REVIEW

Annals of Disaster Risk Sciences

Vol 3, No 1 (2020): Special issue on cyber-security of critical infrastructure

Improving Cyber Security with Resilience

Dejan Škanata, University of Applied Sciences Velika Gorica

Address for correspondence: Dejan Škanata, University of Applied Sciences Velika Gorica, Enconet d.o.o. Zagreb, Croatia, e-mail: dejan.skanata@enconet.hr

Abstract

Cyber security is commonly defined as the practice of protecting computers, networks, programs and data from unauthorized access or malicious attacks that are aimed for exploitation. Hence, cyber security is focused primary on malicious activities prevention and protection from occurring. Prevention and protection objectives have been usually achieved by applying traditional risk assessment and management procedures. Despite these efforts it has been shown that complete security of IT systems and data is almost impossible to achieve. Namely, by increasing number and type of different cyber threats the cyber incidents are becoming inevitable. Thus, even the strong cyber security is not enough anymore. Because of that organizations need to build the cyber resilience which mainly deals with system respond and recovery after disruptive event occurring. Cyber security combined with cyber resilience opens a new perspective towards better overall security of IT systems.

Keywords

Cyber Security, Cyber Resilience, Risk Assessment and Management, Resilience Engineering

1. Introduction

Resilience is a pretty old protection concept. Its origin comes from the elder medicine. The old physicians dealt with the resilience of human body. Improvement of the human body resilience has been a usual practice over the centuries. By using different medicines mankind is fighting nowadays with the challenges of various diseases, infections and traumas.

Resilience is an important property or capacity of the infrastructure systems as well. The first definition dates some 45 years ago by Holling (1973) who used the term in an ecological context. Since then the resilience concept has been extensively explored and systematically developed across many disciplines such as ecology, seismology, economy, business and particularly in the field of critical infrastructure protection.

Strengthening the resilience of critical infrastructure simultaneously increases the resilience of society as a whole. An outstanding example is the recent fight against the coronavirus pandemic when the resilience of the IoT[1] enabled functioning of the educational system particularly. In this way the more effective social isolation and infection reduction has enabled.

However, it might be said that the resilience concept of thinking is more or less rounded theoretically. Also it should be noted that usually is a long way to put theory into the practice.

2. Infrastructure Resilience

There are several definitions of the critical infrastructure resilience. Plenty of them are collected and commented in Mock et al. (2019) and Deublein et al. (2019). Among them the following seems to be the most complete:

> *Resilience is the capacity of an infrastructure system to be prepared for disruptive events (preparedness), to avoid them (mitigation), to overcome them (response) and to recover from them as quickly as reasonably possible (recovery).*

In the related literature there are several graphical illustrations of such definition. Probably the most comprehensive illustration is shown in Figure 1[2]. The figure is taken from Carlson et al. (2012). It shows the qualitative temporal profile of the infrastructure system response and recovery after occurrence of a disruptive event which affects functionality of the system. Actually, the infrastructure system response and recovery are mainly what the resilience is about. The main goal of a well established resilience is to reduce response time and to increase recovery rate of the infrastructure system.

