# DIVERSIFICATION OF CYBER THREATS IN THE CONTEXT OF THE EVOLUTION OF THE SARS-CoV-2 PANDEMIC

Lt.Col. Ovidiu-Dumitru RUSU, PhD Candidate*
Capt. (Navy) Prof. Sorin TOPOR. PhD**

With the onset of the SARS-CoV-2 pandemic, the challenges in communications, information technology and cybersecurity have become much more numerous and complex at the same time. The continued transfer of certain daily activities in cyberspace will give rise to new major challenges, with many elements of novelty and unknown. It is difficult to predict how the virtual space will evolve in the future and how it will respond to the requirements formulated by society. State or non-state entities need to adapt quickly to the new demands of cyberspace. History has shown us that major changes will inevitably lead to other changes in which society will have to find the right solutions to ensure its continuity. The evolution of society in the SARS-CoV-2 pandemic shows us every day that the development of communications infrastructure and information technology, as well as ensuring cyber security, are essential elements without which certain sectors of activity cannot function at normal parameters.

**Keywords:** cyber threats; communications and information technology; cyberspace; cybersecurity; SARS-CoV-2.

For the first time, the SARS-CoV genome was identified in April 2003, following the outbreak of the epidemic of the same name in countries in the Asian region. At the time, SARS-CoV (Severe Acute Respiratory Syndrome CoronaVirus) was seen as a strain of the virus that mainly infected epithelial cells in the lungs.

Following studies conducted by specialists in the field, it was established that this strain of virus was initially developed by various animals (especially palm civets and bats), and later SARS-CoV was transferred to humans[1].

The death toll recorded in 2003 following the development of the SARS-CoV-1 pandemic (named after the outbreak of the 2020 pandemic) was about 774 people[2].

As for the history of SARS-CoV-2, it is very well known because it is an event that was recently launched and is still ongoing.

However, we would like to remind you that SARS-CoV-2 was first identified on 8 December 2019 in Wuhan, CHINA, and the World Health Organization (WHO) was notified of its existence on 31 December 2019.

Although at the beginning of the SARS-CoV-2 pandemic, many states were reluctant to the effects and speed of the spread of this virus, on 11 March 2020 the World Health Organization declared SARS-CoV-2 a global pandemic.

The disastrous effects of SARS-CoV-2, as well as the rapid spread of SARS-CoV-2, have led countries around the world to urgently adopt a series of unprecedented measures, which have inevitably led to a radical change in the way of life of citizens.

The measures taken to combat the SARS-CoV-2 pandemic were gradual and eventually led to an almost total but temporary closure of activities around the world (transport, education, trade, tourism, etc.).

These restrictions imposed by government institutions have generated a number of major changes in the way of life of citizens.

One of the most effective measures imposed to avoid the spread of SARS-CoV-2 was to respect the social distance of people that led to a transfer of many activities in the virtual space.

It was not really an element of novelty because many activities were already taking place in the virtual space (e-commerce, distance

* *”Carol I” National Defence University*
e-mail: *rusuodumitru@yahoo.com*
** *”Carol I” National Defence University*
e-mail: *sorin_topor@yahoo.com*

learning through e-learning platforms, etc.), but what was surprising was the fact that the existing infrastructure was not ready to withstand such a large transfer of information. The information capacity and services required in the virtual space have reached levels that the communications infrastructure and information technology have faced with certain limitations.

Gradually, the communications infrastructure and information technology began to operate at normal parameters, not anyway, but with massive investments.

However, in order for the activities in the virtual space to take place in a normal and secure way, financial investments have been and still are needed to allow the development of communication infrastructures and information technology.

Even before the onset of the SARS-CoV-2 pandemic, the development of communications infrastructure and information technology were already priority objectives planned over a period of time, with the advent of COVID-19, deadlines had to be brought forward so that people could carry out certain activities in safe and cyber security conditions.

The anti-SARS-CoV-2 measures revealed the dependence of certain (and not a few) sectors of activity on the communication infrastructure and information technology and determined the allocation of additional funds to be able to develop and expand the virtual space in cybersecurity conditions.

The SARS-CoV-2 pandemic, through the restrictions imposed, showed that the lack of digital skills in a world where virtual space has become vital, generates a series of problems that can be hardly remedied.

This SARS-CoV-2 pandemic has generated a series of new challenges that have determined and will determine the states of the world to adopt unprecedented measures that will impose a new way of life dependent on virtual space.

### Cyber Attacks In The Context Of Sars-Cov-2

The transfer of many activities from the ordinary environment to the virtual space has inevitably generated an increase in the threats, vulnerabilities and implicitly of the risks to which the people who use the virtual space are exposed.

