International Journal for Quality research
UDK- 007 /005.6
Short Scientific Paper (1.03)

NEW MODEL FOR QUANTIFICATION OF ICT DEPENDABLE ORGANIZATIONS RESILIENCE

Zora Arsovski[1], Slavko Arsovski[2], Aleksandar Aleksić[3], Miladin Stefanović[4], Sonja Grubor[5]

[1]Faculty of Economics, Kragujevac, mail adress: zora@kg.ac.rs
[2,3,4,5]Faculty of Mechanical Engineering, Kragujevac, mail:
[2,5] cqm@kg.ac.rs;
[3] aaleksic@kg.ac.rs
[4] miladin@kg.ac.rs

***Abstract:** : Business environment today demands high reliable organizations in every segment to be competitive on the global market. Beside that, ICT sector is becoming irreplaceable in many fields of business, from the communication to the complex systems for process control and production. To fulfill those requirements and to develop further, many organizations worldwide are implementing business paradigm called – organizations resilience. Although resilience is well known term in many science fields, it is not well studied due to its complex nature. This paper is dealing with developing the new model for assessment and quantification of ICT dependable organizations resilience.*

***Key words:** Resilience, ICT dependable organizations, Quantification model*

1. INTRODUCTION

The concept of resilience had a turbulent history over the last 20 years. It originated in the study of ecosystems, and later it was the subject of study in biological, economic, organizational and information systems.

This paper contains some of the typical approaches to resilience which are used in the authors work during developing the new model for quantifying ICT dependable organisations resilience. In the literature that treats a resilience, there is more ideas that identify concept of resilience from another point of view. In that way, the ecological resilience, engineering resilience, social resilience, organizational resilience can be distiguinshed. The history was dominated by empirical observations of ecosystem dynamics interpreted in mathematical models, developing into the adaptive management approach for responding to ecosystem change. [1]

Each of these concepts has its own structure and laws that are increasingly common to all concepts. Gallopin [2] proposed a conceptual model of vulnerability, resilience and the capacity of response. According this author, resilience is addressed to the capacity of response and system vulnerability. Capacity of response has two components: (1) The ability of the system and (2) the ability of systems to improve their own conditions.Some authors treat the capacity of the response as resilience and some of them as a component of resilience that reflects the aspect of learning in relation to the behavior of the system during disturbances.The contribution of this paper is developing the new model for keystone vulnerabilities of the one organization which is one component of organizational resilience.

2. LITERATURE REWIEV

2.1 The resilience concept

Many organizations today become ICT dependable in many business segments, from communication to products development and economic transfers. That is the main reason why on ICT resilience need to focus attention – in order to achieve support for entire business resilience organization and improve it.

Whitson et all [3] defined a concept of resilience in ICT sector as a component importance measure related to network reliability. According to them, resilience can be defined as a composite of: (1) the ability of a network to provide service despite external failures and (2) the time to restore service when in the presence of such failures. This paper presents the specific aspects of quantifiable network resilience when the network is experiencing potential catastrophic failures from external event and when it is not known a priori which specific components within the network will fail. Authors proposed a formal definition for Category I resilience and defined a step – by – step approach based on Monte – Carlo simulation to calculate it. To illustrate the approach, authors considered the two – terminal networks with varying degrees of redundancy. The results obtained for test networks show that this quantifiable concept of resilience provides insight into the performance and topology of the network.

Arsovski et all [4] investigated impact of Information Systems (IS) on organizational resilience. One of the conclusion of this paper is that of Information Systems (IS) on organizational resilience is through: (1) higher level of knowledge and transparency of business processes, (2) higher level of flexibility, agility and sustainability of organization, (3) enhancement of key competiveness forces, (4) enhancements of awareness about business risks and vulnerability of organizations, (5) enhancement of speed of organization recovery, (6) enhancement of organizational culture and awareness about resilience and (7) supporting the organization sustainability. The second conclusion is that each possible impact of IS varies and depends upon two sides and their relations: (1) characteristics of IS which is related to ICT characteristics and (2) characteristics of organization. Because that, authors made clear different approaches to IS – and organizational resilience and established the model for simulation of this impact. This model is evaluated on an example and presented as a case study.

