The International Journal
ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/aims-and-scope-of-research/

SUSTAINABLE ENTREPRENEURSHIP IN CONDITIONS OF UN (SAFETY) AND TECHNOLOGICAL CONVERGENCE

Joanna Grubicka[1], Ewa Matuska[2]

[1]Pomeranian Academy, Arciszewskiego Str. 22D , 76-200 Słupsk, Poland
[2]Faculty of Management, Higher Hanseatic School of Management, Kozietulskiego Str. 6-7, 76-200 Słupsk, Poland

E-mails: [1]narl@poczta.onet.pl; [2]ematuska@whsz.slupsk.pl

Received 20 November 2014; accepted 20 January 2015

Abstract. These days the Internet has revolutionized lives not only of particular people, but it has also influenced the functioning of market economy in terms of globalization and technological convergence. The key condition of development and increase in popularity of e-services is maintaining the high level of social trust to this form of providing services and preventing social threats. The stability of functioning and information society development depends on open, reliable and safe cyberspace.

Keywords: convergence, information society, cybercrime, norms

Reference to this paper should be made as follows: Grubicka, J.; Matuska, E. 2015. Sustainable entrepreneurship in conditions of UN (Safety) and technological convergence, *Entrepreneurship and Sustainability Issues* 2(4): 188–197.
DOI: http://dx.doi.org/10.9770/jesi.2015.2.4(2)

JEL Classifications: O1

1. Introduction

Modern economy is subject to incessant changes. The connection of technological progress, lower transportation costs and liberalizing the policies within and outside the European Union have led to the increase in trade as well as the flow of foreign investments between the countries with all related consequences (Peker *et al.* 2014; Šabasevičienė, Grybaitė 2014, Korsakienė 2013; Matyasik 2014; Vosylius *et al.* 2013; Teivans-Treinovskis, Jefimovs 2012). Globalization changes the surrounding in which the companies operate. They must quickly adapt to such changes, which actually is the condition of their survival. It is of vital importance for the functioning of the EU economy. Although globalization brings profits and new opportunities, it also means that Europe must face fierce competition both from the side of low cost economies, such as China or India's economies as well as economies based on innovations, such as the America's one. That is of great importance for the present information revolution and its economic consequences is the connection of two originally remote technologies-communication technology related to the transmission of data with the computer technology that influences data processing (Fuschi, Tvaronavičienė 2014). This phenomenon requires from entrepreneurs to undertake an appropriate action plan. In order to facilitate it one must take into account more and more common

phenomenon of convergence. The phenomenon of *convergence* is based on conformity of the processes and systems, it facilitates blurring the boundaries and divisions, and in turn directly influences bonding the international cooperation and developing globalization processes. The word convergence derives from Latin *convergere* (gather) (Kopaliński 1971) and means concurrence. Convergence is appearing more and more often as a definition related to the phenomena occurring in modern media, IT and telecommunication. This expression defines conforming the devices that begin serving similar functions, although originally they were not technologically related to each other, so-called technological convergence. It happens in the area of infrastructure and transportation, which corresponds to the convergence of devices, services and converging the network. The development of e-services is, among others, the response to changing reality, variability and dynamics of the development of modern global, economy as well as creating a new reality, both a market and consumer one. There are many factors contributing to its present shape. The world has become a "global village", in which there is a constant flow of people, goods, services and new technologies. That means changing the standards of living, not once giving them a new shape and conditions. The propellers of convergence in the field of e-services are: the Internet, e-business, the rapid development of information and multimedia applications as well as the increase of computing power and decrease in their prices (Kamiński 2000: 20). The term *convergence* that appears in publications discussing technology, business, and trade and regulation issues in the area of electronic communication is the term relating mostly to the phenomena occurring mainly in modern media, IT and ITC. That is why the changes in the sector of information- communication technologies are labeled as the process of "information technology convergence", in which the integration of computers and ITC into one system of processing and exchanging information has established the new information architecture that enables the companies to gain a global competitive advantage (Laudon, K.C and Laudon, J.P. 1999: 23). Having the access to the network is becoming a must in terms of good functioning in the public life. It refers not only to private people, so owners of computers with the Internet access, mobile phones, smartphones, etc., but also companies, state and social institutions, which give the possibility of using the Internet in the workplace. In this context one can also discuss the general concept of e-offices, thanks to which such institutions can communicate with each other more easily, whereas clients and petitioners get an easier contact with companies and offices. E-consumers of modern services can experience convergence, so-called *place convergence* and technology convergence. There is a process of blurring the boundaries between workplace and house. Digital, internet software is used for creative work as well as management of this work and its control.

