TOWARDS A CI INTERDEPENDENCIES RESEARCH FRAMEWORK

Jose M. Sarriegi[1], Finn O. Sveen[1], J. M. Torres[1], Jose J. Gonzalez[2]

[1]Tecnun (University of Navarra)

[2]University of Agder and NISlab (Gjøvik University College)

Abstract

Research into critical infrastructure (CI) interdependencies is still immature. Such interdependencies have important consequences for crisis management, particularly when the crises are cross-border. We present several aspects that need to be investigated to gain a more complete understanding of the development of crises in these systems of systems. These aspects include: 1) Understanding CI as interdependent elements of a complex system. 2) Ever increasing interdependencies create new complexity. 3) Crises in CI are dynamically complex due to the existence of significant time delays. 4) There is a need for a long term perspective. 5) Knowledge about CI is fragmented and resides with many different stakeholders that need to be identified and brought together. 6) The need for modelling techniques that can unite the fragmented CI knowledge. 7) The creation of effective training and communication tools to transfer insights to crisis managers and policymakers.

Introduction

The consequences of critical infrastructure (CI) failure can be considerable, even to the point where Society stops. CIs such as energy, transportation and ICT need to operate continuously, that is, they must operate reliably 24 hours a day, 7 days a week. Serious crises can occur if CIs are disturbed. Relatively short interruptions may have long tails of disruption, i.e. go on for a considerable length of time. They may also spread to other infrastructures. The modelling and simulation study by Conrad et al. (2006) showed that the loss of energy infrastructure, even only for a relatively short time, is likely to cause deaths, e.g., as emergency services can not be reached when telephone services get disabled. Chang's et al's (2007) analysis of the 1998 Canadian ice storm power outage showed similar effects. The loss of energy infrastructure led to oil supply problems because most gas stations were unable to pump fuel because the pumps were electric. Dorval airport lost its power supply and became low on jet fuel. Railways were shut down because signals and switches were no longer working. The Atwater and Desbaillets reservoirs only had 4-6 hours of clean water left. Patients stayed longer in hospitals to avoid returning to blacked out homes, tying up beds

[1] Tecnun (University of Navarra), Manuel de Lardizábal 13, 20018 San Sebastián, Spain. Email: { jmsarriegi, fosveen, jmtorres }@tecnun.es

[2] University of Agder, Service Box 509, 4898 Grimstad, Norway and NISlab, Gjøvik University College, 2802 Gjøvik, Norway. Email: jose.j.gonzalez@uia.no

needed for new patients. In addition, the distribution of medicines was slowed down as elevators were no longer operating.

Challenges in a CI crisis situation include not only technical, but also legal, economic and social issues. For example, the victim of a power outage may not have control over the means to restore service. Indeed, the origin of the crisis may be in another country. Business priorities, language and cultural differences may exacerbate crises. Multiple regulatory agencies and other unforeseen barriers may cause conflicting actions.

Natural disasters, accidents, criminals and terrorists threaten these systems. Traditionally they have been a direct threat to physical assets. However, ICT is a new vector over which the impacts of these threats can propagate. The "security culture" related to control systems has been shaped by their inception for isolated operation in innocent times of the past: It is a tradition of physical separation, tailor-made proprietary solutions, fragile systems and security-by-obscurity. In addition to the danger from external attacks, the threat from malicious insiders, possibly operating in tandem with outsiders, is considerable. Thus, it is not a question of whether these systems will fail; rather it is a question of when.

But the potential damages caused by disruptions of CI have not still launched significant research efforts. The EU 6FP CI2RCO project (www.ci2rco.com) was established to investigate the current research efforts on CIIP within the EU and identify research gaps (Bologna et al. 2006). The project found only 72 projects on CIIP, including 44 national initiatives and 28 EU co-founded projects. As the following passage from Bologna et al. (ibid) demonstrates, few nations in Europe have complete programs to enhance CIP / CIIP:

"According to the data collected, ten EU countries have released a strategic plan to improve the protection, security and availability of their critical infrastructures including their information infrastructures. Moreover, seven countries have set up specific R&D programmes on CIP/CIIP. However, only Germany, The Netherlands and Norway have promoted both strategic/political and research activities." Bologna et al. (ibid) state bluntly: "… this [critical infrastructures and their protection] represents a still very immature field of research with very fuzzy and confused boundaries."