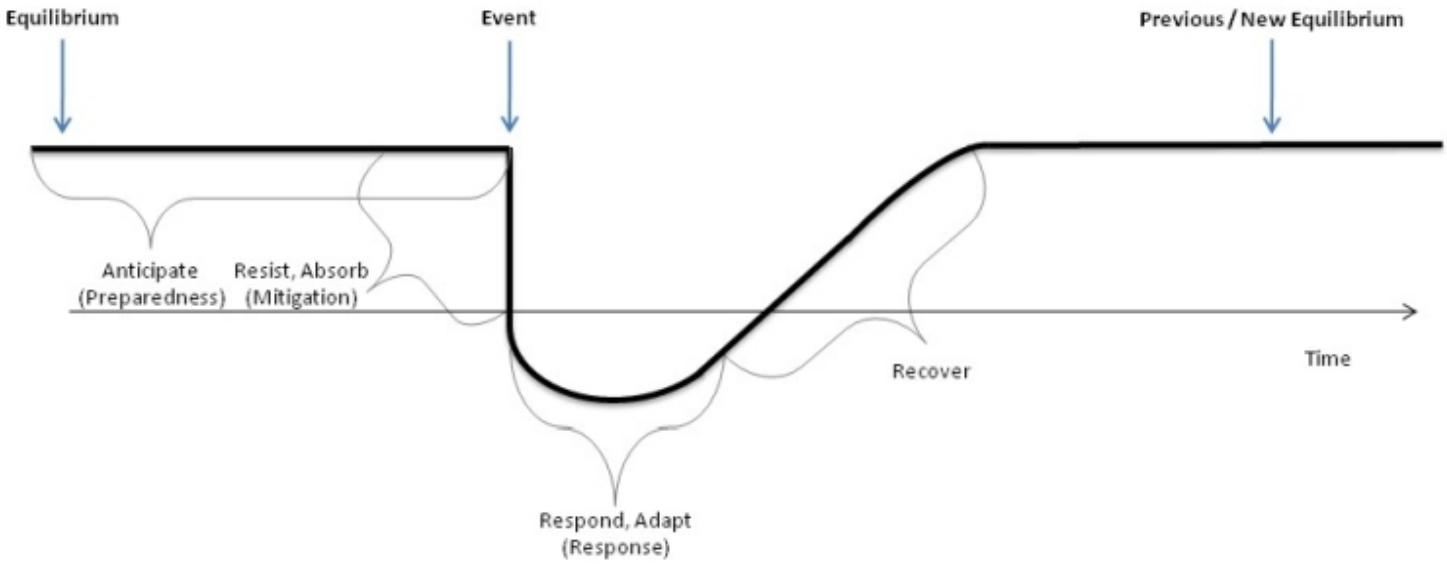

Figure 1. Components of Resilience and the Timing of a Disruptive Event

A well-known example illustrating the figure above is the accident at the Fukushima Daiichi nuclear power plant in 2011, as noted in Linkov et al. (2014). The meltdown of nuclear reactors following an earthquake and tsunami afterwards led to a very dramatic crisis situation from which Japan is still recovering. Experiences gained not just on this situation underline that infrastructure resilience must be considered over different time frames. These are:

1. Immediate respond - Evacuation and medical service,
2. Intermediate recover - Establishing temporary communities to maintain social connections (temporary relocation) and to clean-up radioactively contaminated sites, and
3. Long-term recover - Permanent relocation.

Above mentioned implies that resilience concept of thinking is strategic actually. Resilience concept involves development of long-term plans for identification, absorption and neutralization of disruptive event. Moreover, it seeks development of procedures which will enable fast recover of the critical infrastructure functionality.

Resilience model of the critical infrastructure has the multifaceted structure as described in AIIC (2016). The main structural elements are:

1. Risk assessment and management,
2. Crisis and emergency management,
3. Business continuity, and

4. Security.

Therefore, the resilience model as established above represents an integrated approach towards overall protection of the critical infrastructure system. It suggests that the resilience concept of thinking goes beyond traditional structural elements. It is because the multifaceted model is able to address complexities of large interconnected and interdependent systems as well as uncertainties associated to the future which is characterized with still unknown threats.

A general hierarchical representation of the infrastructure resilience recognizes four levels as shown in Figure 2. The figure is adapted from AIIC (2016). These levels are:

1. Dimensions: technical, personal, organizational and cooperative,
2. Capacities: predictive, absorptive, reactive and restorative,
3. Features: robustness, redundancy, training, management etc., and
4. Indicators: quantified properties that characterize the critical infrastructure.