2. Process of technological convergence in a Polish e-consume life

Digital technology is present in many different fields of economy, which makes the technology in various fields related, which in turns makes the solutions convergence .The solutions convergence is based on unifying the methods of access to network, processes, services and applications (Białobłocki and Moroz 2006: 4). The companies that have the technological advantage enter many different fields in order to exploit them. Those are both the planes of activities that were not in existence before and the new ways of using and joining previous goods and services. The new areas appearing as a result of scientific research and through the division of the areas already existing are established and developed by the companies that work in related sectors. The development of each of those fields depends on and at the same time is the condition of the development of the other one. Their mutual integration facilitates the appearing of completely new goods and markets or it causes the complete change of rules and principles of conduct on the existing markets (Pierścionek 2000: 26). Along with the process of digitalizing and converging of the devices and networks there is most of all convergence of services. The Internet business belongs to the most dynamically developing sectors of national economy in the recent years, but is has also become a new way of providing services, among others in administrative, medical, educational, trade, financial services, tourism, insurance, culture and others. The commonly used by consumers convergences of services of access to the information enable higher standardization and e-clients service. Technological convergence, for example within the field of communication networks enables the companies, e-clients to, f.e. increase business flexibility, reduce costs , increase competence advantage, unify the computer environment, integrate the data, facilitate the management of the systems, simplify the process of service, reduce the time of goods delivery and services for clients, reduce the time and frequency of business workshops, and in case of the necessity of being in touch with the clients- makes it possible to provide services through

many channels of contact with company staff, for instance via mail, Skype or GG communicator. Literature points out three stages of the process of establishing information society. The first stage describes the emergence of companies and corporations that establish new ICT technologies, the second one refers to computerization of the basic sectors of economy and the last one characterizes wide use the new technologies in daily lives (Dąbrowska *et al.* 2009: 8). The rapid development of ICT networks and progress in this area made it possible for new companies that before were deprived of such a possibility to join the world economic system. By the means of a mobile phone, facsimile, and the Internet in particular there are more and more trade transactions made. E-services make it possible to perform economical acts efficiently and also enable the more flexible functioning of the companies, focus on creating new products and services, which in turn will generate profits. The reflection of such development of the technological process is creating the information society. It results in each member of the information society gaining the access to a wide range of resources offered in the network related to goods and consumer services (Grubicka 2012a: 17). E-business takes advantage of a number of Internet applications, where one can point out mail, websites as well as banners and other means of advertising to name but a few. Everything is aimed at one target, which is addressing possibly the largest group of potential clients and recipients. The concept of e-business includes e-commerce, but apart from it also encompasses the internal processes such as production, supplies management, product development, risk management, finances and management of knowledge and human resources. The strategy of e-business is aimed at saving costs and the improvement of effectiveness and production. It leads to the situation where the virtual form of providing services gives more possibilities of choice, and in turn on-line shopping. Nowadays offering the on-line services is the most advanced model of providing services in UE, with Poland being one of e-business leaders in Middle-Eastern Europe.

3. Level of consumer awareness contra consumer's sense of safety

The awareness of the existence of the information and e-services provided in an electronic way and the ability to use them are indispensable for the development of the information society and at the same time for the functioning of a human as a full-fledged member of the information society. According to the report by Forrester Research "European Online Retail Forecast: 2011 to 2016", ale in on-line shops in 17 main European markets will increase from € 96,706 million in 2011 to € 171,957 million in 2016. The yearly rate of sale will be 12,2%. Like in other European countries the value of Polish e-commerce market is rising dynamically year by year. There is still a growing number of internet shops in Poland. At the moment there are 11 thousand of them. Also, group shopping, which is now an important branch of e-commerce market, is gaining in popularity. The rationality of activities of Polish e-consumers is present when trying to buy the goods that are cheap and of good quality. The findings of Forrester Research show that the main reasons for which the consumers buy by in the Internet is time saving (69%) and the possibility to find the best possible offers (68%). Equally important for the consumers in the net is a wider than in traditional shops range of services and products. Moreover, 31% of the questioned claimed to follow the websites of on-line sellers so as to keep up to date with the latest trends.

