Concepts to Analyze the Vulnerability of Critical Infrastructures - Taking into account Cybernetics

Frédéric PETIT, Ph.D.
Département des Génies Civil, Géologique et des Mines, École Polytechnique de Montréal
C.P. 6079, succ. Centre-ville, Montréal (Québec), H3C 3A7, Canada

And

Benoît Robert, Ing., Ph.D.
Professeur titulaire
Centre risque & performance
Département de Mathématiques et de Génie Industriel, École Polytechnique de Montréal
C.P. 6079, succ. Centre-ville, Montréal (Québec), H3C 3A7, Canada

ABSTRACT

Critical Infrastructures (CIs) are complex systems. For their operations, these infrastructures are increasingly using Supervisory Control And Data Acquisition (SCADA) systems. Management practices are therefore highly dependent on the cyber tools, but also on the data needed to make these tools work. Therefore, CIs are greatly vulnerable to degradation of data.

In this context, this paper aims at presenting the fundamentals of a method for analyzing the vulnerabilities of CIs towards the use of cyber data. By characterizing cyber vulnerability of CIs, it will be possible to improve the resilience of these networks and to foster a proactive approach to risk management not only by considering cybernetics from a cyber-attack point of view but also by considering the consequences of the use of corrupted data.

Keywords: Critical Infrastructures, Vulnerability assessment, Cybernetic.

1. INTRODUCTION

Critical Infrastructures (CIs) are complex systems which are highly dependent on the cyber tools for their operations. Then, it seems very important to assess the vulnerabilities that could be related to the degradation of data used by these entities.

This problematic is very important due to the increase use of cyber elements but also due to the importance of CIs for the well functioning of society. Actually, most of the studies in this domain assess and manage the cyber risk in term of security. But, it is also necessary to consider the effects of degradation of data on the functioning of CIs. Furthermore, it is important to consider cyber risk in a safety perspective [1].

In this context, this paper aims at presenting the fundamentals of a method for analyzing the vulnerabilities of CIs in respect to the use of cyber data. By characterizing cyber vulnerability of CIs, it will be possible to improve the resiliency of these networks and to foster a proactive approach to risk management not only by considering cybernetics from a cyber-attack point of view but also by considering the consequences of the use of corrupted data.

2. METHODOLOGY

In a risk analysis, you need to correctly define the objectives and the limits of the study. You need also to correctly precise what is the risk and what are the elements you will use to define the risk it. To do so, you shall use the fundamental components of risk. The risk integrates the notion of vulnerability, resiliency and domino effects (cascading failures). It seems very important to well understand the risk due to the possible difficulty to differentiate correctly risk and vulnerability.

It is important to delimit and define the system that the study should focus on as well as to define the term risk. By considering the risk as a function of hazards, the state of the system and its consequences, it is possible to define the scope of the study.

In fact, the risk can be defined as a combination of six elements:

1. The hazard which is an event that can affect a system;
2. The vulnerability which is the sensitivity of the system facing a hazard;
3. The state of the system which allows to characterize its vulnerability but also its resiliency;
4. The dysfunction of the system which is linked to its resiliency capacity;
5. The consequences that could be caused on the environment by the failure of the system;
6. The domino effect which is the fact that a consequence could become a hazard for another system.

The Figure 1 shows the integration of these six elements.

The six elements constituting the risk evolve during time. It is therefore very important when you want to assess the vulnerability of a system (here a CI) to consider the variation due to time.

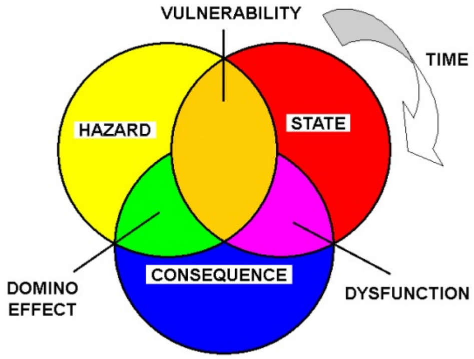

Figure 1: Representation of risk

The vulnerability of the system depends on the state of the system itself, on the capacity of a hazard to affect this state and on the undesired consequences the combination of the hazard and the vulnerability will eventually lead to.

To address the problematic of the vulnerability of CI in relation with the use of data, we propose a consequence based approach divided in three steps:

1. Characterization of the environment of the system;
2. Characterization of the system;
3. Characterization of the needs of the system.

The first step of the methodology (characterization of the environment of the system) allows assessing the downstream vulnerability of the system. The aim is to define a level of acceptable consequences for the environment, in case of dysfunction of the system. In this respect, we propose to create dependences graphs by using the concepts of flexible mapping developed by Robert and Morabito [2]. This step of characterization allows also assessing the possible domino effects in a study area.

The second step (characterization of the system) allows assessing the internal vulnerability of the system. The goal of this step is to analyze CIs in terms of their operations, their functions and the resources they use. The idea is to determine the importance of the functions in a context of operational continuity. For this, we rely on expert judgment in order to differentiate the functions that are critical to the good functioning of the infrastructure and the ones that are supportive. We also characterize how the deterioration of a function can affect the achievement of the mission of the CIs.

