Transporta un sakaru institūts
Transport and Telecommunication Institute

RESEARCH and TECHNOLOGY – STEP into the FUTURE

Volume 13. No. 4 - 2018

ISSN 1691-2853
ISSN 1691-2861
(On-line: www.tsi.lv)

Riga
2018

THE JOURNAL IS DESIGNED FOR PUBLISHING PAPERS CONCERNING THE FOLLOWING FIELDS OF RESEARCH:

- mathematical and computer modelling
- mathematical methods in natural and engineering sciences
- computer sciences
- aviation and aerospace technologies
- electronics and telecommunication
- telematics and information technologies
- transport and logistics
- economics and management
- social sciences

Articles and review are presented in the journal in English, Russian and Latvian (at the option of authors). This volume is published without publisher editing.

EDITORIAL CORRESPONDENCE

Transporta un sakaru institūts (Transport and Telecommunication Institute)
Lomonosov 1, LV-1019, Riga, Latvia. Phone: (+371)67100594. Fax: (+371)67100535
E-mail: junior@tsi.lv, http:// www.tsi.lv

RESEARCH and TECHNOLOGY – STEP into the FUTURE, 2018, Vol. 13, No 4

ISSN 1691-2853, ISSN 1691-2861 (on-line: www.tsi.lv)

The journal of Transport and Telecommunication Institute (Riga, Latvia)
The journal is being published since 2006

CONTENTS

RESEARCH and TECHNOLOGY – STEP into the FUTURE, 2018, Vol. 13, No. 4, 4
Transport and Telecommunication Institute, Lomonosova 1, Riga, LV-1019, Latvia

PREFACE

We are pleased to present the fourth issue of the "Research and Technology – Step into the Future" journal. This issue includes the papers that were presented in the frame of the 18th International Multidisciplinary Conference of Reliability and Statistics in Transportation and Communication (RelStat-18) which was organized 17-20 October 2018, Riga, Latvia.

In the fourth issue of the journal 5 papers of 10 researchers from Hungary and Poland are presented. We would like to thank all who kindly contributed their papers for this issue.

Professor, Dr.Sc.Eng. Irina Yatskiv (Jackiva)

RESEARCH and TECHNOLOGY – STEP into the FUTURE, 2018, Vol. 13, No. 4, 5-9
Transport and Telecommunication Institute, Lomonosova 1, Riga, LV-1019, Latvia

HOW LOGISTICS IS CONNECTED TO INDUSTRY 4.0

Béla Illés [1] and János Végh [2]

[1] University of Miskolc,
H-3515 Miskolc-Egyetemváros, Hungary
altilles@uni-miskolc.hu

[2] University of Miskolc,
H-3515 Miskolc-Egyetemváros, Hungary
j.vegh@uni-miskolc.hu

The twentieth century enabled the explosion-like development of the „unlimited" moving of things. One of the preconditions of that development was the appearance of intelligent devices and systems in the field of logistics. The base of the approach called Industry 4.0 is digitization, that resulted in a paradigm change also in the activities related to logistic processes. The appearance of advanced cyber-physical systems, utilizing advances of information technology and new software methods highlight even more the role of logistics in forming the trends of indicators of competitiveness on the market. The different processes develop in direction of being networked, using real-time automation.

Keywords: logistics, Industry 4.0, digitization, paradigm change, possibilities, trends

1. Introduction

The twentieth century has created (or at least enormously widened) the possibilities of mobility for the persons and has turned the World into a „big village". The twenty first century (or at least its very beginning) has created the possibility of explosion-like rising of mobility of things through utilizing different intelligent devices and systems in the field of logistics. Those systems and devices, based on the facilities of digitized solutions, lead to a paradigm change called Industry 4.0 which covers a revolutionary change in the field of logistic activities. Today the formerly separated activities of manufacturing and logistics (including design, operation, development and controlling) become strongly biased, resulting revolutionary changes in all related fields, so correspondingly also Logistics 4.0 shined up. The postfixes "4.0" in those activity fields cover a new type of approach and operation on those fields, utilizing the possibilities provided by the digitization (Digitalisierte Supply Chains, 2015).

2. Main aspects of the paradigm change "Industry 4.0"

In the operation of the manufacturing and logistics systems initially the centrally controlled systems were preferred. As the result of the development of informatics and information technology the next stage was utilizing systems with hierarchical design and distributed intelligence. The today's digitization and utilization of cyber-physical systems result in decentralized, self-organizing operation of the logistic systems.

The today's tendency is that the former deterministic, hierarchical, complex logistical systems are more and more replaced by more or less stochastic operating algorithms utilizing some basis information set, underpinned/supported by real-time simulation results. Correspondingly, the model of the reality based on deterministic data has been replaced by the cooperation of self-organizing autonomous elements, based on probabilities resulted by real-time simulations. Similarly, the creating of the supply- and value-producing chains the organization based on deterministic data are replaced by ad-hoc organized networked systems, also based on real-time simulation. In the value-producing chains network of autonomous self-

organizing production units are formed in place of pre-installed, deterministic ones. Completely self-organizing systems based on different modules are preferred rather than pre-designed production/manufacturing systems (Logistik 4.0, 2017).

The work pieces, products, logistic devices handled in the manufacturing process turn to active elements of the manufacturing and logistic processes from their former passive state. The self-organizing intelligent logistic devices, work pieces and products will be handled in the self-organizing manufacturing processes. The working time and the number of co-workers will be handled in a flexible way, based on the availability dates, fields of experience. The strict separation of co-workers based on their professional knowledge will be cancelled. The required professional experience will be defined by the tasks to be executed, and the experience might have relations to different fields. The activities with predefined scheduling will continuously shifted towards systems providing maximum flexibility.

3. Implementing the possibilities of Industry 4.0 in logistics

Handling „things" through the Internet, the Industry 4.0 became for today the reality that has its technical implementation facilities. The cyber-physical systems enable to implement optimal process handling of manufacturing and commerce through selecting the proper target functions, quality assurance as customers need it, the proper lead time, expenses, etc. based on utilizing sensors, empirical results of real-time simulations, see Figure 1.

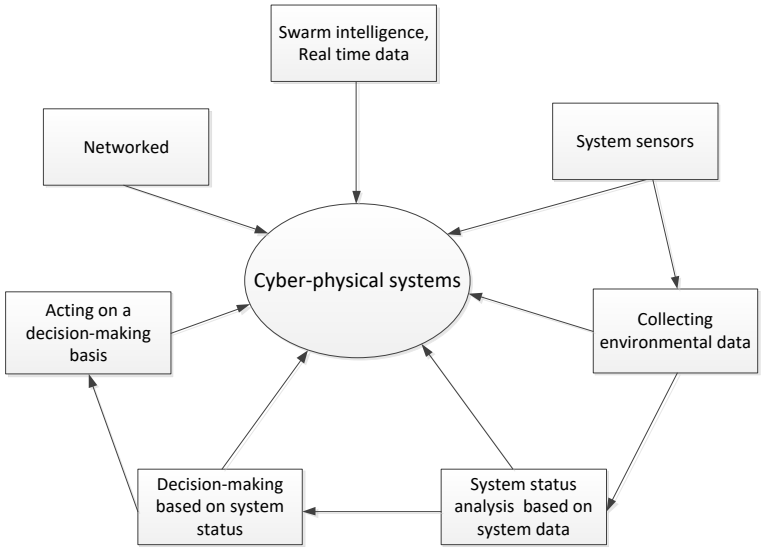

Figure 1. Cyber-physical systems

The cyber-physical systems are able to acquire and evaluate a lot of information about the products, and even they are able to infer conclusions about the way of implementing the remained part of processes.

The intelligent logistic devices – like devices for creating the unit delivery load, intelligent storage, intelligent autonomous delivery vehicles, intelligent packing devices, etc. – are able to handle the actual data describing the status of the device and/or the product they are working with. Based on those data, they create a picture about the instantaneous reality and even (utilizing real-time simulation programs) they forecast the possible future states. Using the provided target functions, they are able to make decisions, and to choose further states of the system.

The intelligent logistic devices and systems are able to operate in an optimal, self-organizing regime in making decisions, with excluding the human. At the same time, it is surely an issue to provide the proper electric power for the sensors, displays, etc. in the system, as well

as storing the energy for the mobile devices. These issues and challenges in the fields of both expenses and technical solutions can be managed, the problems in connection with providing energy for the individual devices can be mitigated. The physical sizes and the expenses of the energy storage devices are decreasing while the energy they can store increases. Provided that solar energy could be used in some form for charging the energy storage cells of those devices, a further revolutionary change could be triggered.

It is getting more and more harder to handle the huge amount of data in connection with (and produced by) the dynamic, complex, autonomous production and logistic systems. This is why building logistic systems from independent, autonomous building blocks needs special care: one must consider the actual informatics infrastructure, and also data filtering (what data have importance for the other building blocks or layers) has growing importance.

The reality of handling the things through the Internet as well as the Industry 4.0 required constructing new business/marketing models, too, with the main characteristics like:

- the tendency of developments towards hybrid services due to logistics and mobility;
- the software and information technology become the strategic resources of the different indicators of competitiveness in applying business-logistic models;
- the principle „if there are no new IT applications in the field of logistics then there is no new business in the field" also orients the developments towards hybrid mobile logistic services;
- the „things" connected to the internet seems to increase exponentially, and the number of such devices may approach 50 billion around 2020;
- the "Internet of Things" provides a solid platform for the implementation and enables the exponential growth of the networking in the field of logistics, which actually forms the basis of the 4th industrial revolution.

4. Current trends in logistics

The logistics, as the field of science dealing with transporting goods and information, plays and important role on the different fields (like industry, service, health industry, etc.) of the economy. The role of logistics is not confined to the operation of the logistic systems, rather includes their development, control, verification, etc. (Illés *et al*., 20097). In order to consider the most important logistic trends for more fields and activities, one needs to consider the aspects shown in Figure 2.

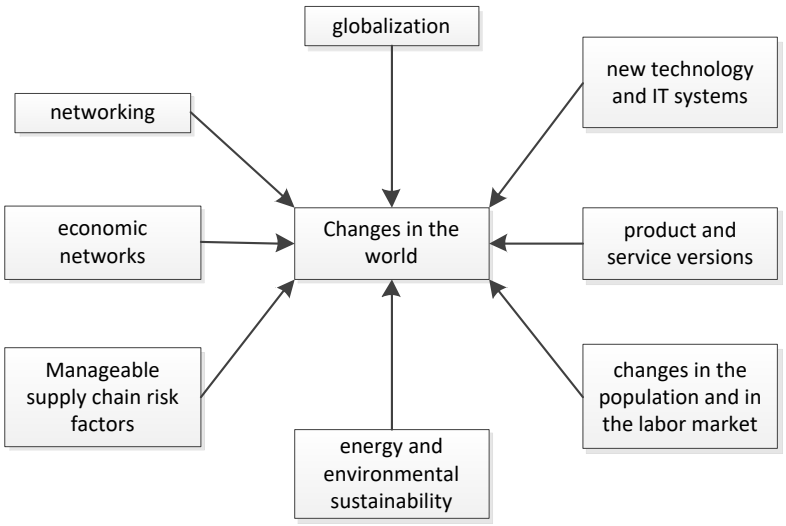

Figure 2. The most important parameters affecting the logistics trends in the world

The changes experienced in the field of logistics basically manifest in handling the complexity of the logistic systems (and also in the expenses of such systems!). The complexity of the logistic systems grows continuously. The handling of those complex systems is based on recognizing the dominant processes, enabling their transparency, forming the optimal complex structures and systems with high levels of automation.

The transparency and automation on one side and the complexity on the other side are conflicting points of view to be considered, because the more complex a system is, the less transparent it is and at the same time it is more hard to automate. The development of the digitization and the networking defines different trends, in the field of logistics, too; for some examples see Figure 3.

Network / Process	Digitization	Standard information exchange	Integrated information handling	Joining integrated information handling
Complex supply chain process	X	X	X	X
Supply chain process	X	X	X	
Provider process	X	X	X	
Manufacturing process	X	X		
Technological process	X	X		
Workplace process	X			

Figure 3. the connection between the different processes and levels of developments of networking

As seen in Figure 3, the more complex systems presuppose the more advanced networking. It can also be concluded, that digitization is a precondition to handle the processes at any level. A different question is, of course, that the digitization technologies also have their own level of development, which provide different possibilities for the material- and information transfer (logistical) systems (Illés, 2017). The levels can be like:

- data exchange using EDI links,
- automatized data exchange links in connection with the activity of the material and information transfer system,
- links between data sets based on cyber-physical systems and real-time simulation methods.

The trends of the development presented above can be utilized in any fields of logistic processes, including the case of providing-manufacturing-distributing-recycling. It should also be emphasized that although the approach *Industry 4.0* is utilized in close connection with the activities in manufacturing and logistics, the trend will soon extend to the different fields of services. For example, in Germany exist already the approaches *Hospital logistics 4.0* and *Other services 4.0.*

5. The possibilities provided by the trends of development of logistics in course of logistic activities

The following (incomplete) list mentions just a few possibilities provided by the trends of development of logistics:

- autonomous logistic systems based on cyber-physical systems;

- intelligent, managed goods in the manufacturing and logistic processes (automatic communication between goods and logistic devices);
- creating networks consumer-provider-manufacturer in the global supply chains;
- utilizing global transfer data sets, data evaluation, data analysis;
- digitized supply chain data for the logistic management (paths, stores, customs, traffic, weather, etc.);
- storing and recalling data of the technical solutions;
- integrating real-time data;
- mitigating risk factors, data security/protection, the 24/7 availability of IT infrastructure;
- logistic data bases, optimizing logistic processes;
- digitization penetrates all fields of industry and logistics.

Despite all of this, the human remains in focus: everything happens in the interest of the human.

6. Summary

The Industry 4.0 is inseparable from logistics, because the manufacturing and the technological activities cannot be executed without making materials- and information transfer. The Industry 4.0 is a revolutionary new approach based on the facilities provided by the digitization, which depends on the actual stage of development of the IT. More and more possibilities open for more and more complex manufacturing and logistic networks, human-machine and autonomous networked systems are utilized. With storing the data in cloud storage the individual needs of customers, the needs of the commerce/production/services can be jointly handled and optimized.

