Analyzing Cascading Effects among Critical Infrastructures: The CERBERUS Approach

Stefan Schauer, Sandra König, Martin Latzenhofer
AIT Austrian Institute of Technology
{stefan.schauer, sandra.koenig, martin.latzenhofer}@ait.ac.at

Stefan Rass, Thomas Grafenauer
Universität Klagenfurt
stefan.rass@aau.at, tgrafena@edu.aau.at

ABSTRACT

In this article, we present a novel approach, which allows not only to identify potential cascading effects within a network of interrelated critical infrastructures but also supports the assessment of these cascading effects. Based on percolation theory and Markov chains, our method models the interdependencies among various infrastructures and evaluates the possible consequences if an infrastructure has to reduce its capacity or is failing completely, by simulating the effects over time. Additionally, our approach is designed to take the intrinsic uncertainty into account, which resides in the description of potential consequences a failing critical infrastructure might cause, by using probabilistic state transitions. In this way, not only the critical infrastructure's risk and security managers are able to evaluate the consequences of an incident anywhere in the network but also the emergency services can use this information to improve their operation in case of a crisis and anticipate potential trouble spots.

Keywords

Cascading effects, interdependent critical infrastructures, Markov chains, simulation.

INTRODUCTION

Critical infrastructures are assets or systems (or parts thereof) which are essential for the maintenance of vital societal functions. Any failure of a critical infrastructure, either in part or as a whole, will have considerable impact not only on the infrastructure itself but also on the social well-being of people (European Commission 2008). Therefore, critical infrastructures are of significant importance for the maintenance of key processes in society such as the supply of essential goods and services. Such critical infrastructures can be found in different areas, including the basic supply chain networks (electricity, gas, water) as well as information and communication (ICT) networks and ranging to complex systems with severe social impact when not working properly, such as medical care or transportation networks.

In the last decade, critical infrastructures became more and more interconnected with each other, resulting in a highly complex and sensitive network with a variety of interdependencies. Not only do many infrastructures depend on the resources other infrastructures provide but they also exchange a vast amount of information or use each other's services. Thus, incidents within one critical infrastructure can have far-reaching consequences, affecting multiple other infrastructures as well as society as a whole. For example, the disruption of the electric power supply in California in 2001 affected several other critical infrastructures, like the production of oil and natural gas as well as the transportation of gasoline through pipelines (Fletcher 2001). In 2003, a major electricity blackout in Italy lasting for twelve hours resulted in a financial damage in the order of 1182 million Euros (Schmidthaler and Reichl 2014). Furthermore, the hacking of the Ukrainian power grid in 2015 and 2016 (E-ISAC 2016; Condliffe 2016) and the resulting outages for large parts of the country underline that the increased interrelation between communication and operational networks can have severe consequences. Hence, identifying, analyzing and assessing the possible cascading effects that might stem from such incidents has become a core duty in critical infrastructures' risk and resilience management.

In this contribution, we present a novel approach for identifying and assessing potential cascading effects within a network of interrelated critical infrastructures. Our method applies concepts from the fields of percolation theory and Markov chains to describe the interdependencies among various infrastructures. Hence, if an infrastructure has to reduce its capacity or is failing completely, these concepts facilitate the evaluation of the possible consequences by simulating the effects over time. Furthermore, our approach uses probabilistic state transitions to account for the intrinsic uncertainty and randomness which resides in the description of potential consequences a failing critical infrastructure might cause. In this way, not only the critical infrastructure operator's risk and security managers are able to estimate the possible consequences of an incident anywhere in the network but also the emergency services can use this information to improve their operation in case of a crisis and anticipate potential trouble spots.

The approach we present here has been developed in the research project CERBERUS (Cross Sectoral Risk Management for Object Protection of Critical Infrastructures) funded by the Austrian Research Promotion Agency (FFG) and therefore is referred to as CERBERUS approach. The main idea behind this project is to collect and represent security-relevant information of critical infrastructures with a core focus on the interdependencies among them. This information is integrated into a risk model, which specifically considers the propagation of threats in as well as their cascading effects on the network of critical infrastructures. Since two public agencies (i.e., the Ministry of the Interior and the Ministry of Defense) are directly involved in the project, one major goal is to establish an appropriate protection level for critical infrastructures from the federal perspective and to apply novel theoretical models for risk management to ensure the infrastructure objects' security.

The remainder of the article is structured as follows: in the subsequent section, we will give a short overview on current research activities related to our methodology. Then, we will provide a detailed overview on the CERBERUS approach, indicating how we build up to our model, how we describe stochastic interdependencies and how we simulate cascading effects. Afterwards, we illustrate the integration of the approach into the larger CERBERUS system and discuss the benefits and limitations of this system, concluding with some final remarks.

