sciendo

Understanding Resilience – a Conceptual Framework

Olga BUCOVETCHI*
National University of Science and Technology Politehnica Bucharest, Bucharest, Romania and National Institute for Research & Development in Informatics - ICI Bucharest, Bucharest, Romania
**Corresponding author, olga.bucovetchi@upb.ro*

Alexandru GEORGESCU
National Institute for Research & Development in Informatics - ICI Bucharest, Bucharest, Romania
alexandru.georgescu @ici.ro

Adrian V. GHEORGHE
Old Dominion University, Norfolk, Virginia, United States and National University of Science and Technology Politehnica Bucharest, Bucharest, Romania
agheorgh@odu.edu

Gabriel POPESCU
National University of Science and Technology Politehnica Bucharest, Bucharest, Romania
gaby.popescu.1987@gmail.com

Abstract. *Nowadays we face a shift of paradigm from risk management to resilience management. Resilience is a complex concept that has become not just a "buzzword", but also a meta-concept used in fields as far apart as biology, psychology, environmental studies, system-of-systems engineering and more. In this regard, the authors conducted fundamental research (mainly a literature review of a selection of open-source papers) to increase awareness towards the conceptual elements related to resilience. There were defined three resilience-related concepts: engineering resilience, organizational resilience and socio-ecological resilience. Afterwards, the main characteristics of resilient systems were highlighted. Nevertheless, the authors described a possible organizational resilience framework. The 6 suggested and detailed steps are: the comprehensive resilience analysis encompassing existing or new methodologies – audit, defining and fleshing out needed strategies, the actual design of measures to be implemented, the implementation phase of the previously designed measures, the monitoring step, and the evaluation phase of the success of the various implemented measures. The main limitation of the present research is the lack of validation of the proposed methodology.*

Keywords: **Resilience management, organizational resilience, framework, business continuity**

Introduction

The issue of organization resilience is increasingly important as part of a diverse array of security governance frameworks, such as crisis and emergency management, disaster management or critical infrastructure protection. In an EU context, the expected translation of the Critical Entities Resilience Directive into national legislation, along with its entry into force at EU levels, are marking a shift from critical infrastructure as the main unit of CIP governance to critical entities, highlighting the role of the operator of CIs. Organizational resilience thus becomes a priority in

DOI: 10.2478/picbe-2024-0201

order to achieve overall resilience for complex systems-of-systems which produce critical goods and services for the functioning of advanced societies.

According to Mitchell, 2013, resilience management represents " an iterative, dynamic and continuous loop that includes how risk is analyzed, how decisions are made to manage that risk and how these decisions contribute towards components that make a system (a unit of society, such as a nation, community, household) better able to achieve and maintain living standards and well-being in the face or changing risks and uncertainty (components of a resilient system)".

The present research demarche aims to raise awareness regarding resilience and its different faces (engineering, organizational, social resilience) and to draw a framework towards organizational resilience. For that, there were investigated Clarivate and Scopus databases in order to retrieve as many open-source documents as possible, both papers and books.

Resilience – key concepts

Engineering resilience typically reflects the ability of an engineered system or element within the system to persist in the event of perturbation. Due to the nature of an engineered system, its ability to adapt or transform is very limited. Infrastructure resilience reflects the independent resilience of the engineered systems supporting the infrastructure as well as the interactions between these systems that create the infrastructure. As a subset of engineering resilience, information and data resilience are typically defined focusing on ensuring availability and accuracy of information throughout its lifespan. Or more simply, ensuring the persistence of the information in the event of perturbations. Cyber resilience, which includes both the information as well as the infrastructure the information resides in has the same primary objective, which is to ensure the persistence of the information.

For engineering resilience, the primary objective is system persistence, this can be defined based on the ability of the system or system elements to withstand stresses without loss of function, the ability of the system to transfer function in the event of system element failure or loss, and speed the system can recover from failures. To support system persistence, there is a need for understanding and evaluation of the system against defined perturbations – proactively (Vugrin, 2016).

Organizational resilience reflects the ability of an organization to anticipate and respond to internal and external disruptions. This includes the ability of the individuals within the organization to persist and adapt in the event of perturbation, and the linkages between these individuals and other organization processes to persist and adapt to support the organizational objectives.

