Vulnerability Analysis of Interdependent Critical Infrastructures upon a Cyber-attack

Ahmed Abdeltawab Abdelgawad
Centre for Integrated Emergency Management (CIEM)
University of Agder, Norway
ahmedg@uia.no

Tor-Edin Farstad
Centre for Integrated Emergency Management (CIEM)
University of Agder, Norway
toredinfarstad@outlook.com

Jose J. Gonzalez
Centre for Integrated Emergency Management (CIEM)
University of Agder, Norway
jose.j.gonzalez@uia.no

Abstract

There is an extensive literature on modelling cascading effects in Critical Infrastructures (CIs). Concerning the cascading impacts of a cyber-attack upon other CIs, a detailed scenario analysis done by the Norwegian Directorate of Civil Protection concludes that a considerable impact could be achieved. However, the analysis admits that the probability of the attack would be very low, since it would require considerable expertise and resources. We argue that a smart attacker could exploit existing knowledge on cascading impacts to plan for perfidiously-timed cyber-attacks requiring low resources that would achieve a significant disruption of CIs. To illustrate our point, we build and simulate a highly-aggregated system dynamics model using estimates of disruptions effects across CIs taken from the literature.

1. Introduction

Critical Infrastructures (CIs) are resources that are essential for the performance of society, including its economy and its security, here understood as safety of citizens and security of society's assets. Different countries might have slightly different definitions of CIs. However, there is consensus that CIs include government, society's ICT (information and communication technology); financial sector; energy supply; water supply; transportation systems; health sector; and security services (police, military).

CIs are exposed to natural hazards and man-made hazards (human errors, human malignity). Critical Infrastructure Protection (CIP) embodies the management of risk assessment, risk mitigation, preparedness, response and recovery against serious incidents threatening the critical infrastructure of a region or nation.

CIs are highly interconnected and, hence, interdependent: a disruption diminishing the capacity of a CI affects other CIs through cascading effects (propagation of the disruption to other CIs that need services from the disrupted CI).

Society depends increasingly on the well-functioning of its information and communication infrastructure. For example, a vulnerability analysis [9] conducted by the Norwegian Directorate for Civil Protection (DSB) concluded that a cyber-attack causing complete disruption of the ICT CI's transport network in Norway would have:

- high impact on security CI;
- high impact on financial CI;
- high impact on railways and airline traffic, and moderate impact on other transport CIs;
- low impact on water CI;
- low impact on energy CI; but then secondary cascading effects from minor disruptions on energy infrastructure would increase significantly the disruption of ICT CI;
- moderate impact on health CI.

The aggregate impact of such a cyber-attack on ICT CI in Norway would be considerable in terms of financial costs (around one billion euro, or 1.2 billion US dollars, which is about 3.5 per cent of Norway's gross national product). The estimate is probably conservative, since the analysis in the report concludes that the ICT CI will not recover completely for about one month. The event may cause social and political instability in addition, with unpredictable long-term consequences.

The dynamics of interconnected CIs are extremely complex. There are numerous approaches for modelling cascading effects; a recent extensive review [10] enumerates six modelling categories, viz. empirical approaches, agent-based approaches, system dynamics-based approaches, economic theory based approaches, network based approaches, and others. The author concludes that none of the existing approaches is completely satisfactory: key challenges are difficulties of data access and collection, or lack of precise data; lack of integration of different modelling

URI: https://hdl.handle.net/10125/59503
ISBN: 978-0-9981331-2-6

approaches, yielding conflicting outcomes; validation problems owing to insufficient or unreliable historical data, and lack of standards for relevant metrics.

Furthermore, most models' predictions rarely can be validated by comparison with real data; few models of interconnected CIs correspond fully to observed scenarios [10].

Rather than focusing on detailed models with a high number of variables and relations between them, we argue that highly aggregated models, with simple model structure, have several advantages. They are simple to understand, they concentrate on a few essential factors and they request only few parameters with down-to-earth relations among them. The estimate of such relations admittedly relies on expert opinion. But the attractiveness of a simple and easy to understand model, and the fact that only few parameters need to be estimated, facilitate a focused discussion and a potentially more reliable estimate in a Delphi [8] or a wisdom of the crowd approach [12] in conjunction with model iterations.

Such a simulation model would allow to analyse the impacts of cascading effects. Specifically, it would allow checking the robustness of a CI system towards series of disruptions, whether arising by chance or planned by a malignant agent, if they are timed and targeted at the weakest links, arising dynamically, as the cascading effects propagate.

An interesting high-level system dynamics modelling approach for interconnected CIs has been recently proposed by Canzani [2]. Canzani considers a system of systems consisting of any number of interdependent CIs for the objective to analyse the performance level of the CIs when disruptions caused by natural or man-made disasters happen.

In Canzani's model, each CI is represented as a structure of three stocks, viz. 'Running operations', 'Down operations' and 'Recovered operations', describing three possible states for a given CI. The stock 'Running operations' represents the number of active operations in a given CI. The stock 'Down operations' represents the number of not running operations, owing to a disruption; such disruption could have been caused directly by a natural or a man-made event. The stock 'Recovering operations' represents a state of transition to 'Running operations', counted as the number of running operations and – but for some unexplained reason – not being susceptible to disruptions.

Interesting as it is, Canzani's approach suffers from three major deficiencies.

First, Canzani's model is structured as an epidemic model known as SIRS, where S refers to a stock of susceptible, I to a stock of infected and R to a stock of recovering individuals. Canzani argues that the stock "Running operations" is analogous to a stock of susceptible individuals; that the stock of "Down operations" is analogous to a stock of infected individuals; and, finally, that the stock of "Recovering operations" is analogous to a stock of individuals recovering from infection.