Of course, one faces also problems when utilizing such systems, for example data security, the sufficient amount of data that still can be handled by the available IT infrastructure, the question of sustainable development. The approach Industry 4.0 surely will considerably transform the methods of application of humans as well. However, the central role of human remains in connection with the development/controlling/handling of those complex logistic systems.

Acknowledgment

“This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 691942”.

References

1. Digitalisierte Supply Chains – Basis zukünftiger Geschäftsmodelle: Andreas Reutter, 2015.09.08, 33. Dortmunder Gespräche, Dortmund.
2. Illés, B., Glistau, E., Machado, N. I. C. (2007) Logistik und Qualitätsmanagement, Miskolc, ISBN 978-963- 87738-1- 4
3. Illés, B. (2017) Logistics and digitalization: Logistics yearbook, pp. 31-36, ISSN 1218-3849
4. Logistik 4.0 – Es geht Ums Ganze: Michael ten Hompel, 2017.11.30, “Cooperation possibilities between centres of excellence in logistics” international conference, Budapest.

RESEARCH and TECHNOLOGY – STEP into the FUTURE, 2018, Vol. 13, No. 4, 10-17
Transport and Telecommunication Institute, Lomonosova 1, Riga, LV-1019, Latvia

SAFETY PROBLEMS IN THE IMPLEMENTATION OF PAYING TRANSACTIONS WITHOUT CASH

Robert Maciejczyk [1] and Natalia Moch [2]

[1] The Jacob of Paradies University,
Teatralna 25, 66-400 Gorzów Wielkopolski, Poland
[2] Military University of Technology,
Gen. Witolda Urbanowicza 2, 00-908 Warsaw, Poland
[1] rmaciejczyk@interia.eu
[2] natalia.moch@wat.edu.pl

The study will present a problem related to the protection of banking systems resulting from the protection of electronic means of payment. Main problem with protection of transactions made with the use of payment cards, online banking or use ATMs is due from threats in the banking area system and the way, which our important data are transmitted over the network.

This work will present the rights and obligations of the bank's service provider in ensuring the security of his clients in the area of electronic banking. Threats of users: payment cards, internet banking and ATMs, result from the desire to unauthorized and criminal gain financial resources.

Crimes against payment means are strictly related to offenses punishable in the Polish criminal code, containing among others falsification of documents, identity theft and false testimony.

The issue will include a description of system solutions that banks introduce to protect their clients and it will show the rights of law enforcement services in the event of a criminal act. In addition, this text is intended to indicate the manner in which the service provider is obliged to provide the investigators with electronic evidence in the area of the criminal offense against the means of payment.

The study will constitute a description of the tasks (including securing evidence of crime) in the process of detecting perpetrators of crimes against means of payment, in the system of cooperation between the service provider and the bank with law enforcement services, with fully protecting the rights of bank clients. The main research method is studies of literature sources.

Keywords: crime; legal tenders; detection process; security of the bank client

Introduction

At a time when payment methods, such as printed banknotes and minted coins, are successively thrown out by modern payment methods, using the Internet or a smartphone, the security of these transactions becomes one of the overriding objectives in protecting property belonging to bank customers (Maciejczyk, 2017). Issues related to the protection of transactions made with the use of payment cards, online banking or services offered by the ATM is the result of threats to banking systems and data transmission networks.

The aim of the article is to present the cooperation of banks with law enforcement authorities in the situation of a criminal event in the area of electronic means of payment. The research question, is as follows: is the system of cooperation between the bank and law enforcement agencies sufficient for proper protection of evidence of committing a crime on electronic means of payment?

The study will constitute a description of the tasks (including securing evidence of crime) in the process of detecting perpetrators of crimes against means of payment, in the system of cooperation between the service provider and the bank with law enforcement services, with fully protecting the rights of bank clients. The main research method is studies of literature sources.

1. Formal and legal aspects of electronic banking

By definitions, the institutions providing electronic financial services are banks. The Polish legislator defines very precisely all rights and obligations of both, the bank and its clients. In addition, the banking market is controlled by an independent institution - the Polish Financial Supervision Authority. The National Bank of Poland also is influential in functioning of the banks on Polish financial market. After Poland's accession to the European Union, its organs also determine the banking market through issued regulations, directives and decisions.

The legal basis for the operation of banks in Poland is the Banking Law Act. The Polish law obliges banks to ensuring the safety of conducting operations to the holder of account, with due diligence and using the appropriate technical solutions. This applies to both the provisions on the protection of personal data, and the obligation to maintain banking secrecy. The bank, providing services under an electronic banking agreement is obliged to: provide the holder with safety of operations, with due diligence and using appropriate technical solutions; provide the holder with information about transactions made and payments made, and fees and commissions collected, on dates and in the manner specified in the contract; inform immediately about the refusal or inability to perform the ordered operation for reasons beyond the bank's control. In addition, issues related to the security of information systems used to collect and process data, including the online banking system, are protected by the law of the Ministry of Internal Affairs.

Another authority regulating the functioning of banks and having an impact on ensuring the security of transactions in the area of electronic banking is the Polish Financial Supervision Authority (pl. Komisja Nadzoru Finansowego - KNF), which is the central government administration body, exercising supervision over the Polish financial market. In accordance with the Act, the tasks of the KNF include, among others, supervision over the banking sector, capital market, insurance and pension market, supervision over payment institutions and payment services offices, electronic money institutions and the co-operative box sector; taking actions to ensure the proper functioning of the financial, insurance and pension market. The KNF carries out its tasks, among others by publishing relevant documents, the so-called recommendations. With regard to ensuring security in the area of electronic banking, KFN issued a resolution recommending the unification of the scope of minimum requirements for the security of internet payments in connection with the provision of payment services offered by banks, domestic payment institutions, national electronic money institutions, and cooperative savings and credit unions. This resolution - recommendations obliges banks to increase the security standards and maintain the ICT infrastructure at a sufficiently high level.

The legal acts issued by the European Parliament and the Council also have an impact on the functioning of the banking services market, including electronic banking. The most current document on this issue is Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market. Member States were required to adopt and publish the laws, regulations and administrative provisions necessary for its implementation.

The need to introduce new regulations in the area of payment services is dictated first of all by the emergence of technical innovations resulting in an intensive increase in the number of electronic payments, and payments made via portable devices, and the emergence of new types of payment services on the market. Significant areas of the payments market, in particular payments made using cards, via the Internet and via portable devices, remain within the competence of individual countries. The primary goal of the Directive is further harmonization of the national laws in the area of payment services. This is to be achieved, among others by clarifying and extending the legal framework defining the rules for the provision of payment services and adapting the payment services market to new technical solutions and new technologies. In order to enable the provision of payment services by new categories of entities, i.e. TPP, the Directive introduces new elements of protective regulation - in particular those related to the new competition rules - and stresses the requirements for the safety of service provision by these entities, especially in the area of ensuring appropriate safety standards for consumers.

2. The tasks of banks in ensuring the security of electronic banking transactions

Banks offering electronic banking services, and in particular online banking, are required to implement effective mechanisms to ensure a high level of security of transactions. Due to the scale of existing threats, it is necessary to secure both communication between the client and the bank, the bank's information system, as well as the client's computer against possible damage, attacks, scams, etc. Leaving even the smallest gap in the security system can be used to commit a crime. To prevent this, various types of cryptographic, hardware, software and, increasingly, biometric solutions are used, which allows to protect against existing dangers, to a greater or lesser extent.

2.1. Security of transactions made with payment cards

In order to increase the security of transactions using payment cards without their physical presentation (transactions carried out via the Internet), new methods of accepting these cards have been introduced, based on 3D Secure technology. The name comes from the Three Domain (three sectors responsible for the card transaction). The individual card market operators offer their services in line with the above-mentioned technology: Visa applied 'Verified by Visa', while MasterCard introduced the SPA (Secure Payment Application). 3D Secure operation is based on additional transaction confirmation with a one-time password provided by the bank that issued the given card. On the practical side, such a transaction is carried out similarly to the 'classic' payment made via the Internet by means of a payment card, i.e. after entering the card number and the holder's data, this information is transferred to the settlement centre. At this point, there is an additional connection from such a centre to the bank issuing the card to check whether 3D Secure technology is supported. A positive result results in displaying a window to the user asking for the password confirming the given transaction. If the entered password is correct, the bank in the next step sends the consent for the transaction to the billing centre. An additional security implemented in 3D Secure is the ability for the customer to define an individual message, known only by its author, which will be displayed with a request for a password confirming the transaction. In this way, potential attempts to spoof the bank's site are much more difficult.

2.2. Security of transactions made with the use of ATMs and POS terminals

Taking into account the number of crimes carried out with the use of stolen cards and the growing number of skimming cases, banks are trying to increase the security of non-cash transactions carried out at ATMs and at retail and service outlets. In the case of ATMs, one of the basic activities is the installation of anti-skimmers. They are designed to make it difficult to attach an overlay containing a skimmer, thus making it impossible to read the magnetic strip of the card. Card readers have unusual shapes. They are equipped with a separate backlight etc. The ATMs are marked accordingly so that the customer using them can pay attention to any differences or irregularities that could suggest that the ATM has become the target of criminals.

The biggest change in ensuring the security of this type of transaction is due to popular use of cards with a special chip as a carrier of information, i.e. cards in EMV technology. The name EMV is an acronym from the first letters of the names of payment organizations, which initiated the development and implementation of this standard on the market, i.e. Europay, Mastercard, Visa. If you use a payment card with a chip, the risk of skimming is minimal. Data stored on the microprocessor placed in the card can be read only by a special reader. The chip fulfils 3 key tasks: permanent storage of information; the ability to perform calculations; secure storage of information along with the possibility of encryption.

Transactions using biometric technologies are introduced more and more frequently to authenticate transactions. They may be based on various features - mainly physical ones, e.g. fingerprints, iris of the eye, retina of the eye, hand blood vessels or articulation, hand shape, bend shape of the hand, ear shape, face, temperature distribution on the face etc. These

technologies are still developing and there are proposals for new ways to use biometrics in electronic banking. However, they are not yet so widespread that it is possible to conduct a factual analysis of potential risks related to the threat of breaking such safeguards.

2.3. Security of transactions made via online banking

The security of communication in online banking means ensuring the integrity of data sent over the Internet and preventing the unauthorized persons from reading confidential information. Finally, secure data exchange is a situation in which the identity of the parties participating in it does not create any doubts. Various cryptographic methods and their modifications allows the assurance of communication understood in this way. The length of the key used determines how easy it is to break a given cipher. There are two encryption methods (Ryznar, 1998): symmetric encryption and asymmetric encryption. Symmetric cryptography (secret key cryptography) is based on encrypting and decrypting data using the same key. The most popular algorithm of this type is DES (Data Encryption Standard) and numerous modifications, such as triple-DES. Asymmetric cryptography (public key cryptography) uses two types of interrelated keys - private and public. The most common asymmetric algorithm is RSA with variable key length. The described methods of data transmission encryption are used in many solutions, ranging from internet banking, to communication with ATMs, and service and commercial outlets using payment terminals (payment card transactions). Perhaps the most popular implementation based on cryptography is the SSL (Secure Sockets Layer) protocol. The use of SSL for transaction encryption is already accepted as the standard on the payment and banking services market. It allows to meet the requirements included in the legal provisions to ensure the security of transactions.

An equally important element ensuring the security of transactions carried out via online banking is the authentication of the transactions themselves. Most of the banks have implemented a two-level authentication system. In the first place it is logging in to the bank's website using the ID and password. The second level of security is required to carry out banking operations, including mainly transfers to accounts that have not been previously defined. A double level of authentication seems to be sufficient from a security point of view. However, a necessary condition is its proper application and preservation of basic safety rules (Maćkowiak, 2007).

The current law imposes numerous requirements on banks to ensure the security of transactions, including transactions via electronic banking. They concern both the operational and, above all, technical aspects. As can be seen above, while for transactions made with the participation of external institutions (payments made with the use of a payment card), which somehow imposed the operating model, one can speak of a standard operating on the market, in the methods used by banks to secure transactions carried out via online banking is huge diversity. For this reason, it is necessary to cooperate between all entities involved in the process of electronic transactions and building the awareness of the users themselves. Further technological advances will probably allow for widening the catalog of applied security. Currently, Poland is one of the fastest growing markets in this respect. Hence, there are more and more crimes committed in the area of electronic banking (Maciejczyk, 2017). This results in the need for the bank to cooperate with the services, which due to the specific nature of this type of criminal activity requires a different approach to the issue of providing evidence, or sharing information covered by banking secrecy.

3. Cooperation between bank and services in the detection process

Detection activities and obtaining evidence of committing crimes in the area of electronic banking are based on the traditional assumption that every event taking place in the surrounding outside world, including every human activity, leaves some traces. This means that such traces should be sought, in particular, on the spot or on the participants of a given incident and on objects located there. They can be the basis for demonstrating the presence of specific people at

the scene of the event or the agency of a specific person or persons. Crimes related to electronic banking constitute a specific category of prohibited acts based on non-cash payments and electronic data processing. The specificity of the electronic banking environment determines the nature of the traces of criminal activity. This means that traces in the traditional sense of the word are in a limited range / quantity, while the traces in electronic records are of key importance.

3.1. Electronic evidence and their specificity in the area of electronic banking

The electronic evidence is information stored or sent in an electronic form of evidential significance, that is an information stored on a medium, a computer document, digital data. Due to the specific features of electronic evidence and given the fact that electronic evidence will play an increasingly important role due to the growing number of crimes that leave electronic traces, it is necessary to discuss the features of electronic evidence and related evidence difficulties, as well as the issue of rules of conduct with electronic evidence at the stage of obtaining, protecting, analysing and storing them, to ensure the possibility of their subsequent use before a court in criminal proceedings, in order to prove the commission of an offense and the fault of the offender (Górnisiewicz, 2014).

