Prof. dr Zoran Dragišić
Faculty of Security Studies, Belgrade
Email: zoran.dragisic@yahoo.com

dr Milica Ćurčić
Vinča Institute of Nuclear Science, National Institute for the Republic of Serbia

Mirjana Kostić, *PhD Candidate*
Faculty of Security Studies, Belgrade and Military Medical Academy, Belgrade

DOI: 10.37458/ssj.5.2.9
Original Research Paper
Received: May 6
Accepted: June 22

INTELLIGENCE AND PUBLIC HEALTH THREATS

Abstract: *The acquisition, processing, and analysis of data about threats against public health have long been recognized as significant areas of work of intelligence operations aimed at protecting national security. Across modern states, public health has been securitized, with health facilities designated as critical infrastructure vital to national security. The organization of medical intelligence activities, particularly following the COVID-19 pandemic, has attracted the interest of experts representing a wide array of scientific disciplines. This paper attempts to highlight certain challenges inherent in establishing an intelligence community tasked with providing timely and relevant information regarding health threats, while also countering the dissemination of misinformation and alarming reports within the realm of public health.*

Keywords*: public health, intelligence, security threat, infodemic, MEDINT*

Introduction

Interest in MEDINT, as a medical intelligence work, has been present since the existence of war as a structured social conflict. The term MEDINT can be connected to the establishment and functioning of military intelligence services and the development of medical security within armed forces. Extending health intelligence efforts to the civil sector requires a serious

examination of the content of such intelligence work, alongside analysis of the capacity of services and healthcare institutions to collaborate effectively in providing timely and relevant information to political decision-makers. Gathering information concerning the health status of enemy troops, their medical capabilities, the well-being of one's own forces, and medical resources, along with assessing the health security of deployed territories, has been a longstanding practice in warfare. This includes acquiring and analyzing data on infectious diseases, water quality, animal and plant diseases impacting local food sources for troops, climatic conditions, air quality, and other health-related factors crucial to military decision-making. Such activities have historical roots and are documented in ancient writings. The biblical account of Moses sending spies into the land of Canaan to assess various aspects, including the nature of its inhabitants, the strength of their dwellings, and the quality of the land, is frequently cited. However, less often acknowledged is Moses' directive for the spies to investigate the environmental conditions of the land, such as its fertility, and availability of resources like wood and water. This passage from the Bible is often used to highlight the existence of intelligence gathering even in ancient times. Yet, it's noteworthy that one of Moses' primary directives to his spies was to gather information that aligns with what is now considered the domain of medical intelligence work.

Apart from gathering information concerning the health status of adversaries, one's own forces, and health hazards inherent to the operational area, what we call in modern vocabulary "subversive activity of the intelligence services" was also highly developed. In addition to classic subversive activities, such as poisoning wells with drinking water, dropping infected human and animal corpses among enemy troops, or into cities under siege, what we would today address as biological warfare, rumors regarding infectious diseases were often used to undermine the morale of adversaries. The technique of spreading rumors, facilitated by spies who propagated false information within the local population about diseases that had appeared or the contamination of essential resources such as food and water, was highly developed. These rumors caused fear in both civilian populations and military forces, swiftly undermining their resolve to resist. The selection of health-related rumors was not arbitrary. The profound fear of infectious diseases is very intense, especially in times when little was known about them and when they were considered a punishment from God. The majority of these diseases were lethal with no viable means of protection against their deleterious effects. The proliferation of rumors

and conspiracy theories is more pervasive today than ever before in history. This trend is particularly pronounced due to the widespread accessibility of communication tools and channels, which intelligence services exploit extensively for conducting hybrid operations.

Intelligence and public health

In the rapidly evolving modern world, there is a clear imperative to redefine security terminology and to reassess the roles of international, governmental, and other entities (non-governmental organizations and corporations) in addressing medical challenges, risks, and threats. The linkage between public health and safety has been extensively documented in the literature, with authors primarily delineating medical intelligence through the analysis of case studies and reports from international and national agencies tasked with addressing these issues. The Copenhagen School of Security theorists underscored, via the framework of Securitization Theory, that health challenges represent a significant threat to global security (McDonald, 2008).