To deserve its name, an epidemic model must include infections transmitted through contacts between the I and the S state. However, there is no such "infection" from "Down operations" to "Running operations" in Canzani's model – nor can it be. The process causing running operations to cease operating is not an internal transmission of kind of "infections" affecting the state of "Down operations" to the state of "Running operations". Rather, the process causing running operations to cease operating is an external disruption: either a direct disruption to the particular CI or indirect disruptions in terms of reduced service from other disrupted CIs through cascading effects.

As a corollary, since Canzani's model does not describe a process analogous to the spread of an epidemic, the stock of "Recovering operations" – which logically would be a state "immune" to disruptions – does not make sense.

Second, Canzani's unit of measure for CI operations is the number of operations in each of the states. This unit of measure, we believe, has been proposed in analogy to the stocks in a SIRS model, where the unit of measure is the number of individuals in the corresponding state (e.g., the number of susceptible, the number of infected and the number of recovering individuals). The proposed unit of measure for CIs – the number of operations in each of the states – is an artificial construct with hardly a correspondence in practice.

Third and last, but not least, Canzani's system dynamics model has not been subjected to tests to create confidence on the model's verifiability and validity [5, see Ch. 21 "Truth and Beauty: Validation and Model Testing", pp. 845-892].

2. Theory

Canzani proposes an elegant representation of the dependence of a CI_j on another CI_k in terms of the service provided by CI_k to CI_j and the effect of a disruption of CI_k on CI_j. The indices j and k refer to the CIs in the system of systems to be modelled; e.g., the index value 1 could represent ICT CI; index 2, could stand for Energy CI; etc. Estimates for the effect of a disruption of CI_k on CI_j have been provided in the Ph.D. thesis of Ana Laugé [6], see §3.

The service provided by a given CI labelled with the index *i*, is given by:

$$S^i(t) = \begin{cases} 1, & OP^i{}_{run}(t) \geq D^i_{Av} \\ \dfrac{OP^i{}_{run}(t)}{D^i_{Av}}, & otherwise \end{cases} \quad (1)$$

where $OP^i{}_{run}(t)$ represents the CI's current running operations fraction of its maximum capability, and D^i_{Av} is its average demand. The function $S^i(t)$ is used to generate a relative value between 0 and 1.

Because the breakdown rate $\alpha^i(t)$ is affected by this function, the interdependencies of the CI are modelled as a formula:

$$\alpha^i(t) = \sum_{j \in J} \frac{e_{ij} \cdot \left(1 - S^j(t)\right)}{|J|} \quad (2)$$

The cardinality (sum of all elements in a set) of J represents the set of all the CIs considered. e_{ij} is a matrix element representing the effect CI_j on CI_i based on the Ph.D. thesis of Ana Laugé.

3. Estimating CI dependencies on other CIs

Laugé conducted a survey with CI managers to obtain estimates on a Likert scale for such cascading impacts caused by a disruption of less than two hours, less than six hours, less than 12 hours, less than 24 hours, more than 24 hours and more than one week; she computed averages of the provided estimates resulting in tables for each of the cases [2, pp.169–182].

The survey was formed as online questionnaires with the aim of analysing the CI interdependencies of 11 CIs mentioned by [3], namely: Energy, ICT, Water, Food, Health, Financial, Public and legal order and safety, Civil administration, Transport, Chemical and nuclear industry, and Space and research. The survey was developed and executed in five concise steps, including a trial run, which ensured that the questions were well written and understandable for the participating experts.

The survey was divided into three sections, where the first section is related to the experts taking the survey and they were asked to select which of the 11 CIs they were the stewards of. Although the survey was sent to several experts around the world, the organizations the participating experts belonged to were predominantly Spanish. The second section is concerned with the measurement of interdependencies and the time required to recover their CI after the interdependent CI have recovered. The answers led to the conclusion that there is no standard recovery time, due to different equipment and procedures. Subsequently from this the average time to restore any of the 11 CI operations after a disruption, is undefined. The last section asked the experts to assess the effect a complete breakdown of a networked CI had on their CI. The aim with this section was to know the magnitude of the effects, ranging from "0 – no effect", to "5 – very high effect". This was concerning a direct dependency from one CI to another and the corresponding table values were calculated by using the average of the responses.

4. System dynamics model

System Dynamics (SD) is a methodology to build simulation models using computers, to study the behaviour of systems [4, 11]. It is an application of Servomechanism or Information Feedback Systems Theory [11] to almost all kinds of social systems. SD is an abstraction of the reality into a system of simultaneous non-linear first order differential equations. These equations should be solved –usually numerically– to reproduce the over-time behaviour of the system, under investigation. Our proposed SD model is a simple model that is an upgrade from Canzani's model [2]. We have introduced several changes that enhanced her model like the CIs included, and basically addressed the three major deficiencies that model suffered from. In the following subsections we will go through the structure of our SD model highlighting the changes we have made, in addition to presenting the model validation and testing results.

4.1. CI System Dynamics Model Structure

In our model, a CI depends on merely two stocks "*CI Running Operations*" and "*CI Down Operations*" instead of Canzani's three stocks. For any CI included in our model, the "*CI Running Operations*" stock initially contains all its correctly functioning operations divided by its maximum capability. When a failure happens to the CI, these operations (fraction of the CI's maximum capability) will be moved via the "*CI Breakdown*" rate to the "*CI Down Operations*" stock. After being recovered, these operations return to work by being moved back to "*CI Running Operations*" via "*CI Return to Service*" rate. Figure 1 shows our model's CI structure.