The paper of Watanabe et all [5], studies a resilience structure for high-technology firms that are experiencing mega competition. Authors claim that the construction of a co-evolutional structure between enhancement of core competences and agile correspondence to dynamically changing external circumstances is essential. External circumstances are related to the dynamic change in customer preferences and competitive conditions. One of the main issues is vulnerable business structure that may be one of outcomes from organizational strategy that is direceted to the implementing new ICT solutions in their business. Qualitative solution for the business development can be obtained using systems resilience incorporating in a stable innovation terms.

In their paper, Murray et all [6], were discussing that companies can develop a resilient capacity through the development of virtual teams and usage enabling technologies such as video-conferencing. Using technologies such as video-conferencing can be qualitative solution when organization has to meet new challenges and overcome them. Authors claim that this solution will enable organizations to respond to the challenges faster and to adapt better.

Huynh et all [7] were dealing with the issue of the choosing the most resilient network service technology related to the organization's field of business. Authors were studying a wide spectrum of applications, ranging from the minimal constraints of home networks to the rigorous demands of Industrial Ethernet Networks. This was followed by a thorough examination of Ethernet layer resilience technologies. Finally, authors proposed the resilience characteristics that are key for each class of application

Davies and Tryfonas [8] have noticed that amongst average computer users there is a global lack of trust when using the Internet. Authors think that this is particularly orientated towards its commercial use and online purchasing, so it requires from website developers to create and maintain web applications that are robust and provide a certain degree of resilience to attack from outside threats. Authors of this paper contributed by providing site developers and system testers, as well as simple site users, a tool for reconnaissance, vulnerability scanning and remote network mapping that is easily accessible and useable due to its web-based and visual, event – driven interface.

Based on the authors experience, the vulnerability of ICT dependable organizations is probably the most sensitive part of their organizational resilience. That is one of the main reasons why this paper attempts to illuminate vulnerability quantification in the complex term of resilience.

2.2 The vulnerability concept

If the wide range of the literature is examined, the conclusion is that in the most of the formulations, the key parameters of vulnerability are the stress to which a system is exposed, its sensitivity, and its adaptive capacity. As the size of vulnerability has direct impact on the size of resilience, it's important to determine all indicators of the organization's vulnerability.

The paper of Adger [9] reviews the research of vulnerability to environmental change and the challenges for present vulnerability research in integrating with the domains of resilience and adaptation. According to this author, vulnerability is the state of susceptibility to harm from exposure to stresses associated with environmental and social change and from the absence of capacity to adapt. The challenges for vulnerability research are to develop robust and credible measures, to incorporate diverse methods that include perceptions of risk and vulnerability, and to incorporate governance research on the mechanisms that mediate vulnerability and promote adaptive action and resilience. These challenges are common to the domains of vulnerability, adaptation and resilience. One of the important issues of vulnerability concept is that it cannot be easily reduced to a single metric and it's not easily quantifiable (Fig. 1).

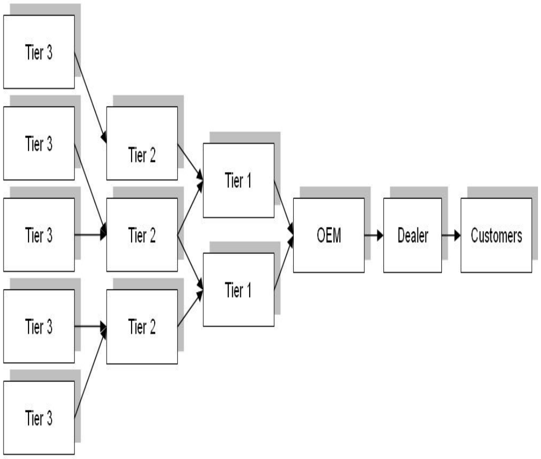

Fig. 1 – Traditions in vulnerability research and their evolution

Organizational systems are vulnerable to multiple stresses and vulnerability is manifest in various outcomes, there are, in effect, different thresholds on vulnerability informed by values and social context which is discussed by Alwang et all [10]. In this paper, a selective review of the literature from several disciplines to examine how they define and measure vulnerability is presented. The disciplines include economics, sociology/anthropology, disaster management, environmental science, and health/nutrition.