According to securitization theory, individuals holding social and political power, termed "securitizing actors," assign security significance to specific phenomena through their decisions. Consequently, they authorize and validate the implementation of emergency measures to address a perceived threat directed towards a particular entity, known as a securitized phenomenon. State actors, primarily responsible for taking measures to protect public health and monitoring its hazards, readily acknowledged that issues pertaining to human, animal, and plant health occupy a prominent position on their political and security agendas. The concept of human security, formulated within the United Nations framework since 1994, garners significant support, notably from Japan and Canada. Its advocacy intensified, especially following the September 11, 2001 terrorist attacks. Human security represents a comprehensive approach capable of addressing diverse security challenges, risks, and threats, offering potential solutions for asymmetric security threats (Dragišić, 2020:31). Today, in addition to all the disputes between different security concepts, there is no doubt that health threats are accepted as existential threats for the entire world population, which directly threaten geopolitical stability and national security. In most modern national security strategies, epidemics and pandemics of infectious diseases are defined as a threat to national, regional, and global security (National Security Strategy of the Republic of Serbia, 2019). All national and international strategic documents adopted after 2019

mark epidemics of infectious diseases as a primary threat to national and global security. The identification of the most severe types of infectious diseases typically draws upon classifications provided by the World Health Organization (WHO).

However, health threats are generally not treated as a global phenomenon, although it is quite clear that today epidemics cannot be contained within the borders of one country, or even one continent, due to the very intense movement of people on a global level. Health threats are generally treated as a threat to the affected community, mostly at the state or federal level. Undoubtedly, the approach was significantly influenced by the experiences stemming from the COVID-19 pandemic. Throughout its course, the world witnessed not only a deficiency in global solidarity but also observed the pandemic exacerbating pre-existing geopolitical tensions and fostering heightened mistrust between China and the United States, along with their Western allies.

The behavior of the Chinese authorities at the very beginning of the pandemic, and later throughout its entire duration, aroused the suspicion of Western countries that China deliberately caused the pandemic, or that it at least did not react adequately at its beginning, by withholding timely information regarding the events in Wuhan. The pandemic has once again opened discussions surrounding the role of intelligence activities in managing health risks. It is evident that China was unwilling to share pertinent information regarding the Wuhan events. The death of Doctor Li Wenliang, the first to publicly caution about the new virus and subsequently encountering challenges with Chinese security services, further fueled suspicions of deliberate infection propagation. The WHO lacked adequate intelligence resources to ascertain the situation in Wuhan, and none of the countries could obtain timely and reliable information about the novel virus through their intelligence channels in China (Gordon and Moy, 2021). All these circumstances have prompted a necessity to reconsider and redefine the issue of health security at the global level, which has been set as one of the main Sustainable Development Goals.

When delineating the Sustainable Development Goals (SDGs), goal number eighteen encompasses global health security. Goal 18 is defined as such: „*Take appropriate action to reduce the vulnerability of people around the world to new, acute, or rapidly spreading risks to health, particularly those threatening to cross international borders*" (Kickbusch et al, 2015:1069). According to Kaufman, "Policymakers have recognized the destabilizing threat that infectious disease and health system failures have on peace and global stability (Kaufman, 2001).

The COVID-19 pandemic has fully confirmed all the catastrophic predictions. A huge number of deaths around the world, serious geopolitical disturbances, the closure of the world economy which led to a huge drop in GDP at the world level, the complete collapse of the health systems of many countries, major problems faced by almost all economic branches, the loss of trust of the population in their governments, are just some of the most visible consequences that the pandemic has inflicted on global society.

The inquiry into the origins and dissemination of the epidemic originating from the Chinese city of Wuhan has prompted speculation regarding whether the pandemic was intentionally triggered and to what end. Social media platforms and traditional media outlets have engaged in a veritable battle against misinformation, amplifying the global reach of the anti-vaccination movement and spawning a plethora of conspiracy theories. This proliferation of falsehoods has led to the emergence of what is termed an "Infodemic," representing a novel challenge concerning health risks. Exploiting social networks for the dissemination of disinformation aimed at instilling fear and sowing discord among populations has become markedly easier than ever before, facilitating the conduct of hybrid warfare tactics.

Intelligence failures during the COVID-19 pandemic

The COVID-19 pandemic has unequivocally demonstrated that intelligence operations concerned with the collection, processing, and dissemination of information regarding infectious disease epidemics are significantly more complex compared to other aspects of national security intelligence. Numerous authors have addressed intelligence failures associated with the COVID-19 pandemic. Some have posited that these failures originated within the classic intelligence cycle, which, as per the American doctrine (endorsed by all NATO members and partner states), comprises five stages. The intelligence cycle encompasses planning, information gathering, information processing, intelligence product creation, and delivery of intelligence products to decision-makers. This cycle serves as a fundamental framework for all intelligence operations, irrespective of their specific focus or type (Lowenthal, 2015). Therefore, the intelligence cycle is useful for examining the steps in the detection, warning, and response to public health emergencies. There is direct application to detection and response to epidemics and pandemics with each step having applicability. Planning and direction manage the process for the entire

cycle from determining needs for medical intelligence to delivery of a product to consumers (Richelson, 2012). The authors previously emphasized that the traditional methods of intelligence work, embodied in the classic intelligence cycle, are also applicable to threats to public health. They argued that these methods can be leveraged to detect infectious disease pandemics promptly, thereby enabling competent health authorities, in collaboration with government agencies, non-governmental organizations, and the private sector, to react promptly. This proactive approach aims to prevent threats to public health and mitigate their consequences effectively.