RELATED WORK

Dependencies between interacting critical infrastructures (CIs) or parts thereof can be manifold and have been extensively studied in recent years. Hence, various approaches to categorize these dependencies can be found in the literature (cf. (Rinaldi et al. 2001; Dudenhoeffer et al. 2006a; b; Pederson et al. 2006; US Government 1996)). There are basically five distinct categories which have been suggested in the above approaches, covering physical, informational, geospatial, procedural and societal dependencies (Rinaldi et al. 2001; Dudenhoeffer et al. 2006a; b). These categories can help to better understand the interplay between the infrastructures, e.g., by visualizing them using an interdependency graph, and support the assessment of the likelihood for an incident to affect related infrastructures. However, in real-life scenarios the dependencies are much more complex and the definition of these categories as provided in the literature is often too generic to be directly applied in practice.

Therefore, more sophisticated approaches to categorize and describe the interrelations between CIs are the Hierarchical Holographic Model (HHMs), the Input-output Interoperability Model (IIM) as well as the Hierarchical Coordinated Bayesian Model (HCBM) (cf. (Haimes et al. 2007) for further details on these models). In this context, the HHM (Haimes 1981) provides a taxonomy, which describes the various possible interdependencies between CIs in further detail than, for example, given in (Rinaldi et al. 2001). This allows to get a more precise and properly defined notion of the existing interdependencies. IIM (Haimes and Pu 2001; Santos and Haimes 2004; Setola and Porcellinis 2009) also provides a detailed view on the interdependencies between CIs (or, more generally, economy sectors) and describes the effects of incidents based on linear equations. However, it is strongly focused on economic aspects, which might not always be the appropriate context when looking at CIs. Rather, extreme events of low likelihood but with a severe impact are of particular interest but, in general, only sparse data is available on such events. Therefore, HCBMs (Yan et al. 2006) allow to combine data on extreme events coming from multiple sources to enhance the accuracy and variance when estimating the consequences.

Interdependency graphs are also frequently used as a basis for methodologies simulating (and also forecasting) the propagation of failures and describing cascading effects. A first approach in this direction was the Cross Impact Analysis (CIA) introduced in (Gordon and Hayward 1968) with an alternative approach described in (Turoff 1971). The CIA allows to describe how the relations between events would affect resulting events in the future. An extension to CIA, called CIA-ISM (Cross Impact Analysis and Interpretative Structural Model) (Bañuls and Turoff 2011), is extensively used in emergency management to analyze the interaction between critical events and obtain a reasonable view on potential future consequences (for a more detailed review on CIA and CIA-ISM for cascading effects, we refer to (Turoff et al. 2016) and the references cited therein).

Another effective way to model (sometimes unknown) dynamics and relations between events, stochastic processes can be applied. By using randomness, these models can account for the intrinsic randomness and uncertainty, which resides in the relations and the interplay between critical infrastructures. A prominent example for this is percolation theory, a methodology commonly used for the analysis of epidemics spreading (Sander et al. 2002; Newman 2002; Kenah and Robins 2007; Salathé and Jones 2010) but only rarely used in the fields of security and risk management so far. For example, an extension of percolation theory has been applied in (König et al. 2016) to model the propagation of malware spreading within a utility provider's network. Additionally, techniques based on Bayesian networks are also used to describe interdependencies between critical infrastructures, as, for example, described in (Schaberreiter et al. 2013). In a more general approach, Interdependent Markov Chains (IDMCs) are used to describe the propagation of cascading effects within an infrastructure (Wang et al. 2012; Rahnamay-Naeini et al. 2014; Rahnamay-Naeini and Hayat 2016). Initially, IDMCs have been applied in the energy sector to describe the system's dynamics in order to analyze overload scenarios and to consider the probability for a blackout (Wang et al. 2012; Rahnamay-Naeini et al. 2014). This work has been further extended to be applied between critical infrastructures as well (Rahnamay-Naeini and Hayat 2016). However, Bayesian models as well as Markov chains are more challenging to apply compared to percolation theory due to the huge amount of data required for analyzing the system and understanding the interplay. Further, the effects of random failures on critical infrastructures can be described with multi-graph models (Svendsen and Wolthusen 2007) or models that take into account higher order dependencies (Kotzanikolaou et al. 2013; Theoharidou et al. 2011).

CERBERUS APPROACH

Defining the Model

A crucial requirement for modelling interdependencies between any type of objects or components is the amount of available information about the dynamics of the overall system. In some domains like the energy sector, the dynamics of specific systems are well known and accurate physical models are available that allow an analytic estimate of the effects implied by an incident. Applying such models, the effects of a short power outage or temporary peak loads on other components can be modeled precisely. On the opposite end of the spectrum lie complex technical or social systems. In these systems, various individual objects or components are interacting with each other based on relations that are not fully known and each system reacts differently on incidents. In this context, the underlying dynamics are typically too complex to admit a concise mathematical description. When trying to understand these systems, we can only rely on observations or historical data to learn the behavior of the system. In case a lot of observations are at hand, Bayesian networks can be used to model the system; otherwise if only scarce data is available, percolation theory can be applied (cf. also Figure 1 below). Given the description of a specific system (either based on observations or the knowledge about internal dynamics), the evolution of the system in the future can then be illustrated using simulations.

