The possibilities of a crisis modeling in the cyberspace of the system security

Jiří Dvořák¹, Jiří Konečný¹*, and Marek Tomaštík¹

¹ Tomas Bata University in Zlín, Faculty of Logistics and Crisis Management, Department of Crisis Management, Studentské náměstí 1532, 686 01 Uherské Hradiště, Czech Republic

Abstract. The paper briefly presents some possibilities of the modern use of cyberspace tools for the theory of artificial intelligence related to the definition of the model and the corresponding possibilities leading to systemic modeling of crises in the modern information and knowledge world and in the area of system security. The modeling process is mainly focused on the specific concept of the virtual model and on the network represented by information and communication systems (ICT) and on the corresponding perspective modeling of the system-based environment used to simulate cyber-attacks and the corresponding levels of cyber-defence. It forms the actual content of the newly conceived modeling with the process of model adaptation in the modern learning environment of artificial intelligence. The paper is based on a scientific task dealing with the possibilities of modeling and adaptation of cybersecurity in a new projected cybersecurity laboratory with the environment of artificial intelligence application in this virtual environment of modern security.

1 Introduction

In view of the growing importance of security issues, both as a result of the international situation and as a result of technological development, the need to intensify and improve the quality of teaching and the necessary research to ensure the necessary number of a quality workforce. The threats of information technology and cyber attacks, which condition the operation of important systems on which the company's basic vital functions depend, are playing an increasingly important role in the structure of current systems risks. At the same time, it is necessary to prepare professional managers of hierarchically structured systems and especially also the state administration, territorial self-government, and critical infrastructure organizations - especially in the area of their coordination in crisis situations. New legislation in the field of cybersecurity and personal data protection necessitates the expansion of highly qualified professionals. These requirements can be met by increasing the technical and content level of relevant research and professional excellence in higher education, as well as by introducing new methods of acquiring practical skills and knowledge using modern teaching laboratories designed to model complex cybernetic systems.

Also, cybersecurity itself has recently seen rapid development - both in technology and in the field of crisis modeling, with a view, of course, to the legal, knowledge and process environment of real and virtual dynamic cybernetic systems. Recently, cyber-attacks have been emphasized as one of the issues caused by the digitalization of instrumentation and control (I&C) systems and the extensive use of networks in industrial control systems. [1] Cyber security refers to the prevention and mitigation of the cyber terror probability beforehand and the appropriate response if a cyber-attack occurs. [2]

In order to ensure the safety of important businesses and organizations, it will be necessary to educate a large number of top competent staff who will be able to combine the acquired new knowledge of systems theory, theoretical and applied cybernetics and other theoretical areas, especially from the perspective of general crisis management and security with new cybersecurity facts and developing methods of artificial intelligence in new technical applications in all fields (ie social, medical, military, police and others). [3, 4]

Our presently designed and already built high-end laboratories, in which real-world models can be created and which is already well modeled and evaluated by attacks on information and knowledge infrastructure and in general on cybernetic systems, are expected to be used for the scientific and research activities of our top workplace and consequently use these funds not only for teaching within the standard activity, but also for commercial activities towards the business environment.

The modern concept of crisis modeling in the area of system security is based primarily on modern expert activities in the recognition of scenes in the laboratory of applied cybersecurity. Brief introduction of the modeling environment of cyber security with artificial intelligence only expresses the difficulty of scientific work in this area of crisis modeling in the area of security of modern
design of socio-technical systems. Partial research results are the subject of the work of students at the faculty.

In recent years, the focus of education has shifted from the behavioral and cognitive models to the constructivist model. [5] The constructivist model of learning purports that knowledge is created and constructed by the learner through discovery. Hence, the focus of educators is to support and provide a learner-centered environment in which learners are able to acquire, construct, and create new knowledge by themselves. An important aspect of the constructivist model is social constructivism, whereby knowledge is created through collaborative problem-solving among learners. [6]

Students constitute the core of 21st society but this society may need technologically-advanced environments for a variety of educational purposes. Until nowadays students want contemporary learning paths that will motivate and increase their interest in learning. The global society is considering the learning approach as an interactive process in which students wish to participate. Therefore, it is expected that educational environments are trying to meet those needs. [7]