Only five CIs were included in Canzani's model, namely: Energy, ICT, Health, Financial, and Transport. To have a more comprehensive picture of the effect of a failed CI on other CIs, we have used the same CI structure for the 11 CIs included in Laugé surveys mentioned before. We have utilized the Vensim DSS subscript capability to index the same

structure for these 11 CIs.

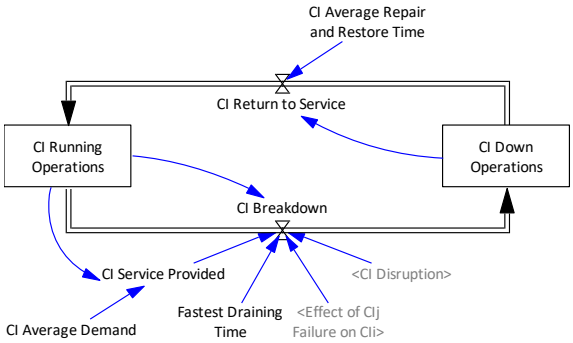

Figure 1: CI System Dynamics Structure

Mathematically, the value of the "*CI Running Operations*" stock is the integration of the "*CI Return to Service*" rate minus the "*CI Breakdown*" rate. Whereas the "*CI Down Operations*" stock is the integration of the "*CI Breakdown*" rate minus the "*CI Return to Service*" rate. The "*CI Breakdown*" rate behaves according to the following equation:

$$CIB[CI_i] = min\left\{\frac{CIRO[CI_i]}{FDT}, \frac{CID[CI_i] + CIRO[CI_i]}{} \cdot \sum_{j \in J}\left(ECIij[CI_i, CI_j] \cdot \frac{1 - CISP[CI_j]}{|J|}\right)\right\}$$

where:

Notation	Meaning/Name in the figure
$CIB[CI_i]$	$CI\ Breakdown[CI_i]$. CI_i represents any of the CIs included in our model.
$CIRO[CI_i]$	$CI\ Running\ Operations[CI_i]$.
FDT	$Fastest\ Draining\ Time$.
$CID[CI_i]$	$CI\ Disruption[CI_i]$.
$ECIij[CI_i, CI_j]$	$Effect\ of\ CI_j\ Failure\ on\ CI_i$ $[CI_i, CI_j]$, which is equivalent to e_{ij} from equation 2. CI_j represents all failed CIs affecting CI_i, which are the elements of J.
$CISP[CI_j]$	$CI\ Service\ Provided[CI_j]$, which is equivalent to $S^j(t)$ in equation 2.

The minimum function and its first term included in the equation of the "*CI Breakdown*" rate are used to prevent the rate from draining the "*CI Running Operations*" stock below zero.

The "*CI Return to Service*" rate is defined as:

$$CIRS[CI_i] = \frac{CIDO[CI_i]}{CIARRT[CI_i]}$$

where:

Notation	Meaning/In the figure
$CIRS[CI_i]$	$CI\ Return\ to\ Service[CI_i]$.
$CIDO[CI_i]$	$CI\ Down\ Operations[CI_i]$.
$CIARRT[CI_i]$	$CI\ Average\ Repair\ and\ Restore\ Time[CI_i]$.

This rate equation will move all operations inside the "*CI Down Operations*" stock back to the "*CI Running Operations*" stock over an average period equal to "*CI Average Repair and Restore Time*", which is the average total time needed to restore and repair the failed operations as the name implies. This value replaces both two separate values for the total average repair time and the total average restore time in Canzani's model. Canzani indicated that these values are not the focus of her work and, apparently, they were arbitrarily chosen. Accordingly, for demonstration purposes, we have arbitrarily chosen 72 hours for this time constant.

In Figure 1, the "*CI Service Provided*" represents $S^i(t)$ of equation 1. In the model, this variable is defined as follows:

$$CISP[CI_i] = \begin{cases} 1, & CIRO[CI_i] \geq CIAD[CI_i] \\ \frac{CIRO[CI_i]}{CIAD[CI_i]}, & otherwise \end{cases}$$

where:

Notation	Meaning/Name in the figure
$CISP[CI_i]$	$CI\ Service\ Provided[CI_i]$.
$CIRO[CI_i]$	$CI\ Running\ Operations[CI_i]$.
$CIAD[CI_i]$	$CI\ Average\ Demand[CI_i]$.

In our model, for demonstration purposes, the "CI Average Demand" was arbitrarily assumed to be 95% of the CI's full capacity required to supply the demand of its dependent CIs.

4.2. Effect on CIi from CIj

In her model, Canzani used Laugé's table of CI dependencies when other CIs fail for less than two hours only. Nevertheless, these dependencies are not static as such; as previously mentioned, Laugé's thesis presented different tables for different disruption time durations. Accordingly, to include such dynamics in our model, we have rearranged the values of Laugé's dependencies tables (see Figure 2) in separate time-based table functions [11, Ch. 14, p. 551-595]. (Figure 3 shows the time-based table function of the effect of the ICT CI failure on the Energy CI as an example.)

These SD time-based graph functions provide a dynamic time-dependent values of the e_{ij} of equation 2, or of the $Effect\ of\ CI_j\ Failure\ on\ CI_i[CI_i, CI_j]$ in our SD model.