In vulnerability research, it is important to provide consistent frameworks for measuring vulnerability that provide complementary quantitative and qualitative insights into outcomes and perceptions of vulnerability. This paper intends to give answer to the challenges in the area of vulnerability research including developing metrics that incorporate human and non human vulnerability factors.

3. THE NEW MODEL FOR RESILIENCE ASSESSMENT

The paradigm for resilience assessment in this paper is model of McManus [11] which is modified and adjusted for quantification. There are papers which are dealinig with the quantification resilience problem and use McManus model in their research [12].

The idea of this paper is to examine and modify keystone vulnerabilities of organizational resilience and acquire mathematical model for IS resilience quantification.

Aspects of policy and organization of the business is associated with resilience management. According McManus et all, resilience of organization "is a function of an organization's":

(1) situation awarness,
(2) management of keystone vulnerabilities and
(3) adaptive capacity in complex dinamic, and interconected environment.

Situation awarness includes:

- the ability to look forward for opportunities as well as potential hazards and crisis,
- the ability to identity crisis and their potential consequences accurately,
- an wider and deeper understanding of the trigg factors for crisis,
- an awarness of the available resources, both internaly and externaly,
- a better understanding minimum operating requirements from an recovery perspective,
- an enhanced awarness of expectations, obligations and limitations of stakeholders.

Management of keystone vulnerabilities defines these aspects of an organization:

- leadership and decision making structures,
- the acquistion, dissemination and retention of information and knowledge, and
- the degrel of creatuvuty and flexibility that the organization promotes or tolerates.

Differencies among resilient and non – resilient organization are (Fig. 2):

- a greater situation awarenes of key stakefolders,
- an increased knowledge of its key vulnerabilities,
- the ability do adapt to changed situations with new and innovative solution and/or to adapt the tools for it.

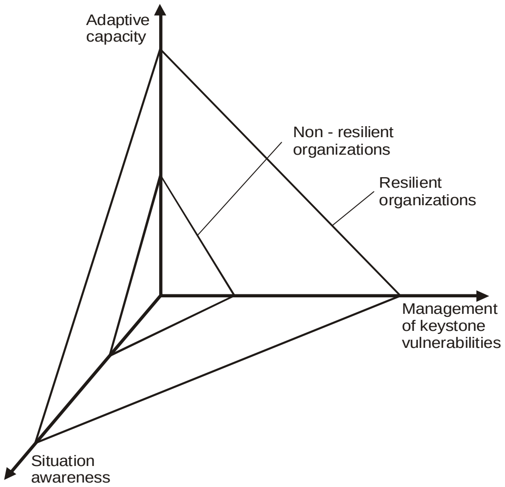
Adaptive capacity
Non - resilient organizations
Resilient organizations
Management of keystone vulnerabilities
Situation awareness

Fig. 2 – Differencies among resilient and non resilient organization

Authors of this paper are proposing the new model for Keystone Vulnerabilities indicators quantification:

- Planning,
- Exercises,
- Internal resources,
- External resources,
- Connectivity.

Factors that describe indicator values are presented in these table. According McManus [11], every resilience indicator (Planning, Exercises, Internal resources, External resources, Connectivity) is quantified on the scale with range 0 ÷ 5. Each assessed value is given by an expert who is working in the selected organization. The values of factors are normalized to the mean value and then different ponder values are associated to them. Values of the different factors (eg. Development or Operational – in this case) have different importance for quantification and that is why they are ponderized. In that way, McManus idea is fully respected.

Table 1: Quantification of Keystone Vulnerabilities – System Risk management and Planning

System Risk management and Planning			Ponder level	ICT resilience	Asessed value
Development	Human made	Software	0.5	0 ÷ 5	[(0 ÷ 15):3] x 0.5
		Hardware		0 ÷ 5	
	Natural	Accident preparedness		0 ÷ 5	
The Sum					0 ÷ 2.5
Operational	Knowledge acquisition		0.5	0 ÷ 5	[(0 ÷ 20):4] x 0.5
	Emergency management planning			0 ÷ 5	
	Business continuity management			0 ÷ 5	
	Risk management			0 ÷ 5	
The Sum					0 ÷ 2.5
Total assessed value of the Resilience component – vulnerability				0 ÷ 5	