However, what we could learn from the COVID-19 pandemic is that there is a serious difference in classic intelligence work when the subject is a different type of information related to national security and information related to public health. Classic intelligence products typically do not include recommendations for political decision-making, as this responsibility falls within the purview of governments or other competent authorities in democratic states. However, concerning information pertinent to public health, health organizations also generate intelligence products and provide recommendations as expert bodies to inform political decisions essential for combating infectious diseases. Such guidance is disseminated by various health organizations, ranging from international entities like the WHO to national and local health authorities tasked with implementing medical and paramedical measures within their respective jurisdictions. The role of citizens differs significantly concerning health threats compared to other intelligence information. Unlike traditional intelligence, citizens are both consumers and decision-makers regarding intelligence related to public health. Unfortunately, during the COVID-19 pandemic, instances emerged where citizens frequently made decisions conflicting with recommendations from health authorities, particularly concerning immunization.

Intelligence failures have followed intelligence services since they existed. Many major historical mistakes made by states stem from intelligence failures, which were not necessarily the result of intelligence service errors. Intelligence failures range from untimely detection of a threat to a misunderstanding of the true nature of the threat by political decision-makers, which leads to decisions that are contrary to national interests (Gentry, 2008). According to ABC News, the first information about the spread of the new virus in the region of the city of Wuhan in China was submitted to the DEA before the end of November 2019. The American service obtained the information by hacking computers and using satellite images. The DEA report

indicated that the half-week spread of the virus could be catastrophic, but the Pentagon denied the existence of such a report. Israeli media reported that the US authorities warned NATO and the Israeli armed forces about the spread of the virus from Wuhan back in November 2019 (Margolin and Meek, 2020). On January 5, 2020, the WHO announced the outbreak of an epidemic in Wuhan, citing the number of infected people, only to announce on January 30 a warning about the highest level of public health concern at the global level (Gordon and Moy, 2021).

As Gordon and Moy stated, the United States' experience with COVID-19 offers a valuable case study in integrating intelligence and public health information, providing insights for future endeavors in detecting, alerting, and responding to epidemics, Public Health Emergencies of International Concern (PHEIC), and pandemics. While other countries worldwide likely have equally important lessons to offer, the United States stands out for its transparency regarding intelligence activities, facilitated through official channels, media leaks, and disclosures such as those under the Freedom of Information Act (FOIA). In 2014, the Office of the Director of National Intelligence (ODNI) initiated its Open Government Plan, aiming to foster collaboration within the U.S. federal government and enhance the transparency of the Intelligence Community with the public (Gordon and Moy, 2021).

After the end of the COVID-19 pandemic, almost all states analyzed the failures that occurred during the pandemic. Intelligence lapses appear critical in every analysis, from the case of the disaster that struck Italy in March 2020, which was a direct consequence of ignoring warnings coming from around the world. Disregarding intelligence reports by the Government of Italy resulted in detrimental and poorly timed decisions, leading to a significant number of casualties and the systemic collapse of the healthcare infrastructure (Pisano et al., 2020).

Most authors cite the inability of governments to collect, analyze, and share data related to the pandemic in a timely manner as a major problem during the COVID-19 pandemic. In addition, other intelligence failures related to untimely warnings were observed, which led to a delay in raising the alert to the highest level. A critical issue identified is the inadequate assessment of vulnerability, resulting in the neglect of measures to enhance resilience, particularly in health capacities, which have witnessed widespread collapse across numerous countries.

The global war on information and misinformation is the most important non-health consequence of the COVID-19 pandemic. This conflict in information warfare originated at the

highest echelons of the world's most influential nations. US President Donald Trump accused China of intentionally creating and disseminating the virus as a form of biological warfare, prompting a rebuttal from the Chinese foreign minister, who asserted that the virus originated in US laboratories and was brought to Wuhan by US soldiers. Additionally, Russian authorities questioned the efficacy of vaccines developed by the American pharmaceutical industry.

