach a final decision.

The success of fake news and disinformation in election processes differed based on several factors like the features of the society, cultural tradition, voters’ internet literacy, their trust in traditional media, and language. The US case included all of the factors, showing that fake-news creators abused sensitive issues as a weakness in order to create divisions, spur social unrest and gain more popular support for their preferred candidates. A Princeton-led study (Guess et al., 2018) confirmed these claims. From the data obtained in the study, its authors concluded that exposure to fake news did have a significant impact on the decisions made by voters. US intelligence agencies stated that Russia’s goal was to undermine public trust in Mr Trump’s opponent and develop a clear preference, which in fact helped Mr Trump win the elections (DNI Report, 2017). Germany and France came somewhat better prepared, aware of the lessons learned from the US elections. In Germany, their security authorities were also put on high alert to detect signs of foreign interference. What’s more, Germans rely to a higher extent on professional media rather than on social media outlets. Sanctions imposed to cyber activities on perpetrators of previous attacks deterred to some extent the foreign influence. An agreement between the political parties not to use fake news in their campaigns was also a step in positive direction in this regard, contributing to a less polarized debate before the Election Day. Unfortunately, this did not apply to the newly established AfD party, who managed to gain an astonishing 12.6%, becoming the first extreme-right party to enter the parliament after the Second World War. It also clearly demonstrated AfD’s election success by means of the success of fake news and disinformation, among other things, which secured their seats in the parliament (DW, 2017). France was exposed to a massive disinformation campaign, as were other states, in the course of the 2016 presidential elections. The failed attempt to significantly affect the election outcome and antagonize the French society was due to the effective reaction by Mr Macron’s campaign personnel and government authorities, who acted like watchdogs, proactively and well in advance, ensuring the integrity of election results, but also alarming the public of possible disinformation during the campaign. Strong civil society and mainstream media, mostly independent from tabloid news and alternative websites, together with France’s cultural tradition of critical thinking, enabled its citizens to elect their candidate in a truly democratic atmosphere. The 2018 Italian elections put two great losers in the spotlight: the EU and the NATO. The reasons were mainly connected to the low levels of trust in traditional Italian media outlets, as many journalists ran for political office during the elections. It forced the public to look for alternative sources of information, which was cunningly used by different actors in the campaign, mainly on sensitive issues like migration and the economy. Indirectly, election victory of populist and far right parties, winning
their seats in parliament, was a symbol of victory of the anti-NATO (Atlantic Council, 2017), anti-West and anti-democratic values (Trevisan, 2018). In the UK, the detected external interference raised even more concern, which puts into question the legitimacy of the vote. Findings clearly showed that external disinformation campaigns were involved with the Leave-option before vote took place (House of Commons Report, 2018), a massive activity on social media that was additionally complicated by the Facebook-Cambridge Analytica data breach, shared with companies that were linked to Russian intelligence services (Euractiv, 2018).

Research done by IPSOS in 2019, covering 25 countries, mostly NATO members and partners, showed 86% of citizens read fake news, and nearly 90% reported to have initially believed in it (IPSOS, 2019). Hence, fake news is now put to a critical juncture, when it cannot be ignored anymore as an aside question, but requires rather in-depth attention, since it affects the credibility of many governments and state institutions. When facts are not convincing anymore, voters lose trust in the official media and turn towards their own truth, obtained from unchecked resources, which diminishes the value of truth in our modern society. But what is even more concerning is that they also diminish the importance of expert voices, undermine the trust in traditional media coverage and impair professional journalism, and thus restrict freedom of choice and democracy. So the question is to what extent elections/referendums were an objective choice of the citizens in the past decade.

**Fake news, terrorism and conflict**

Terrorist activities and their networking have been increasing in the past decade. Non-state actors diffuse disinformation to obtain strategic objectives, commonly to put into question the trust in their respective governments and to strengthen extremist narratives of their recruitment strategies. Absence of an international instrument to address their online activities makes the concern even greater. Terrorist groups have been organizing more and more with the use of modern technology, taking advantage of the absence of universal mechanisms to confront their activities, as well as the limited training on legal actions against terrorist activities by use of internet. Unfortunately, popular social platforms that work with algorithms actually help those groups toward enlarging their networks of associates and supporters, as well as in recruitment. Social media helped them attract and indoctrinate followers systematically with propaganda, by use of specific terminology and emotional language, generally those with a trigger for radicalization (Berger and Morgan, 2015).