The network of interdependent CIs ranks among the second area: although the dependencies might be known or can be described, the details of the dynamics (i.e., how an infrastructure reacts to an incident within another infrastructure) cannot be specified in full detail. Hence, the CERBERUS model lies "in between" the two extreme characteristics of perfectly known dynamics, where the system's behavior can be described by a deterministic flow chart, and entirely stochastic behavior, where effects are captured by conditional probability distributions, e.g., a Bayesian network. The CERBERUS model – as visualized in Figure 1 – unifies the two positions by sacrificing parts of the expressiveness of both models for the sake of a model that can simulate both a deterministic and stochastic behavior (at least in restricted form), is easy and efficient to parameterize, and is fast to simulate.

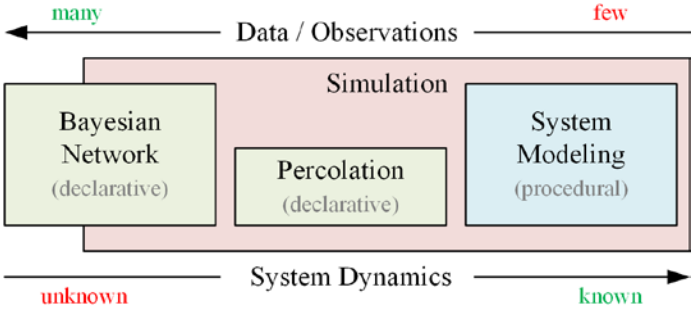

Figure 1. Illustration of the tradeoff between different approaches to model the network of interdependent CIs

Describing Stochastic Interdependencies

The CERBERUS model describes each CI as a node in a directed graph, where the edges indicate the dependencies between these CIs (and in this way adapting the idea of an interdependency graph). In this graph, an edge from CI *X* to CI *Y* indicates that CI *Y* depends on an input from CI *X* to work properly (cf. Figure 2 below). In other words, CI *X* is a "supplier" for CI *Y* (or CI *Y* is a "customer" of CI *X*). Although this representation illustrates the general interdependencies between a certain number of CIs (e.g., the infrastructures located within a specific region or province), it does not provide any detailed information on how much the individual infrastructures influence each other.

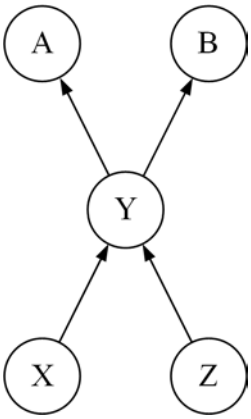

Figure 2. Simple example of a CI interdependency graph

In general, an impairment in the functionality of CI *X* could have a small or large effect on the operational state of CI *Y*, depending on how dependent CI *Y* is on the resource or service provided by CI *X*. Hence, in the CERBERUS model each CI is described by a finite number of different states *k* representing its operational condition. This operational state of an CI may or may not change according to the operational states of its suppliers, based on the individual interdependencies between them. In order to model this state change, each edge between two CIs is extended by a multinomial distributed random variable (König and Rass 2017). This variable then describes the probability that the CI *Y* goes from state k_i to k_j based on the current state of its supplier CI *X*. We assume that all CIs are in one of the *k* states so the change of state of CI Y due to the current state of CI X can be understood as a (generalized) Markov chain, similarly to the approach described in (Rahnamay-Naeini and Hayat 2016) and others (see related work above). As a visual representation, these states can be illustrated using different colors (e.g., ranging from green to red) to reflect the severity of each state, as shown in Figure 3.

Giving a simplified example, we assume that both CI *X* and CI *Y* can be in one of five different states of operation. These states range from "1" describing the normal operation up to "5" describing a complete failure of the infrastructure. Further, the probability of CI *Y* switching from one state to another is given by the state *k* its supplier CI *X* is currently in. Hence, if CI *X* notifies CI *Y* about an impairment in its operation (e.g., CI *X* switches to state "3", corresponding to medium troubles with its service provisioning), CI *Y* switches from state "1" to a state of reduced operation with a certain probability as a reaction to CI *X*'s current condition.

Furthermore, if multiple suppliers notify about their states, a CI may internally undergo transitions into multiple states at the same time. Though paradoxical at first glance, this may indeed happen in reality: if several suppliers report problems or shortages, a CI may encounter multiple issues at the same time. For example, in case a power outage is the main problem, this can imply a shortage of water supply due to pump failures as a secondary (implied) problem later on. A CI depending on both power and water supply will be affected by both incidents. According to the *maximum principle*, such different conditions may be aggregated into the most severe condition for the CI to determine the overall operational state of the CI. That is, if a CI has multiple problems of different severity, its overall operational state is determined by the most severe incident that it currently has to deal with, shown in Figure 3.