2 Laboratory base for cybersecurity process modeling

Very rapid scientific and technological development in the current technological revolution brings and will bring very fast development and use of information and communication technologies (ICT) especially the use of information and knowledge. Another possible use of information is right now in "processes of managing and communicating information (communication) in living and inanimate organisms (in artificial and thus artificial - technical and technological systems)". And this Wiener (1946) has already dealt with this brilliant problem and called it cybernetics. Today's view of cybernetics is in some ways still misunderstood by some individuals and is sometimes (by refined) often replaced by other means of expression. However, from the historical perspective of the world, cybernetics (cybernetics… pilotage) and its principles are embodied in realized and functioning modern technical (eg computer systems and contemporary modern digital systems and information and communication networks, robots and robotic production and service lines, including robots), technical systems and organizations, knowledge and now intelligent AI systems - artificial intelligence.

Information, in general, is always dependent on the processes of recognition, perception, and knowledge of the properties and arrangement of objects around us. Cyberspace is a concept of a new world created by the interconnection of computer, information and communication systems in the real environment and applied cybernetics (especially the socio-technical environment). It is also a space to create, store, use, transform, share and transfer and exchange quality and validated information with each other. Provide its users in the real world with new real possibilities in social communication and in the application of social interaction process (eg in an e-mail, in social networks, in e-business, e-government, e-banking, etc.). [8]

The crisis management is used here (EM: emergency management, the term crisis management in cyberspace, especially in connection with war conflicts) - the term EM is referred to in the literature as crisis management or crisis management. Both terms equally express the management of the entity in the duration of the problem situation threatening its integrity and stability. Most often they are economically, personally, organizationally or otherwise difficult situations, in which the downward development is stopped to a stable position, then in an ascending direction. This is only one of the views that do not respect the vastness and complexity of crisis management. Crisis management is thus still presented only in the range of extraordinary events and crisis situations, or as an economic problem of a company, company, society and less in the context of cybersecurity.

Crisis management should then be presented as an everyday part of our lives. Because all the negative phenomena, events, processes and activities are "a problem." Nevertheless, "crisis management" is most often presented as a procedure by, for example, public authorities, business entities or other organizations in case of crisis (crisis measures). Crisis plans to protect the public interest are processed, for example, by public authorities. Crisis preparedness plans are processed by legal entities and business entities within their jurisdiction and in connection with a territorial crisis plan to protect the public interest and their own (eg economic interests). The Crisis Act and its implementing regulations define the framework for crisis management.

3 The cyberspace and a crisis modeling

Very rapid scientific and technological development in the current technological revolution also brings and will bring very fast development and use of information and communication technologies (ICT), especially the gradual transformation of the information world and corresponding to the cybersecurity area. [9]

The use of information is right now in "management and communication (communication) processes in living and inanimate organisms (in artificial and created, artificial - technical and technological systems)".
Cyberspace is a new concept of the contemporary world created by the interconnection of computer, information and communication systems in the real world and applied cybernetics (as a socio-technical environment).

It is also a space to create, store, use, transform, share and transfer and exchange quality and validated information with each other. To provide its users in a real, secure world with new real opportunities in social communication and social interaction process applications (e.g. e-mail, social networks, e-business, e-government, e-banking, etc.).

Thus, information is of paramount importance for other secure automated management systems (such as command and control of troops). Furthermore, information for remote-controlled unmanned aerial vehicles (airborne drones and now also submarines, rockets, etc.). Furthermore, information for learning and intelligent cybernetic systems - robotic devices also with economic security, etc. [10]

Information for modern (intelligent) learning systems with an artificial intelligence environment in the information and knowledge world for the very near future

Newly Conceived Educational Systems - Given the Need for Top and Qualified Cyber Security Professionals - Learning on the Means of Virtual, Simulation and Modeling Applied Cybernetics - Powerful Optoelectronic, Bionic, etc. and Modeling in Modern Artificial Intelligence Laboratories for University and Science Education.

4 Modeling surroundings in cyberspace security system

It expresses new requirements for the training of security managers with a profile corresponding to technical development, especially in the area of critical infrastructure and the link to the projects implemented so far with the current level of technological development and approach to providing information support for this modeling environment in cyberspace security systems:

- Act No. 412/2005 Coll., On the protection of classified information and on security eligibility, as amended
- Act No. 240/2000 Coll. On Crisis Management as amended
- Act No. 101/2000 Coll. About privacy
- GDPR Regulation: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data
- ISO / IEC 27000 – Information Security
- ISO 22301: 2012 Societal security - Business continuity management systems.