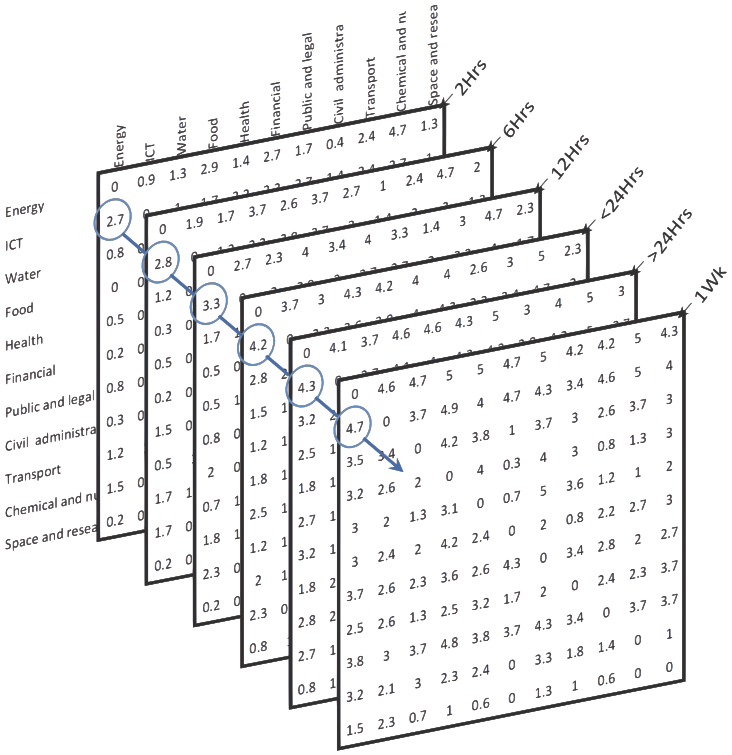

Figure 2: CI Dependencies when other CIs Fail for Different Durations

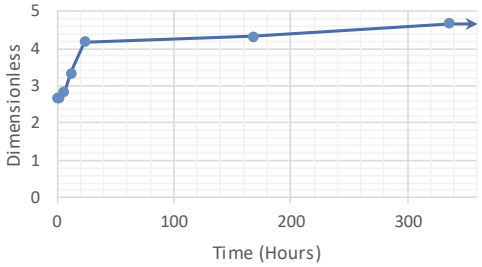

Figure 3: Effect of CI ICT Failure on CI Energy over Time

4.3. CI Disruption SD Structure

CI Disruption structure, as the name implies, emulates a disruption happening to any of the CIs included in our model. Based on a pulse function $\Pi\left(\frac{t-t_d}{\Delta T}\right)$ where t, t_d, and ΔT represent time, the disruption time, and the disruption duration respectively [13], the following equation –which is used by Canzani [2] as well– presents the disruption in CI_i:

$$CID[CI_i] = CIDM[CI_i] \cdot \Pi\left(\frac{t - CIDT[CI_i]}{CIDD[CI_i]}\right)$$

where:

Notation	Meaning/Name in the figure
$CID[CI_i]$	$CI\ Disruption[CI_i]$.
$CIDM[CI_i]$	$CI\ Disruption\ Magnitude[CI_i]$.
$CIDT[CI_i]$	$CI\ Disruption\ Time[CI_i]$.
$CIDD[CI_i]$	$CI\ Disruption\ Duration[CI_i]$.

Because our model has replaced the static e_{ij} with a time-based graph function, in addition to the model simulation time-line, a coexistent simulation time-line that starts with the onset of any disruption is needed. This newly generated time-line will work as an input to the graph function to generate the correct time-based e_{ij} value replacement. In our model, this new time-line is generated inside the model variable $CI\ Disruption\ Time\ Counter[CI_i]$ (shown in Figure 4). Yet, to calculate this variable, the model needs to identify the onset of any disruption. To do so, the model benefits from the Vensim DSS "SAMPLE IF TRUE" function. This function returns its input when certain condition is met, and remains constant otherwise [14].

The condition that triggers this function in our model is the beginning of a disruption, which is identified via subtracting the one time-step delayed $CI\ Disruption\ [CI_i]$ from itself. As such, the "SAMPLE IF TRUE" function is used inside $CI\ Disruption\ Time\ Counter\ Trigger[CI_i]$ (shown in Figure 4) to sample the value of the simulation time when the disruption starts. This sampled time value from the simulation time (done inside the model variable $CI\ Disruption\ Time\ Counter[CI_i]$) as long as the disruption continues. Figure 4 shows the whole CI disruption SD structure. Figure 5 shows the original and one generated simulation time-lines of which disruption starts at hour 48 and ends 24 hours later.

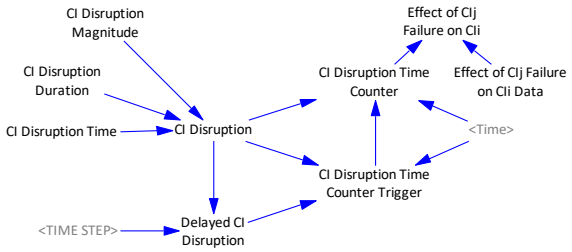

Figure 4: CI Disruption SD Structure

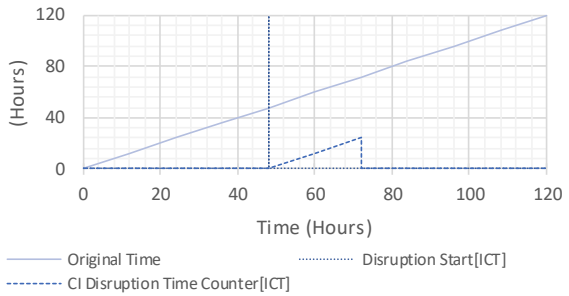

Figure 5: Original and Generated Simulation Time-lines (Disruption Starts at Hour 48)