What is the most important for every third Polish e-consumer while doing shopping different than daily groceries, is saving money. Also, one in three tries to buy the goods of the highest quality. One in four pointed out the convenience of on-line shopping as well as lack of time limits in terms of shop opening hours. Every sixth respondent stresses the fact that shopping in the Internet is more thought-over and that he does not buy on impulse (Wolny 2011: 28). The advantages of on-line shopping mentioned by Polish e-consumers include a wide range of goods. The buyer, having a great choice of the goods and brands available in the Internet, before buying looks for the information about the offer of interest to him. The most searched pieces of information available in the Internet are: price of products, technical data. E-buyer (Kolny *et al.* 2011: 21) looks for the information about the offers of different producers, promotions and the newest products, checks the time of realization of the order and reliability of the seller. Quite often the process of looking for the information does not finish the moment one finds the necessary information, the vast majority of consumers look for the same piece of information in many sources and compares it. The information about offer and the conditions of its purchasing can be available in various sources. The consumer looking for information can use traditional and internet sources. Traditional sources of market information are: family and friends, shop assistants in traditional shops, shop leaflets, package

and advertisements. The internet sources of product information are: producers' and sellers' websites, internet advertisements as well as industry forums. To sum up: e-consumer values time, choice and convenience most of all. It is worth paying attention to the fact, though, that a meaningful aspect that is behind such preferences can be not only rationalism, but also some kind of force reflecting the pressure of vital micro-economic and psychological factors. The most important factor seems to be the stress connected with a common uncertainty of employment (Matuska 2011:25), which is of key importance for the pattern of behavior of a consumer employee. E-consumer is most often an employee as well (apart from the meaningful group of representatives of the learning youth among e-consumers) who has no time for traditional shopping, whereas on-line shopping can be done during the break while working at the computer. Among new psychosocial risks of work in the research by ESENER (European Agency for Safety and Health at Work) the first places are taken by stressor of time pressure (52% of indications) and the stressor of contacts with difficult consumers (48% of indications). Perceived in that way e-shopping can be a form of defensive reaction to work related stress whereas surfing through the Internet shops during working hours can be a new symptom of professional burnout connected with stress at work (Matuska and Figurska 2010:25) or even a new type of defensive mechanism appearing in the form of e-shopaholism. These days, when the value of information is growing all the time, its safety is becoming a more and more common concept. Information is mostly associated with institutions but in fact it touches each of us- a potential user of the Internet (Benkler 2008:1). The growing importance of information causes the increase in their threats, which is why the protection of ICT systems and information processed there is the issue of utmost importance. One of categories of the safety of information is the safety of human resources (Białas 2006: 2). According to L. Ciborowski (1999: 6) safety of information is "information protection that is based on enabling and obstruction of getting the data of a physical nature of actual and planned condition of things and phenomena in its own space of functioning and obstructing the input of informative entropy to the announcements and physical destruction of media data". While doing shopping in the Internet shops we are forced to give our personal data in order to get an ordered product. The barrier for the development of e-market for the consumers apart from the Internet access is becoming lack of transaction safety. While shopping we reveal a great deal about our financial status, preferences, psychological profile. Our data, stored in the database of the internet shops, is incredibly valuable to any kind of advertising agency, competitive shops or it can be used by criminals in order to find potential wealthier victims, make extortions etc. The problem of safety, in any area, is subject to some certain laws. One can distinguish some truisms valid while designing and implementing security. One of such truisms is that there is no absolute safety. We are never able to predict in advance all the possible threats. The rapid development of information technologies implies appearance of still new threats. Nowadays computers realize a great number of activities that up till now have been humans' domain. They do that more quickly and more accurately. However, the imperfections of technology and security policy configuration pose the danger of underdeveloped in terms of safety and reliability of the IT product or its misusage o (Grubicka 2011: 15). Safety is often called the trustworthiness of the computer system, which can be described as trustworthy when it is:

- available- accessible up to date
- reliable- resistant to disorders
- secure- ensuring protection of data
- safe for the surrounding, eco-friendly.

The problem of safety in modern civilization influences versatility of computer technology. There is a number of threats, though the weakest link in the information safety is a human being (Grubicka 2011: 15). The easiest attack in cyberspace can be based on direct attacking the software in a given computer preventing its proper functioning; or the computer itself and causing lasting damage of its parts. Attacks for the data being of state or professional secret are aimed at taking the control over protected systems. Strengthening the protection of the system in terms of protecting critical infrastructure is a postulate to build stronger protection barriers in the cyberspace and physical sense. In the first case the most common way is using the passwords. Application and use of disposable passwords is a protection against its capturing and unauthorized usage in the future. Nowadays, in order to authenticate the users, one can take advantage the things which must be shown when being notarized. Those are, for example, magnetic cards, electronic cards or USB tokens. Moreover, in case of the people, one can take advantage of one's physical features owing to dissimilarity of natural parameters of body elements,

