CYBERSECURITY IN THE POST COVID ERA

Loredana MOCEAN[*]
Miranda-Petronella VLAD[**]

Abstract

The Covid 19 pandemic and then the war in Ukraine affected us all to a greater or lesser extent, but the traces existed and still exist. The Internet has created a huge space of resources, but it has also created the context of new types of damage, theft and fraud. The legislation in force, both in Romania and in the European Union, militates for the creation of a legal context in which adequate and balanced technical and organizational measures are implemented to meet the minimum security requirements of networks and IT systems on the territory of the European Union.

The present work wants to draw attention to the need, in the future, of protection against all cyber attacks. The laws in the field of cyber security, both in Romania and in the European Union, are briefly presented. The authors proposes a security architecture and creates a new model of cyber ontology.

Keywords: *cybersecurity, laws, cybernetic attacks, vandalism, sabotage*

JEL Classification: [K24]

1. Introduction and background

Important authors in the field of cyber security issue a warning about the times to come.

“The COVID-19 pandemic accelerated the transition from the traditional life to a life based on the use of technology (Porcius, 2021). “

“In less than two decades, society, the way people relate, has fundamentally changed, more than it did in thousands of years”. On the one hand, the Internet creates a huge potential for development in all areas of social life, its applications being practically inexhaustible. On the other hand, the technology offered opens up new horizons for the commission of crimes, either “classic” - theft, fraud, or other types of more sophisticated crimes that also develop exponentially (Livescu, 2011).

Romania and the other EU member states have campaigned a lot in recent years for the introduction of new cyber security systems in essential fields and services such as schools, city-halls, hospitals, energy companies networks, railways and airports.

[*] PhD, Associated Professor, Babeș-Bolyai University, Cluj-Napoca, Romania, loredana.mocean@ubbcluj.ro.

[**] PhD, Associated Professor, “Dimitrie Cantemir” Christian University, Bucharest, miranda.vlad@cantemircluj.ro.

There is an increasing demand for the security of connected technology in homes, offices and factories, building collective capabilities to respond to major cyber attacks and collaborating with partners around the world to guarantee the stability of states and international stability in the cyber domain.

The pandemic years created many opportunities to work on computer systems, but they also brought many disadvantages, related to the safety and security of computer systems. Meanwhile, in the post-pandemic years, new cyber security systems have already been implemented.

2. The main normative acts in the field of Cyber Security in Romania and the EU

Ever since 2011, professionals in the field of law have been sounding the alarm about the evolution of the IT sector.

“Although the social and business relations facilitated by information technology are global, the legislations are national[1].

The international and national legislations, as well as the training of legal professionals for the new reality, are outpaced, as a rhythm, by the speed with which the way social life unfolds, the way people relate, between commercial companies or other participants in social life, evolves.

The lack or insufficiency of international regulations in the matter, as well as the lack of specific criminalizations in national legislation, left far behind the development of the phenomenon, can lead to chaos” (Livescu, 2011).

“Digital transformation and connectivity have provided unprecedented opportunities for cyberattacks. Therefore, organizations should make cybersecurity by design a crucial feature of their strategy”, the authors of the article recently stated (Hefley, 2022). Alarm signals have therefore been raised for many years and now after the Covid 19 Pandemic the situation is even more critical.

It was desired and it is still desired to build a strategy on how a cyber unit can ensure the most effective response to cyber threats using the collective resources and expertise available to the EU and the member states.

The main law in the field of cyber security in Romania is Law 362/2018 on ensuring a common high level of security of networks and IT systems. The National Cyber Security Incident Response Center - CERT-RO is designated as the main body dealing with national security through IT services.

According to this law, CERT-RO implements appropriate and proportionate technical and organizational measures to meet the minimum security requirements of networks and computer systems on the territory of the European Union, taking into account the technical norms provided.

[1] https://livesculegal.com/Evenimente-juridice/Page-2.html

It also implements appropriate measures to prevent and minimize the impact of incidents that affect the security of networks and IT systems used to provide services.