One primary impact on organizational resilience is the resilience of individuals within the organization and the organizational communication processes. Individual or psychological resilience is generally considered the ability of an individual to persist and/or to adapt to internal or external stressors. (Dragomir et al, 2023). The objective of organizational resilience reflects both persistence and adaptation of the organization in the event of internal and/or external perturbations. The themes reflected within these objectives include concepts of management support or commitment to the organization, situational awareness to include anticipation of threats and opportunities, effective resource management, organizational agility to include innovation, internal and individual robustness, organizational redundancy, and effectiveness in organizational communication and transparency.

Considering organizational and social-ecological resilience as compared to engineering resilience, concepts within the organizational and social-ecological resilience that support system persistence are like those in engineering resilience. However, the themes supported by those concepts, in some cases, reflect different system aspects. For example, robustness for engineering

can be based on a quantitative value defined based on system functionality over a set of defined perturbations (M. M. Walsh et al., 2013). For organizational resilience (and social-ecological resilience), robustness is often reflected as a softer concept - belief or trust, which is supported by management and organizational communication. Expanding from this, Cote and Nightingale, reflect that resilience outside of engineered systems should be moving away from concepts like flexibility and redundancy but should be focusing on culture, oversight, situational awareness, innovation, and decision-making (Cote & Nightingale, 2012). Additionally, organizational and social-ecological resilience reflects less importance on the rapidity of recovery but more on the ability for recovery or adaptation. (Badea &Ranf, 2023)

Results and discussions

Resilience is a complex concept that has become not just a "buzzword", but also a meta-concept used in fields as far apart as biology, psychology, environmental studies, system-of-systems engineering and more. For the purpose of organizational resilience, we can fall back on the definition given for critical infrastructure protection: Resilience is an intrinsic quality of an organization, entity or system which minimizes the chance of a negative event occurring and, if it occurs, minimizes the damages incurred while ensuring also rapid recovery to a minimum acceptable level of functioning on the part of the entity, in parallel with adaptation to further increase resilience to such events.

There are many dimensions and aspects to resilience found in the speciality literature. This section documents relevant ones with the goal of establishing the conceptual vocabulary of organizational resilience. Table 1 contains the relevant identified concepts. For a better explanation of the research results the author may use graphical illustrations or tables.

Table 1. A corpus of resilience concepts for organizational resilience

Concept of resilience		**Explanation**
The three resilience capacities (Vugrin et al, 2010)	Absorptive capacity	The organization absorbs shocks with minimal damage to facilities, equipment or delivery capacity;
	Restorative capacity	The organization returns to an acceptable level of operation, but undergoes permanent configuration changes, by investing in new technologies, processes, supply sources;
	Adaptive capacity	The organization reacts to a shock by resorting to often temporary measures to adapt to the crisis period. For example, a facility might activate backup generators in response to a power outage. It will not run these generators permanently, because of the expense, the pollution and financial inefficiency, but only until the power outage is resolved;
Reflectiveness		The organization has the quality of being aware of changes in the environment in order to react to them;
Robustness		The organization has the quality of being structurally able to mitigate the impact of a crisis and prevent the uncontrolled degradation of the organization's processes. For instance, multinational corporations have high distribution and decentralization patterns because of their presence in multiple sovereign territories. Often, their networks and databases are also decentralized, making them more resilient to cyber attacks targeting them. Military organizations often have deep pools of personnel and the ability to call up retired or reserve specialists in response to a crisis without crippling financial overhead;