A great deal of work remains. In this paper, we present several ideas that could contribute to reduce the currently huge gap between what has actually been done and what should be done. These ideas include:

1) Understanding CI as interdependent elements of a complex system.

2) Ever increasing interdependencies create new complexity.

3) Crises in CI are dynamically complex due to the existence of significant time delays.

4) There is a need for a long term perspective.

5) Knowledge about CI is fragmented and resides within many different stakeholders that need to be identified and brought together.

6) The need for modelling techniques that can unite the fragmented CI knowledge.

7) The creation of effective training and communication tools to transfer insights to crisis managers and policymakers.

Understanding CI as interdependent elements of a complex system.

"One of the most frequently identified shortfalls in knowledge related to enhancing CI protection capabilities is the incomplete understanding of interdependencies between infrastructures" (Mussington 2002). Consequently, failing to understand these interdependencies and their dynamics will result in ineffective response and poor coordination

between decision makers and agencies responsible for rescue, recovery and restoration (Pederson et al. 2006).

As CIs do not exist in isolation of one another, we need a “system of systems” perspective to analyse them. Furthermore, owing to the last decade’s trend of deregulation, these CI systems are no longer centrally controlled. As such, we are dealing with a large number of tightly coupled networks in which there is a multitude of agents with differing goals. Thus, it may be more appropriate to talk about a “network of networks”.

According to Rinaldi (2004) there are four different types of CI interdependencies:

1. Physical: If the state of each CI depends upon the material output(s) of other CIs.
2. Cyber: If a CI’s state depends on information transmitted through the ICT infrastructure.
3. Geographic: If local environmental changes affect all the CIs in that region, e.g., when the flooding of a reservoir knocks out a generator. This implies close spatial proximity.
4. Logical: If the state of each CI depends upon the state of another via policy, legal, regulatory or some kind of other mechanism.

The presence of any of the four types of interdependencies means that failure in one infrastructure will most likely propagate to other infrastructures.

Ever increasing interdependencies create new complexity

It is not only the incomplete understanding that is problematic, but also the emergent interdependencies owing to fast CI interconnection growth rate. The likelihood of crises within CI is on the rise, owing to the fast growth rate of interconnections seen in modern CI. This growth rate is approximately exponential (Likar, Fatur, and Krizaj 2001). The principal reason is the addition of numerous new sub-systems. The ever increasing connections caused by these additions can potentially be exploited by hostile attackers, or the extra complexity created may cause accidental failures. Systems of CIs are non-linear, may be tightly coupled and only parts of them are visible to individuals at any one time.

The development of information and communications technology (ICT) has facilitated new and more effective business models. But, the new technologies and the evolving operational modes generate unfamiliar risks. The risks have “emergent character”: they derive from interdependencies and circumstances that have not been anticipated by the designers and the users of the energy infrastructure. In other words, they are risks that are shaped in novel ways by the different MTO -relationships (Schneier 2000).

An example is the continuous and faithful performance of control systems, particularly of SCADA systems, which is crucial for CI. Most of these systems were designed during a past age of innocence when attacks were inconceivable and failures could be assumed to only have local consequences. These systems were designed for long life (15 years or more) and for physically isolated operation, as proprietary systems, and – since they were “hidden” elements for the outsider – in a tradition of security-by-obscurity. The hardening of SCADA systems’ security is an extremely costly and complicated endeavour requiring many years of reengineering.

Any one individual organization, concerned with their own problems, is likely to not have a complete understanding of how their actions affect other actors in the system. Hence, unexpected and unintended behaviour is likely to occur in CIs and dependent systems during crisis situations. New knowledge about these systems and how they behave in crisis situations are needed to improve crisis management.

Crises in CI are dynamically complex due to the existence of significant time delays.

