The COVID-19 pandemic brought with it not only the risk of infection with a new virus but also the possibility of attacks on national security by affecting national critical infrastructure. Maintaining a greater focus on national security is a necessity in any situation. During this pandemic period, the most affected critical infrastructure sector is health. We hope that the measures taken will lead us to a stabilisation of the situation and not to witness a more pronounced affectation of this sector. We must also pay special attention to the trust in the public administration in order not to be undermined by state or non-state actors with various economic and geostrategic interests on the Romanian territory.

Keywords: risk; pandemic; national security; COVID-19, China;
INTRODUCTION

The end of 2019 brought with it concerns (COVID-19 pandemic) from China, a country where a new type of virus was identified that was spreading quite quickly among the population. It was initially thought that the virus could be controlled to spread to a limited geographical area, but this could not be achieved because the mobility of citizens has increased substantially, with international events facilitating the spread of the new virus.

More and more countries have started to report the existence of the new virus on their territory. The first major shock was felt by the massive spread in Italy (The worst day for Italy), where the sanitary system barely handled the wave of hospitalisations.

The subsequent evolution of infections in various states of the world, led the World Health Organisation (WHO) to declare, on 11.03.2020, that “the coronavirus epidemic is officially a pandemic” (Radio Free Europe, 11 March 2020). “The COVID-19 viral disease that has ravaged at least 114 countries and has killed more than 4,000 people is now officially a pandemic” the World Health Organisation said on Wednesday. “This is the first pandemic caused by coronavirus”, said WHO Director-General Tedros Adhanom Ghebreyesus. Thus, the official name for the new coronavirus is SARS-CoV-2 (severe acute respiratory syndrome coronavirus 2), and the name for the disease it causes is COVID-19 (Ibid.).

ESTIMATION AND MATERIALISATION OF THE RISK OF MASS INFECTION WITH A VIRUS

Once with the official declaration as a pandemic of the epidemic caused by the infection with a new type of coronavirus, now recognised by the official name of SARS-CoV-2, from the perspective of risk management we are dealing with the manifestation of a potential risk identified by specialists in various official documents. From this point we are not dealing with an identified potential risk, but with a manifested risk that has become a real problem that needs to be managed.

Strong states with a well-developed risk management that had long planned, in official documents, measures to be taken if there is a risk of mass infection, were taken by surprise and probably based on a well-developed public health system they assumed a higher risk, not taking such harsh and early measures.
as in the states where the health system is not performing, in this case, we will refer to that of Romania.

In the analysis made for this article we will refer to the UK and the USA.

We started from the analysis of the risk of infection with a virus or other type of pathogen and the measures established for this type of risk included in the national security strategies of the two states.

In the US National Security Strategy of December 2017, at p. 9, we find the potential risk of biological threats and pandemics, as well as the measures proposed to respond to these potential risks.

The measures proposed in the strategy are:

- **detecting and maintaining biological and pandemic threats at their source** by collaborating with other countries to identify outbreaks in a timely manner to prevent the spread of the disease, encouraging other states to invest in health systems to strengthen global health security, ensuring that laboratories in which dangerous pathogens are investigated will benefit from safety and security measures;

- **supporting innovation in biomedicine** by strengthening the intellectual property system in the biomedical industry;

- **improving the emergency response** by implementing measures to limit the spread of disease and providing emergency medical care (Ibid.).

In the National Security and Strategic Defense Strategy of 2015 of the UK, objective no. 1 is the **Protection of our people** and in Annex A is presented a summary of the National Security risk assessment for the next five years, by 2020.

Among the identified risks we find in Public Health, p.86 of the strategy: risks of diseases, especially pandemic influenza, emerging infectious diseases and increased antimicrobial resistance. These are considered threats to life, public health, services and the economy. The United Kingdom is considered vulnerable due to its large population and open society (Ibid.).

Also, as priority no. 1 (Tier one) we find the protection of Public Health, as it can be seen in the image taken from the strategy (*Figure no. 1*).

A detailed presentation of the risks to public health as well as other types of risk can be found in the National Register of Civil Emergency Risks, 2017 Edition (*Figure no. 2*).
Figure no. 3 presents a risk matrix as well as a more detailed presentation of the risks and measures that have been taken in the past and could be taken in the future.

As a potential to cause a civil emergency, diseases are identified that can cause the infection of a large number of people in a short time. Influenza is mentioned as a disease, not the seasonal one, but the flu caused by a new virus that would spread quickly and cause serious diseases due to lack of immunity. It is stated that there is a high probability of occurrence of this kind of pandemic, taking into account the history of such pandemics, but it cannot be accurately estimated when it will occur.
There are also estimated the consequences of pandemic flu:

1. If up to 50% of the UK population has symptoms, it is estimated between 20,000 and 750,000 deaths and high levels of absence from work.
2. Disruption of essential services, in particular health and education; and
3. Economic disruptions, including disruptions to business and tourism.