The politicization of the pandemic and its utilization for geopolitical confrontation among major powers exacerbated the challenge of understanding the pandemic, its implications, and effective strategies for mitigation. This situation had catastrophic consequences for public health. Masses of information, much of it inaccurate, flooded social media and traditional media channels, exacerbating confusion among the populace and leading to numerous detrimental decisions, ranging from vaccine hesitancy to neglecting preventive measures. Subversive activities, a core function of intelligence services, became prominently manifest during the COVID-19 pandemic. Russian and Chinese intelligence services leveraged the crisis to propagate their narratives, aiming to erode trust in the governments of free nations, challenge Western values centered on human freedoms and rights, and undermine confidence in science and technological progress. Collectively, these efforts sought to diminish the inherent advantages of free societies vis-à-vis autocratic regimes.

In June 2020, the WHO organized the first scientific conference that dealt with the spread of information and misinformation related to the pandemic. On that occasion, the term "infoedema", which was used by Eysenbach in 2002, was launched (Eysenbach, 2002). Eysenbach's basic idea was to explore the gap between what the best knowledge of medical professionals is and what people believe or do about their health.

The term Infodemic

WHO, on its website, explains the term "infodemic", which was used as early as 2002, but the COVID-19 pandemic again put the term at the center of interest of the world public. In addition to (re)defining the term itself, WHO provides recommendations on how to deal with the infodemic. “An infodemic is too much information including false or misleading information in digital and physical environments during a disease outbreak. It causes confusion and risk-taking behaviors that can harm health. It also leads to mistrust in health authorities

and undermines the public health response. An infodemic can intensify or lengthen outbreaks when people are unsure about what they need to do to protect their health and the health of people around them. With growing digitization – an expansion of social media and internet use – information can spread more rapidly. This can help to more quickly fill information voids but can also amplify harmful messages. Infodemic management is the systematic use of risk- and evidence-based analysis and approaches to manage the infodemic and reduce its impact on health behaviors during health emergencies. Infodemic management aims to enable good health practices through 4 types of activities: 1) listening to community concerns and questions; 2) promoting understanding of risk and health expert advice; 3) building resilience to misinformation and 4) engaging and empowering communities to take positive action" (WHO- Health Topics). As evident, the WHO offers four fundamental recommendations to counter the infodemic, primarily directed towards empowering the populace to resist misinformation. This empowerment is crucial in preventing erroneous behaviors that jeopardize public health and undermine the effectiveness of measures implemented by health authorities.

The creator of the term "infodemic" Gunther Eysenbach in his newest article from 2020 specifically addressed the sources of misinformation about health and how we can combat it. Eysenbach emphasizes the very important fact that in the modern world, which is changing very quickly, it is extremely difficult to establish what is true. During the pandemic, even the biggest health authorities did not have information that was completely scientifically verified so that it could be taken unreservedly as correct. Many clinical studies that were conducted during the pandemic could not be taken as "facts", but at best as BETs (Best evidence at the time). The world was then faced with a new strain of the virus for which an effective vaccine, treatment protocols and adequate recommendations to the population for daily behavior had to be found. During this period, it was reaffirmed that science is an ongoing dialogue that flows continuously, which can be an inspiring and exciting experience of science when millions of lives around the planet would not depend on the speed and quality of research. In the same article, Eysenbach gives the "Cake model", which he describes as follows: the current infodemic is a crisis to distill the sheer quantity of information, which is occurring on four levels: (1) science, (2) policy and practice, (3) news media, and (4) social media (Eysenbah, 2020).

Eysenbach presented the "wedding cake" model to illustrate four hierarchical levels as layers, with each layer corresponding to the amount of information generated by different groups

of actors. The size of these layers reflects the volume of information produced. Science occupies the smallest layer at the top of the information cake, symbolizing its rigorous and discerning approach to information production. While misinformation may also exist within this layer, quantifiable by the number of retractions—currently fewer than two dozen as of June 2020—it represents a fraction of the vast body of COVID-19 research. With over 26,000 articles indexed in Pubmed, retractions account for less than 0.1% of published research. However, there may be a higher prevalence of misinformation within unreviewed preprints, some of which may never undergo journal publication. This underscores the importance of studying this phenomenon and submitting findings to scholarly journals. The primary challenge lies not in the prevalence of misinformation within the scientific layer but in effectively translating this information into actionable recommendations and communicating conclusions to diverse audiences and stakeholders across other layers, as depicted by the arrows of knowledge translation. Social media is portrayed as the largest and final segment of the wedding cake, symbolizing the immense volume of largely unfiltered and unregulated information generated or amplified by the public. Notably, information on social media is also disseminated by science organizations, policymakers, healthcare entities, and journalists (Eysenbah, 2020).

