JOURNAL OF SECURITY AND SUSTAINABILITY ISSUES
ISSN 2029-7017 print/ISSN 2029-7025 online
2018 December Volume 8 Number 2
https://doi.org/10.9770/jssi.2018.8.2(2)

Scopus®

TOWARDS INTERNATIONALLY TUNED APPROACH TOWARDS CRITICAL INFRASTRUCTURE PROTECTION

Manuela Tvaronavičienė[1,2]

[1]Vilnius Gediminas Technical University, Saulėtekio 11, 10223 Vilnius, Lithuania

[2]General Jonas Zemaitis Military Academy of Lithuania, Šilo 5A, LT-10322 Vilnius, Lithuania

Received 20 March 2018; accepted 25 November; published 30 December

Abstract. Security of societies has become one of urgent issues in contemporary world. Too frequently we started encountering one or another form of malicious behavior, criminal activities or terrorism. New and complex threats highlight the need for further synergies and closer cooperation at all levels. Awareness, preparedness and resilience of societies emerge as key preconditions of further secure and sustainable economic development and general well-being. A special attention in those conditions has to be paid to development of theoretically grounded approach to protection of critical infrastructure (CIP), damage or disruption of which can be immensely harmful to unprepared and therefore vulnerable institutions and society. The aim of this paper is to lay theoretical foundations for theoretically grounded approach towards research in CIP area, in order to formulate, ultimately, an approach towards action, which, employing leadership societal stakeholders would allow to enhance awareness of society actors about the threats, i.e, to develop ability to recognize, prevent, and, in case of disaster, to resist to consequences of critical infrastructure infringement. Hence, enhanced resilience of society to critical infrastructure infringement is and ultimate goal of fostering of leadership for critical infrastructure protection.

Keywords: security; critical infrastructure protection

Reference to this paper should be made as follows: Tvaronavičienė, M. 2018. Elaborating internationally tuned approach towards critical infrastructure protection, *Journal of Security and Sustainability Issues* 8(2): 143–150.
https://doi.org/10.9770/jssi.2018.8.2(2)

JEL Classifications: K14

1. Introduction: insights into state-of-the art

The topic is not newly emerged, alas, still extremely urgent, especially for some European countries, which appear to be at the very start of this long marathon. European Commission indicated those hazards a decade ago. Hence, in the Directive 2008/114/EC - identification and designation of European critical infrastructures and assessment of the need to improve their protection Critical infrastructure is defined as: "assets or systems essential for the maintenance of vital social functions, health, safety, security, and economic or social wellbeing of people. European critical infrastructure (ECI) is critical infrastructure in EU countries whose disruption or destruction would have a significant impact on at least 2 EU countries (e.g. electricity power plants or oil transmission pipelines)".

The related documents are: Communication from the Commission to the Council and the European Parliament - Critical Infrastructure Protection in the fight against terrorism (COM(2004) 702 final, 20.10.2004), Green Paper on a European programme for critical infrastructure protection (COM(2005) 576 final, 17.11.2005), Communication from the Commission on a European Programme for Critical Infrastructure Protection (COM(2006) 786 final, 12.12.2006), Commission Staff Working Document on a new approach to the European

Programme for Critical Infrastructure Protection: Making European Critical Infrastructures more secure (SWD(2013) 318 final, 28.8.2013).

The Commission has funded over 100 diverse projects under the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks programme (CIPS), during the 2007-2012 period. The programme is designed to protect citizens and critical infrastructures from terrorist attacks and other security incidents by fostering prevention and preparedness, namely by improving the protection of critical infrastructures and addressing crisis management**.** The key objective is to support CIP policy priorities by providing expert knowledge and a scientific basis for a better understanding of criticalities and interdependencies at all levels.

Despite all those efforts and activities, CIP remains urgent unsolved issue, there are a lot of known unknowns and unknown unknowns, especially when we talk about such actors of society, as universities, NGOs, small business companies, which is not directly related with CIP and therefore even more ignorant and vulnerable.