The aim of the second step of the proposed methodology is to define the possible state of the components of the system. For that, we propose three possible states for each component:

1. Normal or optimal state. In this state, all the components of the system function well;
2. Damaged or dysfunctional state. In this state, the system is resilient, even if certain components operate in a degraded way, and no consequences on the environment is generated;
3. Failure or out of order state. In this state, the system can not fulfill its mission and there are consequences generated on its environment.

The Figure 2 shows the integration of these three states which vary in function of time.

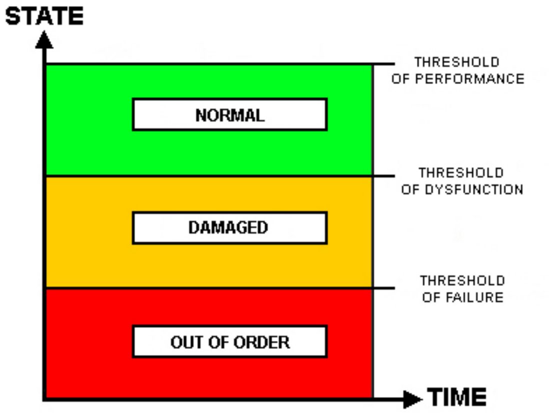

Figure 2: Different possible states of a system

These states are defined in function of the determination of three thresholds (Failure, dysfunctional and performance).

In this second step of our methodology, we define the concepts needed for the aggregation of the states of the components of the system to define the state of the system.

When we have defined the possible state of the system, the next step consists of defining its needs in term of resources used.

The third step (characterization of the needs of the system) allows assessing the upstream vulnerability of the system. This step is the most important for the assessment of the vulnerability of the system in term of use of data.

At this step, it is necessary to define the dependence of each function of the CIs towards the resources they use. We must therefore classify the resources according to their importance for the realization of the functions of the CIs and characterize the level of affectation of these functions whenever a resource is altered or unavailable.

We are looking more specifically the dependence of the CIs towards the use of cyber data. For this, we consider the data as a resource used by the CIs. The objective here is to define the possible states of the data.

To characterize the effects of the degradation of data on the functioning of the system, we propose to use the endorsement theory developed by Cohen [3].

The goal of this theory is to define rules or conditions which can lead to a specific event. In our case, this event is the dysfunction of a function of the system.

We define three types of conditions:

1. The exclusive clauses;
2. The necessary clauses;
3. The supportive clauses.

The exclusive clauses are the conditions which do not lead to the dysfunction of the function. If these conditions are verified, we are certain that the function and the system are in a normal state.

The necessary clauses are the conditions which lead to the dysfunction of the function. If these conditions are verified, we are certain that the function and the system are in a degraded state.

The supportive clauses are the conditions which reinforce the certainty about the dysfunction of a function. If these conditions are verified, the function will not be necessary in a degraded state. But, if these conditions are combined with necessary clauses, then the state of the function will be in a failure state.

To characterize these particular conditions, we consider two elements:

1. The use of data;
2. The state of data.

To define the use of the data, we consider the type and the importance of the data for a particular function.

To define the state of the data, we consider the network performance and the quality of service that are needed to provide the data.

By combining these different criteria, it is possible to define the conditions that could lead to the dysfunction of a function and of the system (CI). So, if these conditions are well defined, it is possible to have anticipation on the possible dysfunction of the system.

3. CONCLUSION

The use of a consequence based methodology to assess vulnerability of a CI and more specifically the use of the endorsement theory allows the consideration of the cyber risk in term of safety.

The consideration of the dependency of the system on the use of data should allow a more proactive approach for risk management. A better understanding of the system organization and its use of data is the first step to develop early warning system which could be useful for emergency management but also for business continuity.

The principles and concepts which will be presented during this presentation will complement the work currently done in the field of computer security. Indeed, this work considers cybernetics from a different perspective, the dependence of CIs towards data. It is important to combine these two types of approach to protect and reinforce the functioning of CIs. By doing so, we also strengthen the resiliency of society.

During the presentation, we will show concrete application and examples of our methodology. More specifically, we will present results obtained for the city of Montreal, which is the economical capital of the province of Quebec (Canada).

REFERENCES

[1] CSIS Commission on Cybersecurity for the 44th Presidency. **Securing Cyberspace for the 44th Presidency**, Report of the CSIS Commission on Cybersecurity for the 44th Presidency, Center for Strategic and International Studies, Washington, DC, USA, December 2008, 96 p.

[2] B. Robert and L. Morabito. “The operational tools for managing physical interdependencies among critical infrastructures”, **International Journal of Critical Infrastructures**, Vol. 4, No. 4, 2008, pp. 353–367

[3] P. Cohen. **Heuristic reasoning about uncertainty: an artificial intelligence approach**. Pitman publishing limited, London, United-Kingdom, 1986, 204 p.