However, what was noticeable during the COVID-19 pandemic was the inability of governments to take measures to protect the population from the hybrid actions of other states or organizations. We must take the fact that the modern world is deeply divided and that, especially after the beginning of the Russian aggression against Ukraine, pandemics and other general calamities, whether deliberately caused or spontaneous, represent a training ground for conflict. Numerous scientific articles and publications published during or after the pandemic have addressed this subject extensively. A wealth of literature now exists on governments' responses to the pandemic, analyses of traditional media coverage, and narratives propagated on social networks in connection with the pandemic. However, what remains largely absent is a comprehensive understanding of the sources—the "producers" of fake news—and the underlying motivations driving the dissemination of such misinformation when it extends into physical spaces.

UN and WHO, as global organizations, certainly have a huge role in the fight against infodemic and defining infodemic management, as a framework that can be a good guide for governments and health authorities, on how to fight against false health information. Global

infodemic management is also a good tool for cooperation between governments and health authorities of countries that fight the infodemic together in good faith. The geopolitical picture of the modern world clearly shows us that many governments, or other political entities, use the infodemic as a means to achieve their military, political and economic goals, at the expense of their opponents.

We contend that the infodemic should be perceived as a component of hybrid warfare. Even post-COVID-19 pandemic, we observe the proliferation of false narratives concerning public health, exemplified by instances such as the alleged existence of NATO laboratories for biological weapons production in Ukraine, disseminated by Russian intelligence services, and the propagation of anti-vaccination sentiments and conspiracy theories involving the "pharmaceutical mafia." These occurrences underscore the imperative for national governments and defense coalitions like NATO and the EU to develop capabilities to effectively counter such challenges.

Narratives pertaining to health challenges have notably broadened the so-called "Overton Window." The Overton Window, a concept named after Joseph P. Overton, Vice President of the Mackinac Center for Public Policy, serves as a technique to validate any idea, introduce it into public consciousness, and render it a topic of public discourse. It delineates the spectrum of ideas that a society deems acceptable and thus appropriate for public debate (Fernandes et al, 2023). Today, subjects that were once deemed unimaginable are now being openly discussed in public forums. Until recently, engaging in public debates regarding the safety of vaccines—an achievement considered among the greatest in human history—was unthinkable. Presently, challenging scientific consensus and authority has become a widely accepted practice, fueled by the desire for increased viewership, circulation, and social media engagement. This phenomenon is particularly perilous, as individuals with formal medical education, including those holding scientific titles, propagate falsehoods concerning medical challenges. Such actions further confound the general public and hinder the efforts of health authorities in managing epidemiological crises.

It is imperative for the authorities of each country to address these challenges as they pose a significant threat to public health, a cornerstone of most contemporary security strategies. The state must establish a pre-planned organizational structure and legal framework to effectively combat the infodemic. Furthermore, it is essential to redefine certain old terms, such

as MEDINT, and precisely delineate the scope of the issue, its stakeholders, and allocate responsibilities between the state and other entities in countering the infodemic, as well as other forms of health information manipulation aimed at jeopardizing the interests of the state and its citizens.

National Health Intelligence System

Despite the predominantly global nature of public health threats, such as infectious disease pandemics, significant ecological disasters, and large-scale natural calamities, it is unrealistic to anticipate a unified response from all members of the international community. The COVID-19 pandemic clearly illustrated that, notwithstanding extensive cooperation among partner nations, each country had to contend with its unique challenges, and its success depended on the extent to which it raised its own resilience.

In the extensive literature that was published during the pandemic and after its end, failures in the field of intelligence were discussed, as well as failures concerning the organization of the health system. The vast majority of authors who have examined organizational failures within the healthcare system have focused on the systems within their respective countries. A very small number of papers are dedicated to the joint response of international organizations, which clearly shows that the scientific (as well as the political) community still perceives nation-states as the basic subjects of the international community and international security.

Citizens see their countries as the main providers of security and rightly expect their governments to take care of their security, including timely information about health hazards and taking measures to eliminate such hazards and mitigate their consequences. The response system to health threats is part of the national security system, which is the only original security system, while international and private securities are derivatives of the national security system (Dragišić, 2020).