The specificity of crimes in electronic banking, and in particular online banking, consists in separating the place of residence (act) of the perpetrator from the place where the effect of his criminal activity occurred. To commit a crime in the area of electronic banking, the physical presence of the perpetrator at the place where he was committed is not required. It is possible to run the program remotely by the perpetrator. In the context of the global reach of the Internet, it is considered a cross-border crime, which additionally hinders conducting detection activities. These forces establish cooperation between the authorities of individual states, sometimes located in different parts of the world, and function according to a different legal culture. These issues have been regulated in a significant way - for crimes committed within the European Union - in the Council of Europe Convention on Cybercrime of November 23, 2001.

In the case of committing a crime with the Internet, it is in vain to look for traces of identification left by the perpetrator, such as handwritten letters, biological traces or fingerprints. It should be noted that using the Internet does not mean total anonymity, at least when it comes to the identification of the device, e.g. a computer that the perpetrator used by committing a crime via the Internet, or the place where he was at the time of the offense. Each device connected to the network has a unique address called IP (Internet Protocol) address. The IP address is not permanently assigned to the user but is assigned each time when connecting to the Internet network for the time of the person's stay on the network. This temporary uniqueness of the IP address assigned during a specific connection to the Internet in connection with the exact determination of the time (date and time of using this IP) allows to uniquely identify the device (e.g. a computer) on the Internet. In this way, by identifying the location of the computer it is possible to identify the place from which it was operated. On this basis, it is also possible to obtain information about specific websites that were visited at a given time and to determine the content of files sent (Górnisiewicz, 2014).

Information data of the IP address assigned to a given computer at a given time is collected in digital logs. For digital logs to be used as evidence in criminal proceedings, they must meet conditions that allow them to be considered as integral and irrefutable evidence. When assessing the evidential value of digital logs, particular attention should be paid to the susceptibility of logs to modification and preparation, resulting from the fact that logs are stored on re-writable media, which gives practically unlimited possibility of interfering with their content. It is important to bear in mind the circumstantial nature of the proof mentioned above and the fact that it is not possible in each case to automatically combine the IP address of a computer with its user and, consequently, to assign him a claim on that basis.

The digital log cannot be used as evidence if it identifies the IP address of the computer used by the perpetrator to commit crimes on the network, using malicious software installed on

the computer of another user to take control of the infected computer, which is usually not known to the computer user, which impersonates a real perpetrator committing criminal behaviour to an "account" unaware of these user activities (Górnisiewicz, 2014). Law enforcement authorities should in any case examine a computer whose IP address was contained in digital logs from a computer where the burglary took place. In the case of finding the presence of the aforementioned software that allows taking control over a compromised computer, the proof from digital logs will be useless from the point of view of the possibility of using it in proceedings before the judicial authorities (Kliś, Stella-Stawiczki, 2001). Likewise, it will be useless for ongoing proceedings if the IP address indicates the use of a computer located in an Internet cafe, where everyone has free access to a computer without registration, which makes it impossible to identify the perpetrator.

Therefore, excluding situations such as: masking actions, using a computer of another person without her knowledge, using an internet cafe (where you can use computers without having to register anything, which makes it impossible to identify the perpetrator) or impersonate another user of the network with the use of malicious software (when it will not be possible to release digital logs as evidence in criminal proceedings) in other cases, provided that the digital log is secured correctly, the digital log identifying the computer's IP address may serve as circumstantial evidence indicating the user's indirectly identified behaviour IP address. A caveat is the fact that indirectly the perpetration of a specific person may result. In connection with other evidence and circumstantial evidence, the probability of showing who was behind the keyboard during the period under consideration increases. Other evidence is, for example, establishing on the basis of personal sources of evidence that only a user could use the computer at a certain time or that no one else has access to the computer outside the user. The hint may also be the lack of alibi of the user of the computer from which the attack took place. It should be emphasized that the specific features of electronic evidence mentioned above determine the way of conducting the evidential process (Górnisiewicz, 2014).

First of all, it is important to ensure participation in activities related to the search, protection and consolidation of electronic evidence of persons (experts) who have specialized knowledge of the operation of hardware and computer systems and information technology. In addition, criminal programs often have a built-in self-destructing procedure that starts automatically after a specific task is completed. However, it should be added that the advantage of electronic evidence is that it is difficult to destroy them definitively in such a way that there is no trace left in the electronic data carrier. It is possible to restore them using dedicated computer programs for this purpose, such as EasyRecovery, which allows you to recover lost or deleted data, files, folders. Deleting data using the "delete" command does not mean immediate destruction, but only loss of the access path.

Another very important issue is the protection, preservation and storage of electronic evidence. In practice, the procedural bodies and computer forensics should pay special attention to rules of proceeding with the evidence, such as: making copies of the information carrier; securing the obtained electronic evidence with an investigative program in order to demonstrate in court proceedings that the evidence was delivered to the court in an unchanged and complete form; data authentication of the checksum; the data should additionally be photographed with a full description of the way of evidence, with the date, time, person who was responsible for the evidence at the particular time, and the place of storage in order to show that the evidence provided to the court arrived in the unchanged and complete form, so it is reliable; use of evidence in the form of an expert opinion with the specialty in the field of information technology, in particular for the analysis of secured data; participation of specialists in law enforcement activities related to the process of gathering evidence at each of its stages, in particular when securing electronic traces during data retention and search operations, including participating in the search of system resources, copying data; the evidence should have the following features: is legal, authentic, complete, accurate, persuasive; the procedures for securing evidence should provide evidence of protection against damage, destruction or any other interference aimed at their inviolability and integrity, which would have the effect of

calling into question their credibility; all data collected on a computer storage medium are subject to analysis, including hidden data, deleted data, copies of files along with logs and registers; activities related to the collection of electronic data must not violate statutory confidentiality provisions; use of a forensic experiment in order to recreate the course of an event carrying out the characteristics of a crime in electronic banking.

3.2. The role of banks in providing evidence

For effective prevention of offenses specified in art. 19 para. 1 of the Police Act or their detection or determination of perpetrators and obtaining evidence Police may use information processed by banks, which constitute bank secrecy. This information is subject to the protection provided for in the regulations on protection of classified information and may be made available only to policemen conducting activities in a given case and their superior, entitled to exercise supervision over the operational and reconnaissance activities conducted by them in this matter.

According to art. 104 of the Banking Law Act, bank employees and financial intermediaries cooperating with banks are obliged to maintain banking secrecy, which covers all information regarding banking operations. According to art. 105 par. 5 of the Banking Law Act, the bank is liable for damages resulting from the disclosure of banking secrecy and misuse thereof. However, according to art. 105 par. 6, the bank is not liable for damage resulting from the disclosure of bank secrecy by persons and institutions authorized to request banks to provide information constituting a banking secret. Such institutions include, but are not limited to, courts, the police, the prosecutor's office, court bailiffs, tax offices and fiscal control offices, and The Polish Social Insurance Institution.

In the case of a justified suspicion that a crime has been committed, the bank is obliged to notify the prosecutor, the Police or other competent body authorized to conduct the pre-trial investigation. In the case of revealing criminal behaviour, the obligation to notify the prosecutor or the Police is not only about employees of domestic banks, but also at employees of foreign banks based in Poland, as well as employees of credit institutions that carry out banking operations in Polish branch offices.

When submitting such a notification, the bank has the right to provide information constituting bank secrecy to the public prosecutor, the Police or another competent authority that is authorized to conduct the pre-trial investigation. In such a situation, the prosecutor does not have to apply to the district court to revoke this secrecy. The bank's provision of information covered by secrecy must be directly related to the submitted notification or its supplementation. Because the bank is a provider of services that make up the broadly defined electronic banking, it is also the data controller and - usually - the owner of the infrastructure used to provide these services. This means that it is probably in possession of electronic records that may contain traces of committed crimes that can be used as evidence.

As is clear from the above, in the case of a crime in the area of electronic banking, the protection of electronic traces is crucial. In this case, the role of the bank, which as a service provider and having the necessary software and infrastructure, can collect all information on the activity of users of individual electronic banking channels on an ongoing basis, is considerable. Legal provisions clearly define the obligations of banks in the collection and storage of this type of information.

4. Conclusions

According to the security policy generally accepted by service providers (banks), the protection system is as strong as its weakest element. Therefore, even the seemingly least important component of the system should be created with the greatest accuracy and attention, and then thoroughly checked.

Due to the threats associated with the use of banking services through electronic channels, there are many regulations that impose on banks requirements for ensuring security for such transactions. It is worth noting that we are talking here not only about strictly national regulations, but also those covering Poland as a member of the European Union. In the light of the existing regulations, banks and other institutions involved in the transaction are required to ensure the security of operations performed by their clients on both the operational and technical side. A multitude of potential solutions implemented by banks and operators makes it difficult to commit a crime.

As it has been emphasized, the overwhelming majority of crimes committed in the area of electronic banking is committed "at a distance". In this case, there are no classic traces that can be secured and presented as evidence in court. Electronic traces are becoming crucial at this time. Due to their specificity, and in particular ease of their modification, an appropriate approach must be applied, as well as the use of specialist knowledge, skills and tools.

The most important and always actual issue, is the form of cooperation between banks and the law enforcement agencies. As a public trust institution operating under the Banking Law Act, the Bank is obliged to maintain banking secrecy. This means that all information, including electronic traces, can be made available to law enforcement authorities only in the circumstances defined in the applicable regulations. In the case of an offense in the area of electronic banking, the protection of electronic traces is crucial. The main role in this area is played by the bank, which, being a service provider with the necessary software and infrastructure, can collect all information on an ongoing basis.

References

1. *Directive (EU)* 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC. OJ L 337, 23.12.2015, p. 35–127.
2. Górnisiewicz, M. (2014) Bezpieczeństwo finansowe w bankowości elektronicznej – przestępstwa finansowe związane z bankowością elektroniczną, pp. 43-46, KNF, Warszawa.
3. Kliś, M., Stella-Sawicki, A. (2001) Identyfikacja użytkownika komputera na podstawie logów cyfrowych, In: *Prokuratura i Prawo* No 7-8, pp. 51-62.
4. Maciejczyk, R. (2017) Bankowość elektroniczna – zagrożenia. In: *Kwartalnik Policyjny*, No 4(43)/2017, pp. 29-44.
5. Maćkowiak, K. (2007) Bankowość elektroniczna – korzyści i zagrożenia, In: *Boston IT Security Review*, No 4, p. 15.
6. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. 2004 Nr 100, poz. 1024 ze zm.).
7. Ryznar, Z. (1998) *Informatyka bankowa*. p. 122, Wydawnictwo Wyższej Szkoły Bankowej, Poznań.
8. Uchwała nr 584/2015 Komisji Nadzoru Finansowego z dnia 17 listopada 2015 r. w sprawie wydania Rekomendacji dotyczącej bezpieczeństwa transakcji płatniczych wykonywanych w Internecie przez banki, krajowe instytucje płatnicze, krajowe instytucje pieniądza elektronicznego i spółdzielcze kasy oszczędnościowo-kredytowe.
9. Ustawa z dnia 21 lipca 2006 o nadzorze nad rynkiem finansowym (tj. Dz.U. z 2018 r. poz. 621).
10. Ustawa z dnia 29 sierpnia 1997 r. – Prawo bankowe (Dz.U. z 2017 r. poz. 1876, ze zm.).
11. Ustawa z dnia 6 kwietnia 1990 r. o Policji (Dz.U. z 2017 r. poz. 2067).

RESEARCH and TECHNOLOGY – STEP into the FUTURE, 2018, Vol. 13, No. 4, 18-26
Transport and Telecommunication Institute, Lomonosova 1, Riga, LV-1019, Latvia

RISK MANAGEMENT IN CRISIS MANAGEMENT PROCESS

Natalia Moch [1] and Robert Maciejczyk [2]

[1] Military University of Technology,
Gen. Witolda Urbanowicza 2, 00-908 Warsaw, Poland
[2] The Jacob of Paradies University
Teatralna 25, 66-400 Gorzów Wielkopolski, Poland.
[1] natalia.moch@wat.edu.pl
[2] rmaciejczyk@interia.eu

The crisis management involves prevention of crisis situations, preparation to control threats by means of planned actions, reaction to emerging threats, removal of the crisis consequences, and reconstruction of resources and infrastructure. In the context of the presented definition, risk management is an action aimed particularly at threat preventions and reduction of its negative effects to an acceptable level, through pre-planned activities. The one of the most important aspects of threats prevention are: identification, analysis and assessment of the risk of potential events, that may contribute to the emergence of a crisis situation.

The aim of the article is to present the role of risk management in the crisis management process. The article presents the definition of threats, selected methods for its identification, analysis, and evaluation. It refers to categories of critical threats, with particular emphasis on threats to people, property and the environment. The article presents the definition of threats, selected methods for their identification, analysis and evaluation. It refers to the category of critical threats, with particular emphasis on threats to people, property and the environment. The authors also discuss the practical aspects of risk management in relation to the threat caused by a hurricane.

The research applied research methods such as analysis, synthesis, induction, deduction, generalization, inference and desk research.

Keywords: risk; risk management; crisis management; crisis situations; security

Introduction

The unpredictability of the current threats, and their global character, makes security predicaments some of the most important problems for the contemporary and the future world. Those problems are becoming more complex nowadays, since the dynamic cultural and civilizational developments are accompanied by the re-evaluation of the environmental questions, considering the challenges and threats of different backgrounds. The environment creates numerous non-military and military crisis situations,situations; hence proper management of those problems becomes increasingly important.

In view of this, one of the most important tasks for the State is to protect the life and health of a population and the undisturbed State functioning. It has to consider and make plans anticipating natural disasters and extraordinary environmental threats that are caused by the forces of nature, and the undesirable effects of civilizational development. And, it must allocate resources for some of the activities that are conductive to the minimalization of potential threats, such as the following: well-designed operational procedures, the ability to evaluate risks, and the efficient management of information, or the strategy selection. The selection of a rational (optimal) management strategy in a crisis situation depends primarily on the threat identification and evaluation. In this case, the proper threat analysis is the basis for choosing a strategy and undertaking specific planning and control activities. As a consequence, crisis management can be understood as the threat management, which includes threat identification, threat analysis and

evaluation, decision making and taking into account the estimated threats, developing threat minimalization plans, and projects control for adopted threat indicators.