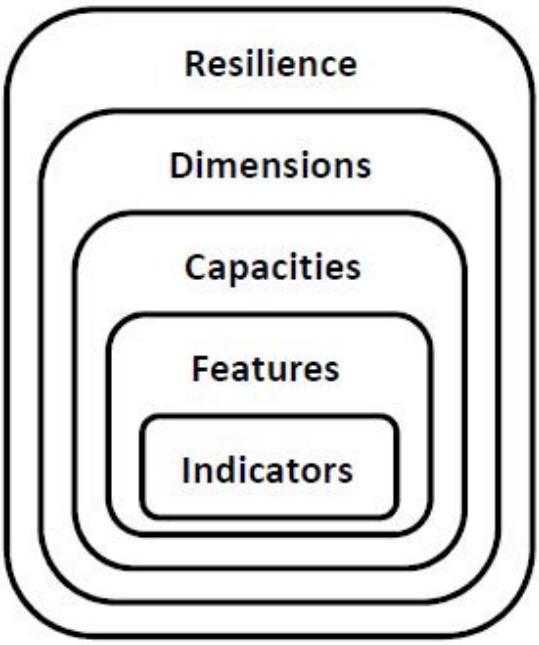

Figure 2. Hierarchical Representation of Resilience

It should be noted here that some authors tend to develop somewhat different hierarchical representation of the infrastructure resilience, particularly related to capacities and related indicators. For instance, EU-CIRCLE (2018) [3] project deals with the following five capacities and 26 corresponding generic resilience indicators:

1. Anticipative capacity
   Indicators: 1) Probability of failure; 2) Quality of infrastructure; 3) Pre-event functionality; 4) Quality of mitigating features; 5) Quality of disturbance planning; 6) Quality of communication sharing; and 7) Learnability
2. Absorptive capacity
   Indicators: 1) Unavailability of assets; 2) Severity of failure; 3) Reliability; 4) Post-event functionality; 5) Resistance; and 6) Robustness
3. Coping capacity
   Indicators: 1) Withstanding; 2) Redundancy; 3) Resourcefulness; 4) Response; 5) Economic sustainability; and 6) Interoperability
4. Restorative capacity
   Indicators: 1) Post-event damage assessment; 2) Recovery time; 3) Recovery-loss ratio; and 4) Cost of

reinstating functionality

5. Adaptive capacity
   Indicators: 1) Substitutability; 2) Adaptability; 3) Impact reducing availability; and 4) Consequences reducing availability

As far as the quantification of the resilience indicators is concerned it should be noted that some theoretical basis is given in Cimellaro et al. (2006). Vugrin and Turgeon (2013) developed method that leads to calculation of resilience costs or functionality losses, while Deublein et al. (2019) proposed a pragmatic approach for the assessment of measures to improve the resilience of the transportation infrastructure systems. Such approach assumes a simplified functionality curve of the critical infrastructure system, so-called resilience triangle which represents the loss of functionality.

3. Resilience and Risk

Infrastructure resilience concept has been developed as an answer on challenges that come from unpredictable natural events such as climatic extremes. Although the number of climatic extremes is becoming more frequent there is currently no scientific method available to predict the long-term evolution of these extremes on acceptable level of precision. In such cases the traditional risk assessment and management methodology proved to be insufficient. Hence, building resilience becomes the optimal course for protecting of the critical infrastructure.

According to Linkov et al. (2014), there are two factors that make traditional risk assessment and management unrealistic and insufficient. The first factor addresses the fact that interconnected social, technical and economic networks create large and complex systems. Risk assessment and management of many individual systems becomes costly. The second one addresses uncertainties associated with vulnerability assessment of these systems which is connected with unpredictability of climatic extremes. Of course, risk assessment and management should be used where possible to help prepare for and prevent consequences of foreseeable disruptive events, but resilience must be build into systems to help them quickly recover and adapt when predictable or unpredictable disruptive event does occur.