When discussing the gathering of intelligence concerning health threats, the term MEDINT frequently arises in the literature, denoting the intelligence capability of armed forces to collect medical data pertinent to troop protection. Contemporary definitions of MEDINT within the Armed Forces of the USA and NATO primarily emphasize its military dimension, without necessitating an in-depth exploration of these definitions. In Serbia, the intelligence

security apparatus of the Serbian Army does not formally recognize MEDINT as a branch of intelligence work in the medical field, nor does the Serbian Military Intelligence Agency acknowledge MEDINT as an intelligence discipline. However, this does not imply the absence of medical security within the Serbian Army. The Institute of Epidemiology of the Military Medical Academy serves as the cornerstone of this system, particularly concerning the deployment of Serbian Armed Forces members to international missions (Mavrak and Živković, 2017).

The Serbian Armed Forces personnel engaged in multinational operations rely on medical intelligence efforts conducted by partner armed forces, as well as those from the UN or EU, whose medical units are responsible for this aspect of mission intelligence security. The Directorate for Military Health, supported by the Military Medical Academy and its institutes and reference laboratories, oversees the health preparations of Serbian Armed Forces members deployed on international missions. This responsibility encompasses pre-deployment and post-deployment medical examinations, as well as providing guidance on disease prevention in mission areas. In their work, Živković and Mavrak propose the establishment of medical intelligence structures within the Serbian Armed Forces or Ministry of Defense, primarily focusing on intelligence security for Serbian Armed Forces operations and fostering interoperability with NATO.

The MEDINT topic was dealt with by Serbian authors Kokoškov and Ristanović who believe that the modern term MEDINT is reduced to three applied forms: military MEDINT falls under the purview of the military intelligence and military security sector within the Ministry of Defense. Civilian MEDINT operates as a component of public and state security, encompassing civilian intelligence-security sectors. Commercial MEDINT represents an independent market activity conducted by legal entities outside the defense and security sector (Kokoškov and Ristanović, 2019:91). Kokoškov and Ristasnović emphasize that MEDINT is a term taken from the military dictionary and that it was developed as a special intelligence discipline within the armed forces and military alliances. We believe that the term MEDINT, which NATO and all its leading members, as well as the EU countries (the vast majority of which are in NATO and apply the same standards), still consider exclusively a military activity, should not be expanded beyond the activities of military intelligence services.

The necessity to broaden intelligence efforts related to health challenges by involving and enhancing coordination among competent civilian structures is undeniable, as evidenced by experiences from the COVID-19 pandemic. However, we argue against using the term MEDINT for intelligence activities conducted by civil authorities in response to health threats. Employing this term outside of military contexts may lead to confusion and undermine interoperability capabilities. Harmonizing terminology and operational practices is crucial for achieving interoperability among security forces. The Serbian Army and other security forces participate in multinational operations under UN and EU mandates, where intelligence preparation of operations, including MEDINT, is vital for mission success and force protection. Past experiences from multinational operations demonstrate the Serbian Armed Forces' strong capacity for cooperation with partner armies, highlighting the imperative to enhance and evolve existing practices in line with evolving needs.

Health challenges represent an existential threat to citizens, national security and geopolitical stability. In its strategic documents, the Republic of Serbia recognizes health threats, which creates a normative prerequisite for the additional development of intelligence work in the domain of health threats. Serbia has serious capacities for health intelligence, which, in addition to security and intelligence, also includes the health system, public administration bodies, the academic community and other organizations dealing with public health. Kokoškov and Ristanović propose the term "integrative MEDINT", which should encompass the intelligence activities of all relevant bodies and organizations that have the capacity to collect information of importance for the protection of public health. In addition to the unquestionable imperative of integrating all capacities at the state level to safeguard citizens and the state from health threats, we maintain the right to utilize the term MEDINT beyond military contexts, as previously articulated.

The response to health threats involves three phases: gathering relevant information about the existence of the threat, fighting against the manifested threat and eliminating the consequences of the threat. Intelligence work refers predominantly to the first phase of the fight against health threats, but it continues in other phases as well, because without having timely relevant information available at all times, the fight against health threats cannot be successful.

The primary national security intelligence service in Serbia is the Security Information Agency, operating as an independent agency responsible for gathering data and information regarding

threats to the national security of the Republic of Serbia. Alongside the Military security agency and the Military intelligence agency, which fall under the purview of the Ministry of Defense, it constitutes the security-intelligence system. The National Security Council serves as the principal entity overseeing this system and holds ultimate responsibility for its operation. Additionally, the Council for National Security houses a Bureau for Coordination of Security Services, tasked with coordinating the functioning of the entire security system.