4.4. Model Testing and Validation

SD model testing and validation increase customers trust in the model, in addition to detecting any problems in that model [11]. We have used what is applicable from the set of tests introduced by [5] and recommended by [11] to test and validate our model. Boundary adequacy test [5, 1, 11] is concerned with answering whether "the important concepts for addressing the [studied] problem [are] endogenous to the model" [11]. While structure assessment [1, 11] is concerned with answering whether the model structure is "consistent with relevant descriptive knowledge of the system" and whether the level of aggregation is appropriate. Our model inherited the same boundaries and basic structure of Canzani's, which, although a simple model, includes all necessary components to study a CI disruption effect at this level aggregation. Moreover, removing the third stock of Canzani's model presented a change to the structure that aims at making the model more consistent with the real system. Accordingly, the structure and aggregation level were found to be relevant and appropriate for the model purpose.

Dimensional consistency test [5, 1, 11] checks whether all equation of the model are dimensionally consistent, maintaining that the parameters should have real system equivalent [11]. Using the unit check feature of Vensim DSS [15] assured the model dimensional consistency.

Parameter assessment [5, 1, 11] is associated with answering whether the values of the model parameter are consistent with relevant descriptive and numerical knowledge of the system, and whether the parameters have real system equivalents [11]. Aside from the few arbitrarily chosen values clearly indicated before, all other parameters used in the model were retrieved from Laugé's survey.

Furthermore, the model robustness has been tested under extreme conditions [5, 1, 11]. Testing extreme conditions is concerned with answering whether "each equation make[s] sense even when its inputs take on extreme values", and whether "the model respond plausibly when subjected to extreme policies, shocks, and parameters" [11]. Accordingly, we have utilized the "automatically simulate a model on changes" functionality of Vensim SyntheSim mode to test the consequences of changing model variables and parameters to extreme values. The usual consequence of changing a variable's value to zero, as an extreme value for example, is several dependent equations failing because of division by zero. However, in other cases the consequence could be implausible behaviour. In all cases, multiple iterations of fixing the equations were conducted until reaching plausible behaviour.

Moreover, the model was tested for integration error, which aims at checking whether "the results are sensitive to the choice of time step or numerical integration method" [11]. Different time step values and different numerical integration methods were tested. The combination of Euler method and time step of 0.125 was found suitable, as by decreasing the time step value and using different integration methods, the behaviour of model was found to be insensitive to such changes. In the same time, the time step was not very small rendering the numerical integration process slow. Behaviours of different variables were also compared under different time step, and no difference was noticed.

Moreover, sensitivity analysis [5, 11], which is concerned with testing the robustness of the model under assumed uncertainties in parameters and initial values, was applied to the model using Vensim DSS. To test model sensitivity, Vensim DSS uses Monte-Carlo simulations [13]. We have run 200 Monte-Carlo simulations per parameter. As no further information about the probability distribution of the parameters was available, we opted for Uniform probability distribution for all parameters. We did not have any benchmark for the numerical changes in the model variables due to the change in any of the tested parameters to test our results against. However, in all sensitivity tests we have conducted, we have not spotted any change in the modes of behaviour, consequently no policy implications change due to the change in the values of the parameters. Accordingly, we find the results acceptable.

5. Simulation

In this section we describe several simulations of small cyber-attacks in different conditions to fully understand the limits of the effect of such disruptions. In agreement with Canzani, we have assumed that a small disruption will have a magnitude equal to two.

5.1. Scenario 1 – a single small cyber-attack

This scenario simulates a single small attack disruption aimed at the ICT CI which happens two days after the beginning of the simulation, and stays active for one day. We have borrowed this scenario from Canzani's research [2] to show the effect of such a small cyber-attack for comparison purposes with other cyber-attack forms.

Figure 6 shows the results of this scenario on two different charts, one showing the effect of the cyber-attack on the running operations $OP^i{}_{run}(t)$ of all 11 CIs, while the other shows the effect on the service provided $S^i(t)$ by these CIs. This single small cyber-attack causes 41% drop in the running operations of the ICT CI in the third day of the simulation. The ICT CI could not regain 99% of its running operations until the 13th day. Nonetheless, the cascaded negative effect on other CIs' running operations did not exceed 3.1% at its highest. In terms of service provided, merely the ICT CI was affected negatively with a 38% drop of its value, i.e. the attack could not be cascaded to services provided by other CIs.

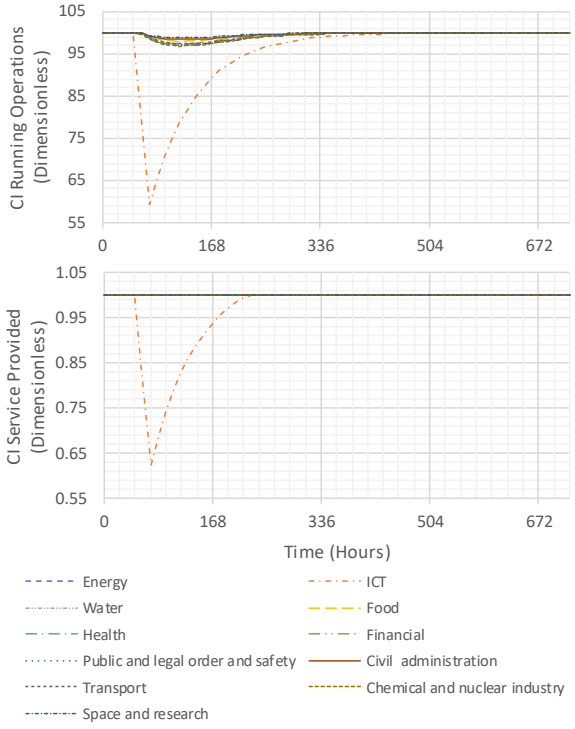

Figure 6: A Single Small Cyber-attack

5.2. Scenario 2 – three successive small cyber-attacks

This scenario simulates three successive small attacks aimed at the ICT CI which happen two days after the beginning of the simulation time. Each attack stayed active for a duration of one day, and there was one day off in-between every two attacks.