Well-formed and closed groups posted extremist propaganda, videos showing them presenting the “great cause,” or constructed religious images as a means of radicalizing young people and motivating them to join the group. Propaganda has often been
aimed to reach audiences based on gender, age or social and economic background. Extremists have invested heavily in tactical campaigns through social platforms and well-structured, closed online groups for the recruitment of minors from marginalized groups, drawn by the sentiment of injustice or the disintegration of society. The initial tactics included indoctrination via different online tools to support their perception of religion and methodology and to end up with recruitment and selection of the most dedicated believers and followers to commit terrorist attacks, securing them their sacred place in heaven (NYPost, 2015). Contemporary times go in favor of their capacities to attract more people due to increased internet use by minors as well as their illiteracy and inability to recognize fake news and disinformation. Back in 2005, Al Qaeda admitted that half of their battle was in the media, for the race of their Muslim community. Media platforms like Facebook and Twitter use algorithms that “help” users find contacts (friends) that share mutual friends, education, or have similar preferences based on their activity logs. Some terrorist organizations prepare special training instructions and strategies (Revkin, 2016), multimedia communication tools that provide both ideological and practical instructions for carrying out terrorist activities in crowded areas, mostly in major European cities or against prominent politicians. Estimates show that the ISIS campaign on social media attracted more than 18,000 foreign soldiers from more than 90 countries (Schori, 2015). Unfortunately, most young people came from NATO member and partner countries. What is worse, they were the ones chosen to carry out terrorist attacks (Major AlSarayreh, 2020) in major Western capitals. The main objective behind this was to undermine state stability and provoke fear and anger among the population and question the rightfulness of government actions and policies of their troops in NATO-led missions during the past two decades.

Language of terrorist groups is an interesting phenomenon, which differs depending on the audience. For example, emotional and violent content is carefully composed for recruitment “bubbles,” with amplifying psychological effects in the Arab language and visual messaging. This multi-faceted propaganda goes through a carefully crafted dissemination process and a peer-to-peer sharing as a tool for greater visibility (Fisher, 2015). It differs from the rather more restrained approach in international propaganda in that its ideology is based on the assistance of an alleged attack on a Muslim community. The network is usually backed by a highly trained sympathetic team whose aim is to provide moral support to all those helping the oppressed Islamic community. It is followed by well-structured intelligence and counterintelligence networks that monitor their proselyting centers for local recruitment of supporters, as well as the media usage of their own fighters. On the other hand, English news language targets Western standards and benefits of modern life as something distant from real values, and finds the cure for Western depression in Jihad (Shane and Hubbard, 2014). Such language
has amplifying psychological effects and provokes its enemies in the West with their videos and photos of systematic assassinations of journalists, leaders, and women. In terms of types of releases, 88% of IS releases were visual (63% picture, 20% video, and 5% graphic), with a very high proportion of emotive media content (Zelin, 2015). Cyber targeted warfare is of lower priority, and it is focused on hacking vital Western state institutions, Twitter accounts and broadcasting companies to advert them to intervene against the Islamic State (Katz, 2015).

Statements using unchecked news addressed to foreign counterparts, like the case of the Pakistani Defense Minister’s reaction to Israel’s fake news nuclear attack (Goldman, 2016), or alleged interest of the Moroccan government to profit from ticket sales of the Alhambra palace in Spain (Ultima Hora, 2011), also raised serious concerns. In 2017, Russian Defense Minister used a fake image to show alleged US support to ISIS that was actually a screenshot of a video game (Higgins, 2017). Such acts emotionally upset the authorities of relevant states, and although some ended with explanations and formal excuses, the damage had already been done, both domestically and internationally.