The aim of the article is to present the importance of risk management in the crisis management process. The research allowed to identify the crisis threats, to indicate the essence of threat management in the process of crisis management, the public administration role in the area of threat assessment, evaluation of methods for threat identification, and to analyse the selected examples. Research problems were formulated in the form of the following questions:

1) What is crisis management about?
2) What are the crises threats?
3) What is the risk and what is the risk management process?
4) What is the role of risk management in the crisis management process in relation to hazards caused by the occurrence of a hurricane?

The research applied research methods such as analysis, synthesis, induction, deduction, generalization, inference and desk research.

1. Threats and crisis management

Conception of "crisis" has become the subject of many analysis, which contributed to the creation of many definitions. Generally, by "crisis" we mean an event that is a decisive turning point, of the moment of breakthrough, as the result of which there is either a deterioration or improvement of the existing situation (Bloch, 2010). Crisis is often identified with the crisis situation. However, these concepts do not mean the same. The concept of crisis situation overrides the concept of crisis – every crisis is a crisis situation, but not every crisis situation must turn into crisis. The crisis is the culmination of the crisis situation and occurs when at the stage of escalation of the threat it will not be possible to remedy its factors (Moch, 2012).

A crisis situation is a special decision situation characterized by a very short decision-making time, very low predictability (surprise effect), very high risk and fear resulting from uncertainty (Sienkiewicz, Świeboda, 2010). The complexity of crisis situations and their dynamic course indicate that solving them will require holistic thinking and synchronizing efforts in all phases of the crisis management process, understood as managing the organization (system) under pressure, carried out for resolving tense situation, whose task is to prepare, and action to prevent, counteract and react in case of disturbances in the stability of the organization (system), and to restore its normal functioning (Kitler, 2007). In this way, it is possible to point out crisis management phases, which includes prevention, preparation, reaction and reconstruction.

Every crisis situation is a consequence of threats. Therefore, the threat is a critical category in crisis management. Its identification allows to determine the risk and take actions aimed at preventing the escalation of threats and, consequently, to its transformation into a crisis. However, it is impossible to define the full spectrum of threats because they evolve all the time. Nevertheless, in order for the planning process for crisis management to be carried out correctly, taxonomy of threats is necessary. Using the most popular source criterion of threats, it can be divided into military and non-military threats (see Table 1).

Knowledge of threats, their identification and analysis contribute to a proper risk assessment, which is an obligatory part of the functioning of the crisis management system. It is reflected in crisis management plans.

Table 1. Taxonomy of threats (Moch, 2013)

Threats			
Non-military			Military
Natural	social	technical	
Fires Atmospheric hazards Biological hazards Geological hazards Ecosystem hazards Cosmic hazards	Social pathologies Mental disorders Migration Gathering Organized crime Terrorism Social unrest Collective disturbances of public order	Transport disasters Construction disasters Technological disasters Mains disasters Mining disasters Failures of industrial facilities Chemical contaminations Failures of technical infrastructure devices	Strength demonstration Military diversion Military blockade Military blackmail Military provocation Border incident Limited use of armed violence Armed border clash Aggression of informal groups Military conflict in the border zone Local conflict Conflict between states

2. Risk management

A very important element in the context of the probability of a crisis situation and its consequences is threat and its analysis. According to K. Fearn-Banks, crisis management is a process of strategic planning for a crisis or negative turning point, a process that removes some of the threats and uncertainly from the negative occurrence and thereby allows the organization to be in greater control of its own destiny (Fearn-Banks, 2009). Analysis and evaluation of the of identified threats is an obligatory part of the crisis management system. It allows to determine, in a systematic way, the impact which is to be expected if different hazardous events occur. On the basis of these findings, it is possible to take directed and efficient measures to prevent hazards, and to adapt to changing conditions of threats, as well as it is possible to reduce the exposure to threats and vulnerability of different subjects, needed of protection. This also includes the preparation to a quick and effective handling of possible damaging events, thanks to the flexible and efficient use of available capabilities (Method of Risk).

In practice, various methods of threat analysis and evaluation are used. These include, for example: team work and the participation of experts; identification of threats based on the catalogue of threats; threat scenarios; hazard maps; maps of threats; assessment - by determining probability, and effects, and then determining threat value by creating the threat map; qualitative methods of risk assessment and determination of the effects of a threat, based on a 3- or 5-point scale and a descriptive scale; risk matrix (Kąkol, 2013). Many of them are used for crisis management purposes.

In Poland, the provisions regarding the necessity of conducting the threat assessment process were introduced in the Act of 26 April 2007 on Crisis Management. Threats analysis and evaluation is carried out for planning purposes. According to the Act, each crisis management plan should include hazard characteristics, threat assessment, threats maps and hazard maps.

The threat management process for crisis management needs should include the following: (1) identification of the entity/entities responsible for risk prevention and response when it occurs; (2) characteristics of the threat; (3) prediction on the probability of the

occurrence of a threat; (4) indication of the effects of the threat; (5) preparation of a threat matrix; (6) threat acceptance and justification; (7) indication of preventive and mitigating actions.

The starting point for threat analysis and evaluation is the identification of the public administration body (governmental and/or local government) that is responsible for protection against the threat (threats). The next step is to assess the threat for individual threat-scenarios. At present, in Poland, for the needs of the crisis management system, the hazard identification methods are used, such as: analysis of historical data; statistical data analysis; expert estimation; field research; assessment of the international situation; mathematical modelling; analysis of data from hazard monitoring systems; trend analysis; case study; environmental recognition (Pamięć przyszłości, 2015).

The threat in crisis management is determined by two basics parameters: the probability of an event, and the potential effects, whereas in the present case the effects are understood as losses:

Threat = probability x effects (loss value) (1)

In the above formula, the probability will mean the assessed possibility of occurrence of a specific threat, taking into account considerations regarding the frequency with which the phenomenon may occur (Wojtyto *et al.*, 2014). In this respect, historical data plays a significant role. In order to determine the probability of a hurricane, the following qualitative (descriptive) scale was adopted (see Table 2).

Table 2. Probability – qualitative (descriptive) scale (Ocena ryzyka, 2013)

Scale	Probability	Description
1	very unlikely	May occur only in exceptional circumstances. It can occur once every five hundred years or more.
2	unlikely	It is not expected that it can happen and/or is not documented at all, does not exist in people's messages and/or events did not occur in similar organizations, facilities, communities and/or there is a small chance, reason or other circumstances that events may have occurred. They can occur once every hundred years.
3	conditionally likely	It can happen at a specific time, events are little documented or exist in people's messages and/or very few events and/or there is a chance, the reason or devices that the event may occur. It can happen once every twenty years.
4	likely	It is probable that it will occur in the majority of circumstances and/or events are systematically documented and exist in people's messages and/or there is a significant chance, reason or devices allowing it to occur. It can happen once every five years.
5	very likely	It is expected that it will happen in most circumstances and/or these events are very well documented and/or exist among residents and are transmitted orally. May occur once a year or more often.

The effect of this is the "accountability" of threats. The effects of the event are analysed from the point of view of the population (P), economy, property, infrastructure (EPI) and the environment (E). To determine the effects, the following classification and characteristics were adopted (see Table 3).

Table 3. Effects – classification and characteristics (Ocena ryzyka, 2013)

Scale	Effects	Cat.	Characteristics
A	insignificant	P	No deaths and injuries. nobody or few people need help (not financial and material).
		EPI	Virtually no damage. None or small financial losses.
		E	Non-measurable effect in the natural environment.
B	minor	P	A small number of wounded, no deaths. Necessary displacement of the population (less than 24 hours). Some people need help.
		EPI	Some damages and difficulties (up to 24 hours). Small financial losses.
		E	Little impact on the environment with a short-term effect.
C	moderate	P	Needed medical help, no deaths. Some require hospitalization (the need for additional places in hospitals and medical staff). Relocation of evacuees in designated places with the possibility of return within 24 hours.
		EPI	Determining damage sites that require routine repair. Normal functioning of the population with little inconvenience. Large financial losses.
		E	Short-term or small effects with long-lasting effect.
D	significant	P	Heavily injured, a lot of people hospitalized and displaced (more than 24 hours). Fatalities. The need for special resources to help people and to remove damage.
		EPI	Partly non-functional community. Some services are not available. Big financial losses. Needed help from outside.
		E	Long-lasting effects in the natural environment.
E	disastrous	P	Many people seriously injured and hospitalized. General and long-term movement of people. A large number of deaths. Big help is required for a large number of people.
		EPI	Extensive destruction. Impossibility of functioning of a community without large external help.
		E	Great environmental impact and/or permanent damage.

Each of the potential identified hazards should be assigned a probability value and its possible consequences (effects). In both cases a 3- or 5-step scale is used. After estimating the threat parameters, its value is determined and placed in a 9- or 25-degree matrix (see Fig. 1).

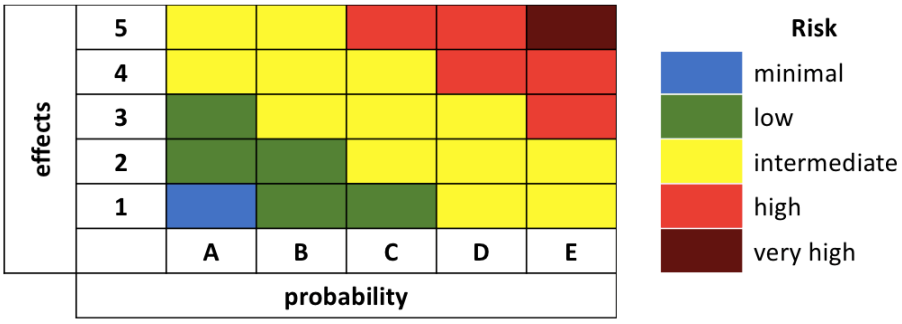

Figure 1. 25-degree risk matrix

Risk acceptance is the next step. The four categories are distinguished:

- acceptable risk (A) - no additional security measures are required, current solutions are accepted, monitoring activities;
- tolerated risk (T) - alternatives should be made, or introducing small changes (organizational, legal, functional) will not contribute to the improvement of safety;
- conditionally tolerated risk (CT) - additional security measures should be introduced, and the solutions applied should be improved;
- unacceptable risk (U) - immediate action should be taken to increase safety, introduce additional/new solutions.

The level of acceptable risk is determined subjectively, which is why it should be justified each time. It should be noted that it is necessary to set the level of acceptability for each risk separately. The level of acceptability does not have to be assigned a specific threat value permanently. The level of risk acceptance indicates the implementation of preventive and preventive actions that will contribute to reducing the overall threat value of given threats in the future.

The individual elements of the process will be described on the basis of the selected threat - a hurricane.

3. Situation analysis

In Poland, the task of emergency reaction and protection against the dangerous phenomena occurring in the atmosphere is assigned to the government and self-government administration. The main institution monitoring the meteorological phenomena in Poland, including the possibility of strong winds, as well as issuing warnings in this respect, is the Institute of Meteorology and Water Management-National Research Institute.

Term “wind” refers to the horizontal movement of air relative to Earth's surface, which arises due to the differences in pressure over a given area. Poland is located in the temperate climate zone. The presence of strong winds is conditioned by atmospheric circulation over Europe, local conditions and the development of storm phenomena. In Poland, windstorms can occur throughout the year, but their highest intensity can be observed in the autumn-winter period (November-March). Whirlwinds, on the other hand, most often occur from June to August, sometimes in May.

The wind is characterized by the average speed (S_{AVG}) and speed in the gusts (S) and the direction from which it blows. According to the definition contained in the Act of 7 July 2005 on insurance of agricultural crops and livestock (Sienkiewicz and Świeboda, 2010), a hurricane is a wind with a speed of not less than 24 m/s, which causes massive damage. However, it should be noted that the wind poses serious threats already at speeds of up to 15 m/s. When assessing the effects of strong wind hazards, it is possible to use the 3- (see Table 3) or 5-degree (see Table 4) scales.

Table 4. Degrees of high wind danger (according to Institute of Meteorology and Water Management-National Research Institute in Poland) (Krajowy Plan, 2017)

The degree of danger	Criteria	Effects
1	S_{AVG} > 15 m/s or S > 20 m/s	damage to buildings, roofs, damage to trees, breaking branches and trees, communication difficulties
2	S_{AVG} > 20 m/s or S > 25 m/s	damage to buildings, roofs, breaking and uprooting trees with roots, communication problems, damage to overhead lines
3	S_{AVG} > 25 m/s or S > 35 m/s	destruction of buildings, roof picking, destruction of overhead lines, large damages in the forest stand, significant communication difficulties, threat to life

Table 5. Degrees of high wind danger – 5-degree scale (Vademecum, 2013)

The degree of danger	Speed (km/h) H=10 m	Characteristic of wind	Wind effects
1	62-74	rapid wind	It breaks branches of trees, it is difficult to walk against the wind
2	75-88	windstorm	It causes damage to buildings, breaks tiles, breaks whole trees
3	89-102	strong windstorm	It pulls trees with roots, causes large damage to buildings, breaking energy poles
4	103-117	violent windstorm	It causes extensive damage, a threat to life
5	≥ 118	hurricane or whirlwind	It causes destruction and devastation, possible deaths

According to the available data, it should be noted that strong winds occur in Poland from 1 to 4 times a year. Compared to countries in the tropical zone, they are relatively rare. However, in recent years, there can be observed an increase in their number and an increase in their negative effects.

The effects of a hurricane can be different. They may occur throughout the entire province, several districts or one commune. A very strong wind is a threat to human health and life. There may be difficulties in moving and the need to evacuate. A hurricane causes significant losses in many areas of the economy. First of all, these are losses in construction, communications, agriculture and power engineering as well as communication difficulties resulting from the limitation of road traffic. Strong wind causes destruction and even degradation of the natural environment. There may also be local contamination of the environment, resulting from damage to installations and technical equipment and the release of harmful substances into the environment.

