MATEC Web of Conferences **134**, 00025 (2017) DOI: 10.1051/matecconf/201713400025
LOGI 2017

Modelling of Processes of Logistics in Cyberspace Security

Jiří Konečný[1,*], *Martina* Janková , and *Jiří* Dvořák[1]

[1]Tomas Bata University in Zlin, Faculty of Logistics and Crisis Management, Department of Crisis Management, Uherské Hradiště, Czech Republic

Abstract. The goal of this contribution is especially to familiarize experts in various fields with the need for a new approach to the system-defined model and modelling of processes in the engineering practice and the expression of some state variables' possibilities for the modelling of real-world systems with regard to the highly dynamic development of structures and to the behaviour of systems of logistics. Thus, in this contribution, the necessity of making full use of cybernetics as a field for the management and communication of information is expressed, and also the environment of cybernetics as a much needed cybernetic realm (cyberspace), determining the steady state between cyber-attacks and cyber-defence as a modern knowledge-based potential in general and specifically of logistics in cyber security. Connected with this process is the very important area of lifelong training of experts in the dynamic world of science and technology (that is, also in a social system) which is also expressed here briefly, and also the cyber and information security, all of which falls under the cyberspace of new perspective electronic learning (e-learning) with the use of modern laboratories with new effects also for future possibilities of process modelling of artificial intelligence (AI with a perspective of mass use of UAVs in logistics).

1 Introduction

Current global economy is faced with a number of challenges in the environment characterized by process engineering in dynamically developing areas and theories of virtual systems, information and communication technologies (ICT), cybernetics (theoretical, technical, and applied, such as in an environment for control and communication in the living and non-living-technical, technological and man-made systems), the theory of models and modelling of systems associated with new designing possibilities (Computer-aided design - CAD used 2D or 3D programs) and also modern construction of safe, optimal, reliable and efficient real systems (based on models of operations research) theoretical approaches to modern logistics in all programmes and also in information and communication technologies (ICT) and last but not least, in the developing areas of modern models for artificial intelligence [1] and learning and smart cyber-security systems (unmanned real resources in logistics).

* Corresponding author: konecny@utb.cz

Nowadays, world economy [3] is also significantly determined by implementation of new scientific and new research knowledge (especially new, efficient technology and logistics) introduced now into practice and also by developing modern means (teaching and laboratory) and tools for lifelong learning in general, particularly in the field of ICT.

The whole of the above mentioned process (as an area of process engineering is associated also with the developing progressive practices and their modelling on powerful IT (self-learning intelligent systems), new system knowledge and assorted possibilities of information security and new cyber-security (CS) from the perspective of system integration of attack and defence modelling, especially from the new perspective of current cyberspace for an information and knowledge based society.

The purpose of this contribution is also to formulate modern systemic uses of models and modelling in the new cyberspace (cyberspace) and formulate fully developed use of the resources of technical cybernetics in practice [5], [2] cyber-security and for further practice durable and upcoming smart means which are already present at the Faculty of Logistics and Crisis Management (FLK) in built laboratories: Cyber Security (LKB) for Bachelor's degree programmes and Applied Cyber-Security (LAKB) for the master's follow-up programmes.

2 The Current State of Logistic Model Solutions in Cyberspace Security

The current state of tasks underway (in the field of modelling in cyberspace security) stems mostly from the understanding of process engineering [4] of the emergence of knowledge society referred to in a number of publications and scientific tasks solved and some other publications [6]. Everything is determined by a wide range of processes across economic and other areas. Knowledge management in logistics with security systems and other programs, for example risk management, therefore becomes a modern and necessary key component of strategic management and also of dynamic development of modern and well-designed intelligent systems of cyber-security in modern society making use of logistics. In preparation of the social system [3] for the stated area of solution, we mainly focus on representation of the professional profile of researchers so that they are able to solve some of the problems associated with the formation of the model and the corresponding processes of modelling real-world systems and their significant surroundings and we sense the essential requirements on the design (especially through their system approach when they design systems) and with the application of creating modern models and with the possibility to model subsystems on the current modelling environment of a computer network, especially on digital computers for secure user environment in the cyberspace of management and of communication of information.