biometric authentication, such as, among others: DNA key, palm thermogram, palmprint, hand signature, voice (Grubicka 2011: 12). Other possible ways are firewalls and proxy servers. Physical barriers can be used in a number of ways: starting with protecting devices against electronic impulses and finishing with mere cutting the wires. Another possible precaution is internal fragmentation aimed at limiting possible damages and getting the possibility of quicker repair after a potential attack (Goodman 2008: 12). Creating backup copies of different versions of information in case of damaging the information enables quick restoration of functioning the system. A potential cybercriminal gets the access to the network forcing acceptance of his/her IP address as the network address, pretending to be a user of the real main computer. Using the program of sniffers type, which after being installed in the network that has been hacked, they get the information moving within this area, and the chosen pieces of it are copied on the attacker's disc. Thanks to programs of sniffers type one can get a lot of valuable information such as personal data, password access and much more. Another threat called Spoofing- forging IP addresses, is aimed at pretending to be the server in the existing network connection, that multiplies its damages even those apparently less dangerous threats (Tadeusiewicz 2008: 27). The technique is to avoid securities which are installed in a given server the administrators of the intranet as well as "impersonating" the network user, which enables the attacker to capture all the data that was supposed to get to the real computer. In accordance with the claim of one of the leading specialists in the area of IT safety, Bruce Scheiner, S*afety is the process, not a product….* Providing safety is not safety. Providing safety is not an easy task and requires constant work, planning and educating the users, which is not doable in each and every environment. Most of all, with no understanding of the scale and consequences of the potential threat one cannot talk about elaborating on an efficient strategy of fighting illegal cybercrime. An effective tool of control and improvement of the precautions implemented in the company is safety audit. Safety information audit is an independent and reliable assessment of the security status of all the areas of company activities, and more specifically it is the assessment of its accordance with normative documents. Thus, managing information safety requires compiling effective methods of preventing and fighting cybercrime and it should be an indispensable, incessant and systematic process of creating the policy of information safety and current updating the protection policy. It is a field bordering IT, law, marketing and organization, dealing with defining aspects of safety for institutions and their ICT systems, its achievements maintenance (Białas 2001: 2). Inefficient, invalid or inadequate principles, rules and mechanisms of protection are the meaningful threat as they give an illusionary sense of safety.

The basic document describing the safety policy is the ISO/IEC Technical Report 13335 norm. In Poland Polish norm PN-I-133335-1 is valid[1]. In this norm there are, among others, all the possible definitions of safety as well as the aims of computer systems safety policy. The norm is a multi-part document which encompasses the following concepts:

TR 13335-1 terminology and models

TR 13335-2 methodology of planning and conducting the risk analysis, specification of requirements of workplaces connected with ICT safety systems

TR 13335-3 techniques of managing safety

- managing the information protection
- managing IT systems configuration
- managing the changes

TR 13335-4 methodology of security selection

WD 13335-5 security of connection with external networks. The basics of system solutions in terms of information safety in the world scale is the British BS 7799 norm. The norm was filed by BSI [2] to International Norm Organization as the basics to establish an international standard of managing information safety. It was given the ISO/IEC17799 number, adapted as well as the Polish norm PN ISO/IEC 17799. When implementing this system of information safety in the company or administrative unit two norms are used most often:

---

1 Act 28.01.1999 r.; Title: „*Technika informatyczna – Wytyczne do zarządzania bezpieczeństwem systemów informatycznych – Pojęcia i modele bezpieczeństwa systemów informatycznych IDT ISO/IEC Tr13335"*

2 *British standards Institute* – the oldest in the world unit considered to be a leading institution in terms of normalization and certification

-PN ISO/IEC 17799:2007 – Information Techniques- Safety Techniques. Practical rules of managing information safety;
-PN ISO/IEC 27001:2007- Information Techniques - Safety Techniques- Systems of managing information safety - Requirements