Determining the probability of an event and its effects gives rise to the creation of a threat matrix. The threat matrix for strong winds in Poland, prepared for the needs of the report on threats to national security, is presented in Figure 2.

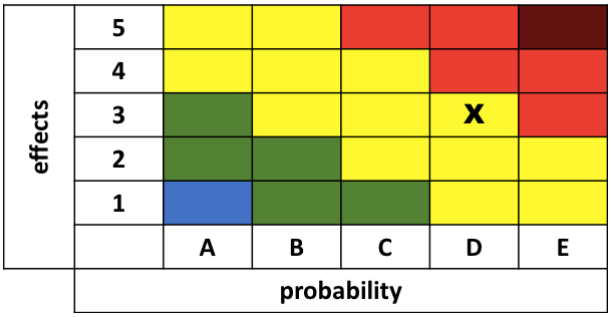

Figure 2. A risk matrix for a hurricane (Ocena ryzyka, 2013)

Strong winds (hurricanes) are a threat that occurs sporadically and is the result of rare adverse events that occur randomly. Although the probability of their occurrence is small, its effects are high. You cannot prevent the occurrence of strong wind, but you can be prepared to avoid full surprise, and thus minimize its negative effects. It is therefore necessary to introduce additional security measures and improve current solutions. These activities include, for example:

- improvement of warning systems for public administration bodies and the public, in view of anticipated storms and potential threats;
- development and implementation of alternative communication systems;
- data preparedness, readiness of forces and means to remove the effects of strong wind;
- carrying out an information campaign among the public on how to behave in the event of a direct threat;
- regular trainings and exercises of public administration bodies and services responsible for combating and removal of hazards caused by strong winds and its negative effects.

4. Conclusions

The considerations carried out by authors, have shown that the identification, analysis and evaluation of the threats is an obligatory part of the entire crisis management system. Threats cannot be measured accurately. However, it is advisable to estimate the scale of consequences of potential threats, and the probability of their occurrence, due to the need of strategic planning, for decision making process, and actions in threat conditions or uncertainty. Threat analysis in crisis management is therefore necessary, since it helps in grasping the full picture of potential dangers.

One often encounters opinions that risk is always managed. However, this is not always a conscious act. Risk, however, is inseparably embedded in the crisis management process. All activities in it should be taken in a conscious manner, based on solid premises. Decision-makers must take into account its consequences. A bad decision made in the process of crisis management may involve not only material losses, but also may pose a threat to the environment and human life and health. The application of risk management in the crisis management process, as research shows, can contribute to minimizing potential negative consequences of threats, as well as increasing the likelihood of decision-makers making the

right decisions. Risk analysis in crisis management is necessary because it allows you to get a picture of potential threats.

References

1. Bloch, N. (2010) Rola mediów w zarządzaniu kryzysowym. In: *Zeszyt Problemowy Towarzystwa Wiedzy Obronnej*, No 4(64), 22-32.
2. Fearn-Banks, K. (2009) *Crisis communications. A casebook approach*. p. 7, Lawrence Erlbaum Associates, Inc., New Jersey.
3. Kąkol, U., Marczewski, M. (2016) Metody analizy i oceny ryzyka stosowane w zarządzaniu kryzysowym na poziomie gminnym. In: *Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie*, No 11(959), 53-69.
4. Kitler, W. (2007) Istota zarządzania kryzysowego. In: *System reagowania kryzysowego*, ed. J. Gryz, W. Kitler. p. 29. Adam Marszałek, Toruń.
5. Krajowy Plan Zarządzania Kryzysowego. Rządowe Centrum Bezpieczeństwa, Warszawa (2017).
6. *Method of Risk Analysis for Civil Protection*. - https://www.bbk.bund.de/SharedDocs/Downloads/BBK/EN/booklets_leaflets/Method_of_%20Risk_Analysis.pdf?__blob=publicationFile.
7. Moch, N. (2012) Identyfikacja niemilitarnej sytuacji kryzysowej. In: *Organizacja wsparcia wojskowego władz cywilnych i społeczeństwa w niemilitarnych sytuacjach kryzysowych*, ed. G. Sobolewski, pp. 9-23, Towarzystwo Wiedzy Obronnej, Warszawa.
8. Moch, N. (2013) Niemilitarna sytuacja kryzysowa – pojęcie, istota, identyfikacja. In: *Paradygmaty badań nad bezpieczeństwem. Zarządzanie kryzysowe w teorii i praktyce*, ed. M. Kopczewski, I. Grzelczak-Miłoś, M. Walachowska. pp. 399-411, Poznań
9. Ocena ryzyka na potrzeby zarządzania kryzysowego, Warszawa (2013). http://rcb.gov.pl/wp-content/uploads/ocenaryzyka.pdf.
10. *Pamięć przyszłości. Analiza ryzyka dla zarządzania kryzysowego*. ed. G. Abgarowicz, Józefów 2015.
11. Sienkiewicz P., Świeboda H.: Ryzyko w zarządzaniu kryzysowym. In: *Studia i Materiały*, No 33, 8-17 (2010).
12. Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, Dz.U. z 2017 r., poz. 209 ze zm.
13. Ustawa z dnia 7 lipca 2005 r o ubezpieczeniach upraw rolnych i zwierząt gospodarskich, Dz.U. z 2017 r., poz. 2047 ze zm.
14. Vademecum – Niebezpieczne zjawiska meteorologiczne – geneza, skutki, częstość występowania. Część 2 (jesień-zima). pp. 5-17. Instytut Meteorologii i Gospodarki Wodnej – Państwowy Instytut Badawczy, Warszawa (2013).
15. Wojtyto, D., Wierzba, A., Madejski, R. (2014) Ocena ryzyka na potrzeby zarządzania kryzysowego. In: *Logistyka* No 5, 1636-1640.

RESEARCH and TECHNOLOGY – STEP into the FUTURE, 2018, Vol. 13, No. 4, 27-34
Transport and Telecommunication Institute, Lomonosova 1, Riga, LV-1019, Latvia

THE CONTINUITY OF LOCAL GOVERNMENTS IN POLAND DURING DISASTERS

Krzysztof Szwarc [1], Piotr Zaskórski [2]

[1,2] Military University of Technology,
Gen. Witolda Urbanowicza 2, 00-908 Warsaw, Poland
[1] fax: +48 261 83 72 62, krzysztof.szwarc@wat.edu.pl
[2] piotr.zaskórski@wat.edu.pl

Emergencies, disasters or generally speaking disruptions affect all segments of the population. Because of increasing risk of natural and manmade disasters (Szwarc and Zaskórski, 2012), it is necessary to establish effective systems that prevent, prepare to, react and recover after disruptive incidents (Blyth, 2009; Szwarc and Zaskórski, 2015; Tucker, 2015; Zawiła-Niedźwiecki, 2008).

The article focuses on the issue of ensuring continuity of local governments in Poland. According to the international and national legislation or standards, the recommendations and requirements were presented.

It is a fact, that during emergencies, public administration used to be challenged by various factors like staff absenteeism, outage of power or the limitation of other critical resources (Szwarc and Zaskórski, 2017). Organizations that function in a such environment are exposed to the impact of various factors. Despite the difficulties, it is crucial to continue the critical processes.

A risk of disruptions in public administration there is not just a hypothetic or theoretical phenomena. A few examples of those incidents were recognised and analysed. Continuity is an important part of security system of any organization, as well as preventive measures. Therefore, it is strongly recommended to establish comprehensive take on security.

Local governments are vulnerable to different kind of threats (Szwarc, 2014). Some of them listed in this article could be treated as the common problems of public administration in Poland. However, both risk assessment and business impact analysis should be conducted in every institution (Zawiła-Niedźwiecki, 2013).

This paper details practical considerations for building successful continuity of local government programmes based on the Business Continuity Institute's Good Practices Guideline, the international BCM standard ISO 22301 (Drewitt, 2013) and polish law requirements. As it is strongly emphasizes in this article, continuity is a universal problem and should be considered in holistic way (Zaskórski *et. al*., 2011).

Keywords: continuity of government, risk assessment, crisis management

1. Introduction

All organizations may be susceptible to unique kinds of threats and hazards such as floods, high winds, cyber-attacks, animal diseases, demonstrations, riots or critical infrastructure failure (Szwarc and Zaskórski, 2015). Those can be also a serious problem for functioning of the public administration, where disruption of normal activities (including essential functions) may have serious impact on local and national security. Considering the matter of activity, it is necessary to sustain a critical function during or aftermath of the crisis situation (Zaskórski and Szwarc, 2017).

According to the changing and evolving nature of risks, the security systems have to be checked and verified accordingly. Day-to-day activities bring a new kind of threats and hazards as well as unpredictable Large Scale, Large Impact, Rare Events (LSLIRE). Finally, in recent years, there were several examples of natural, human-caused or technology-caused disasters, that had potential or actual influence on public administration ensuring the mission-critical

activities. It means that complete security system should contain continuity and recovery measures as well (Zawiła-Niedźwiecki, 2013).

Therefore, public just like private or non-profit entities have to establish comprehensive strategies for prevention, mitigation, response and recovery. After devastating floods in 1997 and 2001 Polish Parliament established the Crisis Management Act (Republic of Poland Parliament, 2017) that focuses on the complex continuity of operation, on the state, regional and local levels (Kaszubski and Romańczuk, 2012). Something similar occurred in USA, when the comprehensive measures were implemented after terrorist attacks on 11 September 2001 (President of the United States, 2007).

Business continuity may be understood as the main measure of confidence that the essential services, like public security, will be preserved at acceptable levels, even after some disruptive incidents. It cannot be achieved without the leadership and commitment from local governments which shall provide the polices, plans, structures and resources needed for business continuity management.

The continuity of central or local governments is strongly dependent on the critical infrastructures that provide the essential services, and the disruption of which would have significant security, safety, economic or social impact. Consequently, the critical infrastructure protection is one of the most important issues for crisis / emergency management system.

The aim of this article is both, to recognize and to describe the role of crisis management system in ensuring the continuity of local governments, during and aftermath of disasters. There are some research questions that were posed here: (1) What should a crisis management system contain to deal with disasters? (2) Are business standards useful to create the public administration resilience? (3) How to improve the crisis management system in Poland? To find the answer to those questions research was done using the analytical and empirical methods. Based on crisis management practitioners' survey some further recommendations were provided. The base terminology was also clarified.

2. Basic terms and definitions

According to literature there is no consensus on a universally accepted definition of "business continuity". The most frequently used definition of this term is related to the guidelines of the ISO 22300:2012 where business continuity is recognized as "capability of the organization to continue delivery of products or services at acceptable predefined levels following disruptive incident" (ISO, 2012a). Despite of this, various definition of business continuity includes "strategic or tactical capability of the organization to plan for and respond to incidents and business disruptions in order to continue business operations" (British Standard Institute, 2006), "management of a sustainable process that identifies the critical functions of an organization and develops strategies to continue these functions without interruption or to minimize the effects of an outage or loss of service provided by these functions" (Tucker, 2015), or "daily activities performed by an organization to ensure that critical business functions will be available to customers, suppliers, regulators, and other entities that must have access to those functions" (Sneadker and Rima, 2014). These definitions fail to provide the distinction between the business continuity, business continuity management and ensuring business continuity. Therefore it will be synthesized that, **business continuity** is a capability of the organization (1) to maintain key processes and to continue delivery of key products (a results of processes) at acceptable predefined levels (2) following disruptive incident (3). First of all, it is a capability, what means that business continuity is a result of managerial and engineering effort. Secondly, the balance between reliability and cost-effectiveness has to be preserved. Redundancy of staff, facilities and communication systems or preparation of site location is very expensive and have to be confined to the vital products (Szwarc and Zaskórski, 2015; Zawiła-Niedźwiecki, 2013). Moreover, the quantity and quality of delivery may be reduced, especially during crisis situation. Business Impact Analysis and Risk Assessment are necessary to recognize key products and processes as well as the business continuity requirements e.g.

Recovery Time Objective (RTO), Maximum Tolerable Period of Disruption (MTPD), Minimum Business Continuity Objective (MBCO) (Drewitt, 2013; Rittinghouse and Ransome, 2006). And thirdly, business continuity is a reactive strategy, although it can be treated as the additional protective measure in case of standard protection fails.

Furthermore, business continuity is both operational and strategic management issue. In the first case this is a subject of operational risk management, which focuses on the matter of forming the organization's ability to respond to disruptive incidents. This perspective focuses on the risks assessment and the business continuity ensuring process. On the other hand, this capability shall be recognized as an ideal system attribute, that can be attained only on the way of continual improvement. In this meaning, it is the subject of strategic management (Zawiła-Niedźwiecki, 2013).