Each of the three services should gather information regarding threats to public health, including identifying the sources of these health threats. Enhancing the capacity of intelligence and security services to detect and prevent health threats can be achieved through two approaches: establishing specialized organizational units within the services staffed with trained professionals dedicated to monitoring such threats, or strengthening coordination with competent health institutions through institutional connections with clearly defined responsibilities and tasks. We believe that the first option is challenging to implement due to its potential costliness and inefficiency. Creating "hybrid experts" who possess expertise in both health and security, even if feasible, may not serve a practical purpose. By systematically integrating security and health services, we could establish adequate intelligence capabilities to promptly alert the National Security Council to the presence of a health security threat. Subsequently, the Council, in accordance with its legal mandate, would take necessary actions to address the threat. The Institute for Public Health of Serbia "Batut," responsible for epidemiological surveillance across the Republic of Serbia, is the primary institution through which the health-related aspect of intelligence work can be conducted. Through this institution, the entire health infrastructure could be mobilized to gather information about a health threat if needed.

Threats to public health can manifest either spontaneously or intentionally. In cases of spontaneous outbreaks, such as epidemics, pandemics, environmental accidents, or other incidents with potential health ramifications for a large population, monitoring rather than intelligence work is typically employed. For global or regional health threats originating spontaneously, information is gathered through entities like the WHO or regional health organizations, facilitated by international collaboration. Should it become necessary to implement paramedical anti-epidemic measures, such as movement restrictions, quarantine enforcement, supervision of protective measures compliance, etc., these responsibilities primarily fall within the purview of police and inspection authorities.

When addressing intentionally caused health threats, such as the deliberate dissemination of infectious diseases, bioterrorism, eco-terrorism, mass poisoning, and other acts posing a mass risk to public health, the perpetrators of such threats are subject to scrutiny by security services. Information crucial for preventing actions by those posing health threats (whether state actors, terrorist organizations, or organized criminal groups) is gathered through the methods employed by security services, utilizing the intelligence cycle. During the processing stage of identifying the threat's perpetrators, security services require expert medical information concerning the methods and means employed by these threat bearers to endanger public health. Such information must also be presented to the prosecutor's office, which approves the implementation of special measures. It is essential for health professionals to undergo security training to maintain operational secrecy, comprehend fundamental security protocols, and facilitate successful collaboration with security and intelligence experts.

A particular concern regarding health threats is the Infodemic, as previously addressed in this paper. The dissemination of false and alarming information pertaining to public health represents a considerable security challenge. The propagation of misinformation can be construed as a component of hybrid warfare, aimed at fomenting unrest among citizens, eroding trust in the state and its authorities, inciting political and economic instability, and fostering panic.

In combating the agents of the Infodemic, security services, prosecutors, and law enforcement agencies assume pivotal roles. Addressing and managing the repercussions of the Infodemic falls within the purview of health authorities, the academic community—including reputable medical, veterinary, pharmaceutical, and other experts—and, above all, the media.

The infodemic should be seen as part of the hybrid war, and measures prescribed by law should be taken against the sources of fake news that are aimed at citizens. In this realm of intelligence work within the health sector, effective coordination between security services and competent health institutions is paramount. Security services should identify the originators of fake news and alarming narratives, along with the communication channels utilized to disseminate such information. Through analysis of the messages crafted and propagated by threat actors, their underlying objectives can be unveiled, enabling the formulation of a communication strategy. This strategy, aided by expert input, aims to furnish citizens with accurate information

and, to the greatest extent feasible, counteract the adverse effects already engendered by fake news.

Conclusion

The practice of gathering information about health threats, whether spontaneous or intentionally induced, dates back to the earliest forms of organized human society. Throughout history, endangering adversaries' health through deliberate means, such as spreading epidemics or contaminating water and food supplies, has been employed in conflicts. With advancements in science, the capacity for conducting biological warfare, biological terrorism, ecological terrorism, and other deliberate acts to jeopardize public health has been significantly enhanced.

In tandem with the evolution of capabilities to pose threats to the public health of adversaries, efforts to develop capacities to respond to such threats are also underway. Similar to addressing other threats to national security, the development of intelligence capabilities to promptly detect the threat, identify its carriers, and uncover their strategies for endangering public health constitutes the initial phase in establishing the capacity to effectively respond to a health threat.