4. Cyber Security

Basic definitions of information security and cyber security are given in ISO (2018) and NIST (2012). It should be noted that cyber security is defined more extensively than information security. Information security is the protection of information which is an asset, while cyber security is not necessarily only the protection of cyberspace itself, but also the protection of those that function in cyberspace and any of their assets that can be reached via cyberspace, Solms and Niekerk (2013).

However, this distinction between information and cyber security is neglect here. It is considered that analogy between two terms is valid. Because of that the following simple definition is chosen here:

> *Cyber security is the practice of protecting computers, networks, programs and data from unauthorized access or malicious attacks that are aimed for exploitation.*

It follows from the above definition that cyber security is focused primary on malicious activities prevention and protection from occurring. This goal has commonly achieved by applying a traditional risk assessment and management procedure which may include the following practical steps:

1. Take inventory of systems and resources,
2. Identify potential weaknesses and threats,
3. Determine the risk impact,
4. Develop and set cyber security controls, and
5. Evaluate the effectiveness of security controls.

Despite such efforts it has been shown that complete security of IT systems and data is almost impossible to achieve. This is because the risk assessment and management deals with known (already experienced) cyber

threats. On the other hand, IT systems are faced today with increasing number and type of different unknown cyber threats. The cyber incidents therefore are becoming inevitable. Actually, the probability of cyber attack is moving from possibility towards inevitability, CBC (2018).

In order to prove inevitability of cyber incidents the text below contains some statements selected from different reports that are dealing with cyber attacks statistics worldwide. These statements are taken from CV (2019), Varonis (2019), Symantec (2019), CRA (2019), SANS (2020) and CBC (2018). All of them contribute to the conclusion that cyber incidents, intrusions and attacks threaten different critical infrastructures on a daily basis.

- The first ever website is dated in 1991. Today there are nearly 2 billion websites. Many of them promote the critical social services.
- There are nearly 4 billion Internet users today (some half of the total world population). A prediction is that there will be 6 billion Internet users by 2022. Some of them are hackers.
- Hackers attack 2,244 times a day on average.
- Average number of websites compromised with formjacking[4] code is 4,800 per month.
- Phishing[5] attacks increased 2.5 times from January do December 2018 worldwide.
- Best estimates calculate that 8.4 billion devices were connected to the IoT in 2017, and it is expected to grow to over 20 billion by 2020. The rapid growth in the adoption of IoT devices creates a new set of cyber security risks. Each IoT device represents an endpoint that could be used for cyber attack.
- Total amount of data stored in the cloud will be 100 times greater in 2021 that it is today.
- The world's digital content is expected to grow from 4 billion terabytes (4 zettabytes)[6] in 2016 to 96 zettabytes by 2020.
- 3,813 breaches were reported through June 30, exposing over 4 billion records. Compared to midyear of 2018, the number of reported breaches was up 54% and the number of exposed records was up 52%.
- There are some 300 billion passwords globally by 2020.
- There are more than 111 billion lines of new software code being produced each year which introduces a massive number of vulnerabilities that can be exploited.
- A prediction says that a business will fall victim to a ransomware[7] attack every 14 seconds by 2019, and every 11 seconds by 2021.
- Global ransomware damage cost is predicted to exceed $20 billion in 2021.
- Cybercrime will cost the world in excess of $6 trillion annually by 2021, up from $3 trillion in 2015. This dramatic rise in damage costs only reinforces the sharp increase in the number of organizations unprepared for a cyber attack.
- Global spending on cyber security will exceed $1 trillion cumulatively for the 5 year period from 2017 to 2021.
- Demand for cyber security professionals will increase to approximately 6 million globally by 2019.

5. Cyber Resilience

Critical infrastructure (energy, banking and finance, transportation, communication, health care system and others) rely on cyberspace[8] consisting of both software and hardware which are vulnerable to disruption or exploitation. Because cyberspace is a part of the critical infrastructure it seems obvious that concept of resilience should be extend to the cyberspace as well. A strong cyber security alone is not enough anymore.

