Cyber Resilience – Fundamentals for a Definition

Fredrik Björck, Martin Henkel, Janis Stirna, and Jelena Zdravkovic

Department of Computer and Systems Sciences,
Stockholm University,
Forum 100, SE-164 40 Kista, Sweden
{bjorck,martinh,js,jelenaz}@dsv.su.se

Abstract. This short paper examines the concept of cyber resilience from an organizational perspective. Cyber resilience is defined as "the ability to continuously deliver the intended outcome despite adverse cyber events", and this definition is systematically described and justified. The fundamental building blocks of cyber resilience are identified and analyzed through the contrasting of cyber resilience against cybersecurity with regards to five central characteristics.

Keywords: information systems security, cyber resilience, cyber security.

1 Introduction

Starting with the 2012 World Economic Forum meeting in Davos, *cyber resilience* [1] has been not only an area of growing importance for individuals, businesses and societies, but also a concept that has gained in attention and usage.

Even though the concept is now widely used among practitioners in the information security industry and political and business leaders in many countries, Cyber resilience as an academic research subject is still in its infancy. As an illustration, only 402 articles in the Google scholar index include "cyber resilience" at all and of these only 21 articles include it in its title [2].

In order for cyber resilience to gain momentum also as an academic research subject, it is important to define the term. Once there is a common understanding of what cyber resilience refers to, research and education will be more efficient and effective. Individuals, businesses and societies are in need for efficient and effective cyber resilience, and to get there we need - among other factors - a common language.

There have been some earlier attempts to define cyber resilience, and this paper aims to build on and integrate some of these attempts so that the fundamentals for a definition of cyber resilience, mainly from an organizational perspective, can be formulated.

Á. Rocha et al. (eds.), *New Contributions in Information Systems and Technologies*,
Advances in Intelligent Systems and Computing 353, DOI: 10.1007/978-3-319-16486-1_31

2 Cyber Resilience – A Definition

This section offers a comprehensive definition of cyber resilience and examines the suggested definition in detail:

> *Cyber resilience refers to the ability to continuously deliver the intended outcome despite adverse cyber events.*

This ***ability*** can be considered at different levels, as discussed by [3] (see table 1). Each level offers its unique challenges, methods and conceivable controls in relation to cyber resilience. Hence, the *ability* to *continuously deliver the intended outcome* can pertain to not only to *e.g.* a nation, but also an organization or even a specific IT system. Nevertheless, as will be clarified later, for cyber resilience to be effective and efficient it needs to be addressed holistically and on several levels and in parallel.

Table 1. Cyber resilience considered at different levels

Level	Description	Example
Supranational	CR for a confederation of nations	European Union
National	CR for a country or society	Sweden
Regional	CR for a region or city	Stockholm
Organizational	CR for an organization	Company, agency, council
Functional	CR for a business function	Division, process, capability
Technical	CR for a technical system	IT system, network

The notion of ***continuously***, means that the ability to deliver the intended outcome should be working even when regular delivery mechanisms have failed, during a crisis and after a security breach. The notion also denotes the ability to *restore* the regular delivery mechanisms after such events [4] as well as the ability to continuously *change* or *modify* these delivery mechanisms if needed in the face of changing risks.

The ***intended outcome*** refers to that which the unit-of-analysis (*e.g.* the nation, organization or IT system) is intended to achieve, such as the goals of a business or business process or the services delivered by an online service.

Adverse cyber events can be caused by either *acts of God* or *acts of man* or a combination of these (see table 2). For a more detailed discussion on classification of such adverse cyber events and threats, see [5]. All events that negatively impact the *availability*, *integrity* or *confidentiality* of networked IT systems and associated information and services are such adverse cyber events.

This focus on *adverse cyber events* in relation to *networked IT systems* also marks the delimitation between *business resilience* in general and *cyber resilience* in particular.

Table 2. Basic types of adverse cyber events

Type of event	Description	Example
Acts of God	Events caused by nature	Fire, flood, earthquake
Acts of man	Events caused by people, intentional or unintentional	Unintentional deletion of data, computer intrusion

In brief, cyber resilience - which can be considered at many different levels - refers to the ability to continuously deliver the intended outcome despite adverse cyber events caused by humans and nature.

