Disinformation as a threat to national security on the example of the COVID-19 pandemics

Wojciech Łukasz Sługocki¹, Bogdan Sowa²

¹slugockywoj@gmail.com
²https://orcid.org/0000-0003-0275-8096

¹, ²The Faculty of the Security, Logistics and Management, Military University of Technology, gen. Sylwestra Kaliskiego 2, 00-908, Warszawa 46, Poland

bogdanwaw19@gmail.com
²https://orcid.org/0000-0002-4870-5806

Abstract

Nowadays, the vast majority of the threats to our security is related to information security, resulting in a significant transformation of national security systems. One such threat is disinformation, which is increasingly being used intentionally. The study examines certain impacts of disinformation on national security as a system, on the example of the COVID-19 pandemic. Therefore, the study explores some processes visible at the international level and reviews some external problems in connection with national security. Research methods and techniques implemented in the research process itself are primarily based on a critical analysis of the literature and the analysis and synthesis of published research results. The main findings show that the phenomenon of disinformation, which intensifies in crisis situations (e.g. related to the outbreak of a pandemic) contributes to the destabilization of public mood, hinders the functioning of the basic organs of the state and, consequently, increases the negative effects of crisis events. Secondly, the disinformation used during the COVID-19 pandemic has exacerbated its effects, causing damage on an unprecedented scale. The analyses show that the fight against disinformation must be based on the assumption that the security of the state depends primarily on the information awareness of each citizen. Social awareness is built through effective education aimed at raising basic medical knowledge. Disinformation has serious consequences for modern countries as it creates a new threat to their national security in peacetime.

Keywords:

national security, disinformation, COVID-19
Introduction

Countries have always strived to obtain a military advantage in numbers and quality in order to ensure national security. Aleksandrowicz (2016, p. 107) alleges that the information fight takes place not only in the military sphere. It is also applicable in politics, culture and economy in the form of: information and propaganda campaigns of political parties, extortions, data theft necessary to use the victim’s bank account, activism, hacktivism, physical destruction of telephone exchanges and control rooms. Bezrzenie (2003) also writes about information and psychological wars, he is convinced that the goal of the information war is to achieve information dominance which is aimed at preventing the opponent from using the information space. Rogozin (2011, p. 96) claims that information war is intense confrontation in the information space in order to achieve information, psychological and ideological superiority, damage information systems, processes and resources, critical structures and communications (Information technology, network-centric and cyberwar), undermining the political and social systems, and also massive psychological processing of military personnel and the general public (information-psychological war).

An important element of the information war is disinformation which according to European Commission (2018) is “verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public.” Disinformation has long been used to erode trust in state authorities, to create social unrest and to obstruct state and social goals related to, for example, the problem of migration or a pandemic. Such activities are becoming more and more common due to the fact that they are hard to find out and track, and not easy to attribute to a particular perpetrator. Invisible threats, both man-made and natural, can be used operationally. Such attacks are commonly known as hybrid threats which are defined as “incorporate a full range of modes of warfare, including conventional capabilities, irregular tactics and formations, terrorist acts that include indiscriminate violence and coercion, and criminal disorder” (Hoffman, 2009, p. 36). This concept is derived from earlier concepts of hybrid war, in which the kinetic and lethal components play an important role, and the main role is played by influencing public opinion and cyber-attacks on infrastructure. Importantly, hybrid threats are not only a feature of overt international conflicts, but the term refers to the disappearing differences between peace and war, creating “conflict continuum.”

While disinformation has long been viewed as a problem, it was only the COVID-19 pandemic that showed its serious effects. Since the COVID-19 outbreak, disinformation has been spreading worldwide, as has the virus itself. “We are not just fighting an epidemic; we are fighting the infodemic,” said Dr Ghebreyesus, Director General of the World Health Organization (WHO) at the security conference in Munich in February 2020. As noted by Gjørv (2020), although the pandemic is not an enemy in itself, it is an invisible threat, which can be politically exploited and has recently been used for the purposes of misinformation and disinformation. The WHO (2020a, 2020b) drew attention to the huge coronavirus «infodemic,» which made it difficult for the public to find reliable information and credible guidance. One of the most serious challenges is that the ability to defend against the negative effects of a pandemic largely depends on the mood, attitudes and behaviour of civilian communities, which largely depend on the effectiveness of defending against disinformation. It should be remembered that a possible lack of trust in the information policy of the authorities could make it difficult or impossible to fight the pandemic, which in consequence would violate economic and social security, and thus national security.