Similarly, news about the bombings at the train station in Spain (El Pais about El Mundo, 2006), or the Paris attacks (National Post, 2015) misled the public about the real perpetrators since those media outlets did not take appropriate steps of fact verification. Malpractices of this kind not only violate the principles of professional journalism, but also augment public prejudice by using false facts. Fake news by mainstream media creates even greater concerns since it reaches many users and enjoys the majority of public trust; intentional or unintentional disinformation causes more damage than if not published at all.

**Covid-19 pandemic**

The fight against disinformation and fake news in times of great national or global crises when citizens feel scared and grasp such narratives that make them feel safer, proved to be much more challenging to both international and individual efforts. The global pandemic caused by coronavirus unveiled the ugly face of internet and media abuse in the dissemination of such news, showing that no media institutions or even international organizations were able to successfully circumvent their influence among the general population. Abuse of power by governments in fertile-soil democracies and autocracies in certain NATO member and partner countries, and the spread of fake news and disinformation about many aspects of the pandemic, were the most commonly detected issues of concern. The thin line between free and unfree societies was very often put into question in most states. Lockdowns, transfers of legislative powers to the executive and the introduction of restrictive measures to mitigate
the devastating consequences of the virus, although deemed necessary, were in themselves very questionable in terms of respect of human rights, freedom of movement and transparency. In autocratic states, this helped governments abuse development and justify the introduction of special powers to strengthen their governance, interfere with the judiciary, discredit political opponents and weaken the balance of power. By using the corona narrative, they turned the war against Covid-19 into war against freedom and democracy. On the other hand, fake news by various interest groups brought dangers to the general management of the crisis on a global level. Many leaderships made timely interceptions by sending official statements via media channels and/or by appearing frequently in public, showing that fake news is best confronted through government transparency, rather than with penalties (Shundovska, 2021). This fake news info-demic that accompanied the great pandemic threatened to be far more dangerous than the virus itself.

Use of modern technology during the pandemic increased rapidly, both by official institutions, who wanted to send accurate information on all developments to the citizens, but also by individual groups and some state actors. Fake news and disinformation were related to the creation of stories on the origin of the virus. Accusations came from China that the virus was created by the NATO. The statement was supported by Russian media outlets who claimed that this had been done in NATO secret labs in the Baltic states, and that NATO military operations there would increase the spread of the virus and endanger the lives of the citizens. Many NATO member and partner countries witnessed disinformation about the possible link between the spread of the virus and the installation of 5G base stations, convincing individuals to destroy their infrastructure (Adams, 2020). A concerning detail in this political disinformation milieu showed that far right members spread more disinformation regarding the pandemic, especially regarding the alleged spread of the virus by migrants and different ethnic minorities (Doward, 2020).

Terrorist groups from the Islamic State, on the other hand, used the situation to accuse the West of creating a virus that kills Muslims, since they were the carriers. The spread of the virus, portrayed as punishment of non-believers of Islam, was a theory placed by some groups in NATO partner countries intended to attract more people to be involved with these radical groups. Some countries in the MENA region abused the poorly regulated domain to enhance their political legitimacy and discredit their opponents. The fertile ground for disinformation created an orchestrated cyber- and social media campaign against one particular country in the region, Qatar, as a deliberate spreader of the virus, who had allegedly made a previous payment to China to create the virus and to damage economies of their neighboring countries, as well as to spread it to other continents. The main reason behind this campaign was to weaken
its economy and its government leadership, as an important US ally (Jones, 2019) and a NATO partner.

Fake information and remedies have been promoted by some religious leaders to increase their reputation, which later also attracted a global audience. Their fabricated stories accused particular members of a religious community as carriers of the virus, instigating animosity among the general population about that particular religious group. Remedies were offered as well on how to protect or cure the citizens from the virus that had nothing to do with medical evidence (Alimardani and Elswah, 2020). A concerning campaign was also led in a country of this region, both by religious leaders and media outlets, blaming Zionist elements for spreading the virus via biological labs against the citizens of their state, one religious group in particular (Lerner and Weinberg, 2020).