Simulating Cascading Effects

One possibility to simulate the CERBERUS model is to use a discrete event-driven system like OMNeT++. This allows to implement the information flow between nodes in a straightforward manner and to reflect a wide range of different dynamics in the CERBERUS model, with the most important being:

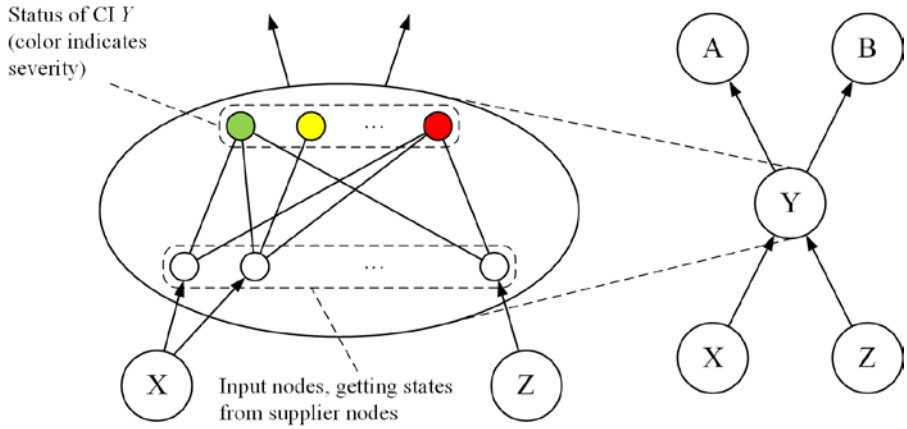

Figure 3. Illustration of the CERBERUS Model (König and Rass 2017)

- *Deterministic effects*: if CI *Y* functionally depends on CI *X*, then the chances for CI *Y* to switch to a problematic state can be set to 1, implying that whenever *X* has a problem, *Y* will have a problem, too (for sure).
- *Random effects*: an incident affecting CI *X* may not immediately trigger a problem for CI *Y*, but only do so with a certain likelihood (as in the case of stochastic models like Bayesian networks) or after a specified period of time. In this way, the model accounts for the intrinsic uncertainty which resides in the interplay between the respective CIs

The number of parameters to be specified in this kind of model is quadratic in the number of states, since the transitions between any two distinct operational states specified in the model need to be specified. For example, for $k = 3$ operational states ("OK" / "problems" / "outage"), a total number of four transitions have to be defined, typically specified in matrix form (cf. Table 1 for an example).

follow-up state of CI *Y* → / **state of supplier *X*↓**	**OK**	**Problems**	**Outage**
OK	1	0	0
Problems	0	0.33	0.33
Outage	0	0.01	0.66

Table 1. Example for a transition matrix in the CERBERUS model

The simulation starts with a specific incident (selected by the user), which affects a certain set of CIs. The CIs depending on them switch from their initial state "OK" to a problem state with a certain probability specified in the *transition matrix* for the respective edge in the dependency graph (cf. Table 1). Further, the transition is specified for three time periods; "short-term", "medium-term" and "long-term". Their meaning can be defined individually for each CI, since the timeframe considered as "short-term" is different for a power provider than for a food provider. Hence, the values of the transition matrix are related to the severity of the dependency between CIs X and Y and the duration of a problem/outage. Additionally, redundancies like emergency power generators or other contingency measures can also be directly modeled in the simulation.

The CERBERUS model can also cope with time-dependent effects, i.e., if a CI can cover short-term outages of a supplier but will eventually stop working itself if the supplier does not continue its service within a certain period of time. In this case, each transition in the matrix above can be made time-dependent, i.e., the probability to switch from "OK" to "Problems" is zero for CI *Y* between $t = 0$ and $t < T_0$, where T_0 is the time window that can be covered from backup resources at CI *X*. After that time, CI *Y* will either require CI *X*'s service or it will itself run into problems. In the above matrix, the transition probability for "OK → Problems" can then be set to $p_{\text{OK}\to\text{Problems}}(t) = 0$ for $0 \le t < T_0$ and $p_{\text{OK}\to\text{Problems}}(t) = 1$ for $t \ge T_0$.

Figure 4 displays the simulation frontend, showing the interdependency graph in the right area of the window in

a simplified form. The configuration of the simulation, specifically the setting and fine-tuning of the transition matrix, is done in the left part of the window, showing some switches and controls to trigger incidents or recoveries at the desired instants of time. The aforementioned transition matrix is highlighted in different colors, using yellow for transitions within short terms, orange for medium term transitions and red for transitions in the long(er) run. Upon starting the simulation, a script is compiled and sent to OMNeT++ simulation backend.