Due to the lack of understanding of origin and symptoms of the attacks, those actors can become easy targets and transmitters of hazards, e.g. related to cyber deceptions. Attacks on citizens, small companies, public companies due to lack of well-developed and well communicated strategies can cascade into consequences, which could appear to be harmful ultimately to infrastructure, which is described as "critical" by the European Commission (EC). Here we want to point out that description of critical infrastructure, provided by the EC just point attention to the most vivid examples of critical infrastructure, while in the reality the scope and spectrum of this infrastructure might appear much wider. According Ambassador Francesca Tardioli, Deputy Assistant Secretary General of NATO's Operations Division,

"To face such wide-ranging threats and challenges, no single organisation can work in isolation," says. *"A comprehensive approach, involving a myriad of international and national organisations, public-private partnerships and academia, is required"* (NATO news).

The p aims to contribute to CIP by involving actors, which do not directly act as critical infrastructure protectors, alas, can contribute by formulating aa approach towards research and innovations in critical infrastructure protection area, which would embrace foreseeing of threats, monitoring of polymorphous changing environment, preventing the threats identified and responding in organized and efficient way to mitigate to consequences if case critical infrastructure was infringed.

Main aim is to contribute to resilience of society against threats related to attacks on critical infrastructure. A resilient society can not merely be a governmental responsibility. It can only be achieved by combining governmental capabilities with those of private partners and individuals. Main aim is to create a shared understanding of Critical Infrastructures, the consequences of disruption and how European cooperation can contribute to enhancing resilience society to Critical Infrastructures infringement. This aim can be reached through intense and innovative learning experience together with colleagues from various organizations, disciplines and countries. The activities focus on cooperation in order to bolster the protection of Critical Infrastructure by bringing together relevant stakeholders in this field.

2. Insigts into to critical infrastructure problematics' roadblocks from stakeholders' point of view

As it was provided above, there has been a lot of attention to problematics of critical infrastructure protection from side of the European Commission, NATO and some governments of some countries, which already adopted legislation in this field (e.g. Spain), and other governments (e.g. Lithuania), which make concrete effors in order to start solving this complex issue of global character.

Alas there is still not unanimoust agreement what has to be included to this complicated network of critical infrastructure. Some authors put emphasis on public infrastructure, coorectly indicating that it is hudge investment, which has to be "reliable". Other authos, as e.g. Brown et al. (2006) indicates that "reliability is

not the answer. We must protect collections of critical components in our infrastructure systems, rather than backing up the least-reliable components. Malicious, coordinated attacks can be more damaging than random acts of nature.“ Since the authors looks at the broad issue of critical infrastructure protection from the military point of view, they make further a valuable insight by saying that „the defender must protect a huge, dispersed target set, while the attacker need only focus on a small set of targets chosen to maximize damage“.

Right here we wanted to continue the elaboration of the issue right from this correct point. It is absolutely obvious that critical infrastructure can not be protected just by increasing realibility of public sector, just by employing military forces, and adopting legislation, which would oblige certain companies to strengthen their infastructure and to attribute some resources for protection of their infrastructure.

Let us pint out that what is being called “critical infrastructure” in contemporary world is closely connected with all infrastructure available. Once we talk about “assets or systems essential for the maintenance of vital social functions, health, safety, security, and economic or social wellbeing of people“ then we need to realize that it is not just public sector, it is private sector as well. In some cases, depeding, on economic policies in privatization of public functions, that might be even private secors prevailing. That concerns any area, to be it electricity supply, banking, health care organizations, banks, or water supply companies.