Examples of pandemic outbreaks are mentioned in the register, an H1N1 strain ("swine flu") in 2009, which caused at least 18,500 deaths worldwide (Figure no. 4).

In 1918, another variant of the same strain of H1N1 ("Spanish flu") killed more than 50 million people worldwide. However, there are other pandemic influenza
strains, such as H5N1 ("avian or avian influenza"). This strain caused several hundred human deaths in Southeast Asia in 1996.

It is mentioned that in the last 25 years more than 30 new (or recently recognised) emerging infectious diseases have been identified worldwide, such as Ebola, Zika and respiratory syndrome in the Middle East. The latter emerged recently in 2012 and posed a global threat to health.

Solutions we find in the registry are:

1. Before the manifestation of the risk
   - **Coordination** – Government departments, decentralised administrations, public health agencies and developed branches need to share plans and information.
   - **International collaboration** – the UK Government works with others to undertake research on prevention, detection and research. The World Health Organisation has an influenza programme that provides member states with strategic guidance, technical support and coordination of activities.

2. The risk response
   - **Disease detection** – there are specialised capabilities in epidemiology and microbiology in the UK to identify, characterise and respond to infectious diseases.
• **Antivirals** – the government stores enough antivirals to help treat people who have symptoms during a flu pandemic. Antivirals can help treat flu symptoms.

• **Vaccines** – vaccines will be developed as soon as possible once new influenza strains are identified. This will take at least four to six months after the onset of a pandemic.

• **Personal protective equipment** – emergency interventions have personal protection with equipment for severe pandemics and infectious diseases. There are also protocols in place to control infections both before and during an incident.

From our research we see that the two governments have assessed this type of risk and have taken action accordingly. However, with the onset of the COVID 19 pandemic, these states have been affected and are having a rather difficult time managing the situation, with the number of cases rising alarmingly from day to day (COVID-19 update at the date of writing the article). (Figure no. 4 and Figure no. 5).

![Figure no. 4: COVID-19 cases on 17.10.2020, USA (Coronavirus update)](image)

**RISKS TO NATIONAL SECURITY IN THE CONTEXT OF THE COVID-19 CRISIS**

Focusing on establishing and implementing measures to combat the effects of the pandemic may lead to a diminished focus on security risks.

In a recent interview for Digi24, NATO Deputy Secretary General Mircea Geoană stated that in the context of the COVID-19 crisis, at NATO level, a certain degree of alertness and vigilance is maintained. “We are, on the one hand, vigilant about the health crisis itself, but especially at the risk of being tempted by state or non-state actors to take advantage of a time when we are all busy – allocating resources, we are concerned with public opinion, the attention of the political and decision-maker naturally goes to this pandemic, the fight against the pandemic, the economic
recovery, all that means the range of measures we must take – to take advantage of a vain hope. We discourage, including through public communication actions, to say very clearly that there is no risk to the citizens of the North Atlantic Alliance and we are paid and have an explicit mandate to prevent a major health and economic risk from turning into a security crisis”.

Security risks are managed through multiple levers, an example being the management of national critical infrastructures. In the US there is a Cybersecurity & Infrastructure Security Agency (CISA), which collaborates with government and industry to identify, analyse, prioritise, and manage the most significant strategic risks to the nation’s critical infrastructure (Figure no. 6).
The main threats to national security are terrorism, espionage, cyber threats and the proliferation of weapons of mass destruction, many of which have an impact on national infrastructure. They have various hybrid forms of attack, such as: misinformation by fabricating false and manipulative information, data collection applications, cyber attacks etc.

National infrastructure sectors are key strategic interests for foreign intelligence services, whose targeting against sectors is likely to include espionage for economic, political, military or commercial purposes. State agencies, the military and companies working on sensitive technologies are the main targets for foreign espionage.

In the USA, 16 critical infrastructure sectors are identified whose assets, systems and networks, whether physical or virtual, are considered vital to any state. Their incapacitation or destruction would have a direct effect on security, national economic security, public health or national security, or any combination thereof.

They can be identified in any state but they can be more or less developed. Threats of any kind to critical infrastructure are important issues that must be addressed as a matter of priority, as a threat to national security.