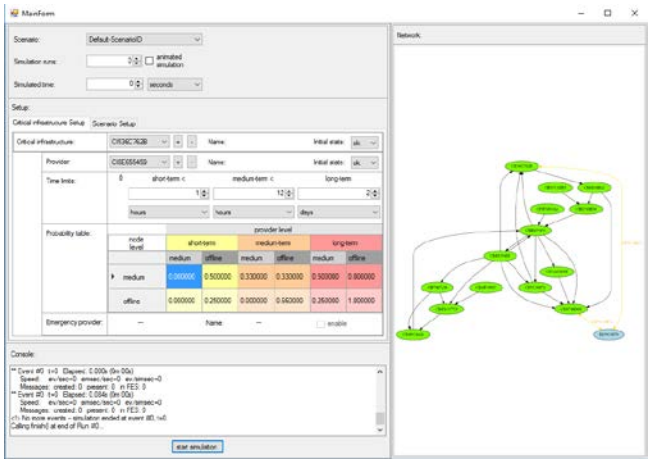

Figure 4 Screenshot of the Simulation Configuration Frontend

CERBERUS SYSTEM OVERVIEW

Our approach to model and simulate cascading effects described in the previous section represents the core of the CERBERUS system (cf. Figure 5 below) developed in the research project of the same name. The approach is the basis for the Dynamic Risk Analysis component as well as the Simulation component of the proposed system, which are illustrated on the right-hand side of Figure 5.

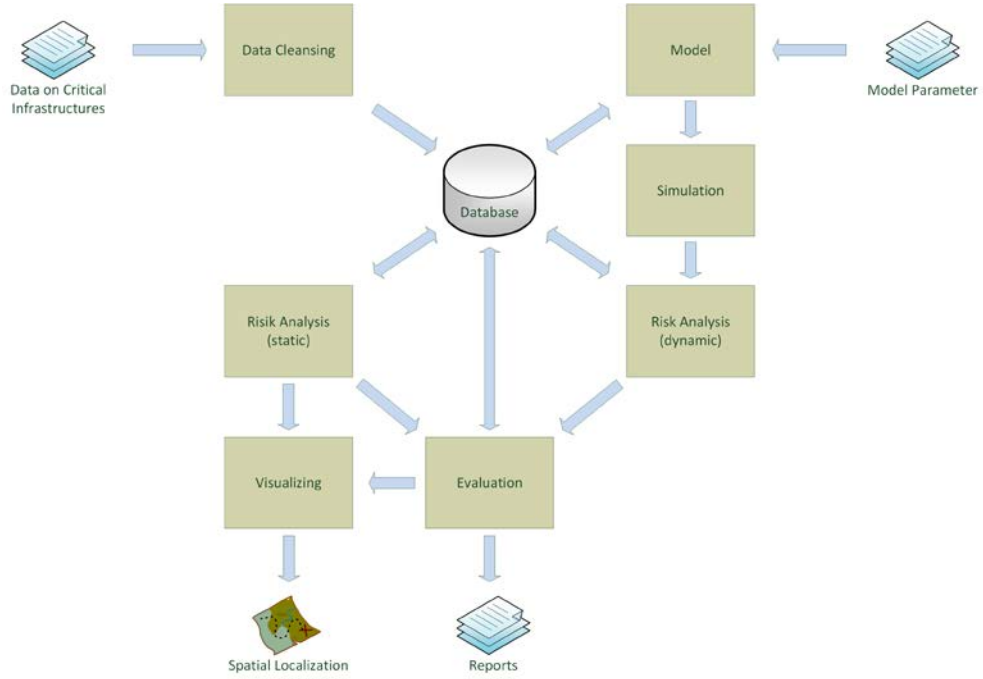

Figure 5. Schematic illustration of the CERBERUS system architecture

More precisely, the CERBEURS system builds upon information about the CIs coming from existing data gathered by the user. In the CERBERUS project, this is done by governmental bodies (cf. the next section for details), which are in close contact to the CIs and support them on security-related issues. This data includes general information on the infrastructures, e.g., its location, responsible contact persons, etc., as well as details on the security measures implemented by the infrastructure, if available. Additionally, for each CI a list of suppliers and customers is given as defined in the CERBERUS model (cf. also Figure 2 above).

Besides the data on the CIs, the parameters of the model have to be defined, e.g., the number of different operational states or how they are visualized. Based on this information, the CERBERUS model is instantiated in the Model component using the collected data on the CIs. Further, the interdependency graph of all infrastructures is created, representing each CI as a node with several "suppliers" and "customers" (as given in the collected data), and the predefined number of operational states, as well as the transition probabilities for each supplier that affects a customer. The graph is then passed on to the Simulation component, where the cascading effects of a specific incident (specified in a scenario) happening at one infrastructure (causing it to reduce its operation or fail completely according to the model) are simulated and assessed. The evolution of the overall interdependency graph, i.e., the state transition of all CIs, throughout the simulation are stored and passed on to the Dynamic Risk Analysis component. Therein, the information is evaluated, inspecting how often a CI is affected by an incident, which operational state it will be in on average and which will be the most severe operational state due to an incident. The results are used on the one hand to form the dynamic risk level but are further used to make estimations about the resilience level of each infrastructure. As mentioned above, the Simulation component together with the Dynamic Risk Analysis represent the dynamic risk model of the CERBERUS system.