Hence, it is absoulutely clear that critical infrastructure embraces public sector plus private sector (organizations and private-public companie, private companies), which comprise interlinked infrastructure. Naturally, a question arrises, if infrastructure of households can be attributed to critical infrastructure. Most likely we need here to look at at the activities, into which the households are engaged. If e.g. household is socially responsible and has installed solar panenels, produces solar energy and sells the surplus of this energy in this process utilizing smart grids, then we can say, rather firmly, most likely that this household is a part of critical infrastructure. In this case attack on this particular stakeholder can, most likely, infrindge smart grid system. We can find many more examples of similar character, since householders nowadays has become an itegral part of various kind of infrastructures, which, ultimately, appear to be critical. Let us try to provide a schematic interconnection of critical infrastructure areas, or to put it in a professional language, so called ‘domains” (Figure 1).

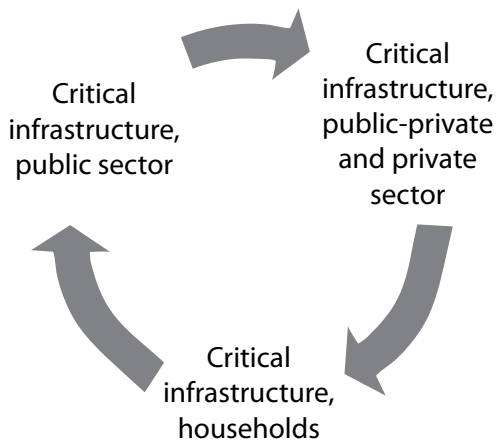

Figure 1. Interconnection of critical infrastructure domains

To conclude, critical infrastructure has to be understood much broadly than perception of critical infrastructure provided in definition above, i.e. at the very beginning of the paper.

Hence the first roadblock of the whole critical infrastructure protection system is to indicate the whole spectrum of critical infrastructure components and make classification of those elements, which ultimately, could transform into standards, which could adapted for more wide use of wide range of stakeholders.

After defining what contains a system of critical infrastructure, and classifying it, we could go further, by

elaborating system of defense and resilience to consequences of its infringement. That would be seen as another roadblock in the research. Military is ready to undertake defense functions, alas, it is obvious that such approach is not sufficient. Most likely, all public, public-private sector and stakeholders will need to contribute to the protection. Simplified depiction of process and factors of critical infrastructure protection is presented in Figure 2.