Figure 7 shows a large negative effect on the running operations of the ICT CI with a 73% drop at its highest in the seventh day. The ICT CI could not regain 99% of its running operations before the 17th day. The effect was cascaded to other CIs' running operations and reached around 5% drop in the case of Water, Civil administration, and Space and research CIs. The drop reached around 10% for all other CIs, reaching 10.1% drop at its highest in the case of Chemical and nuclear industry CI.

In terms of service provided, the drop in the ICT CI service provided exceeded 71%. This negative effect was not cascaded to Water, Civil administration, and Space and research CIs at all. However, the negative effect was cascaded to the service provided by all other CIs with 5% drop at its highest in the case of Public and legal order and safety, and Chemical and nuclear industry CIs.

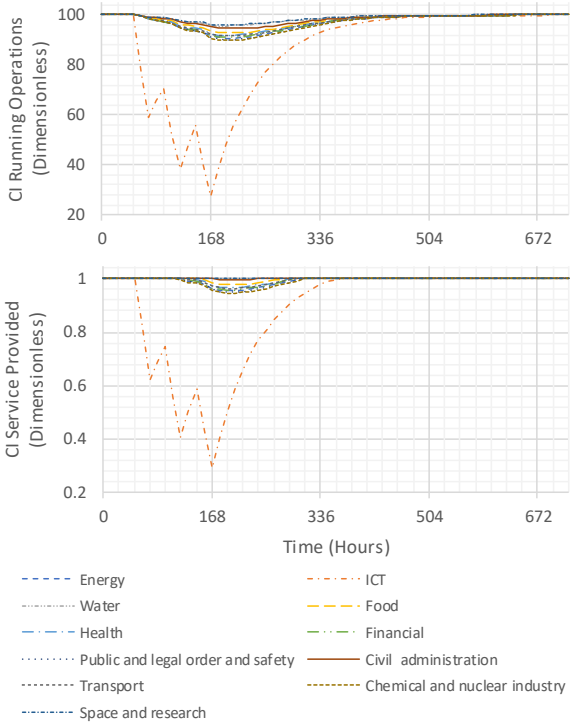

Figure 7: Three Successive Small Cyber-attacks

5.3. Scenario 3 – a single small cyber-attack followed by an energy failure

This scenario simulates a single small attack disruption aimed at the ICT CI which happens 2 days after the beginning of the simulation, and stays active for one day. This cyber-attack is followed by an Energy CI disruption that has a magnitude of eight, starts four days from the simulation time, and stays

active for a duration of one and a half days.

Figure 8 shows the results of this scenario. Similar to Scenario – 1, the attack on the ICT CI dropped its running operations by 41% in the third day of the simulation. As known from Scenario – 1, the cascading negative effect on other CIs is very limited. The disruption that happened in the Energy CI caused the CI to completely stop working at the fifth day for 12 hours.

The effect of both disruptions was cascaded to other CIs' running operations and reached an average drop of 7% in Water, Civil administration, and Space and research CIs, and an average drop of 14% in all other CIs, reaching 18.6% drop at its highest in the case of Chemical and nuclear industry CI.

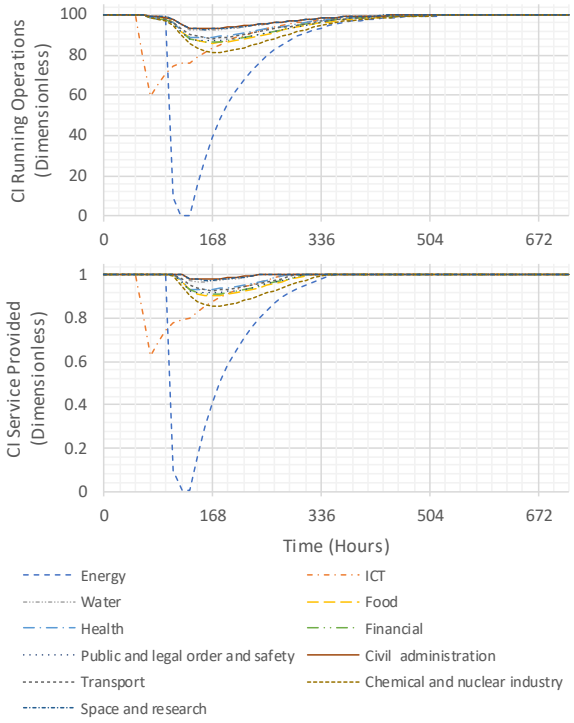

Figure 8: A Single Small Cyber-attack Followed by an Energy Failure

5.4. Scenario 4 – three successive small cyber-attacks following an energy failure

This scenario simulates an Energy CI disruption that has a magnitude of eight, starts at the beginning of the simulation, and keeps on for a duration of one and half days. This disruption is followed by three successive small attacks aimed at the ICT CI which happen two days after the beginning of the simulation, and having one day in-between every two attacks. Each attack stays active for durations of one day as well.