Mentioned fact opens a door for implementation of cyber resilience which is generally defined as the ability of the IT system to return to its original state after being disturbed. A strict definition of cyber resilience as given in CBC (2018) is:

Cyber resilience is an organization's ability to limit the impact of cyber disruptions, maintain critical functions, and rapidly re-establish normal operations following a cyber incident.

Linkage between cyber security and cyber resilience is mainly a linear. Many articles in the field start by discussing cyber security and then shifting to cyber resilience. Some statements discussing difference between them is given below. The statements are mainly taken from Ascentor (2019).

- Cyber security has been around for several years now. Cyber resilience is relatively new term.

- Cyber security is a series of measures focused on preventing hackers penetrating IT systems. Its main objective to keep adversary out.
- Cyber resilient system is one that will be able to respond and recover from a cyber attack, keep operating through it and eventually get back on track and be more capable of withstanding future disruption. So, cyber resilience means responding when adversaries get in, because they inevitably will.
- Cyber security may be seen as the numerous walls (very high and very robust) connected in series probably with a few ditches between[9] (defence in depth). But there is still no guarantee it will completely stop hackers getting through. This leads to cyber resilience.
- Also, cyber security can be seen as binary variable, Dobrygowski (2016). Either something is secure or it is not. It is often relegated to a single, limited technical function, keeping unauthorized users out of a networked system.
- Resilience means the preparations that an organization has made with regard to threats and vulnerabilities, the defenses that have been developed, and the resources available for mitigating a security failure after it happens.
- Resilience should not be taken to be synonymous with recovery. It is not event-specific: it accrues over the long term and should be included in overall business or organizational strategy.

As noted previously the traditional risk assessment and management approaches do not work often in actual situations. Concept of resilience therefore needs a new approach based on a systemic viewpoint. Resilience engineering is a promising idea. It is design methodology of the resilience. A formal definition is:

Resilience engineering is the ability to build systems that can anticipate and circumvent accidents, survive disruptions through appropriate learning and adaptation, and recover from disruptions by restoring the pre-disruption state as closely as possible.

Fundamentals, goals and objectives, techniques and approaches as well as design principles of the cyber resilience engineering are described exhaustively in Ross et al. (2019). Cyber resilience metrics are investigated and proposed in a bunch of literature, for instance in Ford et al. (2012), Linkov et l. (2013), Bodeau and Graubart (2016) etc.

Figure 3 shows the cyber resilience goals and associated activities as seen by NATO (2018). The importance of a deep understanding all goal-related phenomena is highlighted. A short description is given bellow:

1. Goal 1 - Plan/Prepare. Cyber resilience should be prepared by using well-known architecture components, relations and structures with redundancy, segmentation, diversity, monitoring coordination, deception etc. Associated activities are: understand, prepare and prevent.
2. Goal 2 – Absorb. Absorbing may be seen more difficult from an architectural point of view. Continuation of operations or mission assurance may require unforeseen changeability of the basic system architecture dependent on what is down or degraded by a cyber attack. Associated activities are: understand, continue and constrain.
3. Recover: The end-state of recovering is normally supported by the architecture. However, transformation from an unexpected state to a recovered state while still maintaining operational continuity is not well understood either and may also require further investigations and research. Associated activities are: understand, continue and reconstitute.
4. Adapt: The re-architecting phase is often the best understood part of the cyber-resilience architecture process, because it seems pretty easy to make modifications or reconfigurations based on earlier events or inject emerging technologies for improving the resilience. Associated activities are: understand, transform and re-architect.