Concept of resilience	Explanation
Flexibility	The organization has the ability to mobilize resources and undertake the necessary activities to evolve in such a way as to reduce the impact of changes and even turn them into advantages. Many organizations develop flexibility through affordable access to deep capital pools enabling overnight investments and expenditures that give them an advantage over competitors;
Redundancy	The organization has parallel capabilities, in the form of additional facilities, data centers, logistics centers etc., that allow it to withstand shocks that would otherwise incapacitate it. The dimensions of the probable threat are very important – it can be something that affects a particular operation type, leaving others unaffected, or it can affect a certain geographic region;
Inclusivity	The organization accepts input from all stakeholders and co-interests them in good governance; examples include companies cooperating with academia, consumer groups, professional associations, etc.;
Inclusivity	The organization is tightly coupled to enable effective control at critical moments when decision makers need to respond to crises or the changing security environment; involves the ability to collect information and have a feedback loop that informs decision makers of the need to adjust their plans;
Substitutability	The ability of the organization to change providers of critical services and products when a crisis occurs; for example, the fuel source for industrial processes can be changed, the Internet Services Provider can be changed and so too can the cloud services provider or the entity providing Infrastructure-as-a-service;
Fragility	An endogenous quality of organization that exacerbates the impact of a crisis because the organization is more susceptible to all kinds of stress factors. Organizations may be fragile due to lack of facility maintenance, lack of software updates, lack of capital, lack of social capital among members etc.;
Vulnerability	The quality of being susceptible to a specific stressor in the sense of the probability of an interruption occurring, without reference to severity;
Anti-fragility	The systemic quality of responding to numerous small stresses by increasing resilience to the large crises that may occur. Many current problems of organizations are related to the avoidance or ignorance of all stresses, which prevents them from developing the anti-fragility needed to respond to larger crises. A non-threatening cyber security breach that was detected in time provides the impetus for greater investment in cyber security which pays off when organized criminal actors try to infiltrate ransomware;
Margin-rich	The organization does not run operations continuously at maximum capacity. The existing slack, whether in terms of member availability for work or facility under-utilization provides a useful buffer for crisis period, because organizations can rapidly tap into their unused capacities. This requires the adequate management of these margins, since this should be the result of adequate planning rather than inefficiency or indolence;
Capable of graceful decline	The organization is set up so a disruptive event does not lead to an immediate and damaging cessation of all processes. Facilities can be shut down safely, they have some buffer to finish immediate work. Thus, they avoid the impact on themselves and on others of abrupt halts in operation;
Decoupling as a virtue	Organizations often become tightly coupled with other entities and systems as a basis for increasing efficiency and responsiveness. However, this also allows for a more rapid propagation of disruption. True decoupling is unrealistic and

Concept of resilience	Explanation
	also undesirable, due to costs and efficiency impacts. However, opportunities for decoupling can be identified. For instance, having a backup generator enables a less tightly wound coupling with energy providers, so that a power outage does not immediately halt activity and may even be resolved by the time the organization's battery or fuel stores run out. Other forms of decoupling are seen when organizations set possible waiting periods for delivery or payment, which enables them to better manage flows according to need;
Common mental modes	Resilient organizations also foster common mental modes among members, especially those on the same process tracks. This enables them to work better with each other, anticipate needs, reduce frictions and establish responsive feedback loops. Of course, common mental modes may also result in organization-wide blindness of a potential risk;
Complexity reduction	Organizations naturally become more complex as a result of size, interconnectedness with others and sophistication of roles. However, complexity is a byproduct which also makes the organization less resilient through higher uncertainties regarding the consequences of events, less transparency and more ambiguity in how the organizations really functions. Complex systems are hard to manage. Therefore, the resilient organization strives to reduce complexity as much as possible without sacrificing functionality. Examples include flattening or clarifying hierarchies, retooling and reequipping to simplify logistics and maintenance, reforming supply chains to be less complex etc.

Source: Authors' own research

Towards a framework for organizational resilience

We envision a framework for organizational resilience that features five main components that need to be developed or integrated from the existing state of the art or best practices: evaluation criteria, resilience-enhancement goals, recovery measures, resilience-enhancing measures, synthetic indicators:

- Evaluation criteria comprise a growing list of aspects of organizational resilience which can be measured or scored as part of a resilience audit conducted under the auspices of the organization in question or a regulator. Overarching categories may include physical access management to the site, cyber security, data access and process access management, security education, protection of classified information, safety and security of facilities, each with a host of quantitative and qualitative elements such as security spending, number of hours of security culture training yearly for average employee, number of checkpoints and other barriers to access the site's critical infrastructure, minimum number of employees to achieve a minimum acceptable level of functioning etc.;
- Each organization has to define its own goals as part of its internal planning process. The goals can be either short-term or long-term and the same goal can be contributed to by both recovery measures and resilience-enhancing measures. Examples of goals include minimizing short-term and also long-term damage, the resumption of a minimum acceptable level of functioning on the part of the organization as quickly as possible, maintaining the health and safety of organization members in the work context or overall, achieving compliance with various mandates such as minimizing environmental impact, protecting organizational reputation and so on.;