Cross border security crises in CI may be asynchronous (a crisis in one country may be the precursor to a crisis in another), have long tails of disruptions (over time) and mitigation policies may have negative unintended consequences.

The stages of the crisis lifecycle in cross-border crises are asynchronous. For example: A crisis may occur in one country and later spread to another country through cascading effects. Thus, one country's crisis is another country's precursor to a crisis. In addition, the asynchronous stages of a crisis may occur out of phase with each other. What are the consequences of multiple out-of-phase crisis-lifecycles and how can they be effectively dealt with? An events detection and visualization by an appropriate stakeholder is likely to be delayed owing to the multitude of organizations involved in responding to and mitigating cross-border crises.

These time delays make it difficult to identify the relation between causes and effects and could lead to the implementation of solutions that only offer shot term benefits. Delays also generate difficulties for capturing data, as it wil only be available for short periods during crisis occurrence. Furthermore, the longer a crisis is expected to last, the more difficult it will be to acquire relevant data. Data collection systems may not be in place in those parts of the system were unexpected consequences showing up.

There is a need for a long term perspective.

Interdependencies between CIs mean that disruptions and failures in one CI may cascade to others (Beyeler et al. 2004), with the potential to cause extended outages. As a nasty consequence, restoring service and recovering from disruptive effects is likely to take a long time. In contrast to familiar security crises, which are of short-duration and acute, CI crises – whether by failure or attack – could imply long-term, chronic disruption of vital operations. In a worst-case scenario, a successful attack on CI might turn out to be a proof-of-concept for attack weapons that could become widely available to the highest bidding criminal or terrorist groups, and used to unleash high consequence attacks against infrastructure in the energy or transport sector and other CIs of crucial importance for Society.

The strategic aspects of crisis management have to include the lifecycle of crises (Coombs 2007). This demands a bird's eye view in temporal, spatial and configuration space. "Scenarios" have to be generalized to the strategic level, dealing with categories of disruptions and viewing crises as events with a long past, with numerous precursors and early warnings; a critical phase with characteristics shaped by the anterior events and which might last for considerable time, since the replacement of vulnerable CIs cannot be achieved in matter of days, weeks and probably not even in months – even presupposing the strongest imaginable dedication. For serious crises, the ensuing recovery and build up of operations is likely to be matter of weeks, months or even years (in a worst case scenario).

Research studies by Turner and also by Vaughan have shown that crises often have long incubation times (Turner 1976, 1978; Vaughan 1990): There are numerous precursors or warnings that are either not detected or ignored. As Coombs put it, "a crisis do not just happen, it evolves" (Coombs 2007, p. 15).

According to Coombs, three influential classifications of the crisis lifecycle can be found in the literature (Coombs 2007, p. 14). Fink classified the crisis lifecycle in four stages (Fink 1986), while Mitroff used five stages (Mitroff 1994). The three stage approach has been recommended by several authors (Coombs 2007, p. 17). Coombs labelled the three stages precrisis, crisis event and postcrisis (Coombs 2007).

The notion of a crisis incubation period is as true for "digital" crises as for those caused by accidents or natural disasters. Prior to attacking a system it is necessary to probe it to discover

potential vulnerabilities. These probes can be in principle detected and steps taken to mitigate the problem. Negligence of security, both internal and external, contributes to the emergence of a crisis. It can therefore be argued that effective crisis management starts well in advance of the actual physical manifestation of the crisis. Ideally, all crises could be avoided if perfect early warning systems were in place and we understood the interrelationships between CIs.

However, this is not possible. The complexity of the world outstrips our capacity to predict what is going to happen in it. It is therefore necessary to prepare crisis managers to handle crises. To increase the pungency of the point: In interdependent CI networks, with the complication of residence in different European countries, what looks like a local crisis in CI "A" might not be recognized as the trigger of an avalanche with impacts on other CI nodes, including cross-border effects. In other words, different CIs in different locations might ignore the incubation of the impending disaster as irrelevant for them and overlook the need to start managing the crisis. In complex dynamic systems, consequences tend to show up in unexpected locations and with significant time delays. As a consequence, in a pan-European setup rather than having one lifecycle of a crisis one must be prepared to deal with out-of-phase lifecycles in different nodes of CI, a manifest crisis somewhere could become a precrisis somewhere else. With a lifecycle-view in mind, crisis management must encompass asynchronous management of the incubation periods, the physical manifestations of the crisis, the restoration periods and beyond. Hence, crisis management needs a long term approach, resolution of different perspectives and improvement of crisis communication, including developing an appropriate new crisis vocabulary and taxonomy.