Since ancient times, armies have been developing the ability to detect health risks for their members in a timely manner. The collection of all relevant information on the existence of infectious diseases among humans and animals, the existence of plant diseases, the quality of drinking water, food, air, climatic conditions, etc., in the territories where military campaigns are planned, was an established practice based on which military commanders made decisions. Today, a special intelligence discipline, MEDINT, has been developed within the military intelligence and security services, which is used to collect process and analyze all health information related to endangering troops on the ground during military operations. In addition, MEDINT deals with the collection of information about the health capacities of the opponent, the state of health of its troops, and the intentions and abilities to threaten the health of troops in the field. We advocate for restricting the usage of the term MEDINT within its existing definition. However, we emphasize its importance in the advancement of national capabilities for intelligence work within the medical domain. The security intelligence system in coordination with the relevant health organizations is the backbone of the national health intelligence system. When it comes to health threats, we believe that it is not necessary to develop new organizations

that would deal with the collection and processing of this type of data, since there are already developed security and intelligence services, as well as reference health institutions that deal with epidemic monitoring. It is necessary to coordinate health institutions and security services in a systematic way, which would be quite enough to collect data on health threats in a timely manner. The proliferation of false and alarming information regarding health threats, often referred to as the infodemic, poses a significant challenge. Developing the capacity of security services to safeguard the state and its citizens from hybrid actions involving the dissemination of false health-related news requires coordinated efforts with health institutions. While security services can identify the perpetrators of such hybrid actions, combating negative narratives effectively necessitates collaboration with health experts.

Acknowledgments

This work was supported by the Ministry of Science, Technological Development and Innovation of the Republic of Serbia, as part of the funding of the scientific research work of the University of Belgrade, "Vinča" Institute of Nuclear Sciences (Grant number. 451-03-66/2024-03/ 200017, 05.02.2024.)

References

Gardon, K., Moy, W.R (2021). COVID-19 Response - Lessons from Secret Intelligence Failures. *The International Journal of Intelligence, Security, and Public Affairs*, 23 (3), 161-179. DOI: 10.1080/23800992.2021.1956776.

Gentry, J.A. (2008). Intelligence Failure Reframed. *Political Science Quarterly*, 123 (2) 247–270.

Dragišić, Z. (2020). *Sistem nacionalne bezbednosti Srbije*. Beograd: Fakultet bezbednosti.

Eysenbach, G. (2002). Infodemiology: the epidemiology of (mis)information. *The American Journal of Medicine.* 113(9), 763-765.

Eysenbah, G. (2020). How to Fight an Infodemic: The Four Pillars of Infodemic Management. *Journal of Medical Internet Research*, 22 (6). DOI: 10.2196/21820.

Kaufman, D. (2001). Medical Intelligence: A Theatre Engagement Tool. Strategy Research Project, USA: Defense Intelligence Agency.

Kickbusch I, Orbinski J, Winkler T, Schnabel A. (2015). We need a sustainable development goal 18 on global health security. Lancet. Vol. 385 (9973), 1069. DOI: 10.1016/S0140-6736(15)60593-1.

Kokoškov N., Ristanović E. (2019) Medicinski obaveštajni rad, njegove perspektive i značaj u bezbednosnom sistemu Republike Srbije, *Bezbednost*, 1, 89-109.

Lowenthal, M. (2015). *Intelligence: From Secrets to Policy*, 6th Edition. California: Sage Publications, Inc.

Margolin, J., Meek J, G. (2020). Intelligence report warned of coronavirus crisis as early as November: Sources. *ABC News*. Interent: https://abcnews.go.com /Politics/intelligence-report-warned-coronavirus-crisis-early-november-sources/story?id= 70031273. Access date: 02/04/2024.

Mavrak, D., Živković, D. (2017). Model obaveštajnog rada u oblasti medicine u podršci multinacionalnim operacijama Vojske Srbije. *Vojno delo* 69 (1). 279-297.

McDonald, M. (2008). Securitization and the Construction of Security. *European Journal of International Relations*, 14(4), 563–587. DOI:10.1177/1354066108097553.

Molina-Fernández AJ, Robert-Segarra A, Martín-Herrero JA, Sánchez-Iglesias I, Saiz-Galdós J, Fernández-Mora K. (2023). Regulating Gambling Use through the Overton Window: From an

Addictive Behavior to a Social and Epidemiological Problem. *Int J Environ Res Public Health*. 20(8):5481. DOI: 10.3390/ijerph20085481.

National Security Strategy of the Republic of Serbia, "Official Gazette of the RS" No. 94 of December 27, 2019.

Pisano, G. P., Sadun, R., and Zanini, M. (2020). Lessons from Italy's Response to Coronavirus. *Harvard Business Review*. Internet: https://hbr.org/2020/03/lessons-from-italys-response-to-coronavirus. Access date: 3/4/2024.

Richelson, J. (2012). *The US Intelligence Community*. 6th Edition. Colorado: Westview Press.

WHO - Health Topics: Infodemic. Internet: https://www.who.int/health-topics infodemic #tab=tab_1. Access date: 21/3/2024