In this regard, on 22 October 2020, the head of the Cyberint Cyber Security Department within the Romanian Intelligence Service (SRI), Mr. Anton ROG, stated that the SARS-CoV-2 pandemic created a special environment that cyber attackers took advantage of especially due to the lack of information we all face, especially in March 2020, when we publicly signaled that the number and complexity of cyber attacks has increased, the main topic used by attackers being an alleged miraculous treatment[3].

Also, on the same occasion, the head of the Cyberint Cyber Security Department within the Romanian Intelligence Service specified that the main cyber attacks registered during the SARS-CoV-2 pandemic were ransomware and fraud. These two types of cyber attacks mainly targeted institutions in the health system, the banking system, the local and central government system, as well as in the education system.

In a previous statement, published on 14 August 2020, Mr. Anton ROG revealed that during the SARS-CoV-2 pandemic certain state entities (without specifying their identity) carried out cyber attacks and operations for the purpose of cyber espionage[4]. In his opinion, the cyber attackers used social engineering techniques through emails that were disseminated to certain people employed in Romanian state institutions. The content of the messages mainly referred to issues related to the SARS-CoV-2 pandemic (how to protect yourself, statistics on the number of infected, etc.).

At the same time, the official from the Romanian Intelligence Service confessed that one of the main targets of the cyber attackers was the health system through its related institutions[5].

The *CYBERINT Special Bulletin in the context of the SARS-CoV-2 pandemic*, published by the Romanian Intelligence Service details the main types of cyber-attacks registered worldwide.

Thus, the specialists in the cyber field within the Romanian Intelligence Service appreciate that, since the beginning of the SARS-CoV-2 pandemic and until now, the following types of cyber-attacks have been registered:

- Ransomware (Covidlock, Netwalker, Maze, Nemty);
- Web defacement;
- Trojan banking (Cerberus android banker, Qbot)[6].

Covidlock is a ransomware cyber-attack that is transmitted through the mobile application COVID-19 Tracker. This application locks the device and according to the characteristics of the types of ransomware attacks requires the payment of a sum of money in digital format to allow access to the terminal owner to their own information.

Netwalker was first identified in 2019 and was created by a cybercrime group called ”Circus spider”. The main features of this type of ransomware attack are the following:

- works on devices that have the Windows 10 operating system installed;
- has as a favourite target devices used for personal purposes;
- has specific capabilities that allow it to bypass antivirus systems.

Maze also belongs to the category of ransomware cyber-attacks and uses as propagation vectors phishing messages or vulnerabilities of remote communication protocols. The techniques used by cyber attackers are the classic ones, identifying weak credentials or sending documents with the .docx extension for access.

Nemty is another type of cyber attack that belongs to the ransomware family. It was identified in August 2019 by cybercriminal specialists of the American computer company McAffe. Nemty acts to block the access of the device owner to the information by encrypting it, while deleting the data and information backups.

On 20 October 2020, The European Union Agency for Cybersecurity (ENISA) published a List of top 15 threats from January 2019 to April 2020 where the main cyber threats registered in the mentioned period are presented in detail.

In this complex document, cybersecurity specialists analyzed each threat in detail, presenting in particular the vectors of spread, current and future trends of threats and vulnerabilities, as well as the main measures of prevention and cyber security.

According to the List of top 15 threats from January 2019 to April 2020, the main 15 identified cyber threats were the following: malware, web based attack, phishing, web application attack, spam, DDOS, identity theft, data break, insider threat, botnets, physical manipulation, information leakage, ransomware, cyberspionage and cryptojacking.

At a first analysis of the document, we notice that the 15 cyber threats identified in this document are the same as those published in January 2019 in the Threat Landscape Report 2018 ENISA, with small changes in the order of ranking.

### The Need To Ensure Cyber Security In The Virtual Space

The outbreak of the SARS-CoV-2 pandemic and the adoption of restrictive measures to limit its effects have inherently led to major changes in the way citizens live.

As a result of the measures adopted by the governmental institutions of the states, many activities have migrated from their usual environment to cyberspace. The need to communicate, to learn, to work, etc., expressed in a single expression ”to live”, is increasingly dependent on virtual space.

Massive investment in communications infrastructure technology and information technology is a necessary but not sufficient condition. In order to transfer a part of our way of life from the current environment to cyberspace, we need the certainty that it is safe, stable, accessible and efficient. Certainly there are other conditions that cyberspace must provide users in order to carry out normal virtual activities, without risks.

An article published in 2020 by Harvey Nash (a global provider of IT recruitment and outsourcing consulting services) mentions that since the beginning of the SARS-CoV-2 pandemic, the interviewed companies have spent huge sums on the development of communications infrastructure. and information technology and also to ensure cyber security. However, the same article points out that these investments have not been able to stop cyber attacks. In a survey of about 4,400 information technology specialists, 4 out of 10 IT leaders said that during the pandemic there was an increase in cyber attacks. The most important cyber threats were phishing and malware[7].