The stated approach to tasks will allow us to solve the present, necessary questions related to logistics, crisis management and risk control in the required electronic automated systems of management and also with the corresponding required basic cyber-safety.

The current conditions for the solution of the stated task are mainly determined by the professionals who have the knowledge of theoretical bases in mathematics, physics, computer science, ICT systems and models and communication (of tasks and specific areas of logistics, including logistics in ICT), system identification, risk analysis and assessment, management and regulation (in the areas of management, crisis management and security systems, information theory, economics (in the areas of microeconomics, macroeconomics), Cybernetics (in particular in the field of cyber-safety).

The current direction of the solution of this task is further subject to the knowledge of new world economy, in particular, of the new concept of process engineering in the world and the use of secure digital information and communication technologies in the new

cyberspace and planning their activities, including crisis management of systems from the perspective of logistics environment.

Competitive environment is therefore the main driving force of contemporary society, and also the environment for new concept of cyber-security as part of the cyberspace of modern society. Cybernetics (as the "*area of management and communication in living and non-living organisms* "- Norbert Wiener, 1946) and in the modern system-defined environment, it is primarily new information technologies, enabling in a virtual environment to find information resources of the world and the necessary knowledge in the newly introduced cyberspace (cyberspace) defined in Act no. 181/2014 Coll. on cyber-security as amended by related laws (Act on cybersecurity). The starting point of the solution is also the application of this Act in the stated modelling and it also lies in increasing a systemically conceived interdisciplinary security in cyberspace and the protection of adequate infrastructure which is important for the functioning of the State and whose violation would led to damage or danger to the interests of the Czech Republic.

3 Metods

Based on information sources [3] of the world, we list some used selected contemporary modern methods for the production of models, including: Systemic approach to the stated chain of cyber-understanding of the new model which was used in accordance with the principles of general systems theory as a concept for thinking, analyzing real world situations, decision making and acting in terms of a complex reality. The systemic approach provided the methodological basis not only for problem-solving, but also enabled them to be dealt with more comprehensively with respect to other aspects that affect it. A systemic view of management brought about more extensive possibilities in particular in understanding the laws of phenomena and processes, and in researching these principles in its entire breadth. It further enables purposeful abstraction from certain factors and later the description of reality by appropriate models.

Systemic approachs OR/MS (Operatinons research/Management science) the modelling process as scientific solutions to complex problems in decision making. The aim of the aproach used was to improve the existing system and the design of a new system which would better fulfil some of the requirements placed on it. Problem formulation was the most important part of the process in the framework of the mentioned system engineering.

Solving the assigned tasks, it was especially strictly enforced that:

- the formulation of the problem is more important than its solution (theoretical basis of the problem solved, the definition of the system) with a practical experience,
- the definition of the system was the next step after formulation of the problem,
- The creation of a model was formed a basis for modelling approach OR/MS.

Generally, the creation of models is dealt with in theory of identification, in which we will use methods known from theory of artificial intelligence. (AI). They are represented by applications stemming from biology (neural networks and genetic algorithms), physics, mathematics and logic (such as technologies modelling and identifying chaos and technologies using fuzzy sets). These technologies form groups based on computer models of task solving with the supply of expert information (expert systems), on inductive learning and so on.