The need for modelling techniques that can unite the fragmented CI knowledge

Since the exact nature of risk in interdependent CIs is not well understood, an effort is necessary to bring about greater understanding. This lack of understanding translates to a lack of written and numerical records. Consequently, knowledge about interdependencies in CIs resides fragmented in the minds of different experts. Only when brought together in an environment that encourages interaction and exchange of information will new knowledge about interdependencies in CI be created. As we know, knowledge creation is inherently a social process (Nonaka and Takeuchi 1995). Hence, we should launch activities oriented towards the interaction of the different agents that could have valuable pieces of knowledge.

This must, by necessity, be multidisciplinary. CI security needs experienced technical staff who know how CIs work, ICT experts, managers, lawyers, psychologists and anybody else who could provide valuable insights. If we leave anybody out, we will have a vulnerability.

We should use methodologies that have proven to be valid for capturing fragmented and disperse knowledge. One of these techniques is Group Model Building (GMB) (Vennix et al., 1994; Richardson et al., 1995; Vennix 1999). GMB workshops are usually facilitated by a team, which consists of a facilitator, a modeller/reflector, a process coach, a reflector, recorder and a gatekeeper. GMB is an effective way of de-fragmenting partial mental models found in representative multi-disciplinary teams. GMB elicits partial mental models, resolves clashes and ambiguities, achieves insight and creates consensus. The result is new explicit knowledge.

Simulation for Training

The number and characteristics of potential crisis scenarios is beyond imagination. No defender can imagine more than a tiny fraction of possible attack scenarios. Hence, crisis managers must be trained on a wide range of different scenarios that allows them to be generally prepared for a multitude of crises.

Simulation models could be used to train crises managers in ICT, energy and transportation infrastructure and associated political bodies, including regulatory agencies. The simulation

models should span through the whole lifecycle of crisis management, starting with the current latent crisis of lack of defence in depth to the actual scenario of a successful strike, with a long tail of protracted disturbances.

The simulation models should include early warning signals and incident reporting schemes so that crisis managers can make early decisions in rampant crisis development; depending on type and timeline of the intervention the impact range from minor, ephemeral crises to sustained crisis with a long disruption tail. Incorporation of resource use and payoffs allow decision-makers to perform cost-benefit analysis of early vs. late interventions. Furthermore, the simulation may include typical crisis-communication problems, which in cross-border crises may be exacerbated owing to different languages, cultures and legal environments.

Training and communication tools

Effective lifecycle crisis management in CI depends significantly on understanding their structure and functioning, and their interactions with threats. As any other complex system, CIs consist of factors (variables) that form many feedback loops, and there frequently exist non-linear relationships between these variables. In addition, delays between actions and responses add another dimension to complex behaviour, while all issues are further blurred because of existence of accumulators.

Non-linear relationships between variables, feedback loops, delays and accumulators are well known and studied in the System dynamics (SD) field, because they are of great importance when it comes to decision making processes to manage complex systems. However, it is documented in many places in the scientific literature that humans have significant problems with proper decision making when these factors come into play (Dörner 1974, 1976, 1982, 1989, 1997; Sawicka and Rydzack 2007; Sterman 1989). Various reasons are stated for this situation like e.g. misperception of feedback (Sterman 1989). Therefore, many authors believe that provision of the system's structure should improve the subject's ability to manage the system, and one such way is to reveal the underlying causal structure. In Machuca (2000) this belief has been subject to experiments that proved it; the group with knowledge of causal structure outperformed the group which had been exposed to a black-box based simulation model. However, other authors claim that causal structure does not matter significantly – what matters is the decision-making interface. A paradigm of so called ecological design interface has been introduced and subjects that have been using such interfaces tended to outperform those who have been using original interfaces (Sterman 1987). The main idea of these interfaces was not to convey the causal structure in an explicit way, but to use information arrangement, metaphors, and animation to elucidate all the elements and relationships that are central to SD. Another interesting approach is described in (Sawicka, Qian, and Gonzalez 2005), where tracing of system behaviour during decision making is presented by graphs, but this approach seem to have negligible effect on learning process.