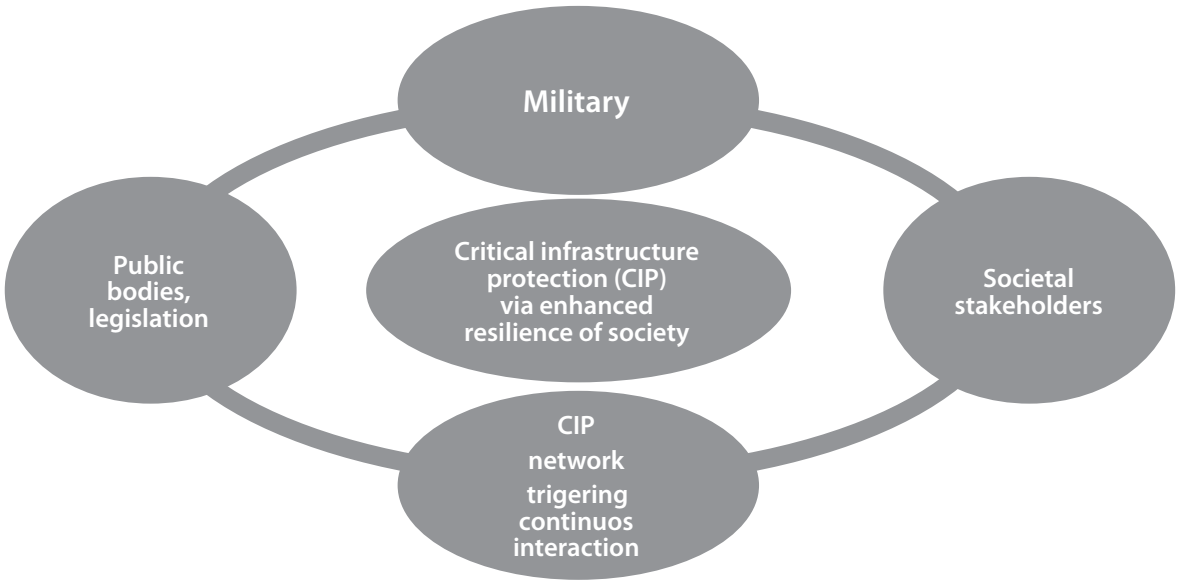

Figure 2. Process and factors of critical infrastructure protection

Here a lot of known unknowns and unknown unknowns will arise, e.g. who would finance critical infrastructure protection, especially when it comes to private sector and households, how to gauge the threats, and recognize damage, how to neutralize infringements, how to deal with consequences if any in organized and prudent ways. Those only questions raised, which will have to be put on the international agenda sooner or later, alas, better sooner.

In order to approach such complex problematics as critical infrastructure protection a grounded methodology, or approach has to be devised. As we already indicated above, currently description of critical infrastructure is too general, the spectrum of foreseen threats, respectively is still rather fragmented. Cybersecurity issues in rather frequently is perceived as synonymous of security of critical infrastructure (e.g. Protecting Critical Infrastructure in the EU 2010; Korauš et al. 2016; Korauš et al. 2017; Veselovská et al. 2017; Korauš, Kelemen 2018; Limba et al. 2017a; 2017b; Šišulák 2017; Limba, Šidlauskas 2018; Prause, Atari 2017). Other examples of the focus are: energy networks (Shakhovskaya et al. 2018; Banerjee et a. 2018), including electrical power grids (Weaver et al. 2018); water distribution system is being considered as critical infrastructure element, alas "assess the detection of attacks and vulnerabilities" remains an issue under discussion (Deng et al. 2017; Palleti et al. 2018). Here we need to point out, protection of that natural resources, such water (lakes, rivers), forests, infrastructure as food reservoirs, etc. are not being included into critical infrastructure perception, at least at the current moment, despite their significance for society cannot be underestimated (e.g. Tireuov et al. 2018; Arbidane, Mietule 2018; Cardoso et al. 2018; Muniz et al. 2018; Monni et al. 2018; Iorio et al. 2018).

We claim that the diverse perceptions, knowledge and experience have to be pulled, in order to come to novel approaches, insights, reveal unknown unknowns, which will facilitate developing resilient societies. Interaction of inter and multidisciplinary approaches, we believe, would foster birth of unconventional ideas and solutions, allowing to reduce fragmentation of efforts and increase of efficiency in using of resources, both public, and private (Batkovskiy et al. 2018; Žižka et al. 2018; Fomina et al. 2018; Oganisjana et al. 2017; Wang et al. 2018).

We believe that critical infrastructure protection issues, which are issues of the global scale and cause immense

threats of wide range could be tackled through capacity building of stakeholders via technology transfer, which will ultimately lead to building of one of world-leading CIP Competence Network. Though research, expertise sharing, good practices, cases, scenarios building and active community engagement, CIP Competence Network aims at increasing awareness, expertise and resilience across wide array of domains. To wrap up, capacity-building objectives are:
1. Bringing together relevant organizations, both on the national level and in the EU and beyond.
2. Strengthening awareness of:
• The need for cooperation for protecting of critical infrastructure.
• The need for joint exercising of academic, i.e. research and technology organizations (RTOs) and other stakeholders, such as NGOs, business companies, decision making bodies etc. for more efficient protecting of wide range of critical infrastructures.
3. Enhancing ability of international societal actors to recognize, prevent and react to infringements of Critical Infrastructure including mitigation of cross-border effects.

Here we need to point out that there were a lot of efforts at European and/or international level put already for the solving issues related to critical infrastructure protection. Besides already above mentioned documents, the following actions can be mentioned. Hence, the European Commission has developed a Critical Infrastructure Warning Information Network (CIWIN) and European Reference Network for Critical Infrastructure Protection (ERN-CIP). Those effort have to be supported by multiple emerging networks concerned about critical infrastructure protection, which ultimately would develop abibily to share, discuss and generate novel approaches leading to fruifuil outcomes related to critical infrastructure protection and enhancement of resilience of international community to the possible disasters.