Romania's cyber security strategy[2] for the period 2022-2027, was approved by Government Decision no. 1.321 (Dec. 30, 2021) as well as through the Action Plan for the implementation of Romania's Cyber Security Strategy.

An updated vision is promoted according to the developments of the cyber security issue at the national and international level.

Five objectives of maximum strategic importance are identified, based on GD no. 271 of 2013[3]:

1. Secure and resilient IT networks and systems
2. Consolidated regulatory and institutional framework;
3. Pragmatic public-private partnership -
4. Resilience through proactive approach and deterrence -
5. Romania - relevant actor in the international cooperation architecture

Cybersecurity assurance activities are also completed both at the national and European level based on the commitments undertaken at the level of the European Union and NATO.

In order to achieve the cyber security objectives, Romania developed the Action Plan for the implementation of the Cyber Security Strategy. The plan is proposed for the period 2022-2027 and contains the concrete measures necessary to achieve the objectives. They represent a shared responsibility of all actors involved.

According to the assumed commitments, Romania has undertaken measures to develop the national normative framework harmonized with the provisions of EU legislation, which would meet international requirements and which would facilitate bilateral cooperation and the exchange of information between the competent authorities.

The main laws adopted in Romania are described below.

- *Law 362/2018* on ensuring a common high level of security of networks and IT systems[4], establishes the legal and institutional framework, measures and mechanisms necessary to ensure a common level high security of networks and information systems and the stimulation of cooperation in the field.

  The law creates a multi-system of national geographical spread with the role of prevention and response to incidents. Requirements for ensuring the IT security of the services provided and requirements for notification of incidents, response mechanisms at the national level are established.

[2] www.infoeuropa.ro
[3] https://securitypatch.ro/strategia-de-securitate-cibernetica-a-romaniei-2/
[4] https://legislatie.just.ro/Public/DetaliiDocument/209670

- *OUG 104/2021* on the establishment of the National Cyber Security Directorate, develops the institutional architecture[5] to meet the requirements of ensuring the security of the national civil cyber space and fulfilling the obligations assumed by Romania through the transposition of the NIS Directive into national legislation.
- *Law 163/2021*[6] regarding the adoption of measures related to IT and communications infrastructures of national interest and the conditions for the implementation of 5G networks. The normative act was promulgated for the adoption of measures related to ensuring security in the field of 5G electronic communications. The measures recommended at EU level by the 5G Security Toolbox are implemented.

Romania aims to update and expand the regulatory framework in the field of cyber security, by adopting laws to regulate Romania's cyber defense[7].

The bodies of the European Union regulate through Regulation (EU) 2019/881 of the European Parliament and of the Council on ENISA (European Union Agency for Cyber Security) enforcement measures of all cyber security rules in the member countries emphasizing the fact that networks, IT systems and services communications play a vital role for society. They have become the basic infrastructure of economic growth.

3. Cybernetic attacks

„The protection of personal data is subsumed by the protection of privacy provided by Article 8 of the European Convention on Human Rights" (Apan, 2021). Thus, the creation of an IT system requires joint actions to ensure all the component elements, the neglect of even just one of them may bring damage to the entire action. The actions that an IT system supports are complex and are represented schematically in figure 1.

The need for interventions in the IT system is due to the following chain of actions, as we can see in Figure 1.

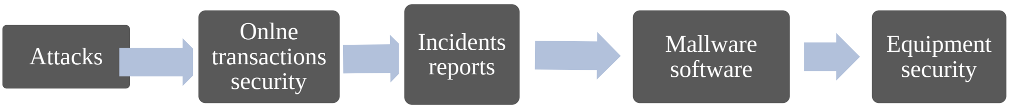

Figure 1. Chain of actions preceding the installation of a cyber security system

The creation of such a system implies the execution of a project that must take into account the possibility of a cybernetic attack at every stage.