- Recovery measures represent either individual or complex actions that are planned in advance for implementation in order to deal with an ongoing crisis or emergency situation and achieve the goals defined by the organization in its planning. Recovery measures may include switching to a full or partial work-from-home setting up, moving to a secondary work space, shutting down operations which have unacceptable levels of risk regarding explosions during the uncertain periods of a crisis situation, performing checks before reinitiating operations, authorizing the accessing of stores of consumables, raw materials or spare equipment and components set up for such situations, preparing intermediary reports for distribution to higher echelons of the organization, to regulators or to the authorities in charge of crisis and emergency situation management etc.;
- Resilience-enhancing measures represent either individual or complex actions that are planned and implemented in advance of a disruptive event in order to increase the organization's resilience to particular risks and threats or to general ones. They can be either set by the organization in accordance with its goals, or defined as part of compliance with regulatory framework or even explicitly mandated by regulators or other competent authorities (such as military authorities in wartime). Often, the resilience-enhancing measures are implemented to make certain recovery measures feasible. Such examples include the establishment of reserve stocks of consumables, components or raw materials which can be used during a crisis. These reserves either supplement or substitute for shipments from suppliers, or they can be emergency stores to deal with particular issues (sanitary equipment, firefighting equipment, provisions for the autonomous functioning of the facility etc.). Other examples of resilience-enhancing measures include security education for organization members, regular drills for emergency situations, hardening facilities against various threats, preparing facilities for some desired level of autonomous functioning, streamlining operations to reduce the minimum absolute number of members required, drafting and implementing specific plans such as a maintenance, upkeep and update policy, a cybersecurity strategy or a technological transition plan (for instance, a quantum cryptography transition plan);
- Synthetic indicators are based on defined formulas that integrate numerous indicators of different types in a single, easily understood and remembered package. They lose detail and complexity but gain brevity and are able to inform a wide array of stakeholders about a specific issue, even though they are faced with insufficient time or lack specialized knowledge to process in-depth reports. For organizational resilience, the development of synthetic indicators can create significant added value in terms of communicating with various stakeholders such one's own members, suppliers, clients or the general public. They can also be used to drive efforts at improving resilience through specific measures by giving an easily understood benchmark which can be shown to visibly improve over time. We propose that an "organizational resilience scorecard" could integrate physical security, cyber security, human security, resilience to crises and resilience to systemic threats under a simple ABCDE key that is already used in the financial and environmental sectors. Numerical scores are also possible. The development of such a scorecard is beyond the scope of this article, but achieving this would create not only a useful framework for evaluation and communication, but also a product in itself for the security industry.

The framework for organizational resilience relies on a six-step iterative process for resilience enhancement, as seen in figure 1.

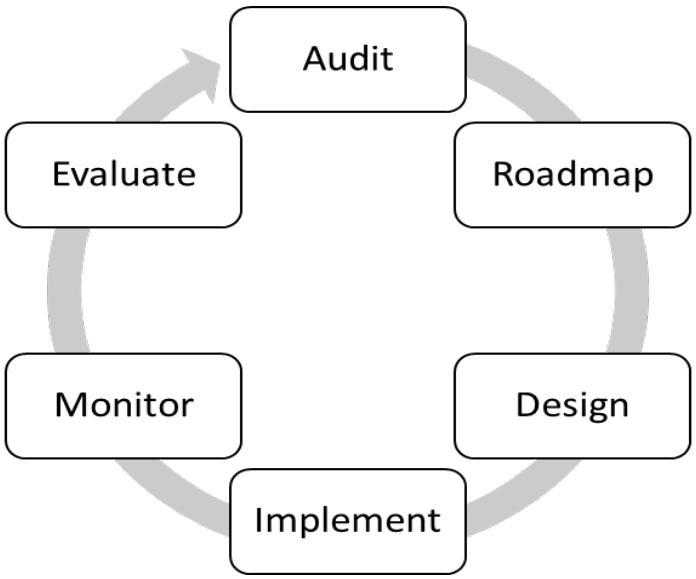

Figure 1. The organizational resilience enhancement process

Source: Authors' own research.

The steps are as follows:

- Audit – the comprehensive resilience analysis encompassing existing or new methodologies. This is a multidisciplinary and multidimensional process, which includes elements of physical security, cyber security, human security, process security, information security and more. The evaluation criteria used can cover a wide range of issues and the auditing process can result in a detailed report, but also synthetic indicators of interest to organization members, to the media, to shareholders and to other stakeholders lacking in-depth knowledge or opportunity to review extensive documentation;
- Roadmap – defining and fleshing out needed strategies in terms of facility security, cyber security development, information security transition, and anything else required on a case-by-case or sectorial basis;
- Design – the actual design of measures to be implemented, including resilience-enhancing measures, or concrete action plans to implemented the pre-defined strategies. For instance, the audit identifies a gap in information security given industry trends and stakeholder expectations, the roadmap identifies quantum cryptography as a key threat and lays out a quantum transition strategy, and, in the design phase, the competent organization members decide that they need to train some quantum cybersecurity skills, they need to air-gap systems with important data with rare access as well as backups, double the key sizes for symmetric encryption algorithms to gain time against the march in quantum computing power while proposing to perform market research on what post-quantum encryption services are available from vendors based on technologies developed by bodies such as the US National Institutes for Standards and Technology, which is currently engaging in work on lattice-based approaches, code-based cryptography, multivariate cryptography and hash-based cryptography;
- Implement – the implementation phase of the previously designed measures;