Figure 9 shows the results of this scenario. The disruption that happened in the Energy CI by the beginning of the simulation caused the CI to completely stop working after one day for 12 hours. Moreover, similar to Scenario – 3, the cyber-attack causes a large negative effect on the running operations of the ICT CI that exceeded 76% drop at its highest in the seventh day (compared to 73% in Scenario – 3).

The negative effect of both disruptions was cascaded to other CIs' running operations and reached around 8% drop in Water, Civil administration, and Space and research CIs, and around 16% drop for all other CIs, reaching 20% drop at its highest in the case of Chemical and nuclear industry CI.

In terms of service provided, there were a total drop in the Energy CI, and another drop in the ICT CI service provided which exceeded 74%. The negative effect was cascaded to the services provided by Water, Civil administration, and Space and research CIs with an average drop of 4%. Moreover, the negative effect was cascaded to the service provided by all other CIs with on average drop of 12%; and at its highest in the case of Chemical and nuclear industry CI with 15.8% drop.

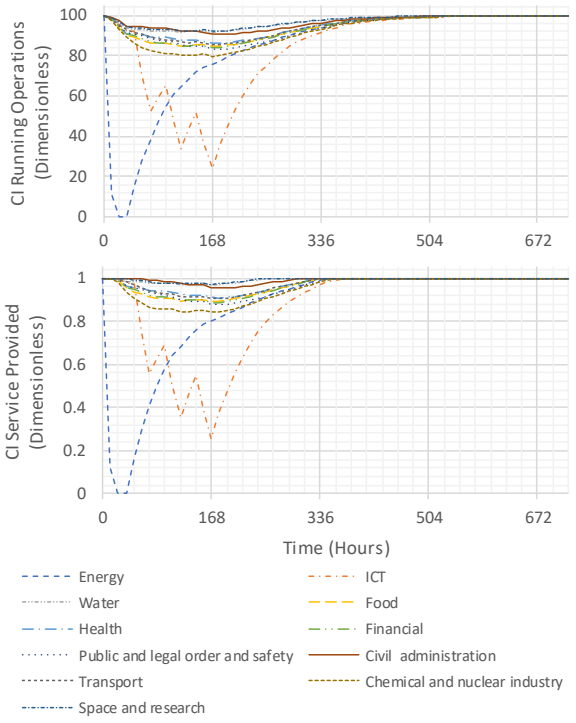

Figure 9: Three Successive Small Cyber-attacks Following an Energy Failure

5.5. Scenario 5 – three successive small cyber-attacks followed by an energy failure

This scenario simulates three successive small

attacks aimed at the ICT CI which happen two days after the simulation, and having one day in-between every two attack. Each attack stays active for durations of one day. These cyber-attacks are followed by an Energy CI disruption that has a magnitude of eight, starts eight days from the simulation time, and keeps on for a duration of one and a half days.

Figure 10, similar to Scenario – 3, shows a large negative effect on the running operations of the ICT CI with a 73% drop at its highest in the seventh day. The disruption happened in the Energy CI caused the CI to completely stop working at the ninth day for 12 hours. Clearly from the figure, this caused the ICT CI to require three more days to go back to 99% of its running operations compared to Scenario – 2 (not before the 20th day of the simulation).

The negative effect of both disruptions was cascaded to other CIs' running operations and reached around 10% drop in Water, Civil administration, and Space and research CIs, and around 18% drop for all other CIs, reaching 22.4% drop at its highest in the case of Chemical and nuclear industry CI.

In terms of service provided, the drop in the ICT CI service provided exceeded 71%. This negative effect was cascaded to the services provided by Water, Civil administration, and Space and research CIs with an average drop of 5%. The negative effect was cascaded to the service provided by all other CIs with an average drop of 13%; at its highest in the case of Chemical and nuclear industry CIs with 18% drop.

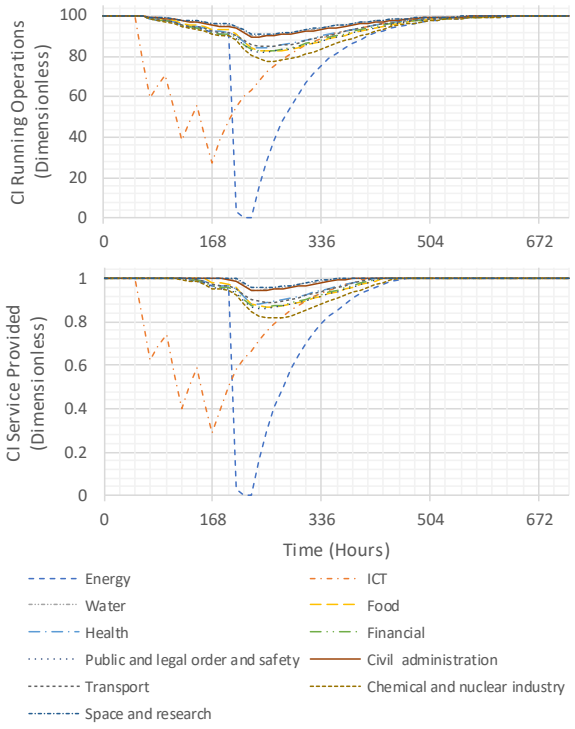

Figure 10: Three Successive Small Cyber-attacks Followed by an Energy Failure

5.6. Scenarios summary

Table 1 summarizes the results of all tested scenarios from 1 to 5. In the table, the scenarios are referred to by their corresponding number.