2. Suggestions for further elaboration of critical infrastructure protection directions

Here I wanted to provide insights and suggestions, which I believe could facilitate finding new paths from blind alleys. Hence, after just three decades of massive use of the accessible Internet, which accelerated globalization process, we are forced to talk about critical infrastructure protection. Threats to the critical infrastructure, or just infrastructure, have been caused by many factors, among which is very high level of interlinking of complex systems. The task of protection of interlinked complex systems is very challenging, therefore parallel tasks of another character have to be raised, i.e. conditional autonomy and independence in terms of accessibility of certain objects of crucial importance has to be reconsidered. In the conditions of global accessibility, inaccessible islands have to be re-created, or restored, it could be put in such a way. Various innovative unconventional alternatives to contemporary style of interacting have to be through trough and implemented, ultimately. Only diversity of ways to responding to critical infrastructure protection challenges could lead to efficient and smart solutions.

Conclusions

Despite critical infrastructure protection is not a new topic in the political, scientific and practical landscape of the EU and other countries, a systematic approach towards this contemporary threat of huge scale has not yet been develop.

There are a lot of rather fragmented attempts to tackle this issue, alas majority of them concentrate to cybersecurity threats to energy supply, water distribution, transport disruptions etc. Despite those valuable efforts frequently supported by the European Commission and NATO guiding documents and funding, there is still a lot of room for further elaborations in the area of Critical Infrastructure Protection.

We claim, that leadership in this domain is crucial, since can lead to collaboration of internationally scattered stakeholders for commonly joint actions directed to development of methodology of Critical Infrastructure research and development, involvement of wide range stakeholders and creation of new critical infrastructure protection competence networks. Those attempts would allow to consolidate gradually fragmented

competences and, with active involvement of wide range of societal actors would ultimately allow to develop resilience of society to wide array of known and unknown threats (e.g insecurity of small actors, which could transfer threats in myriad way to other e.g. servicing companies, what is probability of such risks, what is level of interdependency of societal actors, etc). Essence of such resilience would lie in the systematic research and innovations in the area of critical infrastructure protection, which would lead to novel and unconventional well thought trough strategy in this crucially important area.

References

Arbidane, I., Mietule, I. 2018. Problems and solutions of accounting and evaluation of biological assets in Latvia, *Entrepreneurship and Sustainability Issues* 6(1): 10-22. https://doi.org/10.9770/jesi.2018.6.1(1)

Banerjee, J., Basu, K., Sen, A. 2018. On hardening problems in critical infrastructure systems, *International Journal of Critical Infrastructure Protection* 23: 49-67. https://doi.org/10.1016/j.ijcip.2018.08.001

Batkovskiy, A. M., Kalachikhin, P. A., Semenova, E. G., Telnov, Y. F., Fomina, A. V., Balashov, V. M. 2018. Conficuration of enterprise networks, *Entrepreneurship and Sustainability Issues* 6(1): 311-328. https://doi.org/10.9770/jesi.2018.6.1(19)

Brown, G., Carlyle, M., Salmerón, J., Wood, K. 2006. Defending Critical Infrastructure, *Interfaces* 36: 530–544. http://hdl.handle.net/10945/36732

CIPS https://ec.europa.eu/home-affairs/content/specific-programme-prevention-preparedness-and-consequence-management-terrorism-and-other_en

COMMISSION STAFF WORKING DOCUMENT on a new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures more secure 2013. https://ec.europa.eu/energy/sites/ener/files/documents/20130828_epcip_commission_staff_working_document.pdf

Communication from the Commission to the Council and the European Parliament - Critical Infrastructure Protection in the fight against terrorism. 2004. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52004DC0702&from=ES

Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. In force ELI: http://data.europa.eu/eli/dir/2008/114/oj

Critical Infrastructure Warning Information Network (CIWIN) https://ec.europa.eu/home-affairs/what-we-do/networks/critical_infrastructure_warning_information_network_en