[5] https://legislatie.just.ro/Public/DetaliiDocumentAfis/ 246652)
[6] https://legislatie.just.ro/Public/DetaliiDocument/243213
[7] www.monitoruloficial.ro

„The pandemic has stretched companies' networks, accelerated their digital transformation and exposed them to more cybercrime. Cybersecurity has never been more important", states Mike Azzara in his article (2022).

Cyber attacks are attempts to gain unauthorized access to hardware and software systems and to steal, modify or destroy data. As specified on the Microsoft website[8] cyber attacks are distributed by individuals or organizations for political, criminal or personal intentions to destroy or gain access to classified information.

There are several types of cyber attacks:

Web vandalism - results in damage to web pages or denial of access to certain pages. These attacks are quickly countered and cause very little damage.

Propaganda – political messages can be spread by or to anyone with access to the internet.

Data collection - classified information that is not kept secure can be intercepted and even modified, thus making espionage possible.

Computer virus attacks – Once activated, a virus can corrupt, alter or destroy information, generate fictitious transactions and even transfer data.

DoS attacks - using tens of thousands of compromised computers to exceed the capacity of a Web server through traffic. Once launched, attacks are difficult to stop because information flows come from different locations. Most of the time, system users do not realize that their system is attacking other computers. In the event of such an attack, web pages are quickly overwhelmed by fake accesses launched by compromised computers spread throughout the world.

Equipment sabotage – military activities that use computers and satellites for coordination are vulnerable to such an attack.

Attacking critical infrastructure – Electricity, water, oil, communications, trade, transport are all vulnerable to a cyber attack.

Figure 2 shows in detail the vulnerable places that can be the targets of cyber attacks, starting from e-mail and up to the final stage, the infrastructure attack.

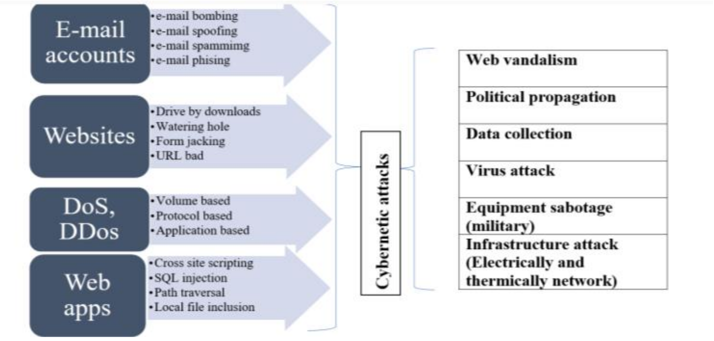

Figure 2. Vulnerable components to cyber attacks in an IT system

[8] https://www.microsoft.com/ro-ro/security/business/security-101/what-is-a-cyberattack

The Covid 19 pandemic and more recently the war in Ukraine have brought to the fore how fragile all IT infrastructure can be, what damage a cyberattack can cause and how important it is for each entity to ensure that it is not “at the disposal” of anyone.

A correct automation of the information flow brings a project to a successful end, no matter how complicated it may be. Properly designed and implemented automation operations build a robust and coherent security information center.

Applying automation to daily activities allows analysts to see, identify, track and, more importantly, respond to threats before they affect systems.

The logical flows in a cybernetic attack are presented in figure no. 3. Starting from the data of the organization, an attack with a high impact on the person and his family members is reached.