According to the standard imposed by norm PN-ISO/IEC 17799, the basic attributes of safety of the information are confidentiality defined as the possibility to restrict the access to the information to only authorized people. Integrality is defined as the providing the completeness and accuracy of the information and the methods of its processing in order to prevent such modification of the data which could lead to its change or damage by unauthorized people. Availability is the possibility to guarantee that authorized people always have the access to suitable information whenever it is necessary (Białas 2006: 2). Standard ISO/IEC 17799 includes also descriptions of securities which should be applied in order to reduce the risk of losing the information. It is, among others, safety policy, safety organization, personal safety, management of systems and networks. Norm PN ISO/IEC 27001 is the basics to certify systems of management safety information. The norm in a complex way comprises all the concepts connected with managing information safety in a company, and within that physical, ITC and legal safety. Norm PN ISO/IEC 27001 is the component of the series of norms 27000. Their aim is to unify previous developments and standards devoted to safety of information. Strengthening the protection system in the area of critical infrastructure protection is a postulate to build stronger protection barriers in the cybernetic and physical sense. In the first case the most common is applying the system of passwords. Other possible ways are firewalls and proxy servers. Physical barriers can be used in a number of ways: starting with protecting the devices against electronic impulses and finishing with mere cutting off the wires. Another possible precaution is integral fragmentation that is aimed at reducing any possible damages and getting the possibility of quicker restoring after a possible attack (Goodman *et al.* 2007: 12). Making backup copies of the information versions in case of damage will enable the quick restoration of the functioning of the system.
Creating the Safety Policy should include the following stages:

- assessment of the information processed in the information system,
- classifying the value of gathered and processed information
- defining the appropriate directions of the information flow in the area of an administrative unit
- development of the information protection adapted to the peculiar information system
- development of the safety norms
- implementing Safety Policy
- development and protection of the Safety Policy.

The appropriate management of resources, including information resources, especially in the aspect of information safety requires the right identification of those resources as well as defining the place and way of its storing. The choice of the appropriate for the specific resources methods of management of its protection and distribution depends on the applied information carriers, type of applied devices, computer equipment and its software (Grubicka 2012b: 114). One can distinguish two leading strategies of information systems protection. The first, traditional one is based on risk analysis. Risk analysis identifies the areas of information system where it is required to introduce precautions. The precautions should be used first of all to protect the resources of the greatest value, which most often are the data and such resources that are at great risk and that are risk-prone. Conducting the risk analysis, alongside with allocating the appropriate priorities to a number of threats that could possibly influence the information system one should also carry out the suitable documentation in the form of risk analysis form. The risk analysis form should include such pieces of information as risk description, its potential consequence, assessed cost of eliminating the consequence, probability of its occurrence, description of precaution activities and the cost of securities. Another strategy is of more practical character. It derives from the assumption that abuse of safety in the information systems are inevitable (for example viruses attacks, hacking) and one must be prepared to handle it (Grubicka and Motyka 2011: 15). It is recommended to use security packets that include both antivirus protection as well as additional protection modules: anti-spam, antispyware/anti-adware, anti-phishing, heuristic and behavioral analysis as well as firewall and Web Filtering (limiting access to undesired WWW websites). Firewall, software system and device protection of the computer

linked to the network make remote logging impossible and give information about its users and the resources of the whole station. Apart from that there are also the functions of automatic critical backups of data or blocking the access of a user to some designated resources, for example applications, files and services. The used precautions should be chosen while keeping in mind the profile of a unit, its competences and the position of the user, as well as the fact whether the computer is a desktop or a laptop. Each working station should have an antivirus application installed that would comprise the modules protecting both against the known viruses, Trojans, worms or threats of spyware type as well as heuristic and behavioral analysis that can provide safety against unknown threats. The gate scanning the Internet movement does not protect particular working stations against a mean code brought on a CD or another mobile information carrier. As burglary protection one can also use different kinds of security software. There are many programs and software techniques of protecting the equipment. One of such software is Open Source program Prey, which not only protects the data but also a mobile computer against theft. Such an application, available for Windows, MacOS, Linux or Android platforms, send a report to a given e-mail address. In a prepared by the application report there is the following information: IP number at which a thief was logged on, the number of wireless networks in the vicinity, recently browsed Internet pages and a photo of a thief taken by an installed Webcam. All this information can help retrieve the stolen equipment. Thus, the development of legal infrastructure related to electronic transactions is a must. The popularizing of the Internet and directly connected with that electronic trade resulted in recent appearance of a number of legal issues previously unknown to the traditional legal system. While looking for causes of such a situation one can point out for example lack of general understanding in terms formal-legal definition of crime activity and types of behaviors supposed to be of crime character; different responsibilities of law enforcement and judiciary system to undertake trial activities connected with the access to computer systems and securing computer data as the evidence; maladjustment in particular countries procedure regulations connected with prosecution of computer crimes. Since that time there have appeared new technological and legal solutions, the level of revealing law violation committed by the usage of the computer or in ITC network has increased significantly, yet there is still visible lack of cooperation and heterogeneous state of regulations related to this type of crime in different countries, and the criminals avoid responsibility.