4 Results and discussion

Gradually obtained results of the research are regularly published and one of the most interesting results of modelling is according to [3] for example, this graph obtained as identified behaviour of the system:

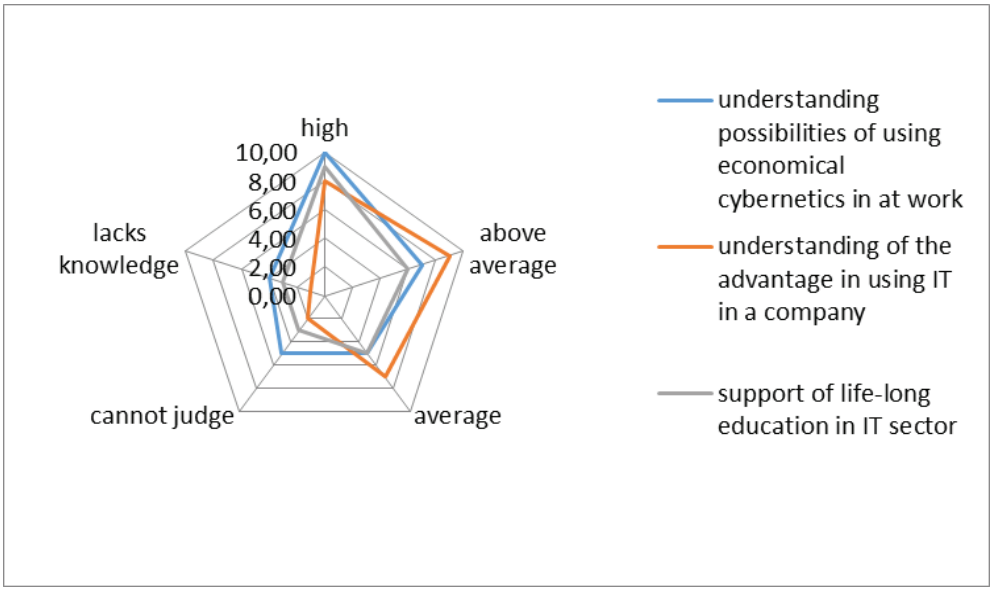

Fig. 1. Assessment of selected models of behaviour in cyberspace of companies. Source: [3]

Based on the detailed analysis of the results obtained by modelling, a comprehensive training program for professionals was created, including the following basic sections:

- System definition of security and protection of information and of communication assets (hardware, software, databases, communications networks, etc.).
- Defining cyberspace for possible recognition of vulnerabilities and identifying security threats.
- Modelling of a cybernetic system for a possible analysis of threat sources, of attacker and of the security attributes of information assets from the perspective of process engineering.
- Possibilities of early systemic detection of cyber attacks and defence against attacks (e.g. cyber-crimes, cyber-bullying, cyber-threats, cyber-terrorism, cyber-espionage, cyber-disinformation, etc.).
- Information sources and work with them in the implementation of legal, economic, technical and logistical standards for theapplicability of cyber security (Cybernetic Law, Information Security Management according to ISO 27000).
- Protecting social and technical system from highly efficient means of modern cyber warfare and from the possibility of new information weapons of mass destruction.
- Preparing the population for efficient use of resources and protection against cyber-attacks and restoration of safe assets in cyberspace and intelligent robotic systems.
- Technical, legal and economic environment in the dynamics of cybespace of the new information and knowledge-based society in the civilized world.

- Development and use of new means of cybernetics and their safety (UAV, robotic lines, 3D printers, modern cryptographic and optoelectronic devices and the use of bionic assets).

4.1 Systemic Process Modelling and Cyber Security

"*The Laboratory of Applied Cybernetics*"(LAKB) is a completely new perspective on solving very promising areas of application of cybernetics in safe environments with recognized and predicted (generated) and possible attacks and a balanced and therefore adequate adaptation of defence to these generated attacks and the resulting need for systemic definition of cyber-security for building (that is especially designing and constructing new and justified by a certain steady state between attack and defence for cyber security of the system). This will be in the near future already part of intelligent systems (with a proportional level of information) and importantly, with systemically conceived cyber-security on the social and artificial, therefore primarily technical level of applied cybernetics. Designing new systems without cyber security (as a background for all new systems) based on current scientific publications will no longer be possible (economically, technically, legally, ...). And so we must already now prepare experts for substantial knowledge and skill in the specific specialization (discipline) and for knowing how to systematically create a model system, model various variants of the reality prepared with its significant environment, how to systematically construct the desired hierarchical system level (appropriate means of hardware and software equipment modelling the environment, for example using appropriate CAD means, and other mathematical projects of promising models for real environments) and also formulate how to build a safe new real systems based on deep theoretical knowledge and knowledge acquired on (virtual) models in new laboratories already for the new knowledge-based society (in addition to information and other foster literacy among professionals, a new perspective on the optimal structure of the system and acquire the knowledge required for a knowledge-based literacy.)