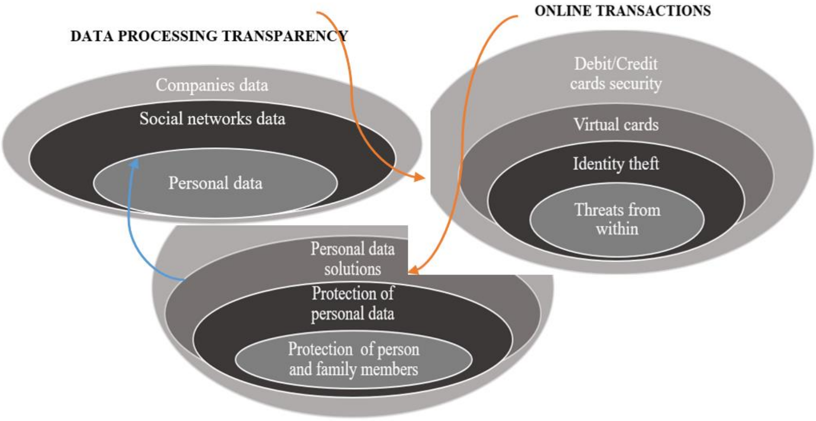

Figure 3. Logical flux of a cybernetic attack

4. Cybernetic Security Architecture

„Cybercrime is much better developed than people imagine,” said Adam Palmer, a consultant at Symantec Corporation, involved in an international study on computer security.

The adoption of a cyber security architecture ensures advanced protection against security threats of the entire IT system and involves the cooperation of security systems in all stages of computer attacks.

Cyber security must be treated dynamically and reevaluated according to threats in the current context, when new security breaches appear every moment.

Everything that intervenes on the cyber system must be monitored, thus through continuous analysis of threats, we identify, treat and reduce risks and establish specific procedures and mechanisms. Thus, we manage to reach an acceptable level of security depending on the allocated resources, as we propose in figure 4.

We propose to integrate cybernetic honeypot systems at as many levels of the architecture as possible.

In terms of security, a cyber honeypot works in a similar way, acting as a trap for hackers. It is a computerized sacrificial system that aims to attract cyber attacks, like a decoy. It impersonates a target for hackers and uses their intrusion attempts to gain information about cybercriminals and how they operate, or to distract them from other targets.

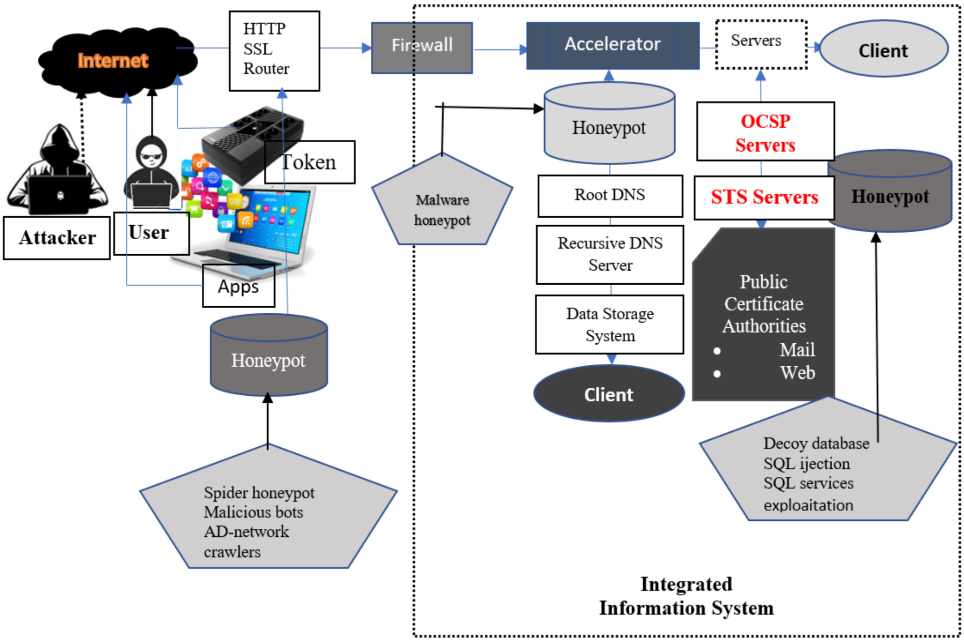

Figure 4. Architecture of a cyber security system

After the creation of the architecture, the problem of creating an ontology arises. In cybernetic systems, the ontological problem concerns the nature and characteristics of the entities that threaten and are threatened. According to Eric Little and Galina Rogova, “threat is a very complex ontological object, and therefore an appropriate ontology must be constructed according to formal metaphysical principles that can account for the complexity of objects, attributes, processes, events and relationships that make up these states of affairs” (Eric G. Little and Rogova, 2006).