Unifying the law is indispensable everywhere where one deals with global network. Many countries introduce into the valid legal system regulations defining responsibilities for unauthorized access to computer data, where computer data is a wide expression encompassing digital data stored or processed by the means of either only one computer or a number of devices connected in one network or sent by the means of ITC network. Nowadays legal regulations related to the Internet are the most dynamically developing legal field and should be created at the national and international level. Global computer network enables exchange of data in the process of communication and making trade deals with clients (Dolińska 2010: 10). However, closing contracts in the Internet is connected with a number of threats for the interests of both parties of the deal, though especially for the consumer. Contracts made by the means of the Internet websites, internet shops, e-mail or other means of electronic communication belong to so called- distance sale contracts. As a result, the Internet caused the introduction of new legal regulations providing network users, especially e-consumers, with safety. A number of crimes that are particularly connected with illegal business in the Internet have been recognized. Those are for example:

-on-line financial services: share purchase, offers to gamble virtually or invitations to virtual casinos, money laundering in the form of cyberlaundering, frauds on auction portals, stocks and shares manipulation, documents forging, extortion and money theft, inaccurate documentation,

-wiretapping and surveillance, taking over electronic mail or blocking the account, hacking, phishing- getting PIN and credit card number captiously, which means confidential data by impersonating a trustworthy person or institution;

-cash-machine skimming- illegal card copying and withdrawing money by unauthorized people

-theft identity- by taking over the access to the account the criminal knows all the client's personal data, takes over his/her passwords, can look into financial operations, credit cards data, pension schemes, investments, insurances etc.

-dishonest competition and economic spying

-purchase over-the-counter medicines from the foreign countries in the country where it is illegal or where the procedure of admission the medicine to a given market is not over yet or mere fakes, etc. (Filipkowski 2007: 11).

The key condition of development and increase of e-services popularity is maintaining the social safety audit among potential consumers. These issues should be based on the user's sense of security (Dąbrowska *et al.* 2009: 8), which means lack of fear of illegal usage of personal data. Technical and organizational means indispensable to provide the processed data with confidentiality and integrity at the same time secure accountability of the number of activities causing the processing of personal data. The applied technical and organizational means indispensable to provide the processed data with confidentiality and integrity of the processed data must be adequate to the threats resulting from the ways as well the category of processed personal data (Grubicka and Motyka 2011: 15). These means should provide accountability of any activities, both in case of people and the systems undertaken in order to process the personal data. The evolution of threats is connected with the race of the attackers and defenders. Another significant reason of impossibility of reaching 100% security is human weakness, in particularly fallibility of designers, programmers, information system users which result in mistakes in system and application software and inappropriate and irresponsible usage. For e-consumers only those companies are trustworthy which on their sites put a complete regulations of purchases and with which one can contact by the means of phone. The reliability of the shop increases if it allows various forms of paying, it has esthetic and functional design and allows a personal pick-up of the ordered goods. In the light of the above reflections it is important to create the climate of trust of the consumer to e-shopping.

Conclusions

Convergence is not something spontaneous, it is the effect of human activities, decisions, goal setting, and evaluation of the effects. The phenomenon of convergence means a serious challenge for traditional business models, but it is also a threat to companies which will not manage to use convergence and will stay behind in the competitive race. Only educated and able to absorb the knowledge societies can efficiently build modern, competitive economy and at the same time participate in the effects, improvements of the conditions of functioning European market raising its competitiveness in comparison to other regions in the world. Antoine de Saint-Exupery words can serve as the motto here "*Those who are threatened by the technology development cannot distinguish between objectives and measures. Those who fight hoping to gain only materialistic goods will gain nothing worth living for*". Nevertheless, there is still a need for a number of activities- popularizing and arranging the knowledge on ITC safety, analyzing the importance of different aspects of the issue for the national safety, developing a unified model of activities with a view to increasing all the key systems for the countries, increasing cooperation with the private sector and also establishing and practicing schemes of activities that clearly define the competences of institutions and national services in crisis situations. It is in the interest of the country, as well as within its duties, to care about meeting the highest standards of protection. The cooperation between national and private subjects should be of subsidiary character, and in case of attack it is only a coordinated action that can prevent or significantly reduce the losses (Goodman *et al.* 2007: 12). Yet, it shouldn't be forgotten that progressive convergence imposes the revision of legal regulations, which creates indispensable aspect of trust to the institution offering the service motivated by the possibility of legal execution of the responsibility for potential damages connected with using a specific service.