5 Modeling possible crises in the system security area

The security of the electronic data interchange system is a crucial aspect in assessing the weight and legal strength of files, and therefore ensuring security is one of the most important parts of electronic (and other) data exchange in the new system security area:

- The physical protection method represents the security of objects, communication lines, etc. Thus, the data is physically inaccessible to unauthorized systems (persons and their equipment).
- The logical way of protection includes a set of software and hardware measures and the use of new as well as modern cryptographic methods.
- A great danger is hypocrisy (masquerading), when the attacker sets out to be someone else

Security of Information and Cybernetic Systems It is defined from these perspectives:

- physical security of information and communication systems (ICT);
- operation of information systems (manual, semi-automatic, automatic and learning systems);
- network and data security (cryptography and confidentiality system);
- information handling and use and abuse;
- ICT security (adaptive management systems, robotics, and cybernetics, System Recovery Planning (Organizing Systems);
- hardware (HW) software development (SW) and also orgware (OW);
- theory of renewal and cybernetics;
- change management in systems, etc.

Reasons for implementing information and cyber security principles are

- information Systems Interconnection (IST) requirements;
- rapid development, use and new physical principles of information technology (ICT);
- IS/IT connection requirements within the organization;
- advanced e-commerce in a new intelligent knowledge system environment;
Barriers to the faster promotion of information and cybersecurity:
- generally relatively low-security awareness
- high financial demands
- the absence of security standard models,
- low and uncoordinated support from organizations
- unbalanced legislation
- lack of real information in the dynamics of new trends and applications of scientific disciplines (physics, cybernetics, etc.)
- lack of experts in the education and research system, etc.

The use of current digital signature technology and asymmetric encryption is closely related to the issue of public key distribution, as the use of asymmetric encryption alone does not guarantee the necessary authentication. The recipient of the message needs to be sure that the used public key belongs to the sender. Probably the best solution is to use the services of a certification authority, which issues so-called digital certificates for individual entities and also serves as their warehouse.

6 Conclusion

Here are some of the modern possibilities of modeling crises in the cybersecurity system area, and in this article are expressed mainly the partial conclusions of the solved scientific tasks and the practical tasks solved for partial modeling of crises with regard to the current very rapid development of information and cyber security and also application of systems theory disciplines, technical cybernetics, artificial intelligence and other areas necessary for higher education professionals in this new and prospective cybersecurity environment. Therefore, the overview of partially solved tasks was focused on the definition of hierarchical systems classification and their possibilities of modeling on an interesting crisis management environment for defined management systems. The picture of possible modeling was included in cyberspace with adequate laboratory base and in connection with the basic possibilities of modeling complex dynamic systems for new means of modeling cybersecurity processes.

Crisis modeling and corresponding models of cybersecurity attacks and defenses are conducted in an artificial intelligence environment and is a proposed modern environment of our laboratory base TBU - FLKŘ and thus the current means for future necessary lifelong learning. Gradually, it will be expanded to include a significant portion of artificial intelligence in cybersecurity processes for system design models.

The contribution represents an output of a specific research project, System definition of appropriate cyber-safety models for the needs of scientific and research activities and pedagogical at the Faculty of Logistics and Crisis Management of Tomas Bata University in Zlín. This research was supported by support research program of Tomas Bata University in Zlín (RVO).

References

1. B. B. Gan. Nuclear science symposium and medical imaging conference (IEEE; New York, 1992)
2. B. Kesle. SI, 10, 15-25 (2011)
3. J. Andress. Cyber warfare: techniques, tactics and tools for security practitioners (Syngress, Waltham, 2014)
4. M. Dawson, et al. New threats and countermeasures in digital crime and cyber terrorism (IGI Global, Hershey, 2015)
5. B. Eschenbrenner and F. Nah. IJMLO, 1, 159-183 (2007)
6. L. Yuan, N. Fui-Hoon, B. Eschenbrenner, T. Schoonover. IMDS, 113, 605-623 (2013)
7. N. Pellas. IJIL, 17, 326-358 (2015)
8. J. Konecny. et al., MATEC, 134, 00025 (2017)
9. J. Konecny. et al., IDS, 3, 147-153 (2017)
10. J. Konecny. et al., KMU, 13, 147-153 (2018)