Starting from the information held, applying the desired security levels, we arrive at the ontology that generates knowledge through concepts and the description of the relationships between the concepts (see figure 5).

Information modeling methods have become an important means for the development of relevant IT applications, suitable for modern information technologies (Andone, 2005).

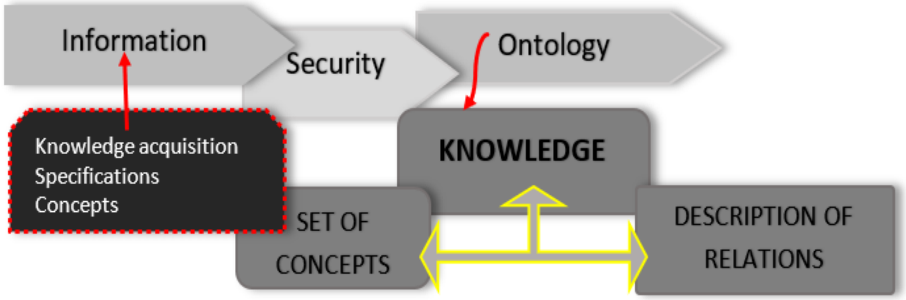

Figure 5 Ontologies in Security systems

The structured set of terms and concepts that represent the meaning of a Cyber Security system, either through the metadata of a namespace or through the elements of a knowledge area, are specified in the following figure (see figure 6).