No matter how good modelling of a system is and no matter how accurately a model represents some real life phenomenon, it is all in vain if the computing environment where simulation is taking place is not designed in a way that takes into account human-related learning factors. More precisely, cognitive processes should be addressed in a way that simulating environment not only enables effective learning by addressing all subtle elements of this process, but also speeds it up, i.e. improves the learning curve

Conclusions

Given the immaturity of the CIs interdependencies research we have identified several aspects that can be helpful for organizing and transferring a coherent body of knowledge. The cooperation of the involved stakeholders, who may have different perspectives and interests

over the analyzed problem, will lead to a more holistic and deep definition of the characteristics and widespread repercussions of CIs interdependencies.

Bibliography

Beyeler, Walter E., Stephen H. Conrad, Thomas F. Corbet, Gerard P. O'Reilly, and David D. Picklesimer. 2004. Inter-Infrastructure Modeling—Ports and Telecommunications. Bell Labs Technical Journal 9 (2):91-105.

Bologna, Sandro, Giovanni Di Costanzo, Eric Luiijf, and Roberto Setola. 2006. An Overview of R&D Activities in Europe on Critical Information Infrastructure Protection (CIIP). In Critical Information Infrastructures Security (Lecture Notes in Computer Science 4347), edited by J. Lopez. Berlin, Heidelberg: Springer Verlag.

Chang, Stephanie E., Timothy L. McDaniels, Joey Mikawoz, and Krista Peterson. 2007. Infrastructure failure interdependencies in extreme events: power outage consequences in the 1998 Ice Storm. Natural Disasters 41:337-358.

Conrad, Stephen H., Rene J. LeClaire, Gerard P. O'Reilly, and Huseyin Uzunalioglu. 2006. Critical National Infrastructure Reliability Modeling and Analysis. Bell Labs Technical Journal 11 (3):57-71.

Coombs, W. Timothy. 2007. Ongoing Crisis Communication: Planning, Managing and Responding. 2nd ed. Los Angeles, London, New Delhi and Singapore: Sage.

Dahl, O. M., and Stephen D. Wolthusen. 2006. Modelling and Execution of Complex Attack Scenarios using Interval Time Colored Petri Nets. In Fourth IEEE International Workshop on Information Assurance. Royal Holloway, UK: IEEE Press.

Dörner, Dietrich. 1974. Die kognitive Organisation beim Problemlösen. Bern, Stuttgart, Wien: Huber.

———. 1976. Problemlösen als Informationsverarbeitung. Stuttgart, Berlin, Köln, Mainz: Kohlhammer.

———. 1982. Lohhausen. Bern: Huber.

———. 1989. Die Logik des Misslingens. 1st ed. Reinbek bei Hamburg: Rowohlt.

———. 1997. The Logic of Failure. 1st ed. Reading, Massachusets: Addison-Wesley.

Fink, S. 1986. Crisis Management: Planning for the inevitable. New York: AMACOM.

Likar, B., P. Fatur, and D. Krizaj. 2001. Innovation Management (in slovene). FM: Faculty of Management, Koper.

Machuca, J. A. D. 2000. Transparent box-business simulators - An aid to manage complexities of organizations. Simulation & Gaming 31 (2):230-239.

Mitroff, I. I. 1994. Crisis Management and Environmentalism: A Natural Fit. California Management Review 32 (2):101-113.

Mussington, David. 2002. Concepts for Enhancing Critical Infrastructure Protection Relating Y2K to CIP Research and Development: RAND's Science and Technology Policy Institute.