Table 1: Scenarios Summary

#	Number of cyber-attacks	Energy disruption	Highest drop in other CIs' running operations	Highest drop in other CIs' service provided
1	1	-	3.1 %	0.0 %
2	3	-	10.1 %	5.4 %
3	1	Yes	18.6 %	14.3 %
4	3	Yes	20.0 %	15.8 %
5	3	Yes	22.4 %	18.3 %

While scenario 5 causes about 10 percent higher drops in CI operations, comparing Fig. 9 with 10, it is quite evident that the cyber attacks following the energy outage also prolong the duration of the outage and of the disruptions in other CIs.

6. Concluding remarks

The approach presented in this paper combines the simplicity of disruption dynamics of interconnected Critical Infrastructures with a matrix e_{ij} encapsulating the complexities of the cascading effect from disruption originating in CI_j upon CI_i, where the indices *i* and *j* are labels for the Critical Infrastructures of interest. We have proceeded on the assumption that the approach pioneered by Laugé [6] and Laugé et al. [7], i.e. that the expert assessment of e_{ij} can render a sufficiently accurate metrics of the cascading effects, is viable. By "viable" we mean that a door has been opened for iteratively assessing such expert assessment with simulation results.

Then, we wanted to investigate whether malicious agents could design effective attacks on Critical Infrastructures without needing to plan for one major disruption. To this effect we relied on the expert assessments of e_{ij} obtained by Laugé and simulated various scenarios. The combination of a major energy failure followed by three "opportunistic" small cyber-attacks did indeed show major cascading effects. Massive energy failures happen occasionally; malicious attackers can sit on the fence and release of-the-shelf cyber-attacks when such failure happens. Slightly larger service drops, albeit of shorter duration occurred if the energy failure followed after a series of small cyber-attacks. Such scenario is not unrealistic, since energy

failures occur more and more often as consequences of predictable extreme weather.

It is indeed a weakness that no empirical estimates of the restore times are available. Not having such estimates, we do not emphasize the quantitative consequences but rather stick to the qualitative consequences (patterns of disruption).

An open question is whether Laugé's estimates of CI dependencies [6, 7] have general validity. In Laugé's study, the organizations the participating experts belonged to were predominantly Spanish. To what extent this "Spanish" data is valid for other countries has not been investigated: it would require. duplicating Laugé's study in other countries. On the other hand, critical infrastructures are reasonable similar across countries; hence, one would expect similar interdependencies in different countries rather than very different ones.

A note of caution: the fact that the aggregated CI dependencies provided in [6, 7] are disruptive does not mean that organizational and behavioural effects are excluded in the experts' estimates. It is a weakness that the estimates are "static", in the sense of referring to the status quo. Hence, at the time being we lack data to enhance the model to explore different policies to mitigate the impact of disruptions.

Finally, we wonder whether we should rejoice if the path sketched in this paper does lead to simple but accurate enough description of attack scenarios on Critical Infrastructures. A door would open for using simple tools to plan serious CI attacks.

7. Acknowledgment

This work has profited from exchanges of Tor-Edin Farstad with Elisa Canzani, for which we express our gratitude.

8. References

[1] Barlas, Y., "Formal Aspects of Model Validity and Validation in System Dynamics", *System Dynamics Review 12*(3), 1996, pp. 183–210.

[2] Canzani, E., "Modeling Dynamics of Disruptive Events for Impact Analysis in Networked Critical Infrastructures", *ISCRAM 2016 Conference Proceedings – 13th International Conference on Information Systems for Crisis Response and Management*, Federal University of Rio de Janeiro (2016).

[3] European Commission, "Green Paper on a European Programme for Critical Infrastructure Protection, COM(2005) 576 Final", 2005. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52005DC0576

[4] Forrester, J.W., *Industrial Dynamics*, The MIT Press, Cambridge, Massachusetts, USA, 1961.

[5] Forrester, J.W., and P.M. Senge, "Tests for Building Confidence in System Dynamics Models", In G.P. Richardson, ed., *Modelling for Management: Simulation in Support of Systems Thinking*. Dartmouth Publishing Group, 1996.

[6] Laugé, A., "Crisis Management Toolbox: the Relevant Role of Critical Infrastructures and their Dependencies", 2014. http://hdl.handle.net/10171/37071

[7] Laugé, A., J. Hernantes, and J.M. Sarriegi, "Critical Infrastructure Dependencies: A Holistic, Dynamic and Quantitative Approach", *International Journal of Critical Infrastructure Protection 8*, 2015, pp. 16–23.

[8] Linstone, H.A., and M. Turoff, eds., *The Delphi method: techniques and applications*, Addison-Wesley Pub. Co., Advanced Book Program, Reading, MA, USA, 1975.

[9] Norwegian Directorate for Civil Protection (DSB), *Risikoanalyse av «Cyberangrep mot ekom-infrastruktur»*, 2015.

[10] Ouyang, M., "Review on Modeling and Simulation of Interdependent Critical Infrastructure Systems", *Reliability Engineering & System Safety 121*, 2014, pp. 43–60.

[11] Sterman, J.D., *Business Dynamics: Systems Thinking and Modeling for a Complex World*, McGraw Hill Higher Education, Boston, MA, USA, 2000.

[12] Surowiecki, J., *The wisdom of crowds*, Anchor Books, New York City, NY, USA, 2005.

[13] Ventana Systems, Inc., *Vensim Reference Manual*, Ventana Systems, Inc., Harvard, MA, USA, 2007.

[14] Ventana Systems, Inc., *Vensim DSS Reference Supplement*, Ventana Systems, Inc., Harvard, MA, USA, 2007.

[15] *Vensim DSS*, Ventana Systems, Inc., Harvard, MA, USA, 2009.