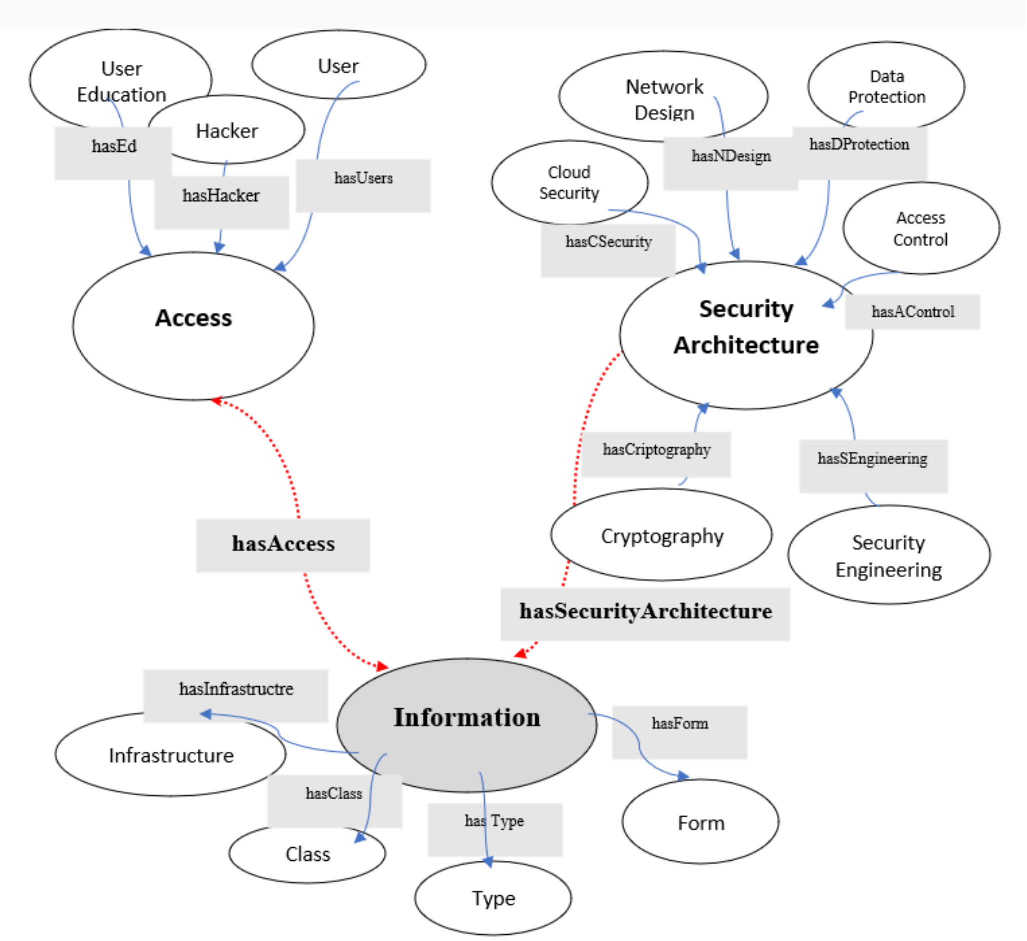

Figure 6 Ontology model in the field of cyber security

Ontology as a term and technology is the representation of a representative data model for a set of concepts and the relationships between these concepts in a field.

In the present paper it is used to argue the objects of the field of cyber security.

Resources may be divided into groups named classes. The data model is based on three big classes: *Information*, *Access* and *Security Architecture*, each with its properties and own class extensions, organized hierarchically.

Relationships between classes are established with the help of relationship type properties:

- *hasType,*
- *hasAccess,*
- *hasSecurity Architecture.*

In the final phase of ontology construction, the surveillance module is added, consisting of monitoring platforms, reports, analytical tools and alert systems. Alerting tools should inform the administrator and the user to take quick action (see figure 7).

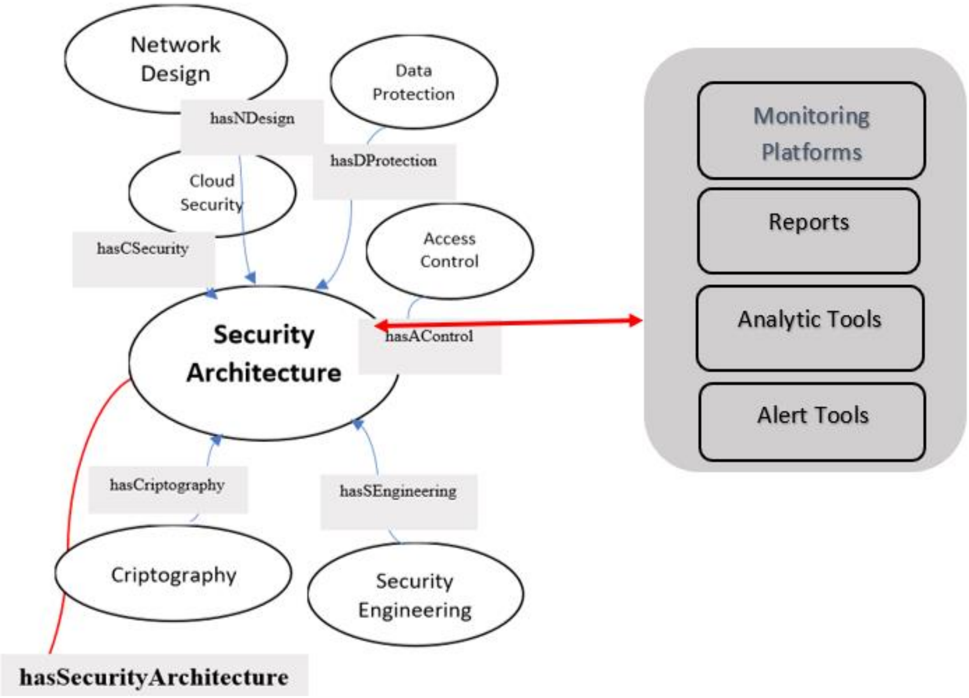

Figure 7 Superimposition of the surveillance module over the ontology

Conclusions

Starting from the existing legislation in the pre-covid period, then continuing with the pandemic period and the years that followed, the need to implement security and mitigate risks became increasingly urgent. More and more attention has been drawn both by national and international forums to the need for such implementations.