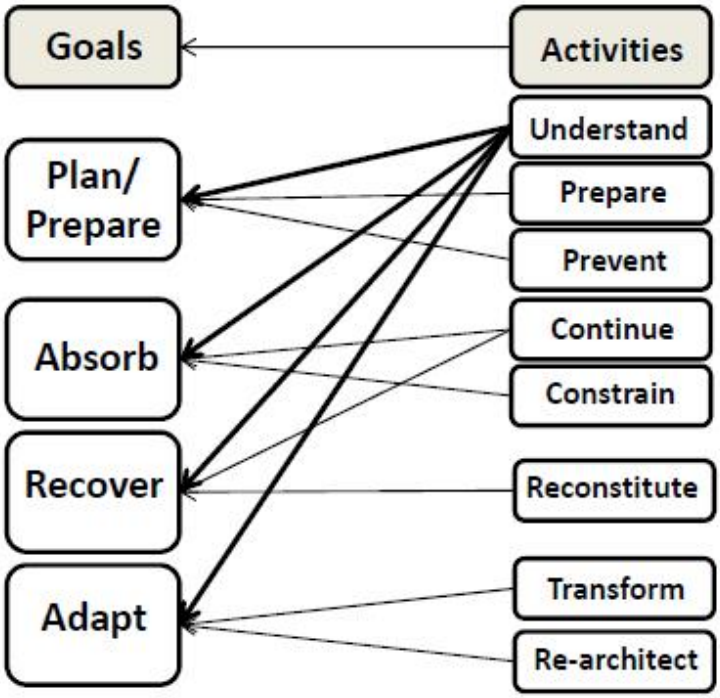

Figure 3. Cyber Resilience Engineering Framework

Cyber resilience framework as proposed by Symantec (2014), CBC (2018) and NIST (2019) is built on five pillars[10]. These pillars include identifying capabilities and vulnerabilities, protecting and securing vital infrastructure, detecting security threats as soon as possible, responding to breaches properly and recovering quickly and efficiently with as little downtime as possible as shown in the figure that follows.