Nonaka, Ikujiro, and Hirotaka Takeuchi. 1995. The Knowledge-Creating Company. New York & Oxford: Oxford University Press.

Pederson, P., D. Dudenhoeffer, S. Hartley, and M. Permann. 2006. Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research. Idaho Falls, Idaho: Idaho National Laboratory Critical Infrastructure Protection Division.

Radianti, Jaziar, and Jose J. Gonzalez. 2006. Toward a Dynamic Modeling of the Vulnerability Black Market. Paper read at The Workshop on the Economics of Securing the Information Infrastructure, at Arlington, VA.

———. 2007. Understanding Hidden Information Security Threats: The Vulnerability Black Market. Paper read at Fortieth Annual Hawai'i International Conference on System Sciences (HICSS-40), at Waikoloa, Hawaii.

Richardson, George P., and David F. Andersen. 1995. Teamwork in group model building. *System Dynamics Review* 11 (2):113–137.

Rinaldi, Steven M. 2004. Modeling and Simulating Critical Infrastructures and Their Interdependencies. In Proceedings of the 37th Hawaii International Conference on System Sciences. Hawaii.

Sawicka, A., Y. Qian, and J. Gonzalez. 2005. Managing CSIRT capacity as a renewable resource management challenge - An experimental study. In 23rd International Conference of the System Dynamics Society. Boston.

Sawicka, A., and F. Rydzack. 2007. Incorporating delays in decision making interface - an experimental study. forthcoming.

Schneier, Bruce. 2000. Secrets & Lies: Digital Security in a Networked World: Wiley.

Sterman, John D. 1987. Testing behavioral simulation models by direct experiment. Management Science 33 (2):1572-1592.

———. 1989. Modeling managerial behavior - Misperception of feedback in a dynamic decision making experiment. Management Science 35 (3):321.

Turner, B. 1976. The Organizational and Inter-organizational Development of Disasters. Administrative Science Quarterly 21 (3):378-397.

Vaughan, Diane. 1990. Autonomy, Interdependence and Social Control: NASA and the Space Shuttle Challenger. Administrative Science Quarterly 35 (2):225-257.

Vennix, Jac A.M. 1999. Group model-building: tackling messy problems. *System Dynamics Review* 15 (4):379–401.

Vennix, Jac A.M., David F. Andersen, George P. Richardson, and John Rohrbaugh. 1994. Model building for group decision support: issues and alternatives in knowledge elicitation. In *Modeling for Learning Organizations*, edited by J. D. W. Morecroft and J. D. Sterman. Portland, OR: Productivity Press.

Author Biographies

Jose M. Sarriegi is a Professor of Information Systems, Knowledge Management and Modelling and Simulation at the University of Navarra Engineering School. His research interests include information systems security, knowledge management and complex systems modelling. He has led several research projects in all these topics. He has published several papers in journals and international conferences.

Finn Olav Sveen is currently undertaking PhD studies at the University of Navarra, San Sebastian, Spain. He resides in the Industrial Management Department. He has a bachelor degree in Computer Science from Buskerud University College, as well as a Master of Science degree in Industrial and Information Management from Agder University College (Now University of Agder), both in Norway. His principal research interest is information security management with focus on incident reporting and learning. To learn about and solve these problems he applies System Dynamics modelling and simulation.

Jose M Torres, Industrial Engineer (2003, PhD 2007) is a lecturer of Information systems and Electronic Commerce at the University of Navarra Engineering School. His research

interests include information systems security management and complex systems modelling. He has published his research results in conference proceedings such as the Lecture Notes in Computer Science and he has also presented several papers in international conferences. Torres received a PhD in industrial engineering from the University of Navarra.

Jose J. Gonzalez is a Professor of System Dynamics and Information Security at the Faculty of Engineering and Science at the University of Agder, Norway. He leads the Security and Quality in Organizations group with two Postdoctoral fellows and two PhD fellows. In addition to numerous publications in the fields of system dynamics and information security, he was co-founder of Powersim and developer of one of the leading system dynamics tools.