References

Benkler, Y. 2008. *Bogactwo sieci. Jak produkcja społeczna zmienia rynki i wolność* [Network wealth. How social production changes markets and freedom] Wydawnictwa Akademickie i Profesjonalne [Academic and Professional Publishing House], Warszawa.

Białas, A. 2006. *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, [Information and services security in a modern institution and company] Wydawnictwa Naukowo-Techniczne [Science and Technical Publishing House], Warszawa.

Białas, A. 2001. *Zarządzanie bezpieczeństwem informacji* [Managing information security]. NETWORLD 3/2001.

Białobłocki, T.; Moroz, J. 2006. *Nowoczesne techniki informacji i komunikacji–ich rozwój i zastosowanie* [Modern techniques of information and communication - their development and application], in *Społeczeństwo informacyjne. Istota, rozwój, wyzwania* [Information society. Its essence, development and challenges]. Warszawa.

Ciborowski, L. 2009. *Walka informacyjna* [Information battle]. Wydawnictwo Marszałek [Marshall Publishing House], Toruń.

Dąbrowska, A.; Janoś – Kresło, M.; Wódkowski, A. 2009. *E-usługi a społeczeństwo informacyjne* [E-services and information society]. Difin, Warszawa.

Dolińska, M. 2000. *Zastosowanie Internetu w marketingu* [Internet application in marketing], *Przegląd Organizacji* [Organization Review] No 6.

Filipkowski, W. 2007. Internet – przestępcza gałąź gospodarki [Internet- criminal branch of economy], *Prokurator* [Prosecutor] No 1(29).

Fuschi, D.L.; Tvaronavičienė M. 2014. Sustainable development, Big Data and supervisory control: service quality in banking sector, *Journal of Security and Sustainability Issues* 3(3): 5–14. DOI: http://dx.doi.org/10.9770/jssi.2014.3.3(1)

Goodman, S. E.; Kirk, J. C.; Kirk, M. H. 2007. Cyberspace as a medium for terrorists, *Technological Forecasting & Social Change* 74 (2): 193–210.

Goodman, S.E. 2008. *Critical Information Infrastructure Protection, Responses to Cyber Terrorism*. Centre of Excellence Defence Against Terrorism, IOS Press, 2008 ISBN 978-1-58603-836-6

Grubicka, J. 2012a. *Bezpieczeństwo danych osobowych w administracji samorządowej przy wykorzystaniu środków komunikacji elektronicznej* [Personal data security in self government administration by means of e-communication], in Dziemianka, Z.; Stach, W. (Ed.) *Komunikowanie społeczne w badaniach młodych naukowców* [Social communication in young scientists' research]. Instytut Naukowo Wydawniczy [Science and Publishing Institute] Maiuscula, Poznań.

Grubicka, J. 2012 b. *Bezpieczeństwo państwa polskiego wobec cyberterroryzmemu* [Poland security against cyberterror] Metodologia badań bezpieczeństwa narodowego tom 1 [Methodology of national security research, volume 1], AON Warszawa.

Grubicka, J. 2011. *Przeciwdziałanie wiktymizacji zagrożeń internetowych – bezpieczeństwo* [Prevention of internet threat victimasation-security]Acta Po merania No 3, Chojnice.

Grubicka, J.; Motyka, R. 2011. *Człowiek jako ważne ogniwo zapewnienia bezpieczeństwa informatycznego jednostce administracyjnej* [Human being as an essentail link providing information security to an administrative unit], in Chrabkowski, M.; Tatarczuk, C.; Tomaszewski, J. (Ed.). Bezpieczeństwo w administracji i biznesie we współczesnym świecie [Security in administration and business in the modern world] p. II, Wyd. WSAiB Gdynia.

Kamiński, F. 2000. *Konwergencja w obszarze komunikacji elektronicznej* [Convergence in the area of e-communication]. Przegląd telekomunikacyjny [ICT Review].

Kolny, B.; Kucia, M.; Stolecka, A. 2011. *Produkty i marki w opinii e-konsumentów* [Products and brand names in e-consumers' opinion]. Helion, Gliwice.

Kopaliński, W. 1971. *Słownik wyrazów obcych i zwrotów obcojęzycznych* [Dictionary of Foreign Words and Expressions]. Rytm,Warszawa.

Korsakienė, R. 2013. Internationalization of construction firms: what strategy do they follow? *Entrepreneurship and Sustainability Issues* 1(2): 99–107. DOI: http://dx.doi.org/10.9770/jesi.2013.1.2(4)

Laudon, K.C.; Laudon, J.P. 1999. *Management Information Systems – A contemporary Perspective*, Macmillan Press Ltd.