Humanity is currently facing other types of vulnerabilities and threats specific to the currently used technologies, in a physical, psychological, technical and organizational / managerial context totally changed by the COVID-19 pandemic. The dangers are much greater than they were before the pandemic, the war in Ukraine also only increased them.

The current work proposes a solution to implement a cyber security architecture completed by an ontology based on the proposed knowledge system, in which the metadata is constituted on the model based on the architecture. Knowledge is the basis of the organization and description of the ontology and protection systems such as monitoring, reports, analytical tools or alerts complete it.

The cyber attacks directed against Ukraine endanger the security of European citizens, so the European Union will continue to take additional measures for cyber resilience and regaining a stable IT ground.

The Covid pandemic brought with it a new type of company, mostly online shopping, payment methods, new types of contracts and a new type of education. The informational society has become the rule, not the exception.

Bibliography

1. Andone, I., (2006), “Ontologies and Enterprise’s Information Modelling”, *Analele Ştiinţifice ale Universităţii “Alexandru Ioan Cuza” din Iaşi*, LII/LIII Ştiinţe Economice 2005/2006.
2. Apan, R.D., (2021), “Personal data protection in health; A perspective of European Court of Human Rights (ECHR)”, *Journal of Law and Public Administration*, 1(VII).
3. Apan, R.D., Perju-Dumbravă, D., Bora, F., (2021), “Vulnerabilities of IT infrastructure in the medical field. Legal framework on data breach liability”, *Fiat Iustitia Journal*, 2.
4. Azzara, M., (2022), *Why Is Cybersecurity Important in the Post-Pandemic World?*, https://www.mimecast.com/blog/why-is-cybersecurity-important-in-the-post-pandemic-world/.
5. Hefley, B., Pańkowska, M. & Vasiu I., (2022), “Cyber Trust Cultivation Premise and Development”, *Forthcoming, Trust, Digital Business and Technology,* Routledge, p. 33-48, DOI: 10.4324/9781003266495-4.
6. Jrme, E., Pavel, S., (2010), *Ontology matching*¸ New-York: Springer Publishing.
7. Little,E., Rogova, G., (2006), “An Ontological Analysis of Threat and Vulnerability”, 9th *International Conference on Information Fusion*, Florence, Italy, pp. 1-8, doi: 10.1109/ICIF.2006.301716.

8. Livescu, D., Livescu, M., (2011), “Profesionistii dreptului in era informationala”, *Conference “Infractiuni la granita de est a UE criminalitatea informatică”*, Vâlcea.
9. Microsoft, n.d., *What is a cyberatack?*, https://www.microsoft.com/ro-ro/security/business/security-101/what-is-a-cyberattack, accessed ian 2023.
10. Moise, A.C., (2020), “Access to a computer system as a special method of forensic investigation”, *Fiat Iustitia Journal*, 1.
11. Porcius,I., (2021), “The Rise Of Telework And The Struggle Towards Cyber Security”, *Fiat Iustitia Journal*, 1.
12. Zalhan, P., (2019), “Transforming big data into knowledge using semantic stream processing technology: challenges and early progress”, *18th International Conference on INFORMATICS in ECONOMY. Education, Research and Business Technologies*, doi:10.12948/ie2019.06.04.
13. Zălhan, P., Silaghi,G., Buchmann, R. A., (2020), “Marrying Big Data with Smart Data in Sensor Stream Processing*”,* Siarheyeva, C. Barry, M. Lang, H. Linger, & C. Schneider (Eds.), *Information Systems Development: Information Systems Beyond 2020 (ISD2019 Proceedings)* Toulon, France, https://aisel.aisnet.org/isd2014 /proceedings 2019/ManagingISD/8/
14. Zhou, H., Kang, L. et al., (2022), “An intrusion detection approach based on incremental long short-term memory“, *International Journal of Information Security*, doi:10.1007/s10207-022-00632-4.