The aim of the research was to analyse the impact of disinformation on the effectiveness of counteracting the negative consequences of the coronavirus pandemic by analysing
present research and publications. Following is the main research problem: What challenges in the area of national security result from the experience of the COVID-19 pandemic in the context of the disinformation phenomenon?

**Significance of information security**

In the literature in the field of security studies, information security is classified under the subject criterion next to political, military, economic, social, cultural, environmental, ideological and universal security, but it is derived directly from public security, as a process including activities ensuring protection against prohibited activities. It is most often defined as all activities undertaken in order to ensure the integrity of the collected, stored and processed information resources (Potejko, 2009, p. 194). In modern times, which can be called the “electronic age,” information and the ability to use it are what decides and ultimately determines the success of people, organizations, states and communities in almost all spheres of their functioning (Pisarek, 2007, p. 117). As Kaźmierczak (2017, p. 111) notes, information has always been an important resource, and along with the development of communication technologies enabling its more effective use, it is classified as a strategic resource. The amount of available information is increasing, the number of sources is growing, and their availability is not limited by time or space. The speed of communication and competition on the market make information increasingly superficial and interpreted. In today’s world we experience an overload with a huge amount of information. The inability to control their rush makes it impossible to select them or assess their credibility.

Nowadays, information is becoming one of the key resources influencing the functioning of the economic, social and cultural life of modern nations. Information also has an increasing impact on the national security of states. The development of technology, homogeneous tele information networks (Internet), the universality of access devices, the emergence of social networks, makes information a key factor determining knowledge, power, and, importantly, the security of citizens, organizations and entire countries (Liderman, 2012, p. 12). It should be emphasized that the role of information has changed compared to previous ages. The traditional values of many societies have also gradually changed due to globalization and the spread of modern technology (Górni kiewicz and Szczurek, 2017, p. 472). As these authors note, the pace of information flow has increased, but also its impact on human behavior has increased significantly and the information activities that will be successful are those that can be adapted to the behavioural and thought patterns of the affected people including their emotional reactions and perceptions (Górni kiewicz and Szczurek, 2018, p. 116). Information has become a valuable resource that is an integral part of most of the processes taking place in society (Castells and Cardoso, 2008, pp. 103–104).

In the near future, an increase in the number of information threats related to national security should be expected. As a consequence, in order to ensure security, there will be a necessary pattern of interference by state institutions in the privacy of an individual. This is evidenced in the following words of Szczurek (2019, p. 196):

The technological and information revolution caused by artificial intelligence will change our everyday and professional environment to an unimaginable degree. It is conceivable that people will start living in interconnected houses and will be in contact with each other on a level that is difficult to understand today. Privacy will disappear completely, and the interference of public safety systems in private life will become a generally accepted norm.
Disinformation during COVID-19

In recent researches, the current period is often described as the age of fake news, with misinformation, generated intentionally or unintentionally, spreading rapidly (Wang et al., 2019, pp. 1–12). At present, there is too much incomplete information, misleading information and, most importantly, too much information (infodemia) that is misleading and leads to information chaos. This information chaos is supposed to influence human behavior and result in destabilization. Thus, in the contemporary public space, the information provided can be deformed and distorted, which is defined as disinformation. Disinformation is understood as “the intentionally false meaning, which actors spread and know to be false” (Søe, 2014, pp. 21–30). Disinformation is such a way of providing information - true or false, in order to deliberately mislead a selected group of recipients and persuade them to behave in accordance with the assumed expectations. Disinformation is therefore an intentional deception with the most severe consequences for societies during crisis situations.

Disinformation during a public health crisis is particularly dangerous. At this particular time, accurate, precise and timely transmission of truthful information to society by state administration bodies is essential. Unprepared health communication may result in negative consequences at all levels (individual, social and economic). Nowadays, the communication of authorities may become less persuasive because of major competing factors and, above all, disinformation. There is too much information from non-experts presenting their views on scientific and specialist topics. This can be especially noticed on social media: amid the so-called influencers who talk about the disease, only a few are qualified health informants and try to support or replace institutional communication.