The said proposal of LAKB has not been submitted anywhere in this way and thus has not been introduced into teaching at universities in the field of cyber-security and therefore cannot build on the experience of other departments in the modern area. The dynamics of the changing environment of industry and new promising technologies (not only in production but also in science and other areas related to the management of modern society based on knowledge literacy and new concept of robotics, such as mechatronics, nanotechnology and bionic systems). Thus an over-arching theme of cyber-security will make its projection into the very information and communication technologies (ICT) and lead us to this new view of qualified design of system approach of artificial intelligence for the modelling of cyber-security.

5 Conclusion

The contribution briefly introduces some of the possibilities of the developing principles of cyber-security and of the selected environment for the proposed workplace using artificial intelligence methods already in the design of LAKB.

The aim of the paper is primarily to point experts to the possible systemic definition of the real environment and also to the opportunity to express the environment of artificial intelligence in the newly conceived cyberspace of the modern society; and in the LAKB, such environment may be used as basis for new final theses of students and projects of scientific tasks solved by pedagogical researching staff of the university.

The modern approach is precisely in LABK intertwined cyber-security and interoperability of technical drawing in CAD and in other programs generating the attack

and such conditions for the model and the modelling that would be inappropriate, uneconomical, dangerous to use in socio-technical environment, whereas the defending side needs to explore these inappropriate conditions to succeed through modelling in proving that cyberspace has to be described so as it is safe for use. This environment must above all be mastered by educators and provoke in students rational use of the environment (CAD and other programs) for the stated modelling and inducements of solutions of other variants. Modelling will create such a variety of situations that the qualified teachers must prepare instructions for the use of resources in such laboratories and devise so far only school tasks and later tutorials on "*practical*" but not secret tasks, which have solutions and lead to the validation of theoretical theoretical assumptions of modern design in a safe cyber-environment, and fulfilling the systemic the systemic conception of artificial intelligence for modelling of cyber-security.

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 paper is supported by the research project “From horse-drawn railway to intermodal transport” within Visegrad Fund.

References

1. M. Janková, J. Dvořák, *EBES Conference*, 43-51 (Ekaterinburg: EBES, Russia, 2014)
2. M. Janková, J. Dvořák, M*athematics, Information Technologies and Applied Sciences 2014*, 59-65 (Brno: MITAV, Czech Republic, 2014)
3. M. Janková, *Internetové nástroje pro celoživotní vzdělávání v sektoru IT (Internet Tools for Lifelong Learning on the Field of IT)*, 234 p. (Brno: Technical University in Brno, Faculty of Business and Management, Czech Republic, DDP, 2016).
4. V. Šefčík, J. Konečný, *Procesní inženýrství (Process Engineering), Bezpečné a spolehlivé vedení procesů (Safe and Reliable Process Management)* (Course Reader, Zlín: Tomas Bata University in Zlín, Faculty of Logistics and Crisis Management, Czech Republic, 2013).
5. J. Křupka, *Základy technickej kybernetiky, Liptovský Mikuláš (Basics of technical cybernetics, Liptovsky Mikulas)* (Armed Forces Academy of General M.R. Štefánik, Slovak Republic, 2008)
6. R. Petříková, *Moderní management znalostí (Modern Knowledge Management)* (Prague: Professional Publishing, Czech Republic, 2010)