- Monitor – if the measures must be implemented over time or their efficacy and efficiency become apparent over several cycles (such as the rate of successful cyber intrusions), then there should be a dedicated monitoring staff with regular reports;
- Evaluate – the phase for evaluation of the success of the various implemented measures, estimating also advances in key performance indicators which might then be captured by synthetic indicators during the course of a new resilience audit.

Conclusion

Resilience is a useful concept that has been weighed down by the burden of a too-wide application in a too-wide range of fields. Its use in public discourse has turned it into a useful buzzword. However, it still has conceptual depth and practical use. It can express succinctly a combination of key attributes within the framework for Critical Infrastructure Protection that denotes the capacity to prevent negative events and, should they happen, to minimize the damage, resume acceptable levels of functioning as quickly as possible, recover fully and then integrate important lessons for the future. In this article, we have created a conceptual framework for understanding resilience based on three elements:

- A thorough delineation of attributes of resilience based partly on the literature and partly on the understanding of the reality of systemic disruption. This also establishes a conceptual vocabulary for resilience-enhancing programs;
- A division of the elements that make up a framework for resilience, as building blocks for a resilience-enhancing program;
- A framework action plan for resilience-enhancement that provides an iterative process through which changes in the security environment and in the system's context can be taken into account on a cyclical basis or when triggered by a systemic shift, such as a radical change in the security environment or a change in the legislative and administrative framework. This framework is also useful for changes in the management of CIs or Critical Entities, by allowing new managers or new owners a ready-made plan for enhancing the resilience while reducing the asymmetry of information inherent between the previous operator and the future one.

We propose that future research into resilience should focus on three "weak links" in such a framework – tools for self-evaluation and then resilience planning (which the EU recognized as necessary through, for instance, the Cyber Resilience Act's mandates for improving cyber resilience also in SMEs); common standards for resilience measurements in ways that are readable to the management team of CI operators, including to express the positive or negative changes as a result of environmental shifts or their actions; finally, we propose further research into how resilience overall can fit into the organization of a CI operator, for instance by creating an executive level position such as a Chief Resilience Officer that is in close contact with but separate from the Department of Security or the groups that perform CIP compliance.

Acknowledgement

This work was supported by a grant from the National Program for Research of the National Association of Technical Universities - GNAC ARUT 2023.

References

Badea, D. & Ranf, D.E. (2023). Challenges of Post-Pandemic Urban Resilience Management. Studies in Business and Economics, 18(1), 37-53. https://doi.org/10.2478/sbe-2023-0002

Cote, M., & Nightingale, A. J. (2012). Resilience thinking meets social theory: Situating social change in socio-ecological systems (SES) research. Progress in Human Geography, 36(4), 475–489. https://doi.org/10.1177/0309132511425708

Dragomir, C. C., Zamfirache, A., Albu, R. G., & Foris, T. (2023). Implications of Crises on Start-Up Management and Ways to Increase Business Resilience and Sustainable Development. Studies in Business and Economics, 18(3), 118-135.

Mitchell, A. (2013), "Risk and Resilience: From Good Idea to Good Practice", OECD Development Co-operation Working Papers, No. 13, OECD Publishing, Paris, https://doi.org/10.1787/5k3ttg4cxcbp-en.

Walsh, M. M., Einstein, E. H., & Gluck, K. A. (2013). A quantification of robustness. Journal of Applied Research in Memory and Cognition, 2(3), 137–148. https://doi.org/10.1016/j.jarmac.2013.07.002

Vugrin, E., Wahren, D., Ehlen, M. (2010) A Resilience Assessment Framework for Infrastructure and Economic Systems: Quantitative and Qualitative Resilience Analysis of Petrochemical Supply Chains to a Hurricane. Sandia National Labs, Proc. Safety Prog., Vol. 30, pp. 280–290, doi:10.1002/prs.10437

Vugrin. E.D. (2016). Critical Infrastructure Resilience. in Florin, M.-V., & Linkov, I. (Eds.). (2016). IRGC resource guide on resilience. pp. 223-229, Lausanne: EPFL International Risk Governance Center (IRGC). DOI: 10.5075/epfl-irgc-228206