Cardoso, P. P., Swan, A., Mendes, R. 2018. Exploring the key issues and stakeholders associated with the application of rainwater systems within the Amazon Region, *Entrepreneurship and Sustainability Issues* 5(4): 724-735. https://doi.org/10.9770/jesi.2018.5.4(2)

Green Paper on a European programme for critical infrastructure protection/* COM/2005/0576 final */ In force https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=celex:52005DC0576

Communication from the Commission on a European Programme for Critical Infrastructure Protection/* COM/2006/0786 final */In force https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52006DC0786

European Reference Network for Critical Infrastructure Protection (ERN-CIP) https://ec.europa.eu/home-affairs/what-we-do/networks/critical_infrastructure_warning_information_network_en

Fomina, A. V., Berduygina, O. N., Shatsky, A. A. 2018. Industrial cooperation and its influence on sustainable economic growth, *Entrepreneurship and Sustainability Issues* 5(3): 467-479. https://doi.org/10.9770/jesi.2018.5.3(4)

Iorio, M., Monni, S., Brollo, B. 2018. The Brazilian Amazon: a resource curse or renewed colonialism?, *Entrepreneurship and Sustainability Issues* 5(3): 438-451. https://doi.org/10.9770/jesi.2018.5.3(2)

Korauš, A., Kelemen P. 2018. Protection of persons and property in terms of cybersecurity in Ekonomické, politické a právne otázky medzinárodných vzťahov 2018/Economic, Political and Legal Issues of International Relations 2018. Fakulta medzinárodných vzťahov Ekonomickej univerzity v Bratislave, 1-2 Júna 2018, Virt, Vydavateľstvo EKONÓM, ISBN 978-80-225-4506-8, ISSN 2585-9404

Korauš, A., Dobrovič, J., Ključnikov, A., Gombár, M. 2016. Customer Approach to Bank Payment Card Security and Fraud, *Journal of Security and Sustainability Issues* 6(1): 85–102. http://dx.doi.org/10.9770/jssi.2016.6.1(6)

Korauš, A., Dobrovič, J., Rajnoha, R., Brezina, I. 2017. The safety risks related to bank cards and cyber-attacks, *Journal of Security*

and Sustainability Issues, 6(4): 563-574. http://doi.org/10.9770/jssi.2017.6.4(3)

Korauš, A., Veselovská, S., Kelemen P. 2017. Cyber security as part of the business environment in Zborník z konferencie Medzinárodné vzťahy 2017: Aktuálne otázky svetovej ekonomiky a politiky, Smolenice 30. Novembra - 1. Decembra 2017, Vydavateľstvo Ekonóm, 1113 s., ISBN 978-80-225-4488-7, ISSN 2585-9412

Limba, T., Agafonov, K., Paukštė, L., Damkus, M., Plėta, T. 2017a. Peculiarities of cyber security management in the process of internet voting implementation, *Entrepreneurship and Sustainability Issues* 5(2): 368-402. https://doi.org/10.9770/jesi.2017.5.2(15)

Limba, T., Plėta, T., Agafonov, K. Damkus, M. 2017b. Cyber security management model for critical infrastructure, *Entrepreneurship and Sustainability Issues* 4(4): 559-573. https://doi.org/10.9770/jesi.2017.4.4(12)

Limba, T., Šidlauskas, A. 2018. Secure personal data administration in the social networks: the case of voluntary sharing of personal data on the Facebook, *Entrepreneurship and Sustainability Issues* 5(3): 528-541. https://doi.org/10.9770/jesi.2018.5.3(9)

Monni, S., Iorio, M., Realini, A. 2018. Water as freedom in the Brazilian Amazon, *Entrepreneurship and Sustainability Issues* 5(4): 812-826. https://doi.org/10.9770/jesi.2018.5.4(8)