We appreciate that one of the factors that contributed to the increase of cyber threats during the SARS-CoV-2 pandemic was the fact that a large part of the active population started working from home, being much more exposed to cyber attacks precisely due to minimal measures or sometimes non-existent cyber security. Among these we would like to mention the lack of an adequate security culture, the endowment with equipment and programs that do not ensure cyber security, information from unofficial sources, etc.

In this context, we state that investments will have to target both communications infrastructure and information technology, as well as the provision of cyber security with resources.

The lack of ensuring cyber security in the virtual space can have serious consequences both on the security of state or non-state actors and on the security of citizens.

## Conclusions

The SARS-CoV-2 pandemic, through the measures taken and the effects generated, revealed to the whole world a new way of life, the absolutely necessary symbiosis between man and cyberspace.

Human activities are increasingly dependent on virtual space, which makes us even more responsible for ensuring cybersecurity.

A secure virtual space automatically generates comfort for citizens who carry out various daily activities.

Asking us one question *How would we have lived in a pandemic without the existence of cyberspace?* we realize that the variables in such an equation would have been completely different.

Human progress achieved through the existence of communications infrastructure and information technology can not be denied, but must be recognized, supported, continued and used for noble purposes.

By virtue of the above, to ensure a modern communications infrastructure and information technology, with high-performance cyber security, in the context of the evolution of the SARS-CoV-2 pandemic, we propose the following:

- allocating sufficient funds for the development of communications infrastructure and information technology;
- ensuring a normal and secure virtual space by implementing efficient cyber security solutions;
- continue training and support a qualified human resource to ensure the cyber security of communications infrastructure and information technology;
- ensuring access to the Internet for all citizens, so that they can carry out their activities in cyberspace;
- ensuring the digital literacy of all citizens by organizing dedicated programs in this regard.

## NOTES:

[1] https://www.chinadaily.com.cn/china/2006-11/23/content_740511.htm, accessed on 29.12.2020.

[2] https://romania.europalibera.org/a/coronavirus-de-ce-%C3%AEn-epidemia-de-sars-%C3%AEn-2003-au-murit-mult-mai-pu%C8%9Bini-oameni/30545956.html, accessed on 29.12.2020.

[3] https://economie.hotnews.ro/stiri-telecom-24369538-oficiali-din-guvern-sri-confruntam-adevarata-pandemie-spatiul-cibernetic-victime-fost-romania-semnalul-alarma-privinta-securitatii-5g.htm, accessed on 29.12.2020.

[4] *Ibidem*.

[5] https://www.digi24.ro/interviurile-digi24-ro/cine-sunt-spionii-din-telefon-si-din-calculator-interviu-cu-directorul-cyberint-anton-rog-1352811, accessed on 30.12.2020.

[6] [Romanian Intelligence Service], *Special CYBERINT Bulletin in the context of COVID-19 Pandemic*, 2020.

[7] https://home.kpmg/xx/en/home/media/press-releases/2020/09/covid-19-forces-one-of-the-biggest-surges-in-technology-investment-in-history-finds-worlds-largest-technology-leadership-survey.html, accessed on 30.12.2020.

## REFERENCES

*** *Threat Landscape – Cyber espionage*, ENISA, 2020.

*** *Threat Landscape – List of top 15 threats*, ENISA, 2020.

*** *Strategia națională de apărare a României pentru perioada 2020-2024*, Bucharest, 2020.

[Ministry of National Defence], *Carta albă a apărării*, Bucharest, 2020.

[Romanian Intelligence Service], *CYBERINT Bulletin*, 1st semester, 2020.

[Romanian Intelligence Service], *Special CYBERINT Bulletin in the context of COVID-19 Pandemic*, 2020.

https://home.kpmg/.html

https://www.defence.ro

https://www.sri.ro

https://certmil.ro

https://www.chinadaily.com.cn/china/2006-11/23/content_740511.htm

https://romania.europalibera.org/a/coronavirus-de-ce-%C3%AEn-epidemia-de-sars-%C3%AEn-2003-au-murit-mult-mai-pu%C8%9Bini-oameni/30545956.html

https://economie.hotnews.ro/stiri-telecom-24369538-oficiali-din-guvern-sri-confruntam-adevarata-pandemie-spatiul-cibernetic-victime-fost-romania-semnalul-alarma-privinta-securitatii-5g.htm.

https://www.digi24.ro/interviurile-digi24-ro/cine-sunt-spionii-din-telefon-si-din-calculator-interviu-cu-directorul-cyberint-anton-rog-1352811