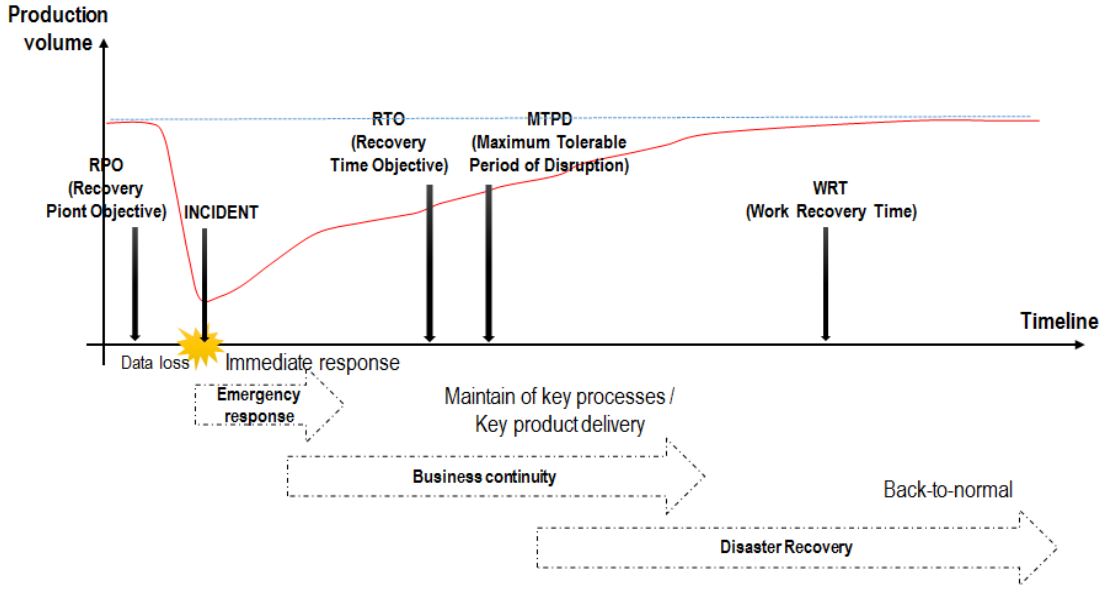

Figure 1. Business continuity objectives
Source: own work based on: (British Standard Institute, 2006)

Many definitions of "**business continuity management**" (BCM) may be cited as well. In (Business Continuity Institute, 2013; British Standard Institute, 2006; ISO, 2012a) BCM is defined as a holistic management process that (1) identifies and assess the impact of disruptions (2) provides organizational resilience framework and (3) ensure the effective response that safeguards the interest of key stakeholders, brand and value-creating activities. In other way, BCM may be understood as a specific set of processes that identify and evaluate risks, develop organization's resilience by providing necessary resources and defining the objectives (Sneadker and Rima, 2014).

It is also necessary to provide distinction between emergency management, business continuity and disaster recovery (Figure 1). In fact, business continuity management is a form of crisis management, and its evolution is widely deliberated in (Drewitt, 2013; Ficoń, 2007).

The first step of crisis response process is to deal with the immediate effects of the incident. Therefore, the aim of this stage is to gain control of the situation and to prevent the secondary risk occurring. It is also a managerial process that contains the information gathering, response plans implementing and the response team motivating (Blyth, 2009). Business continuity is the next step, when minimal tolerable quantity of key products delivery should be provided. The previously prepared resources are essential for process sustain or resumption, on the site location (Liderman, 2017). During recovery stage the full system functionality has to be

restored. It is the time for collecting all incident documentation, evaluation of responses taken, gaps and shortfalls reflection as well as policy or plans revision.

Another term that should be explained is "disruption". To begin with, it is important to distinguish between two terms: "**incident**" that shall be understood as a "situation that might be, or could lead to, a disruption, loss, emergency or crisis" (ISO, 2012a) and "**disruption**" that can be defined as anticipated or unanticipated event, which causes unplanned, negative deviation from the expected delivery of products according to the organization's objectives (British Standard Institute, 2006), or as a results of perturbatory influences, that may affect operations, processes, plans, goals or strategies (Ivanov and Sokolov, 2010). As mentioned, incident may lead to **crisis situation** which Crisis Management Act defines as a "situation that impacts negatively on the safety of people, property in large sizes or the environment and produces significant restrictions on the operation of competent public administration authorities due to the inadequacy of possessed capabilities and resources" (Republic of Poland Parliament, 2017).

According to this act, crisis management has a wider context and includes preventive and preparing measures (Republic of Poland Parliament, 2017), when business continuity management may be understood as (Szwarc, 2014; Zawiła-Niedźwiecki, 2013):

- mechanism by which the organization can respond to disruption
- additional protection against risk when the nominal security solutions fails.

3. Ensuring Continuity of Local Governments in Poland

The establishing and maintaining of continuity management system in country is a comprehensive process. Based on the ISO 22301:2012 (ISO, 2012b), and other standards and norms like the Polish Crisis Management Act – the necessary components of effective continuity system was identified (Figure 2). This Act states that the "crisis management is the activity of public administration authorities that constitutes an element of managing the national security system" (Republic of Poland Parliament, 2017). As was mentioned, a particular part of this activity deals with responding and recovering (incl. reconstructing critical infrastructure) after disruptive event. It is a managerial process which includes (Ficoń, 2007; Republic of Poland Parliament, 2017):

- Civil planning contains both planning and organizing functions. The main aim of this process is to prepare the public administration to manage crisis (incl. preparing: crisis management plans, structures to be run in crisis situations, resources needed to perform defined tasks and communication systems) and establish terms of bilateral cooperation with Armed Forces;

Figure 2. Main components of effective continuity system
Source: own work

- Critical infrastructure protection – establishing the public-private partnership for ensuring the functionality, continuity and integrity of critical infrastructure. The owners and holders of critical infrastructures are responsible for preparing and implementing critical infrastructure protection plans and holding reserve systems that sustain the key function on acceptable level. The main responsibility of public administration on the local level refers to organizing and implementing of critical infrastructure protection tasks. The structure of the critical infrastructure protection plan and the responsibilities of the public and private sector details (Council of Ministers, 2010);
- Risk assessment and monitoring – which is essential to establishing successful risk mitigation strategy. Crisis management plan contains risk map as well as task and organization related to monitoring, warning and alarming system;
- Responding in case of emergency – that refers to implementation of the crisis response procedures, the effort coordination of engaged services, inspections and guards, the coordination of evacuation process, the rescue organizing, the medical care, the social- and psychological support and the maintenance of the supply of essential resources (e.g. water, food, medicaments, warm clothes);
- Crisis communication – that ensures a successful communication inside and outside of the crisis management system. Therefore, crisis management have to establish secure and reliable communication system, as well as the rules of providing information to the population.;
- Recovery – that refers to removing of effects of incident, and rebuilding resources and critical infrastructures. This function contains also the evaluation and documentation of damage;
- Testing, exercising and review – that conduct the verification and validation of existing plans and mitigation strategies, as well as recognition of current needs and deficits in necessary capabilities and resources. It is also a chance to gain new experience of acting under stress and uncertainty.

Crisis management is a complex system organized at five levels of administration, starts on the State and ends up on commune level. Every territorial structure contains the one-man authority that is responsible for crisis management (which is a chief of the administration or the Council of Members at the State level). The authority is supported by advisory body, a crisis management team that includes experienced practitioners (e.g. the chief of police) or fire chief and the administrative staff. At all levels (beyond municipal) a crisis management centres provides a 24-hour information flow. Government Centre for Security is a multidepartment structure that provides the standardization (e.g. risk assessment guides, Critical Infrastructure Protection Programme) and interoperability between all entities. This centre serves all bodies of crisis management at State level and provides the information flow to EU and NATO, as a national contact point. Based on (Council of Ministers, 2009) selected ministers and central government administration authorities have to establish crisis management centres which should be able to ensure the continuity of operations despite the outage of external power supply, communication system fails, or other failures. There is not a similar recommendation for the local level, where the crisis management centres used to be establish in collaboration with fire departments or another services or guards supervised by the head of district (Szwarc, 2014).

All systems require permanent supply of essential resources (e.g. energy, information, raw materials, office articles and so on). Ensuring continuity of supply may be a significant problem, especially in case of emergency (Ficoń, 2007). From this perspective, business continuity may be considered in five dimensions (Szwarc and Zaskórski, 2015; Zaskórski and Szwarc, 2017):

- human – most important resource of each organization, that contains staff and managers (leaders). The risk of absence of key actors (Kandel, 2015) should be

mitigated with the clear line of succession, substitution schedule, additional training (an ability to perform the peers functions – functional redundancy) and the engagement of additional staff (parametric redundancy);

- material – that contain facilities, raw materials, consumables, technical equipment and machinery. Ensuring business continuity in this dimension contains (1) side location, (2) special security of supply measures (e.g. stock of materials, additional capacity, redundant suppliers), (3) maintenance and monitor of equipment and machinery (Zaskórski and Szwarc, 2017);
- energy – which includes heat (minimal office working conditions) and electricity power (according to impact of power outage a different categories of electrical loads may be recognised: high impact – even short disruption may cause a major impact; medium impact – if the short period of outage may be tolerable; minor impact – when the outage does not have to be removed immediately). In both cases a risk of disruption may be mitigated with additional electricity connection or uninterruptible power supply (UPS);
- financial – that refers to allocating funds for reaction, and to ensure liquidity. According to Crisis Management Law, local governments should create a special reserve in the budget for the carrying out of crisis management tasks related to own activity, and can receive subsides for the financing of entrusted tasks related to the scope of government administration or particular activities;
- informational – which contain data essential for public services, especially stored in national registers (e.g. personal identity number, registry of cars and drivers, or Electronic Platform of Public Administration Services). This dimension refers to providing continuity of gathering, storage, processing and distribution of information (Zaskórski *et al*., 2011), what is strongly associated with material (ICT, facility) and human (knowledge, wisdom) dimensions (Szwarc and Zaskórski, 2017). To reduce a risk of disruption local governments in Poland (1) multiplying (e.g. Internet, GSM, TETRA, courier services, paper copies) and (2) upgrading (e.g. from analogy to digital, devices purchases) the information systems. Another strategy based on the cloud service is deliberated here (Szwarc and Zaskórski, 2013). According to the Polish law, public administration units establish comprehensive information security systems containing disaster recovery measures.

As highlighted, ensuring continuity of government requires a huge effort. During disasters, if capabilities and resources are insufficient local government may be supported by the military forces, at request of the regional administration chief ("voivode") and permission from Ministry of Defence. To preserve a good preparation their tasks should be previously planned in chief crisis management plan.

According to evolving nature of threats, security systems must evolve as well. Therefore, a two-years planning cycle have been established. Moreover, according to the law each authority is obligated to managing, organising and conducting exercises and training of crisis management. Knowledge on many numbers of incidents that happened in the last ten years may be also useful for system improvement process.

4. Conclusion

Our world is increasingly uncertain and vulnerable. Over the last decade, Polish society has witnessed many types of disasters, including floods, high winds or critical infrastructure failure. In this sense business continuity used to be understood as a measure of confidence, regardless of the matter of activity. It can be also seen as an essential attribute of public administration, where disruption has a serious impact for public security, and welfare of the society.

Organizations that function in a turbulent environment are exposed to the impact of various factors. A lot of disruptions of public activities were identified during empirical research. It proves that disruption in public administration is not just a hypothetical or theoretical phenomena.

While it is difficult to reduce the likelihood of most unpredictable disruptions, there are several ways to reduce the impact of disruption on public administration and societies, so that these units can become more robust. Obviously, it is hard to say how to deal with a disaster like Ebola outbreak (Kandel, 2015) or massive cyberattack. However, regardless of sources the disturbances manifest as one of four possible outcomes (Watters, 2014):

- Loss of staff: leaders or key staff members are unable to attend the work;
- Loss of facility: the building is out of action or the access to this building is not allowed for the medium or long time;
- Loss of technology: the technology does not work or is unavailable;
- Loss of supplier: a critical services, products or resources cannot be provided.

Naturally, each incident has different impact on the organization but generally, local governments should be prepared for mentioned scenarios. Therefore, different types of redundancy, which is an universal strategy of ensuring business continuity, were presented in this article.

Notwithstanding, redundancy may be too expensive strategy for public administration. To preserve the balance between resilience and efficiency, the organization should establish, implement and maintain a formal and documented process for business impact analysis and risk assessment (ISO, 2012b). First of them should provide the information about key products and processes as well as the priorities and requirements for resuming activities when the second should be helpful to obtain effective and efficiency strategy. According to *local crisis management practitioners' survey* and conducted analysis some recommendations have been identified:

- A **human capital** of crisis management system on the local level **should be strengthened**, or its tasks have to be verified;
- The local government units should receive **fixed technological and financial support** from the State level for servicing own tasks in the field of crisis management;
- Cooperation between civil and military structures in the field of crisis management should be strengthened;
- **A minimal requirement for functioning crisis management centres at regional and local levels related to** (Council of Ministers, 2009) **should be established;**
- **The horizontal and vertical communication between the different crisis management authorities requires strengthening.**

References

1. Blyth, M. (2009) *Business Continuity Management. Building an Effective Incident Management Plan*. New Jersey: John Willey & Sons, Hoboken. p. 362.
2. British Standard Institute, (2006) *BS 25999-1:2006 Business continuity management – Part 1: Code of practice*. London: BSI.
3. Business Continuity Institute, (2013) *Good Practice Guidelines: 2013 Global Edition. A Guide to Global Good Practice in Business Continuity*. Caversham Reading, Berks: BCI.
4. Council of Ministers, (2009). *Rozporządzenie z dnia 15 grudnia 2009 r. w sprawie określenia organów administracji rządowej, które utworzą centra zarządzania kryzysowego, oraz sposobu ich funkcjonowania*. Warsaw: Journal of Laws.
5. Council of Ministers, (2010) *Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytycznej*. Warsaw: Journal of Laws.
6. Drewitt, T. (2013) *A Manager's Guide to ISO 22301*. Cambridgeshire: IT Governance Publishing. p. 220.