Muniz, J., de Melo, M. d., Liberato, M. A., Wahnfried, I., Vieira, G. 2018. Towards sustainability: allowance rights for using water resources in Amazonas State of Brazil, *Entrepreneurship and Sustainability Issues* 5(4): 761-779. https://doi.org/10.9770/jesi.2018.5.4(5)

NATO news https://www.nato.int/cps/en/natolive/news_92793.htm

Oganisjana, K., Svirina, A., Surikova, S., Grīnberga-Zālīte, G., Kozlovskis, K. 2017. Engaging universities in social innovation research for understanding sustainability issues, *Entrepreneurship and Sustainability Issues* 5(1): 9-22. https://doi.org/10.9770/jesi.2017.5.1(1)

Palleti, V.R., Joseph, J.V., Silva, A. 2018. A contribution of axiomatic design principles to the analysis and impact of attacks on critical infrastructures**,** *International Journal of Critical Infrastructure Protection* 23: 21-32 https://doi.org/10.1016/j.ress.2016.10.015

Prause, G., Atari, S. 2017. On sustainable production networks for Industry 4.0, *Entrepreneurship and Sustainability Issues* 4(4): 421-431. https://doi.org/10.9770/jesi.2017.4.4(2)

Protecting Critical Infrastructure in the EU. 2010. https://iris.luiss.it/retrieve/handle/11385/36860/860/Critical_Infrastructure_Protection_Final_A4.pdf

Shakhovskaya, L., Petrenko, E., Dzhindzholia, A., Timonina, V. 2018. Market peculiarities of natural gass: case of the Pacific Region, *Entrepreneurship and Sustainability Issues* 5(3): 555-564. https://doi.org/10.9770/jesi.2018.5.3(11)

Šišulák, S. 2017. Userfocus - tool for criminality control of social networks at both the local and international level, *Entrepreneurship and Sustainability Issues* 5(2): 297-314. https://doi.org/10.9770/jesi.2017.5.2(10)

Tireuov, K., Mizanbekova, S., Kalykova, B., Nurmanbekova, G. 2018. Towards food security and sustainable development through enhancing efficiency of grain industry, *Entrepreneurship and Sustainability Issues* 6(1): 446-455. https://doi.org/10.9770/jesi.2018.6.1(27)

Veselovská, S., Korauš, A., Polák, J. 2018. Money Laundering and Legalization of Proceeds of Criminal Activity, Second International Scientific Conference on Economics and Management - EMAN 2018 , March 22, Ljubljana, Slovenia, Printed by: All in One Print Center, Belgrade, 2018, ISBN 978-86-80194-11-0 https://doi.org/10.31410/EMAN.2018

Žižka, M., Valentová, V. H., Pelloneová, N., Štichhauerová, E. 2018. The effect of clusters on the innovation performance of enterprises: traditional vs new industries, *Entrepreneurship and Sustainability Issues* 5(4): 780-794. https://doi.org/10.9770/jesi.2018.5.4(6)

Wang, S., Stanley, H. E., & Gao, Y. 2018. A methodological framework for vulnerability analysis of interdependent infrastructure systems under deliberate attacks, *Chaos, Solitons and Fractals* 117: 21-29. https://doi.org/10.1016/j.chaos.2018.10.011

Weaver, G.A., Klett, T., Holcomb, T. 2018. Structure and Function of Interconnected Critical Infrastructures. Proceedings - Resilience Week 2018, RWS 2018, art. no. 8473545, pp. 95- 99. https://doi.org/10.1109/RWEEK.2018.8473545

Deng, Y., Song, L., Zhou, Z., Liu, P 2017. Complexity and vulnerability analysis of critical infrastructures: a methodological approach, *Mathematical Problems in Engineering*, Article ID 8673143 https://doi.org/10.1155/2017/8673143

Short biographical note about the contributors at the end of the article (name, surname, academic title and scientific degree, duties, research interests):

Prof. Manuela TVARONAVIČIENĖ
ORCID ID: orcid.org/0000-0002-9667-3730

Register for an ORCID ID:
https://orcid.org/register