Along with the dynamic risk model, the CERBERUS system also evaluates a static risk model, implemented in the Static Risk Analysis component (illustrated on the left-hand side of Figure 5). The static risk model mainly builds upon information related to the security measures which are put into action in each CI. In detail, best practice guidelines on security like the ISO 27001 (International Organization for Standardization 2013a), ISO 27002 (International Organization for Standardization 2013b), the German IT Baseline Security (Bundesamt für Sicherheit in der Informationstechnik 2016) or others defined a catalog of security measures, which should be implemented to be prepared against specific threats. Although CIs are, in general, aware of these frameworks and implement many of the suggested security measures, it is not possible to do so for all of them. Hence, the static risk level for the CI is computed based on the resulting gap.

As it is shown at the bottom of Figure 5, the CERBERUS system aims at providing different outputs to the user: on the one hand, reports are combining the information coming from the static and the dynamic risk analysis. These reports will be prepared to fit the needs of different addressees, for example, technical experts, crisis response teams or managers. On the other hand, a visualization component supports a geospatial overview on the potential effects of a specific incident. Since the GPS information for all CIs is at hand, they can be located in a GIS tool and the infrastructures affected by an incident can be highlighted according to their current state throughout the simulation. Therefore, the users of the system will obtain all the available information for an overview on the potential cascading effects of an incident, which will support them in making the right decision to counter these effects.

APPLICATIONS AND LIMITATIONS OF THE CERBERUS SYSTEM

Outputs

The CERBERUS approach aims at studying resilience of a system of interdependent CIs against externally triggered incidents. This assumes that every CI can handle internal incidents as part of the daily business, hence these events are not modeled or discussed here further. First and foremost, the CERBERUS system (implementing the CERBERUS approach) provides a detailed overview on the dependencies between the considered CIs in the form of the interdependency graph. This graph is built from the relations between individual infrastructures, which links all the infrastructures together based on their suppliers and customers, as described above. The simulation component of the CERBERUS system uses this graph to discover cascading effects that an incident occurring at one infrastructure can have on downstream (dependent) infrastructures and the whole network as such. In this way, the CERBERUS approach extends the direct dependencies among CIs (visible in the interdependency graph) by making indirect dependencies of higher-order visible, i.e., indicating how dependent a CI is on the seamless operation of the suppliers of its suppliers (and so forth).

Furthermore, the data retrieved from the static and the dynamic risk model are combined and integrated into a general risk level for each infrastructure. This risk level is essentially the CI's expected "robustness" (cf. Figure 3) in the light of different incidents. This value is averaged from multiple simulations, based on the various security measures that an infrastructure has implemented to prevent specific threats and on its interdependence with other infrastructures. In other words, the more security measures a CI has implemented, the lower its risk level will be, meaning an expectedly better operational status. In addition to the risk level, a resilience level is defined based on this degree of dependence of one infrastructure upon others. More precisely, the less affected an infrastructure is by a failure of one of its suppliers, e.g., due to redundancy, the higher is its resilience level. Essentially, the resilience level is computed in a similar way compared to the risk level, but the

underlying hypothesis between the two levels is different: risk levels are conditional expectations in light of certain incidents. Resilience is the respective unconditionally expected operational status. Both, the risk level and the resilience level are designed on abstract qualitative scales, e.g., ranging from "low" to "high" or from "1" to "5". The scales and the different levels can be defined by the user and thus are fully tailored to his or her needs.

Finally, all output information can be used to increase the preparedness of each individual CI but also of the emergency response teams, which should assist the infrastructures in case of an incident. In detail, if a CI's risk or resilience level is above a certain threshold this indicates that the infrastructure needs to implement additional security measures to be better prepared for an emergency. The risk and resilience level, together with customized simulations, also indicate which infrastructures might need special attention in case of a specific incident happening somewhere in the network. This information can later be used to optimize the preparation and operation of emergency response teams.

Application Fields

We foresee two different fields of application for the CERBERUS system. On the one hand, the system is designed to be used by governmental bodies, which have an overview on the different types of CIs in a specific region (e.g., a city, county or province). The assumption is that the governmental body either has explicit information about the interdependencies between the CIs already at hand, e.g. from previous studies, or gets in contact with experts from the CIs to obtain the relevant information. If this information can be used as an input, the CERBERUS system can model an incident and simulate its consequences for the CI network. The resulting risk and resilience level identify current weak spots among the infrastructures, e.g., if a specific CI encounters severe problems in many simulations due to its dependencies on other CIs, the governmental body might approach the CI operator suggesting additional security measures to be implemented.