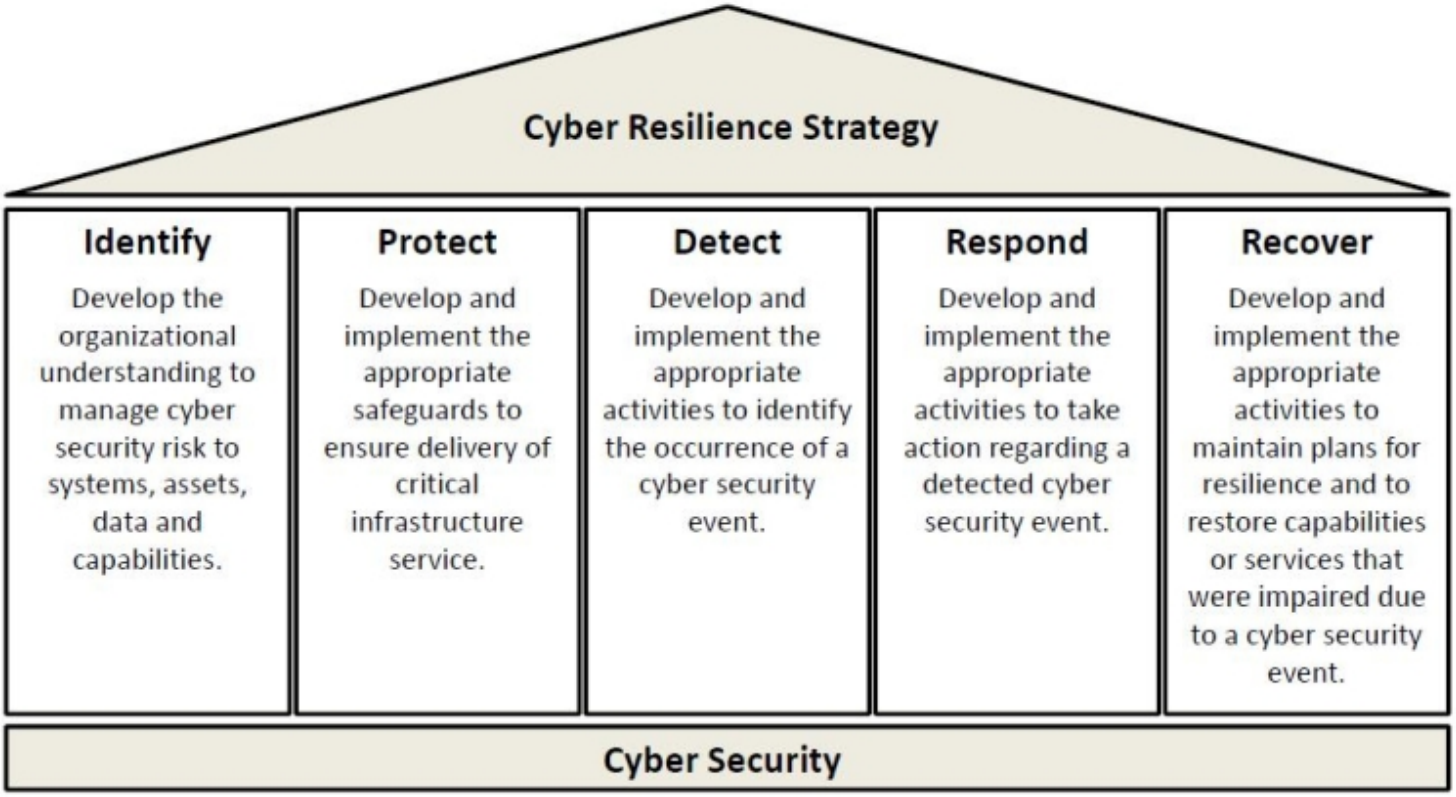

Figure 4. Cyber Resilience Framework

6. Conclusions

Based on what is written in this paper the following conclusions may be drawn out:

- Even the strong cyber security system is not enough anymore. It is because cyber attacks are inevitable. Dilemma is not if but when.
- Organizations responsible for cyber security cannot protect themselves from every single cyber threat. These organizations need to shift approach taken from cyber security to cyber resilience.
- Cyber resilience implies that it should be built on a strongly established cyber security. Therefore, cyber security is a pre-condition for achieving cyber resilience. An organization responsible can have cyber security without being resilient but not the other way around.
- Cyber security combined with cyber resilience opens a new perspective towards overall protection of IT systems.
- Cyber resilience engineering is a promising systematic approach for building proper cyber resilience strategy.
- An effective cyber resilience strategy should be built on five key pillars which are identify, protect, detect, respond and recover.

Acknowledgment

This paper was designed as a preparation for the course lecture on Critical Infrastructure Protection at University of Applied Sciences Velika Gorica.

References

AIIC (2016). Guidelines for Critical Infrastructures Resilience Evaluation, Italian Association of Critical Infrastructures Experts

Ascentor (2019). Cyber Security, What's the difference between cyber security and cyber resilience – and why does resilience matter?

C. Holling (1973). Resilience and stability of ecological systems, Annual Review of Ecology and Systematics, 4, 1-23

CBC (2018). Building Cyber Resilience, Conference Board of Canada

CRA (2019). 2019 MidYear QuickView Data Breach Report, Cyber Risk Analytics

CV (2019). 2019 Official Annual Cybercrime Report, Caybersecurity Ventures

D. Bodeau and R. Graubart (2016). Cyber Resilience Metrics: Key Observations, The MITRE Corporation

D. Dobrygowski (2016). Cyber Resilience: Everything you (really) need to know, World Economic Forum

E.D. Vugrin and J. Turgeon (2013). Advancing Cyber Resilience Analysis with Performance-Based Metrics from Infrastructure Assessments, International Journal of Secure Software Engineering, 4(1), 75-96

EUCIRCLE (2018). D4.2: Resilience Prioritization Module and D4.5: CI resilience Indicators, Fraunhofer (Germany), Artelia (France), NCSR (Greece) and UVG (Croatia)