Disinformation is a serious communication danger during the fight against COVID-19. An example is Russia, which is often very active in promoting disinformation about virus epidemics through its RT TV network, often presenting the United States as a source of contamination, including COVID-19 (Broad, 2020). According to BBC investigation, Russia launched a big media campaign in Georgia to slander the US-funded Public Health Research Center Richard Lugar (Lentzos, 2018). As a result of a public opinion poll, the authors and colleague, in a recent working paper, concluded that a large part of respondents in Georgia believe the Lugar Center is being used for, or undecided, research on the US-led biological weapons (Buckley et al., 2020). The cunning of Russian government’s disinformation effort, presented by Russian media in Georgia, is noteworthy as the Lugar Center is the country’s primary testing facility for COVID-19, but is presented as the source of the virus (Cockerell, 2020).

Glasdam and Stjernswärd (2020) argue that the COVID-19 pandemic is seen as an infodemic when huge amounts of true and misleading information are spread quickly through the Internet. The researchers conducted a latent thematic analysis of qualitative data from an international online survey on COVID-19 and social media. The results confirmed that scientific knowledge and political views were viewed with both blind trust and scepticism, journalists’ information was a combination of truth and lies, knowledge of healthcare professionals fluctuated between trusted and guessers, social media was the place for all kinds of information and the need to filter information on COVID-19, while this was extremely difficult as knowledge of COVID-19 was generally considered uncertain. In creating disinformation, state actors use methods, channels and topics as they see fit to achieve their goals. For this reason, while COVID-19 is currently the dominant topic of disinformation, the topic may change at any time at the perpetrator’s discretion. And similarly, channels and methods may have been used.
As stated in study revealed in the Royal Society Open Science, disinformation about COVID-19 is serious threat to public health. In this study, researchers investigated vulnerability to coronavirus-related disinformation and its impact on key health behaviors in large national studies in Ireland (n = 700), the United States (n = 700), Spain (n = 700) and Mexico (n = 700), conducted from mid-April to early May 2020, and two separate UK studies (n = 1050 and 1150; Roozenbeek et al., 2020, pp. 2–4). Participants were recruited through a series of large-scale international COVID-19 surveys. They argue that despite of the fact that public belief in disinformation about COVID-19 is not very common, a large part of respondents view this type of misinformation as highly credible. They also find that increased susceptibility to misinformation reduce people’s willingness to get vaccinated against the virus and to suggest the vaccine to vulnerable people. The results indicate a clear association between vulnerability to misinformation and reduced likelihood of adherence to health recommendations.

The role of the media in disinformation during the COVID-19 pandemic

The role of the media in conveying and interpreting information should not be forgotten either. Along with the development of the mass media and access to information (satellite TV, Internet), the role of the media in the country has also increased. Kabat-Zinn (2020, pp. 1570–1574) shows that the media messages, the context of the events presented, and the variety of narratives are created under the influence of people and organizations with different programs and views. The problem lies in the need of increasingly precise selection and assessment of the reliability of information provided in the media. According to Szcurek et al. (2020, p. 86):

The increase in the importance of information, the development of IT infrastructure and technologies has created a completely new sphere of social activity, and at the same time a platform for competition and possible abuse and crime – cyberspace.

Access to an unlimited number of sources (reliable and unreliable) makes it difficult to fight disinformation. Social media has come to be seen as a common tool for an increasing number of people and enables political, private and professional use, such as a source of information, news, entertainment or networks (Ventola, 2014). With the use of social networking sites on the rise, studying the correlation between social media use and disaster management is becoming important (Domalewska, 2019, pp. 32–43). During the COVID-19 pandemic, societies searched for any information about the virus in panic, trying to improve the level of medical knowledge on their own. The role of social media in healthcare prior to the COVID-19 situation has been controversial. Despite the fact that more and more healthcare professionals and organizations engage on social media platforms continually increasing recently (Wong et al., 2020, pp. 1–3). The panic-stricken search of Internet resources to find a way to deal with panic disorder has led to information chaos. Addressing the urgent need to scale up public health measures to combat the outbreak is not enough, we need to combat the pandemic of social media panic (Atlani-Duault et al., 2020).

The COVID-19 pandemic has highlighted the problem of the need for extensive media coverage and “during the COVID-19 pandemic, social media use has accelerated to the point of becoming a ubiquitous part of modern healthcare systems” (Wong et al., 2020, p. 1). People often used untested data when looking for information about the virus, which heightened the sense of social fear. To meet the expectations and information needs, Facebook has introduced the COVID-19 Multilingual Information Center on its official social network. Google search provides an SOS alert, new information forums,
and an information and resource center on COVID-19. Twitter features information about the coronavirus from news media and authorities (Nielsen et al., 2020). Although social media can be valuable in tracking a pandemic (Li et al., 2020, pp. 110–118), it can also be a source of panic and confusion as it enables the fast travel of information and disinformation (Depoux et al., 2020, pp. 1–2).