Furthermore, the results from the simulations also support the governmental body in optimizing the preparation and operation of emergency response teams in disaster management. Simulated scenarios may help allocating resources and setting up emergency plans. The CERBERUS system allows to identify which CIs might need special assistance by providing an overview on the potential effects of an incident on the overall CI network. Hence, emergency response teams plan their support actions (i.e., where to send their people first) by learning from the simulation results. Moreover, simulations can be automatically generated from the infrastructure model, e.g., simply by iterating over all combinationally possible outage scenarios. In this way, conceivable but yet unknown worst-case scenarios can be identified and the existing disaster management plans can be adapted and extended based on these simulation results.

On the other hand, the CERBERUS system can also be applied by the operators of large CIs, which want to get an overview on the interrelations between different parts of their organization (e.g., subsidiaries, production lines, internal services, etc.) and on the dependencies on their suppliers. In this context, more details on the internal processes, system dynamics and the resulting dependencies will be available, providing much more data for the CERBERUS model. Accordingly, the simulations can be more fine-grained, e.g., with a higher number of operational states. Here again, the results coming out of the CERBERUS system can be used to identify weak spots, indicating crucial processes and services within the CI.

We stress that in both cases the human factor can be modeled quite explicitly with the CERBERUS approach, since human actors with strong influence on certain parts of the system can simply be assigned their own node in the interdependency graph. It is conceptually no problem to treat a human entity as a CI on its own, on which other parts of the system depend (e.g., requiring the person's skills) and who itself depends on other systems (e.g., information sources, telecommunication, etc.). Incidents influencing a human actor would then primarily relate to social engineering (externally triggered incidents), treating human failure as an internal incident whose treatment is (or should be) part of the internal risk management maintained by a CI.

Limitations

Since the CERBERUS approach is designed towards a tradeoff between flexibility (expressive power) and usability (simple to parameterize), it is necessarily a compromise between different models and as such limited, relative to other models (as shown in Figure 1). The approach is very much data driven, requiring detailed information on the individual CIs and on the interdependencies between them as well as on the consequences of certain events (cf. Figure 5 and the description of the CERBERUS system above). Furthermore, the probability matrix describing the state transitions for a CI also needs to be estimated, which can be a lengthy and complex process.

All the required information usually has to be gathered from experts within the CI. Due to the sensitivity of this

information, the CI operators might be particularly reluctant to provide it to externals (e.g., governmental bodies, as mentioned above). A crucial aspect in this context is the question of authority and jurisdiction regarding who is allowed to collect this sensitive information. In Austria, the Ministry of the Interior and the Ministry of Defense have the joint duty to protect the Austrian CIs and thus they are gathering information from CI operators. However, there is no legal obligation for the CIs to provide the information to the ministries, which leads to more complex situations. In other countries, there is often no central agency entrusted with the task of protecting all the CIs within the country. Rather, different agencies and governmental bodies are in charge of different sectors like electric power, gas or water, as for example in the United States, which makes the communication and mutual information exchange very difficult as well as raises issues on the jurisdiction.

Additionally, the experts providing the information within the CIs might not have enough experience on a specific matter such that not all or incorrect information is fed into the system. This could be due to the fact that the person responsible for carrying out the risk analysis does not have a full overview on the field (e.g., because the person is supervising several organization units) or is not qualified enough (e.g., because the person is working on risk analysis as an add-on due to budget constraints). Consequently, this might lead to less accurate results from the model. However, we have seen that the direct contact with experts might also reveal latent information, e.g., about implicit dependencies between CIs.

CONCLUSION

In this article, we presented the CERBERUS approach to model and assess the consequences of cascading effects in a network of critical infrastructures. It allows to represent a critical infrastructure in different operational states directly depending on the corresponding state of the infrastructure's suppliers. We showed how the propagation of cascading effects among these critical infrastructures can be described and simulated using stochastic processes to account for the intrinsic randomness and uncertainty which resides in the interplay of critical infrastructures. As an output, the approach provides a certain risk level (based on static and dynamic aspects) and a resilience level (based on the interdependencies) for each infrastructure. We are currently implementing the CERBERUS approach as a software solution, which will support operators and governmental bodies in ensuring a high degree for security and preparedness of critical infrastructures.

ACKNOWLEDGEMENTS

This work was conducted in context of the project ``Cross Sectoral Risk Management for Object Protection of Critical Infrastructures (CERBERUS)", supported by the Austrian Research Promotion Agency under grant no. 854766.

REFERENCES

Bañuls, V. A., and Turoff, M. (2011). "Scenario construction via Delphi and cross-impact analysis." *Technological Forecasting and Social Change*, The Delphi technique: Past, present, and future prospects, 78(9), 1579–1602.

Bundesamt für Sicherheit in der Informationstechnik. (2016). *IT-Grundschutz Catalogues*. Bonn, Germany.

Condliffe, J. (2016). "Ukraine's Power Grid Gets Hacked Again, a Worrying Sign for Infrastructure Attacks." <https://www.technologyreview.com/s/603262/ukraines-power-grid-gets-hacked-again-a-worrying-sign-for-infrastructure-attacks/> (Jul. 26, 2017).