G.P. Cimellaro, A.M. Reinhord and M. Bruneau (2006). Quantification of Seismic Resilience, Proceedings of the 8th U.S. National Conference on Earthquake Engineering, Paper no. 1094

I. Linkov, D.A. Eisberg, K. Plourde, T.P. Seager, J. Allen and A. Kott (2013). Resilience metrics for cyber systems, Springer

I. Linkov, T. Bridges, F. Creutzig, J. Decker, C. Fox-Lent, W. Kroger, J.L. Lambert, A. Levermann, B. Montreuil, J. Nathwani, R. Nyer, O. Renn, B. Scharte, A. Scheffler, M. Schreurs and T. Theil-Clemen (2014). Changing the Resilience Paradigm, Nature Climate Change, 4, 407-409

ISO (2018). ISO/IEC 27000:2018, Information technology - Security techniques - Information security management systems - Overview and vocabulary, International Organization for Standardization

L. Carlson, G. Bassett, W. Buehring, M. Collins, S. Fologa, B. Haffenden, F. Petit, J. Phillips, D. Verner and R. Whitfield (2012). Resilience: Theory and Applications, Argonne National Laboratory

M. Deublein, F. Roth, C. Willi, K. Anastassiadou and U. Bergerhausen (2019). Linking science to practice: a pragmatic approach for the assessment of measures to improve the resilience of transportation infrastructure systems, 29th European Safety and Reliability Conference, 1351-1356

NATO (2018). Approaches to Enhancing Cyber Resilience: Report of the North Atlantic Treaty Organization, Workshop IST-153

NIST (2012). Guidance for Conducting Risk Assessments, Special Publication 800-30 Rev.1, National Institute of Standard and Technology, US Department of Commerce

NIST (2019). Cyber Security Framework V1.1, National Institute of Standard and Technology, US Department of Commerce

R. Ford, M. Carvalho, L. Mayron and M. Bishop (2012). Towards Metrics for Cyber Resilience, 21st EICAR Conference, 151-159

R. Mock, B. Hulin and A. Leksin (2019). An Ontology of Risk Associated Concepts in the Context of Resilience, 29th European Safety and Reliability Conference, 1351-1356

R. Ross, V. Pillitteri, R. Graubart, D. Bodeau and R. Mcquaid (2019). Developing Cyber Resilient Systems: A Systems Security Engineering Approach, NIST Special Publication 800-160, Volume 2

R. von Solms and J. van Niekerk (2013). From information security to cyber security, Elsevier

SANS (2020). Top New Attacks and Threat Report, SANS Institute

Symantec (2014). The Cyber Resilience Blueprint: A New Perspective on Security

Symantec (2019). Internet Security Threat Report, Vol. 24

Varonis (2019). 100 Must-know Cybersecurity Statistics for 2020

Endnotes

[1] This term comprises all devices that are connected to the Internet.

[2] Although there is missing on the right side visualization relating to possible functionality improving.

[3] PanEUropean Framework for Strengthening Critical Infrastructure Resilience to Climate Change was a project funded by the EU Horizon 2020 Research and Innovation Program. The project brought together some 20 scientific and research institutions. One of them was the University of Applied Science Velika Gorica (UVG).

[4] When cybercriminals inject malicious JavaScript code to hack a website and take over the functionality of the site's form page to collect sensitive user information.

[5] A type of social engineering attack often used to steal user data, including login credentials and credit card numbers.

[6] zetta – 10^{21}; tera (trillion) – 10^{12}; giga (billion) – 10^{9}.

[7] A type of malicious software designed to block access to a computer system until a sum of money is paid.

[8] Interdependent network of IT infrastructures including the Internet, telecommunications networks, computer systems, embedded processors and controllers in critical industries.

[9] Defense in depth strategy

[10] Some minor terminological differences between proposed frameworks are neglected here.