3 Characteristics of Cyber Resilience

Let us examine the most essential characteristics of cyber resilience and thereby also highlight the differences between cyber resilience and its sibling cybersecurity. Please note that any given approach to cybersecurity might include components and characteristics from cyber resilience. We distinguish five defining characteristics of cyber resilience (table 3):

Table 3. Characteristics of Cybersecurity vs. cyber resilience

Aspect	Cybersecurity	Cyber Resilience
Objective	Protect IT systems	Ensure business delivery
Intention	Fail-safe	Safe-to-fail
Approach	Apply security from the outside	Build security from within
Architecture	Single layered protection	Multi layered protection
Scope	Atomistic, one organization	Holistic, network of organizations

3.1 Objective

While the general objective of cybersecurity is to protect networked IT and information systems, cyber resilience is focused on the higher-level objective of *ensuring business delivery* (table 3). Business delivery is the intended outcome of the object in question, in other words; the value it aims to generate as conceived by internal or external stakeholders. Consequently, a system can be said to be resilient when it is able to deliver business value, even in the face of adverse cyber events, *e.g.* by making use of alternative means of business delivery. As a result, any efforts concerning cyber resilience must take *business* as its starting point rather than information technology. For example, one way of starting a cyber resilience review is to have a clear definition of the overall goals of the business Merrell *et al.* [6].

3.2 Intention

In relation to objective, intention refers to the desired properties of a system or systems. From a security perspective, the intension is to design, or protect, systems so that they have the property of being fail-safe (table 3). Essentially the system should be running as usual and be able to withstand cyber events. In addition to this it is important for resilient systems to be able to fail in a controlled way. We refer to this as *safe-to-fail* in table 3. The importance of the ability to fail in a controlled way is evident in several methods for the design of resilient systems. For example, Linkov *et al.* [7] explicitly mentions the need for systems to "adapt" and "recover", while the framework from MITRE [3] refers to the similar activities "respond" and "recover". Thus, a resilient system needs to be, by design, able to fail.

3.3 Approach

The third defining aspect of cyber resilience is the general *approach* applied. A somewhat simplified view of security is that it is applied on a system. For example, encrypted communications can be applied on the communication between a system and its users. A similar example is that organizations can set up separate security teams that only deal with the protection of its systems. However, a resilience approach would have a much more profound effect on the systems being "secured", leading to the need to let the resilience be an inner part of the IT systems and the general operation of the business. Resilience simply needs to be built-in rather than an add-on. For example, Goldman *et al.* [8] refers to the need to use several re-active techniques such as alternative operations, and dynamic composition of features when building resilient systems.

3.4 Architecture

The architecture concerns the inner structure of a system, and is expressed as the systems constituent modules and their relationships. When it comes to resilient systems, the architecture needs to be structured to allow for partial failure. Thus, it is better to view the architecture as consisting of several layers of protection, rather than constituting of a hard outer shell. Each layer should then be designed to follow the principle of safe-to-fail as described earlier. While the use of several layers of protection is commonly advocated when designing secure systems (see for example Williams *et al.* [9]), the difference here is that the architecture should be especially suited for the recovery of each layer.

3.5 Scope

The scope of a cyber-resilient analysis cannot only consider a single system or organization and its immediate surroundings. The reason for this is twofold: firstly the threat can come from any on the multitude of interconnections the system got. Secondly, the interconnections with other systems (such as sub-suppliers) can also be strength when it comes to the capability of the systems to recover from adverse events. As Joseph [10] states: "If networks expose us to vulnerabilities, they also form the basis of our resilience”. Thus, it is important to have a wide scope and examine the network of organizations and systems that the system under study is a part of. The increased scope forms the basis for both a vulnerability analysis and as a source for resilience. This is captured in the following principles:

4 Summary

The above aspects may seem fundamental, however they capture key concerns when dealing with resilient systems and provide and way to discuss and contrast security and resilience approaches. In one way it can be said that the concept of resilience essentially treats adverse cyber events as a part of normal operations. The difference to the concept of security can therefore be crucial – it allows organizations to incorporate counter measures and contingency plans as a part of what could be considered as this new “normal” condition [11].