7. Ficoń, K. (2007) *Crisis Management Engineering. System approach*. Warsaw: BEL Studio. p. 501.
8. Herbane, B. (2010) The evolution of business continuity management: A historical review of practices and drivers. Business History 52(6), 978-1002.
9. ISO (2012a) *ISO 22301:2012 Societal security — Business continuity management systems — Requirements*. Geneva: ISO.
10. ISO (2012b) *ISO 22313, Societal security – Business continuity management systems – Guidance*. Geneva: ISO.
11. Ivanov, D., Sokolov, B. (2010) *Adaptive Supply Chains Management.* London: Springer-Verlag. p. 269.
12. Kandel, N. (2015) Is there a business continuity plan for emergencies like an Ebola outbreak or other pandemics? *Journal of Business Continuity & Emergency Planning.* 8(4), p. 295-298.
13. Kaszubski, R., Romańczuk D. (ed.) (2012) *The Best Practices in Business Continuity Management*. Warsaw: Polish Banking Association. p. 216.
14. Liderman, K. (2017) *Information security. A new challenges*. Warsaw: PWN. p. 423.
15. President of the United States, (2007) *National Security Presidential Directive/NSPD-51 and Homeland Security Presidential Directive/HSPD-20 on National Continuity Policy*. Washington DC.
16. Republic of Poland Parliament, (2017) Crisis Management Law, Warsaw: *Journal of Laws*.
17. Rittinghouse, J., Ransome, J. (2006) *Business Continuity and Disaster Recovery for InfoSec Mangers*. Burlington, Oxford: Elsevier Science. p. 338.
18. Snedaker, S., Rima, Ch. (2014) *Business Continuity and Disaster Recovery Planning for IT Professionals.* Waltham: Elsevier, Inc. p. 557.
19. Szwarc, K. (2014) Conditions for crisis management system continuity. *National Security Studies* (5), p. 205-219.
20. Szwarc, K., Zaskórski, P. (2012) Identification of the threats for business continuity. *National Security Studies* (3), p. 215-235.
21. Szwarc, K., Zaskórski, P. (2013) "Cloud" Computing as a service that reducing the risk of discontinuity. In: *Proceedings of the 4th Scientific Conference: Man-made and Technical Disasters,* Bełchatów, March 2013. Wroclaw: Tadeusz Kościuszko Mechanized Infantry Officer School, pp. 201-211.
22. Szwarc, K., Zaskórski, P. (2015) The continuity of security systems. In: *Proceedings of the 2nd Scientific Conference*. *Zagrożenia bezpieczeństwa państwa - geneza i charakter uwarunkowań,* Warsaw, November 2014, Warsaw, Military University of Technology, pp. 43-63.
23. Szwarc, K., Zaskórski, P. (2017) Providing information security in emergency management systems. In *Proceedings of the 3rd Scientific Conference: Multidisciplinary of European Security*, Jachranka, September 2016, Warsaw, Military University of Technology, pp. 109-140.
24. Tucker, E. (2015) *Business Continuity from Preparedness to Recovery.* Waltham: Elsevier, Inc. p. 301.
25. Watters, J. (2014) *Disaster Recovery, Crisis Response & Business Continuity. A Management Desk Reference*. New York: Apress. p. 296.
26. Zaskórski P., Szwarc K. (2017) Modelling of Security and Continuity of Government Processes. *National Security Studies* (12), p. 335-364.
27. Zaskórski, P. (ed.) (2011) *Management in terms of informational continuity risks*. Warsaw: Military University of Technology. p. 227.
28. Zawiła-Niedźwiecki J., (2008) *Business continuity of organization*, Warsaw: Warsaw University of Technology. pp. 108.
29. Zawiła-Niedźwiecki, J. (2013) *Operational risk management in ensuring business continuity.* Krakow: edu-Libri. p. 180.

RESEARCH and TECHNOLOGY – STEP into the FUTURE, 2018, Vol. 13, No. 4, 35-42
Transport and Telecommunication Institute, Lomonosova 1, Riga, LV-1019, Latvia

PROBLEMS OF CHANGING EMPLOYMENT RULES FOR THE FOREIGNERS IN POLAND

Małgorzata Walendzik [1], Cezary Krysiuk [2], Rafał Kopczewski [3], Arkadiusz Matysiak [4]

[1] Motor Transport Institute,
Poland, Jagiellońska 80, 03-301 Warsaw
fax: +48 22 43 85 401, malgorzata.walendzik@its.waw.pl

[2] Motor Transport Institute,
Poland, Jagiellońska 80, 03-301 Warsaw
fax: +48 22 43 85 401, cezary.krysiuk@its.waw.pl

[3] Military University of Technology,
Gen. Witolda Urbanowicza 2, 00-908 Warsaw, Poland
fax: +48 261 83 72 62, rafal.kopczewski@wat.edu.pl

[4] Motor Transport Institute,
Poland, Jagiellońska 80, 03-301 Warsaw
fax: +48 22 43 85 401, arkadiusz.matysiak@its.waw.pl

At present over half of Poland-based companies have difficulties in finding employees. The reasons are both low unemployment and outflow of domestic manpower to Western Europe.

Changes in the foreigner employment regulations in Poland are necessary. The development of the economy strongly depends on the influx of foreigners in order to become a destination for qualified labour force. Additionally, efficient employment mechanisms should be ensured in order to limit potential irregularities.

These issues significantly affect the domestic road transport sector, lacking about 100.000 professional truck drivers. The relevant article's findings come from ICT-INEX, an EU project led by Motor Transport Institute. It aims at improving the access to professional driving for the disadvantaged social groups, including migrants, through personalized, ICT-based training methods. One of the project's key aspects is to analyse the current situation of the foreign migrants willing to enter the profession, regarding both Polish and European context.

Keywords: employment, foreigners, migration, professional drivers, Poland

1. Introduction

According to the UN Population Department, Poland has found itself among 51 countries which would be affected by the population decrease by the year 2050 and also among the countries where the decreasing number of inhabitants would be the biggest problem. Now, Poland, with a population of 38 million, is 6th most populous EU Member State. According to demographers, the population decrease by over 15% will affect many other Eastern European countries, beside Poland.

Poland is one of the countries where the shortage of employees is mostly visible. The International Business Report, in which 33 countries were examined, shows that only Japan has a greater difficulty in recruiting employees (76%) than Poland. The problem of the inhabitants' decline is not only a problem of the future. Already, more and more enterprises have problems with finding and retaining qualified employees.

Decreasing human resources will cause increased competition for employers on the market. The problem of employees shortage occurs in about 34% of the companies in the EU, and in Poland, about 60% of companies from the SME sector have problems with recruitment of

the qualified employees. According to the data of the Polish Agency for Enterprise Development, the SME sector is one of the main pillars of the Polish economy in which over 1.8 million enterprises were active last year. Additionally, 253,000 new companies were created in Poland during this time.

The main research question of the paper is to answer how to improve employment of the third countries citizens in Poland according to the binding law.

To resolve the aforementioned question, the following sub-questions have been formulated:

1. How the creation of legal provisions improves the employment of foreigners?
2. In which areas should the actions be taken?
3. How ICT-INEX project could improve professional driving situation?

The following theoretical research methods were used: definition, analogy, analysis, synthesis, to resolve above problems.

2. Legalization of work and residence of foreigners in Poland

Taking up employment abroad with foreign employers is carried out in accordance with the procedures and regulations in force in the state of employment and on the principles set out in the international agreements.

In order to be able to legally entrust conducting work to a foreigner, a number of conditions must be met. These requirements result from the Act of 20 April 2004 (The Polish act, 2004) on the promotion of employment and labour market institutions, the Act of June 15 2012 (The Polish act, 2012) on the effects of entrusting work to foreigners who live on the territory of the Republic of Poland, against the provisions, as well as the Act of 12 December 2013 (The Polish act, 2017) on foreigners. The Act of 20 July 2017 (The Polish act, 2017) amending the act on the promotion of employment and labour market institutions and some other acts are aimed at implementing the provisions of the Directive 2014/36/EU of the European Parliament and the Council of 26 February 2014 on the conditions of entry and residence of foreign nationals for the purpose of employment as a seasonal worker in the Polish legal order. The aforementioned directive obliges Member States to introduce conditions and procedures for issuing residence and seasonal work permits for the foreigners.

According to the Article 21 of the Treaty on the Functioning of the EU (Treaty of Lisbon, 2007), every citizen of the EU has the right to move freely and reside in the Member States, subject to the conditions laid down by EU law. According to Article 45 of the abovementioned treaty, it guarantees free movement of workers within the Union. The free movement of employees also includes members of the migrants' families. The regulations on the free movement of workers entitle them to:

- seek employment in another Member State,
- work in another Member State without the necessity to obtain a work permit,
- the right of entrepreneurship and the providing services in all Member States
- reside in another Member State due to work,
- remain in another Member State even after finishing the employment,
- non-discrimination in employment, equal treatment of the citizens of a given Member State regarding access to employment, social and tax benefits,
- exercise the right to take up education in any Member State.

At present, people with the citizenship of an EU Member State, the European Economic Area (EEA) and Switzerland can undertake employment in Poland without having to obtain a work and residence permit. This does not mean that EU citizens do not have any responsibilities. Every EU citizen staying in Poland for longer than 3 months has to register the stay in the appropriate Province Office. Registration of the residence should be made at the latest on the next day after the expiry of a 3-month stay in Poland.

Citizens of the countries outside of the EU who reside in Poland based on the permanent residency permit and a long-term EU resident's stay permit do not need additional documents entitling them to take up and perform work. Based on a permanent residency permit issued in

Poland, a foreigner has the right to work only in Poland. A permanent residency permit is valid for an indefinite period; however, every 10 years there is an obligation to replace the residence card. Permanent residency permit entitles to travel to other Schengen countries, but only for tourist purposes.

Any foreigner who in accordance with the applicable regulations is not exempt from the obligation to have a work permit in Poland must have an appropriate authorization in the case of an intention to take up employment on the territory of the Republic of Poland. Employment permit is issued on the employer's application to the appropriate province governor, or in the case of a temporary residence permit and work permit (from May 1, 2014) - applies foreigner who resides legally on the territory of Poland. A foreigner should enclose the information from the region governor on the inability to satisfy the staffing needs of a given employer with the application, which was previously obtained and handed over to the foreigner by the employer. To obtain seasonal work permit, introduced from January 1, 2018, the employer applies to the appropriate region governor. In order for a foreigner to work in Poland on a work permit, he/she must have a residence permit which entitles to work on the territory of Poland.

A foreigner may not work under different conditions or in a different capacity than the one specified in the work permit (with the exception of entrusting work of a different character or in a different capacity than specified in the permit for the periods summing up to no more than 30 days in a calendar year; in this case one must notify province governor who issued the permit about this fact in writing, within 7 days). In the case of a uniform permit for temporary residence and work, the work under other conditions or a position other than those specified in the permit is possible provided that the content of the permit is changed. This can be made at the foreigner's request

Citizens of 6 countries: Armenia, Belarus, Georgia, Moldova, Russia and Ukraine are entitled to work in Poland based on a simplified procedure which involves entrusting work on the basis of a formal statement without having to obtain a work permit. These foreigners have the right to work for 6 months in a period of 12 consecutive months. In order to be able to use the simplified procedure, the employer has to register in the regional employment office a statement of the intention to entrust work to a foreigner and a document confirming his/her residence title in Poland. Due to low costs and lack of formalities, it is a very popular way in Poland to obtain employees. From 1st January 2018, the employer has to inform the regional employment office in writing about the foreigner actually taking up work within 7 days from the date of commencement of work indicated in the statement. According to the regulations, the Province governor may issue a decision refusing entrusting work to the foreigner. This can be done in case the circumstances indicate that the statement has been made under false pretences, and would be used by a foreigner for purposes other than work for a given entity or the entity entrusting the work to a foreigner will not comply with the duties resulting from running a business or entrusting work to other people.

The Department of Labour Market in 2017 issued over 267,000 work permits to the foreigners, and more than 1.8 million declarations of intent to entrust work to a foreigner were registered. Ultimately, however, the number of foreigners who started work in Poland based on the permits or statements is lower for various reasons, e.g. personal resignation, visa refusal or foreigner's formal failures. Similarly as in previous years, the share of Ukrainian citizens in the number of issued permits and the number of registered declarations has been growing. Approx. 85% work permits and 95% statements go to the citizens of Ukraine. Employees from Ukraine are the majority, but there has been an increase of workers from Nepal, China or India. Employers are interested in long-term cooperation, especially when they invest considerable resources in the employee training. Employees from Ukraine find their place on the Polish labour market more easily for cultural and linguistic reasons, make use of its opportunities and then seek better solutions. That is why the labour market has been re-focusing on Asia.

Currently, the greatest demand for employees occurs in construction, transport, industrial processing, trade, gastronomy or in the households. The transport services market is at risk due to the lack of professional drivers. The volume of transport by road is systematically increasing,

and the labour market lacks qualified drivers. The report prepared by PwC shows that there may be a shortage of up to 100,000 professional drivers on the Polish market. This situation creates a huge threat to the road transport sector. The problem of driver shortage may lead in the future to disturbances in transport-related industrial sectors, and thus this problem will affect the entire Polish economy. Table 1 shows number of work permits issued in 2010 -2017.

Table 1. Number of work permits issued in 2010 -2017 and growth rate y/y (Turka *et al.*, 2015)

Year	Number of work permits issued	indicator %r/r
2010	36 622	24,82%
2011	40 808	11,43%
2012	39 144	-4,08%
2013	39 078	-0,17%
2014	43 663	11,73%
2015	65 786	50,67%
2016	127 394	93,65%
2017	267136	108,69

3. Employer's obligations towards foreigners

From January 1, 2018, written contracts with a foreigner in Poland have to be concluded and translated. This obligation also applies to the foreigners exempted from the obligation to have a work permit, and the entity entrusting the execution of work has to conclude a written contract with a foreigner.

Before signing the contract, the company has to provide the foreigner with a translation of the contract. In the contract, the company is required to take into account the conditions contained in the statement.

Primarily, the employer needs to comply with the Labour Code. No employee, regardless of nationality, may be discriminated against at the workplace. Table 2 presents number and the structure of statements registered by regional employment offices in 2017.