Matuska, E. 2011. Bezpieczeństwo psychologiczne w zarządzaniu zasobami ludzkimi – potrzeba prewencji wypalenia zawodowego [Psychological safety in human resource management - the need for prevention of burnout], in Chrabkowski, M.; Tatarczuk, C..; Tomaszewski, J. (Ed.). Bezpieczeństwo w administracji i biznesie we współczesnym świecie [Security in government and business in the modern world]. Wyd. WSAiB Gdynia.

Matuska, E.; Figurska, I. 2010. Job insecurity during economic crisis time as a psychosocial stressor, in Vojtovic, S. (Ed.). *Health as a basis for human resources development*. *Eastern* European Development Agency, Podhajska (Slovakia).

Matyasik, M. 2014. Secure sustainable development: impact of social media on political and social crises, *Journal of Security and Sustainability Issues* 4(1): 5–16. DOI: http://dx.doi.org/10.9770/jssi.2014.4.1(1)

Peker, S.; Tvaronavičienė, M.; Aktan, B. 2014. Sustainable risk management: fuzzy approach to volatility and application on FTSE 100 index, *Entrepreneurship and Sustainability Issues* 2(1): 30–36. DOI: http://dx.doi.org/10.9770/jesi.2014.2.1(4)

Pierścionek, Z. 2000. *Nowe kierunki rozwoju przedsiębiorstw* [New directions of companies' development], in Pierścionek, Z. (Ed.). *Strategie rozwoju współczesnych przedsiębiorstw* [Development strategies of modern companies]. SGH, Poznańska, Warszawa.

Raport Internet Standard E-commerce 2011. V edition, September 2011. Available on the Internet: http://files.idg.pl/news/Raport_eCommerce_2011.zip [10.11.2013]

Raport ESENER. Europejskie badanie przedsiębiorstw na temat nowych i pojawiających się zagrożeń [European Survey of Enterprises on New and Emerging Risks], Europejska Agencja Bezpieczeństwa i Zdrowia w Pracy [European Agency for Safety and Health at Work], 2009. Available on the Internet: http:/www.eurofund.europa.eu/ESENER/pl.Pdf

Raport Forrester Research - European Online Retail Forecast 2011 to 2016. Available on the Internet: http://www.ipo.pl

Šabasevičienė, V.; Grybaitė, V. 2014. Main foreign direct investment factors as precondition of sustainable entrepreneurship: evidence from Lithuania, Central and Eastern Europe, *Entrepreneurship and Sustainability Issues* 1(4): 230–238. DOI: http://dx.doi.org/10.9770/jesi.2014.1.4(5)

Tadeusiewicz, R. 2008. *Człowiek w Społeczeństwie Informacyjnym* [Human being in Information Society], in Gielarowski, A.; Homa, T.; Urban, M. (Ed.). *Odczarowania – Człowiek w społeczeństwie*. *Humanitas – Studia* Kulturoznawcze [Breaking a spell cast- A human being in society]. Ignatianum, Kraków.

Teivans-Treinovskis, J.; Jefimovs, N. 2012. State national security: aspect of recorded crime, *Journal of Security and Sustainability Issues* 2(2): 41–48. DOI: http://dx.doi.org/10.9770/jssi.2012.2.2(4)

Vosylius, E.; Rakutis, V.; Tvaronavičienė, M. 2013. Economic growth, sustainable development and energy security interrelation, *Journal of Security and Sustainability Issues* 2(3): 5–14. DOI: http://dx.doi.org/10.9770/jssi.2013.2.3(1)

Wolny, R. 2011. *Dochody i wydatki polskich* e-konsumentów – analiza porównawcza [Income and expenses of Polish e-consumers-comparative analysis], *Handel Wewnętrzny* [Internal Trade] No. 09-10.

Joanna GRUBICKA, PhD is a Maths graduate, doctorate in technical sciences completed at Systems Research Institute Polish Academy of Sciences, lecturer at Plant Security Engineering in National Security Institute at Pomerania Academy in Slupsk. She has attended workshops on risk analysis for confidential information processed in ICT systems. The main area of academic interests is application of calculus of probability, statistics in reliability engineering, risk analysis and computer systems security.

Ewa MATUSKA, PhD is Assistant Professor and Chair of Management in Higher Hanseatic School of Management in Slupsk, Poland. Specialist in area of human resources management and organizational psychology. Research interests: innovations, competencies, psychological safety.