Same patterns followed in the Western Balkans and countries bordering Russia, with misleading stories and manipulations about the origins of the virus, blame games about its spread towards certain national minorities and foreign states. The strongest narrative prevailing was the glorification of Moscow and Beijing as saviors of the people of those regions during difficult pandemic times, and both the NATO and the EU were demonized as abandoners, failing to provide assistance in critical times as a result of late distribution of vaccines (EEAS, 2020). Vaccine quality was also questioned by some so-called experts, and a lot of fake news stories and videos were created, with thorough explanations of why people should not get vaccinated. This theory was supported by the fact that vaccines were created to depopulate the planet. Vaccines produced by Western manufacturers were the ones mostly called into question, and preferences were given to Russian and Chinese vaccines, if any, with the explanation of their superior quality and composition. Unfortunately, despite the development of science, strong anti-vax protests were observed in most NATO countries, and their numbers should not be disregarded. The percentage of vaccination in all NATO member countries did not reach the expected level. These actions were all taken to discredit legitimate governments of NATO member and partner countries, and also to damage the image of the NATO as a defense alliance of democratic states and its capacity to deal with emergency situations in critical times.

In general, the pandemic was largely abused by autocratic leaders and actors to challenge NATO unity and its values and to delegitimize governments in its member countries. Luckily, coordinated joint efforts and individual measures by countries themselves helped to prevent major changes in the public information sphere. Partner countries were more vulnerable to disinformation and destabilization, Western Balkans and the MENA region in particular. Special attention needs to be paid to those regions, since fake news and information flows are intense to a disconcerting level, which can create other problems in the future if not combatted by official information.
Conclusions

The origin of fake news and disinformation is not limited to borders, racial, religious, or any other background. They come in all shapes and sizes. However, if limits needed to be established, they would mostly come from political parties against political opponents, media outlets supporting external actors, some government authorities targeting their own population or other states, and external actors with particular interests abroad. They use all available means to spread disinformation to larger audiences and to gain as many supporters and followers as possible. Many of them succeed in achieving their goals, manipulating users by their own individual preferences. The anti-NATO mantra came strong across the majority of its member and partner countries. Questioned legitimacy of election processes, disabling the true choice of the preferred political options, comes to the forefront of this fight. Amendment of election legislation is necessary in order to regulate the use of meddling methods on social media platforms during elections.

The time has come when it is not about the personality of political candidates or their party programs, but about the ability to gain the attention of voters with post-truth propaganda. Commitments publicly taken by political candidates before the start of campaigns, or prompt institutional reactions of disclosing the right information and presenting true facts as opposite to fake news platforms, prevented greater interference with election processes or the polarization of society in several states. Political culture proved to play a very important role during elections. The gentlemen’s agreement between political opponents to verify facts before sharing any news about their opponents was among the key factors to disable major dissemination of fake news among voters. The level of democratization, as well as historical tradition of trust in long-established media outlets, determine the dominance of disinformation in individual states.

A light at the end of the tunnel is the fact that in old democracies traditional media outlets are still among the most respected information sources for the general public. Citizens of those states tend to put more trust in content and source validity. Strong media outlet traditions and the people’s affinity to prioritize obtaining information from them reduce the percentage of those who fall for fake news or disinformation. Internet illiteracy is also a very important success factor in the spread of fake news and disinformation, especially with respect to the 3R rule: recognize-react-resolve.

Countries which have invested more in literacy campaigns and fake news recognition face less problems with implementing their policies and processes. This was accompanied by transparency in financing of the media and safeguarding of their independence and freedom. On the other hand, new democracies or developing countries in the NATO wider cooperation area, with shorter histories of media pluralism, showed more vulnerability to fake news penetration. Both external and internal actors consumed social me-
dia, a powerful tool of transmission due to its global dispersion, the balanced approach of countries toward the respect of the freedom of speech, as well as absence of stronger regulations. They turned in particular to younger populations that grew up with modern technology, grasping information on social media and thus becoming more susceptible to manipulation. Young people find it more convenient and trendier to obtain information through such media, usually via unchecked sources, which is then shared with their contacts. Another problem is that the everyday user does not care as much as they used to about information accuracy, due to complex modern insecurities and information landscapes, and tends to believe online experts more than official state institutions.