Table 2. Number of statements registered by regional employment offices in 2017(BY - Belarus, RU - Russia, UA - Ukraine, MD - Moldova, GE - Georgia, AM - Armenia) (Turka *et al.*, 2015)

Specification	Citizenship						Total
	BY	RU	UA	MD	GE	AM	
1. Number of statements	58046	6150	1714891	31465	11126	2786	1824464
1.1. No of statements for persons who already have a visa or a residency permit	15527	1728	718621	13429	5798	797	755900
2. Number of women	9076	1916	615631	9213	1399	621	637856
3. Employee's age							
3.1. Under 26 years old	12873	1187	454050	9641	1664	586	480001
3.2. 26-40 years old	30351	2887	747883	13935	6116	1249	802421
3.3. 41-65 years old	14768	2046	510747	7863	3338	936	539698
3.4. Over 65 years old	54	30	2211	26	8	15	2344
4. P.C.of A. sections							
4.1. Agriculture, forestry, hunting and fishing	1261	363	303462	713	291	317	306407
4.2. Mining and quarrying	144	14	970	23	11	2	1164
4.3. Industrial processing	7277	660	217750	6548	2372	287	234894
4.4. Production and supply of electricity, gas, hot water for air conditioning systems	17	0	380	0	1	0	398
4.5. Water supply; sewerage and waste management and activities related to reclamation	121	65	10890	711	63	22	11872

Specification	Citizenship						Total
	BY	RU	UA	MD	GE	AM	
4.6. Architectural construction	15496	910	214793	4026	1570	544	237339
4.7. Wholesale and retail trade, repair of motor vehicles, motorcycles	2150	429	63230	521	328	226	66884
4.8. Transport and storage	8921	509	76267	891	314	180	87082
4.9. Accommodation and food service activities	850	212	41788	388	226	109	43573
4.10. Information and communication	226	263	5128	56	47	32	5752
4.11. Financial and insurance activities	62	41	2677	27	4	14	2825
4.12. Real estate services	102	21	5154	75	106	22	5480
4.13. Scientific and technical activities	788	186	28624	391	145	73	30207
4.14. Administrative and support services activities	18840	2172	676264	14241	5323	839	717679
4.15. Public administration and national defence; obligatory social security	7	2	115	1	3	2	130
4.16. Education	70	13	2059	1	3	8	2154
4.17. Health care and social assistance	70	28	3690	30	11	24	3853
4.18. Activities referring to culture, entertainment and recreation	101	45	2792	19	9	11	2977
4.19. Other service activities	1429	179	44967	2770	285	51	49681
4.20. Households employment, households producing goods and services for their own needs	113	38	13855	33	14	23	14076
4.21. Extra-territorial organizations and teams	1	0	36	0	0	0	37
5. Large groups of professions and specialties							
5.1. Representatives of public authorities, senior officials	95	64	1134	3	4	9	1309
5.2. Specialists	551	461	7057	32	49	72	8222
5.3. Technicians and other mid-level personnel	880	368	44024	276	194	129	45871
5.4. Office employees	2455	315	80379	1184	742	138	85213
5.5. Service employees and vendors	1789	328	74237	1018	269	220	77861
5.6. Farmers, gardeners, foresters and fishermen	641	71	54842	303	56	50	55963
5.7. Industrial workers and craftsmen	20564	1205	309353	10814	3032	663	345631
5.8. Operators and assemblers of machines and devices	12377	814	190946	3838	1767	271	210013
5.9. Workers at simple jobs	18691	2524	952917	13990	5013	1234	994369
5.10. Armed forces	3	0	2	7	0	0	12
6. Type of contract							
6.1. Contract of employment	22286	2227	419807	9433	2959	987	457699
6.2. Contract of mandate	30283	3092	948187	20004	7482	1394	1010442
6.3. Contract work	5353	809	339876	2010	611	398	349057
6.4. Other	124	22	7021	18	74	7	7266
7. Period for which the statement was issued							
7.1. Less than 1 month	565	103	35412	506	242	44	36872
7.2. From 1 to 3 months	3663	459	219371	11019	5028	238	239778
7.3. From 3 to 6 months	53818	5588	1460108	19940	5856	2504	1547814

An employer intending to entrust work to a foreigner is required, above all:

- to check (before entrusting work) whether the foreigner has a valid document entitling him/her to stay in Poland, make a copy of this document and keep it for the whole period of employing the foreigner,

- to check if there is a requirement to apply for a work permit in relation to a person seeking employment,
- to direct an employee at his own expense for preliminary medical examinations in order to determine if he/she is capable to work in a given capacity,
- to provide minimum statutory remuneration (CHYBA at least) if the work is entrusted under a contract of employment or contract of mandate,
- to report a foreign employee to the Social Insurance Institution within 7 days from the date of the insurance obligation,
- to keep a record of working time and personal files (e.g. storing a copy of the foreigner's residency document),
- to set work regulations when an employer has more than 50 employees.

4. Shortage of professional drivers in Poland

According to the PwC report (Turka *et al.*, 2015), there are around 600-650,000 professional drivers in Poland, including 500-550,000 truck drivers. Currently, 20% of the transport company's experience constant shortage of drivers, and over 60% have periodic problems with necessary driving personnel to conduct transport activities. It is estimated that since joining the EU in 2004 the intensity of vehicle stock usage in Poland rose by 12-15% while the drivers' work intensity rose by 20%. The problem of drivers' shortage may lead in the future to disruptions in the transport-related industrial sectors, and thus this problem will have an impact on the entire Polish economy.

The deficit of professional drivers in Poland derives not only from significantly hard working conditions, but also from a negative image of the profession. In the last years, a number of campaigns were launched to change this perspective and encourage young people (including socially vulnerable groups, such as unemployed women or so-called NEETs - Not in Employment, Education and Training) to become professional drivers. The initiatives were taken by TSL industry, regional agencies and parliamentary entities. The most comprehensive campaign introduced so far was called 'Ready to go' which then transformed into a wider 'National Driver Training Programme' project after gaining the attention of the Members of Parliament. The main aim of such campaigns is to acquaint young Poles with the advantages of the professional driver occupation. Unfortunately, so far they have not reached a desired impact and employers are refocusing their interest on employing foreigners.

The PwC report (Turka *et al.*, 2015) shows that in recent years, the number of foreigners working for the Polish carriers has increased - in 2016 alone twice as many Ukrainians and Byelorussians arrived, compared to the previous year. In the long-term perspective, foreign workers will not eliminate the drivers' shortage, mainly due to the forthcoming human resources drain in Eastern Europe countries. The poor demographics of Ukraine in Belarus might eventually result in obtaining the workforce from more distant, post-Soviet countries, e.g. Kazakhstan.

The lack of professional drivers has been also addressed through regional, occupational development programs which provided funds for projects resulting in training aimed predominantly at NEETs (Bejnar, 2017).

Polish research organizations actively participate in targeting the professional drivers' deficit under Polish conditions. ICT-INEX project (Gasiorek and Matysiak, 2017) led by the Motor Transport Institute, aims at increasing the accessibility and effectiveness of training for professional driver candidates and professional drivers with the use of innovative ICT tools. The project is funded from Erasmus+ Programme and focuses on strengthening the wide recognition of innovative training methods which could significantly facilitate the training, increase its efficiency and eliminate the cost barrier which play a big role in entering the profession.

The project includes different educational and cultural contexts, since the foreigners from Partner countries (Poland, Finland and Austria) are coming both from different countries and need to go through different paths towards the professional driving profession. In the Polish

context, project's initial recommendations indicate that the need for introducing more professional drivers onto the market needs to be addressed by i.e. reasoning the procedures of obtaining initial qualification training by foreign employees which could be done by formally introducing the training in their mother tongues. Poland was identified as having fairly good conditions which yet still need to be strengthened by introducing legal framework allowing to provide the ICT-based, in situ training for foreign professional driving candidates as well as specific non-driving related training elements in Polish language.

The work permit authorizes foreigner to work legally in Poland, with the possibility of performing professional duties. The permits are not necessary in the case of, among the others, citizens of the EU and the European Economic Area and foreigners who have a permanent residency permit, holders of the Polish Charter, etc. Citizens of Ukraine, Georgia, Armenia, Belarus, Moldova, and Russia can work without permission 6 months during the year, which shows Table 3.

The employer who intends to employ a foreigner applies for a permit. As an attachment to the application, the regional governor's information regarding the needs of the labour market should be included. Earlier, the employer has to submit an offer at the Employment Office for a position on which he/she would like to hire a foreigner. If the offer does not attract any Polish citizens, then there are no obstacles to employ a foreign citizen.

Table 3. Number of statements registered by regional employment offices in the individual provinces in 2017, arranged by the citizenship (Gieranczyk, 2017)

Province	Citizenship						Total
	BY	RU	UA	MD	GE	AM	
Dolnośląskie	4501	794	209763	1488	1741	365	218652
Kujawsko – Pomorskie	1566	189	65636	1367	284	73	69115
Lubelskie	3027	226	81350	498	206	108	85415
Lubuskie	1695	379	75799	931	661	301	79766
Łódzkie	3096	331	141276	1057	981	186	146927
Małopolskie	1751	641	127231	3633	1058	186	134500
Mazowieckie	17840	1329	384388	9266	1313	625	414761
Opolskie	938	143	35830	623	418	108	38060
Podkarpackie	640	40	17205	228	67	10	18190
Podlaskie	4278	48	14715	93	124	24	19282
Pomorskie	7215	779	120182	2970	699	171	132016
Śląskie	2804	363	145893	2104	1254	187	152605
Świętokrzyskie	455	34	37273	1777	148	26	39713
Warmińsko – Mazurskie	1926	167	19412	1100	111	74	22790
Wielkopolskie	4620	437	172424	2948	1624	141	182194
Zachodniopomorskie	1694	250	66514	1382	437	201	70478
Total	58046	6150	1714891	31465	11126	2786	1824464

The point is that a foreigner can only be employed if no person registered as an unemployed in the employment office meets the employer's requirements. A work permit is issued for a definite period, not longer than 3 years and may be extended. Obtaining a work permit does not exempt from the requirements laid down in separate regulations that conducting regulated professions or economic activity depends on.

According to the Ministry of Family, Labour and Social Policy, 2016 was record-breaking both in terms of the number of work permits issued to the foreigners (over 127,000) and registered declarations of intention to entrust work to a foreigner (over 1.3 million). The

number of permits issued until the end of 2016 increased by approx. 94% compared to 2015, and registered declarations by approx. 68%. Also, in the first two months of 2017, the number of permits issued, and declarations registered continued to rise. Around 30,000 permits were issued in the January/February period (increase over 100% y/y) and about 290 thousand registered statements (increase of approx. 44% y/y).

The division of work permits with respect to the citizenship shows that the most dominant foreign employee group comes from Ukraine. In 2016, of the total number of permits issued, 83% (106,223 permits) concerned this group. In 2015, Ukrainian citizens referred to 76.71% of issued permits, in 2014 over 60%. Further countries of origin of the foreigners are Belarus (increase by 139% from 2015), Moldova, India, China and Nepal.

5. Conclusions

1. The creation of legal provisions is aimed at counteracting current abuses, better supervision over the employment-targeted migrations, as well as raising the standards of employing foreigners.
2. Legal regulations, decisive actions should be taken to mitigate the impact of the labour shortages on the Polish economy. Activities should be undertaken by both public administration, entrepreneurs and training centres.
3. According to the findings of ICT-INEX project, training of the foreigners in some labour demanding areas such as professional driving, should be facilitated in a way which could effectively shorten the time of entering the profession. In professional driving context, this can be done by implementing innovative ICT-based training tools which allow to take the training faster, even before arriving in the country.

References

1. Bejnar, K. (2017) *Narodowy Program Szkolenia Kierowców pomoże wykształcić 10 tys. kierowców zawodowych.* Available online at: https://www.trans.eu/pl/aktualnosci/narodowy-program-szkolenia-kierowcow
2. *Directive 2014/36/EU of the EP and the Council of 26 February 2014 on the conditions of entry and residence of foreign nationals for the purpose of employment as a seasonal worker.* (2014) OJ L 94, 28.3.2014, p. 375–390.
3. Gasiorek, K. and Matysiak, A. (2017) Outcomes of ICT-INEX project, *Guidelines for the integration of simulator-based training with other PD candidate training methods* (2017).
4. Gieranczyk, W. (2017) *Zezwolenia na pracę cudzoziemców w Polsce w 2017 r.,* Warsaw: Main Statistics Office.
5. The Polish act on change of engagement promotion in institutions of labour market and other acts. (2017) *Ustawa z dnia 20 lipca 2017 r. o zmianie ustawy o promocji zatrudnienia i instytucjach rynku pracy oraz niektórych innych ustaw.* Dz. U. 2017, pos. 1543.
6. The Polish act on engagement promotion in institutions of labour market. (2004) *Ustawa z dnia 20 kwietnia 2004 r. o promocji zatrudnienia i instytucjach rynku pracy*. Dz. U. 2004, no. 99, pos. 1001.
7. The Polish act on foreigners (2017) *Ustawa z 12 grudnia 2013 o cudzoziemcach.* Dz. U. 2017, pos. 2206.
8. The Polish act on the results of mandate of performance work to foreigners staying in spite of rules at republic of Poland area. (2012) *Ustawa z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej.* Dz. U. 2012, pos. 769.
9. *Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community* (2007) OJ C 306, 17.12.2007, p. 1–271.
10. Turka, R., Wojtczuk-Turek, A., Marczak, K. (2015) Report of Mazowieckie voivodship Labor Office. *Wsparcie młodych osób na mazowieckim rynku pracy.* Warsaw: Mazovian Labour Market Observatory.

RESEARCH and TECHNOLOGY – STEP into the FUTURE

ISSN 1691-2853 & ISSN 1691-2861 (on line)

THE JOURNAL IS DESIGNED FOR PUBLISHING PAPERS CONCERNING THE FOLLOWING FIELDS OF RESEARCH:

- mathematical and computer modelling
- mathematical methods in natural and engineering sciences
- computer sciences
- aviation and aerospace technologies
- electronics and telecommunication
- telematics and information technologies
- transport and logistics
- economics and management
- social sciences

Articles and review are presented in the journal in English, Russian and Latvian (at the option of authors). This volume is published without publisher editing.

EDITORIAL CORRESPONDENCE
Transporta un sakaru institūts (Transport and Telecommunication Institute)
Lomonosov 1, LV-1019, Riga, Latvia. Phone: (+371)67100594. Fax: (+371)67100535
E-mail: junior@tsi.lv, http:// www.tsi.lv

RESEARCH and TECHNOLOGY – STEP into the FUTURE, 2018, Vol. 13, No 4
ISSN 1691-2853, ISSN 1691-2861 (on-line: www.tsi.lv)

The journal of Transport and Telecommunication Institute (Riga, Latvia)
The journal is being published since 2006