In Romania, the critical infrastructures were established by Emergency Ordinance no. 98/2010 on the identification, designation and protection of critical infrastructures, following the implementation of the European Council Directive no. 114/2008 on the identification and the designation of European Critical Infrastructures and the assessment of the need to improve their protection. The preamble to the emergency ordinance mentions an essential element in the link between the maintenance and development of critical infrastructure and national security “ensuring an adequate level of protection of critical infrastructure is essential for economic development, the maintenance of vital functions of society and the safety of citizens, as well as the fact that failure to adopt such regulation in an emergency could undermine national security” (Ibid.). This was amended in 2018 by Law no. 225/2018 for the amendment and completion of the Government Emergency Ordinance no. 98/2010 on the identification, designation and protection of critical infrastructures.

According to the national legislation, at the level of Romania, 12 sectors of national critical infrastructure have been established. They are presented in figure no. 7.

Not coincidentally, the Romanian Intelligence Service was appointed responsible for authority for the IT&C and national security sectors, together with other institutions. The Ministry of Health and the Ministry of Education, Research, Youth
Figure no. 7: Romania’s national critical infrastructure sectors

and Sports are responsible for all matters related to public health and research in this critical infrastructure sector according to the law:

“5.1. Medical and hospital care;
5.2. Medicines, serums, vaccines, pharmaceuticals;
5.3. Biolaboratories and bioagents;
5.4. Medical emergency services and medical transport”. (Ibid.)

Also, according to art. 4. of the law, “(1) The coordination, at national level, of the activities regarding the identification, designation and protection of ICN / ICE is carried out by the Prime Minister, through the appointed adviser. In order to fulfil the responsibilities established by this emergency ordinance, the Prime Minister issues decisions.

(2) The responsibility for organising and carrying out the activities necessary to implement the legislation specific to the PIC field rests with the Ministry of Internal Affairs, hereinafter referred to as MAI, through the National Center for Coordination of Critical Infrastructure Protection, hereinafter referred to as CNCPIC” (Ibid.).

One aspect that caught our attention is the fact that in Romania, national security is considered a critical infrastructure sector. From our point of view, taking into account the analysis of critical infrastructures in other states such as the USA (see figure no. 6), Canada – sectors: Energy and Utilities, Finance, Food, Transport, Government, Information and Communication Technology, Health, Water, Manufacturing, Safety (Canada’s Critical Infrastructure, May 2020) and Australia
– Banking and Finance, Communications, Data and Cloud, Defence Industry, Education, Research and Innovation, Energy, Food and Agriculture, Health, Space, Transport and Water (Protecting Critical Infrastructure and Systems of National Significance, August 2020), national security covers all sectors of national critical infrastructure and any deficiency in one of the sectors has repercussions on national security.

Based on these aspects, we can deduce that a poor or medium-developed health sector, in the face of a pandemic, faces much more difficulty than a well-developed sector, which can lead to national security by triggering chain reactions: the inability to provide specialised medical care for all sick people, the increase in the number of deaths leading to the loss of human resources, the need to take too harsh measures to limit the spread of the virus (closing restaurants, schools, theaters etc.) which can lead to a unwanted damage to the national economy, to the financial resources of the population, which becomes a threat to the security of the nation – national security.

CONCLUSIONS

In this period of pandemic, unfortunately, we live these measures in Romania and we can only draw the attention of public authorities to the need for a careful analysis of the situation and the maintenance of a level of alert, so as not to endanger national security in the medium and long term.

The most affected critical infrastructure sector today is health. We hope that the measures taken will lead us to a stabilisation of the situation and not to witness a more pronounced affectation of this sector, because it entails the affectation of other sectors as well.

We must also pay special attention to the trust in the public administration in order not to be undermined by state or non-state actors with various economic and geostrategic interests on the Romanian territory.

Risks to national security must be analysed and treated with the utmost care. The risks can be identified most easily, according to the specialists in the field, by formulating cause – risk – effect (Mulcahy, 2010, pp. 70-77).

BIBLIOGRAPHY:

3. COVID-19 Update, https://www.google.com/search?ei=doeMX7HeMeLMrgSsqqPocG&q=cazuri+covid+sua+azi&oq=cazuri+covid+sua+&gs_lcp=CgZwc3ktYWIQARgA
Risks to National Security in the Context of the COVID-19 Pandemic

DEFENCE RESOURCES MANAGEMENT


8. Radio Europa Liberă, *Organizația Mondială a Sănătății a declarat oficial pandemie de coronavirus*, https://romania.europalibera.org/a/organiz%ca%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-%83%ca-19.html, retrieved on 18 October 2020.

9. https://www.google.com/search?ei=ioeMX5H2KY7qwhJsoaQDg&gs_lcp=CgZwc3ktYWIQARgBMgUJABDJAzLCQA6BggAEBYQHICq5AxY3r8MYPfRDGgAcAB4AIABqwmIAcQekgENMC4yLjEuNSOyLjEuMZgBAKAABaoBB2d3cy13aXrAAQE&sclient=psy-ab, retrieved on 13 September 2020.