It is not entirely known about how people understand, process and sort (real) information and disinformation in general. For that reason, shaping the role of the media in the context of national security becomes one of the key challenges in the near future. The challenge is to simultaneously provide the media with the possibility of unfettered transmission of information in accordance with the principles of freedom of expression, while preventing manipulation phenomena. The contemporary recipient is looking for up-to-date and interesting information (Szczurek, 2009).

Contemporary state administrations must be ready to face the new threats in the information sphere. In addition to the previously described disinformation activities, attempts to penetrate databases or conduct manipulative activities aimed at paralyzing the state security system are also significant challenges. Due to the significant increase in security threats in the information sphere, states should gradually adapt their structures to new challenges, focusing increasingly on the need to protect cyberspace. States should focus their efforts on acquiring new technologies (especially, information technologies), and expanding the information structure, which should ensure a safe flow of data in near real time. The infrastructure that should be created by systems and subsystems for acquiring source information, managing and controlling electronic devices is also important.

COVID-19 in the context within national security

The current unpredictable conditions related to the COVID-19 pandemic have highlighted the importance of civil preparedness, crisis management and maintaining state defence readiness. The North Atlantic Treaty Organization (NATO) should be prepared for many accidents that can have a severe impact on societies, critical infrastructure and, consequently, on national security. COVID-19 affects everyone, including those who are not infected with the virus. The pandemic basically affects all people (not just the sick) because it has a great impact on people’s lives in general (Roy et al., 2020).

The coronavirus pandemic proves that non-military aspects can destabilize, if not paralyze, entire societies and states. It is an important verification of society as a whole, as well as the chance to test the efficiency of the state administration. The pandemic expands our existing perception of major security issues, among others those related to hybrid threats and hybrid warfare. However, we must be able to react proportionally, mitigate damage and adapt their thinking to the context (Gjørv, 2020).

Under Article 3 of NATO’s founding treaty, which deals with the resilience of societies, each member state must be able to resist and recover from a major shock, such as a natural disaster, critical infrastructure failure, hybrid or military attack. Resilience is defined as a society’s ability to respond appropriately and effectively through civil preparedness and military capabilities. As Roepke and Thankey (2019) point out, the principled importance of resilience (Article 3 of the Alliance’s founding treaty) requires that all Allies “maintain and develop their individual and collective capacity to resist armed attack.” This comes down to strengthening the continuity of government and supporting essential services in the member states.
In 2016, at the Warsaw Summit, Alliance leaders committed to strengthening resilience by pursuing the seven baseline civil readiness, such as:

- Guaranteed continuity of government and essential government services
- Resilient energy supply
- The ability to deal effectively with the uncontrolled movement of people
- Resilient food and water resources
- The ability to deal with mass casualties
- Resilient civilian communication systems
- Resilient civil transport systems (Roepke and Thankey, 2019).

Back in 2016, the ability of society’s ability to deal with epidemics and pandemics was not classified as a priority, now, taking into account the events of recent months, this approach should be revised.

The study of the current pandemic is useful in the context of this resilience, as well as the national security of NATO countries for the following two reasons:

- COVID-19, in a short time, threatened the health sector, economy and social cohesion of societies on an unknown scale, generating an emergency response equivalent to military actions.
- The pandemic is increasingly affected by disinformation campaigns, which provides us with real-time data on how societies and their populations might respond in emergencies.

In *The New Yorker*, the words of Michèle Flournoy (the former Undersecretary of Defense for Policy, USA) were quoted:

This President’s failure to manage the Covid-19 pandemic effectively, his failure to reduce the dire economic impacts, and his propensity to inflame rather than heal the deep divisions in this country have all contributed to a perception, among allies and adversaries alike, of an America that is in crisis, if not decline (Wright, 2020, p. 2).