Platform providers clearly need legal regulations of algorithms for the respect of human rights as well as data protection. Their role should be to promote diversity, giving priority to trustworthy sources. Fact-checking mechanisms seem to have a critical role in this. A very important aspect of the success of fake news outreach is the language in which news was created. The analysis has shown that disinformation created in the local language of a particular country had more effect than if it were written in English, especially in countries whose citizens have little or no knowledge of English. Language style mattered in orchestrated strategies of terrorist organizations in that softer language was used for English speaking users, with an international focus of news presentation, unlike local languages used in different countries, which employed more violent and emotional language for recruitment and support.

Although the NATO is already acting via the twin track model of understanding and engaging, some steps still need to be taken in the future to fight this modern menace. Having in mind that all legal standards on this are without reference to particular values, or geopolitical tastes, and also being aware of the complexity of the information age today, which will not disappear in the future, a strategic approach is vital in the long run. The fight against fake news is a complex process that requires joint activities between state institutions, journalists, NGOs, fact-checking organizations, and citizens in general. Experience has shown that it is a multilateral problem that cannot be solved by states alone. Hence, the Alliance must consider joining the efforts with other international partners like the Council of Europe, United Nations and the European Union. Also, it has to channel its activities through established, specialized units in all of its member countries or information centers in partner countries that will counter fake news and disinformation. Success stories of individual member countries may also be taken into consideration. More efforts will be needed to invest in cooperation and support of developing partner countries since their activities affect NATO member countries directly or indirectly. Steps are required now, without further delay, since damage is already done and it is a matter of time when it will become even more problematic. It is in our interest to safeguard our contemporary democracies so that we can protect our liberal order.
References


Posljedice lažnih vijesti i dezinformacija za sigurnost zemalja članica i partnerskih zemalja NATO-a

Sažetak

Zloupotreba digitalnih platformi za širenje lažnih vijesti i dezinformacija online postaje sve ozbiljnijii problem i za pojedine države i za multilateralne organizacije. Alternativne činjenice predstavljene pod krinkom buđenja kritičkog mišljenja ili lažne i navodne informacije plasirane u društvene medije od strane državnih i nedržavnih aktera za vlastite potrebe, narušavaju vjerodostojnost tradicionalnih medija koji provjeravaju činjenice kako bi javnosti prezentirali stvarne informacije. Shvaćanje parezije kao dijela demokratskog slobodnog izražavanja u liberalnom društvu putem društvenih mreža ozbiljno dovodi u pitanje uobičajene objektivne standardе istine. Namjerno zadiranje u lažne vijesti i dezinformacije u suvremenim demokracijama, posebice tijekom izbornih kampanja, korištenje anti-NATO narativa, osobito u zemljama s bivšim komunističkim režimima, te promicanje lažnog osjećaja sigurnosti ili nesigurnosti, vrlo nedavno, u vezi s pandemijom Covida-19, postaju zabrinjavajuće pitanje za cijeli Savez i njihov terenski rad. Iako je u biti vojna organizacija s ciljem osiguranja mira i sigurnosti na svom širem području i promicanja svojih vrijednosti na globalnoj razini, ono čemu je NATO svjedočio u posljednjem desetljeću jest to da se mir i sigurnost u tradicionalnom smislu ne mogu uzeti zdravo za gotovo. Pojava suvremenih ne-vojnih taktika koje protivnici koriste za destabilizaciju zemalja članica i partnerskih zemalja zahtijeva specifične pristupe i mjere odvracaњa i obrane. Ovaj rad analizira kako te alternativne činjenice utječu na državnu stabilnost, kao i stabilnost čitavog Saveza, moguće implikacije na smanjenje povjerenja javnosti u državne institucije te radnje potrebne za ublažavanje takvih učinaka.

Ključne riječi: lažne vijesti, dezinformacije, državna stabilnost, izbori, pandemija.