Table 2: Quantification of Keystone Vulnerabilities – System Exercises

Exercises		Ponder level	ICT resilience	Asessed value
Resources	Stuff	0.3	0 ÷ 5	[(0 ÷ 15):3] x 0.3
			0 ÷ 5	
	Stakeholders		0 ÷ 5	
	Equipment			
The Sum				0 ÷ 1.5
Procedures	Standard procedures	0.2	0 ÷ 5	[(0 ÷ 20):4] x 0.2
			0 ÷ 5	
	Crysis procedures		0 ÷ 5	
			0 ÷ 5	
The Sum				0 ÷ 1
Training	Standard trainings	0.2	0 ÷ 5	[(0 ÷ 10):2] x 0.2
	New trainings		0 ÷ 5	
				0 ÷ 1
ICT maintenance	Condition based maintenance	0.3	0 ÷ 5	[(0 ÷ 15):3] x 0.3
	Preventive maintenance		0 ÷ 5	
	Proactive maintenance		0 ÷ 5	
The Sum				0 ÷ 1.5
Total assessed value of the Resilience component – vulnerability			0 ÷ 5	

Table 3: Quantification of Keystone Vulnerabilities – Internal resources

Internal Organisational Components				Ponder level	ICT resilience	Asessed value
Physical	Buildings	Security systems		0.3	0 ÷ 5	[(0 ÷ 25):5] x 0.3
		Computers/IT hardware/contents			0 ÷ 5	
		Software/IP			0 ÷ 5	
	Services & Equip	Generators/other equipment			0 ÷ 5	
		IT (internal networks)			0 ÷ 5	
The Sum					0 ÷ 25	0 ÷ 1.5
Human	Communications and relationships	Senior managers		0.5	0 ÷ 5	[(0 ÷ 65):5] x 0.5
		Emergency staff			0 ÷ 5	
		General staff			0 ÷ 5	
		IT staff	Administrators		0 ÷ 5	
			Project managers		0 ÷ 5	
			Network staff		0 ÷ 5	
	Mgmt.	Leadership			0 ÷ 5	
	Information & Knowledge	Backup of information			0 ÷ 5	
		Privacy and protection			0 ÷ 5	
		Knowledge acquisition			0 ÷ 5	
		Knowledge retention			0 ÷ 5	
		Knowledge transfer			0 ÷ 5	
		Training and review			0 ÷ 5	
The Sum					0 ÷ 65	0 ÷ 2.5
Process	Direct planning	Strategic planning		0.2	0 ÷ 5	[(0 ÷30):6] x 0.2
		Risk management			0 ÷ 5	
		Continuity planning			0 ÷ 5	
		Crisis planning			0 ÷ 5	
		Cashflow/wages/super etc.			0 ÷ 5	
		Insurance			0 ÷ 5	
The Sum						0 ÷ 1
Total assessed value of the Resilience component – vulnerability					0 ÷ 5	

Table 4: Quantification of Keystone Vulnerabilities – External resources

Internal Organisational Components				Ponder level	ICT resilience	Asessed value
Physical	Services & Equipment	Security systems		0.3	0 ÷ 5	[(0 ÷ 20):4] x 0.3
		Computers/IT hardware/contents			0 ÷ 5	
		Software/IP			0 ÷ 5	
		IT (external networks)			0 ÷ 5	
The Sum						0 ÷ 2
Human	Communications and relationships	General staff		0.5	0 ÷ 5	[(0 ÷ 50):10] x 0.5
		IT staff	Administrators		0 ÷ 5	
			Project managers		0 ÷ 5	
			Network staff		0 ÷ 5	
		Leadership			0 ÷ 5	
		Backup of information			0 ÷ 5	
		Privacy and protection			0 ÷ 5	
		Knowledge acquisition			0 ÷ 5	
		Knowledge transfer			0 ÷ 5	
		Training and review			0 ÷ 5	
The Sum						0 ÷ 2.5
Process	Indirect planning	Risk management		0.2	0 ÷ 5	[(0 ÷25):5] x 0.2
		Continuity planning			0 ÷ 5	
		Crisis planning			0 ÷ 5	
		Cashflow/wages/super etc.			0 ÷ 5	
		Insurance			0 ÷ 5	
The Sum						0 ÷ 1
Total assessed value of the Resilience component – vulnerability					0 ÷ 5	