The quoted words prove the great impact of the COVID-19 pandemic on the security of the state. As Hamilton (2020) points out “if we adhere to a minimalist definition of American national interests, COVID-19 has done more to damage them than almost any war America has ever fought. The first two - and most important - interests articulated in the 2017 NSS are protect the American people, homeland and way of life", and “promote American prosperity”. Hamilton (2020, p. 4) reminds that

COVID-19 has also ravaged the US economy like no event since the Great Depression. The pandemic has been responsible for 48 million initial jobless claims in only 15 weeks, and a spike in the unemployment rate from a 50-year low of 3.5% in February to 14.7% in May. Although the jobless rate declined to 11.1% by the end of June, a new surge in infections is causing some states to shut down again, promising further economic dislocation.
It is important to understand that all societies have specific weaknesses and it follows that states should in the first instance be ready to prevent malign influence attacks against elements of state capacity (Buckley et al., 2020). In terms of state capacity, public health is a particularly sensitive target against which cross-platform attacks were launched on various platforms long before the virus pandemic. Dr Tedros Adhanom Ghebreyesus, the Director General of the WHO, described the desired way of response planning that states need to implement “these are plans that start with leadership from the top, coordinating every part of government, not just the health ministry – security, diplomacy, finance, commerce, transport, trade, information and more – the whole government should be involved” (Hamilton, 2020). After two decades of rising defence budgets, the COVID-19 pandemic has made it painfully clear that military spending alone will not ensure America’s national security (Bilmes, 2020, p. 1). As Senator Bernie Sanders (McLaughlin, 2020) observed in March 2020, “this crisis is beginning to teach us that we are only as safe as the least [health] insured person in America.”

It should, therefore, be recognized that all states should take all possible measures to prepare an effective defense against future pandemics, but it is not a simple task due to the threats in the media.

Conclusions

The aim of the research was to analyse the impact of disinformation on the effectiveness of countering the negative effects of the COVID-19 pandemic. Research results (study published in the Royal Society Open Science) show a clear relationship between vulnerability to misinformation and a reduced likelihood of adherence to health recommendations and the willingness to vaccinate (Roozenbeek et al., 2020, pp. 2–4). The effects of disinformation may affect social behavior, which may make it difficult for state administration to counteract the negative effects of crisis situations such as the COVID-19 pandemic. Disinformation during the COVID-19 pandemic has proved that it can paralyze entire societies and states, and exacerbate the negative effects of other threats. This broadened our current understanding of major security scenarios, including those related to hybrid threats and hybrid warfare. The consequences of a long-term pandemic resemble those of armed attacks and pose a real threat to national security. In this case, however, the army and the built-up military potential can protect the security of states to a very limited extent. In this case, the organization and the so-called social resilience, which co-decide on the scale of the pandemic’s effects. COVID-19 has exposed serious problems and gaps in government defense systems, state capabilities, and information policy. Importantly, it demonstrated the need to revise the perception of national security. The coronavirus has shown that equating security with the amount of the accumulated nuclear arsenal is misleading. As it turned out, a pandemic, which is difficult to fight with conventional weapons, may pose a greater threat to humanity.

The analyses carried out have shown that the development of an effective national response to COVID-19 should begin with the implementation of a coordinated pandemic information management plan. The phenomenon of disinformation plays an important role in managing the pandemic crisis. Disinformation is used to polarize views among the civilian population and generate distrust of state actions. The way citizens choose their actions and responses to disinformation says a lot about how effectively governments, partnership with communities, ensure the security of the nation.

NATO’s task is to understand the dangers of a pandemic, learn from COVID-19, and develop responses and work with partners. The experience of the current pandemic clearly shows that dealing with crises requires states to conduct an effective information policy.
and ruthlessly fight any attempts to disinformation. It is not all that societies need to strengthen their resources, such as: development of educational programs, activities of local non-governmental organizations, development of grassroots social initiatives. The aim is to build public confidence in reliable sources of information at all levels. Bottom-up initiatives, supported by the activities of competent local and state authorities, will contribute to strengthening the ability to manage crisis situations.

**Funding**
This research received no external funding.

**Author Contributions**
Conceptualization, W.L.S.; methodology, B.S.; software, W.L.S.; validation, B.S.; formal analysis, W.L.S.; investigation, W.L.S.; resources, W.L.S.; data curation, W.L.S.; writing—original draft preparation, W.L.S.; writing—review and editing, W.L.S.; project administration, B.S. All authors have read and agreed to the published version of the manuscript.

**Data Availability Statement**
Not applicable.

**Disclosure statement**
No potential conflict of interest was reported by the authors.
References