Table 4. Cyber resilience aspects and principles

Aspect	Cyber Resilience Principles
Objective	Ensure business delivery: 1) Resilience focuses on keeping business goals intact, rather than IT systems, during adverse cyber events. Thus, 2) Resilience analysis needs to have the business as a starting point, rather than the IT systems.
Intention	Safe-to-fail: 3) Resilient systems should be designed to be able to fail in a controlled way, rather than being designed to solely protect against failure.
Approach	Build security from within: 4) Resilience is built into organizations and IT systems, rather than added as separate functions or teams.
Architecture	Multi-layered protection: 5) A resilient architecture contains several layers, each capable of protection and recovery, rather than having a single layer of protection.
Scope	Holistic, network of organizations: 6) To manage resilience, the business and IT systems need to be viewed as an interconnected network, rather than as a single unit of analysis with an environment. Moreover, 7) Resilience is viewing networked interconnection of organizations and systems as both strength and a weakness, rather just a source of threats.

In table 4 we summarize the aspects of resilience, and provides a seven guiding principles on how to address resilience.

5 Conclusion

In this paper we set out to define and analyze the concept of cyber resilience. In particular, we describe cyber resilience in contrast to the concept of cybersecurity. A conclusion from the analysis is that cyber resilience is business oriented, in the sense that it aims to continuously deliver the intended business outcome despite adverse cyber events. To contrast cyber resilience with cybersecurity we made use of five aspects; objective, intention, approach, architecture and scope. In each of these aspects there are a difference in how resilience and security are approached. Finally, we have outlined as set of fundamental principles that can be applied in order to guide initial work with cyber resilience as well as lay a foundation for a definition of the term. Further work entails analysis and extension of existing security methods and frameworks to cope with the aspects of cyber resilience.

References

1. Partnering for Cyber Resilience, World Economic Forum Davos (2012), `http://www3.weforum.org/docs/WEF_IT_PartneringCyberResilience_Guidelines_2012.pdf` (accessed December 07, 2014)
2. Google Scholar Search for "Cyber Resilience", `http://scholar.google.se/scholar?q=%22cyber+resilience%22` (accessed December 07, 2014)
3. Deborah, B., Graubart, R.: "Cyber Resiliency Engineering Framework", MITRE Report, p37 (2011)
4. Kahan Jerome, H., Allen, A.C., George, J.K.: An operational framework for resilience. Journal of Homeland Security and Emergency Management 6(1), 10 (2009)
5. Luiijf, H.A.M., Nieuwenhuijs, A.H.: Extensible threat taxonomy for critical infrastructures. International Journal of Critical Infrastructures 4(4), 409–417 (2008)
6. Merrell, S.A., Moore, A.P., Stevens, J.F.: Goal-based assessment for the cybersecurity of critical infrastructure. In: IEEE International Conference on Technologies for Homeland Security (HST), pp. 84–88. IEEE (2010)
7. Linkov, I., Eisenberg, D.A., Plourde, K., Seager, T.P., Allen, J., Kott, A.: Resilience metrics for cyber systems. Environment Systems and Decisions 33(4), 471–476 (2013)
8. Goldman, H., McQuaid, R., Picciotto, J.: Cyber resilience for mission assurance. In: 2011 IEEE International Conference on Technologies for Homeland Security (HST), pp. 236–241. IEEE (2011)
9. Williams, P.A., Manheke, R.J.: Small Business-A Cyber Resilience Vulnerability. In: Proceedings of the 1st International Cyber Resilience Conference, Research Online (2010)
10. Joseph, J.: Resilience in UK and French Security Strategy: An Anglo Saxon Bias? Politics 33(4), 253–264 (2013)
11. Kaufmann, M.: Cyber-resiliens i EU. Internasjonal Politikk 71(02), 274–282 (2013)