Table 5a: Quantification of Keystone Vulnerabilities – Connectivity

Connectivity	Ponder level	ICT resilience	Asessed value
IS Architecture	0 .4	0 ÷ 5	0 ÷ 2
Redundancy of IS in percentage	0.6	0 ÷ 5	0 ÷ 3
Total assessed value of the Resilience component – vulnerability		0 ÷ 5	

Table 5b: Detail explanation for quantification of Keystone Vulnerabilities – Connectivity

Connectivity		Resilience level
Redundancy of IS in percentage	IS Architecture	Grade (0 ÷ 5)
95 - 100	Net enabled	5
80 – 94	Distributed	4
70 – 79	Mixed	3
50 – 69	Centralized	2
< 49	Hierarchical	1

4. CONCLUSIONS

The new model is going to be tested soon. It has intention to provide a qualitative tool for organizational resilience assessment to the management of organization.

Future work on this area will be directed in a few directions:

- Determining the degree of importance of the resilience components: (1) situation awarness, (2) management of keystone vulnerabilities and (3) adaptive capacity for each treated organization during resilience assessment process,
- Expanding the mathematical model by exploring situation awareness and adaptive capacity,
- Conducting a research which will include small, medium and big organizations and determine the correlation between their organizational resilience and resilience of their ICT sector

REFERENCES

[1] Folke, C., Carpenter, S., Walker, B., Scheffer, M., Elmqvist, T., Gunderson, L., & Holling, C.S. (2004). Regime shifts, resilience and biodiversity in ecosystem management. Annual Review of Ecology and Systematics, 35, 557-581.

[2] Gallopin, G. C. (2006). Linkages between vulnerability, resilience, and adaptive capacity. Global Environmental Change, 16(3), 293-303.

[3] Whitson, J., C., Ramirez-Marquez, J., E., Resiliency as a component importance measure in network reliability, Reliability Engineering and System Safety 94 (2009) 1685–1693.

[4] Arsovski, S., Arsovski, Z., Andre, P., Stefanović, M., Relation Between Organizational – And Information Resilience: A Way For Improvement of System Capacity, 4th International Quality Conference, May 19th 2010, Center for Quality, Faculty of Mechanical Engineering, University of Kragujevac.

[5] Watanabe, C., Kishioka, M., Nagamatsu, A., Resilience as a source of survival stategy for high – technology firms experiencing megacompetition, Technovation 24 139–152, 2004.

[6] Scott, M., Sorcinelli, G., Gutierrez, P., Moffatt, C., DesAutels, P., The Transfer and Diffusion of Information Technology for Organizational Resilience, International Federation for Information Processing (IFIP), Volume 206, pp. 219-227, 2006.

[7] Huynh, M., Goose, S., Mohapatra, P., Resilience technologies in Ethernet, Computer Networks 54 57–78, 2010.

[8] Davies, P., Tryfonas, T., A lightweight web – based vulnerability scanner for small – scale computer network security assessment, Journal of Network and Computer Applications 32 (2009) 78–95, 2009.

[9] Adger, W., N., Vulnerability, Global Environmental Change 16, 268–281, 2006.

[10] Alwang, J., Siegel, P.B., Jorgensen, S.L., 2001. Vulnerability: A View from Different Disciplines. Discussion Paper Series No. 0115. Social Protection Unit, World Bank, Washington DC.

[11] McManus, S., T., Organizational resilience in New Zealand, A thesis submitted in partial fulfilment of the requirements for the degree of Doctor of Philosophy in Civil Engineering at the University of Canterbury, University of Canterbury, 2008

[12] Arsovski, S., Andre, P., Đorđević, M., Aleksić, A., Resilience of Automotive Sector: A Case Study, 4th International Quality Conference, May 19th 2010, Center for Quality, Faculty of Mechanical Engineering, University of Kragujevac.

Received: 15.11.2010 Accepted: 15.12.2010 Open for discussion: 1 Year