Dudenhoeffer, D. D., Permann, M. R., and Boring, R. L. (2006a). "Decision consequence in complex environments: Visualizing decision impact." *Proceeding of Sharing Solutions for Emergencies and Hazardous Environments. American Nuclear Society Joint Topical Meeting: 9th Emergency Preparedness and Response/11th Robotics and Remote Systems for Hazardous Environments*, 211–218.

Dudenhoeffer, D. D., Permann, M. R., and Manic, M. (2006b). "CIMS: A Framework for Infrastructure Interdependency Modeling and Analysis." *Proceedings of the 2006 Winter Simulation Conference*, Monterey, USA, 478–485.

E-ISAC. (2016). *Analysis of the Cyber Attack on the Ukrainian Power Grid*. Washington, USA.

European Commission. (2008). "COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection." *Official Journal of the European Union*, (L345), 75–82.

Fletcher, S. (2001). "Electric power interruptions curtail California oil and gas production." *Oil Gas Journal*.

Gordon, T. J., and Hayward, H. (1968). "Initial experiments with the cross impact matrix method of forecasting." *Futures*, 1(2), 100–116.

Haimes, Y., Santos, J., Crowther, K., Henry, M., Lian, C., and Yan, Z. (2007). "Risk Analysis in Interdependent

Infrastructures." *Critical Infrastructure Protection*, E. Goetz and S. Shenoi, eds., Springer US, Boston, MA, 297–310.

Haimes, Y. Y. (1981). "Hierarchical Holographic Modeling." *IEEE Transactions on Systems, Man, and Cybernetics*, 11(9), 606–617.

Haimes, Y. Y., and Pu, J. (2001). "Leontief-Based Model of Risk in Complex Interconnected Infrastructures." *Journal of Infrastructure Systems*, 7(1), 1–12.

International Organization for Standardization. (2013a). *ISO/IEC 27001 - Information technology – Security techniques – Information security management systems – Requirements*.

International Organization for Standardization. (2013b). *ISO/IEC 27002: Information technology - Security techniques - Code of practice for information security controls*. Geneva, Switzerland.

Kenah, E., and Robins, J. M. (2007). "Second look at the spread of epidemics on networks." *Physical Review. E, Statistical, Nonlinear, and Soft Matter Physics*, 76(3 Pt 2), 036113.

König, S., and Rass, S. (2017). "Stochastic Dependencies Between Critical Infrastructures." Rome, Italy, 106–110.

König, S., Rass, S., and Schauer, S. (2016). "A Stochastic Framework for Prediction of Malware Spreading in Heterogeneous Networks." *Secure IT Systems. 21st Nordic Conference, NordSec 2016, Oulu, Finland, November 2-4, 2016. Proceedings*, B. Brumley and J. Röning, eds., Springer International Publishing, Cham, 67–81.

Kotzanikolaou, P., Theoharidou, M., and Gritzalis, D. (2013). "Assessing n-order dependencies between critical infrastructures." *International Journal of Critical Infrastructures*, 9(1/2), 93–110.

Newman, M. E. J. (2002). "Spread of epidemic disease on networks." *Physical Review E*, 66(1), 016128.

Pederson, P., Dudenhoeffer, D. D., Hartley, S., and Permann, M. R. (2006). *Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research*. INL, INL/EXT-06-11464, Idaho Falls, USA.

Rahnamay-Naeini, M., and Hayat, M. M. (2016). "Cascading Failures in Interdependent Infrastructures: An Interdependent Markov-Chain Approach." *IEEE Transactions on Smart Grid*, 7(4), 1997–2006.

Rahnamay-Naeini, M., Wang, Z., Ghani, N., Mammoli, A., and Hayat, M. M. (2014). "Stochastic Analysis of Cascading-Failure Dynamics in Power Grids." *IEEE Transactions on Power Systems*, 29(4), 1767–1779.

Rinaldi, S. M., Peerenboom, J. P., and Kelly, T. K. (2001). "Identifying, understanding, and analyzing critical infrastructure interdependencies." *IEEE Control Systems*, 21(6), 11–25.

Salathé, M., and Jones, J. H. (2010). "Dynamics and Control of Diseases in Networks with Community Structure." *PLOS Computational Biology*, 6(4), e1000736.

Sander, L. M., Warren, C. P., Sokolov, I. M., Simon, C., and Koopman, J. (2002). "Percolation on heterogeneous networks as a model for epidemics." *Mathematical Biosciences*, 180(1), 293–305.

Santos, J. R., and Haimes, Y. Y. (2004). "Modeling the demand reduction input-output (I-O) inoperability due to terrorism of interconnected infrastructures." *Risk Analysis: An Official Publication of the Society for Risk Analysis*, 24(6), 1437–1451.

Schaberreiter, T., Varrette, S., Bouvry, P., Röning, J., and Khadraoui, D. (2013). "Dependency Analysis for Critical Infrastructure Security Modelling: A Case Study within the Grid'5000 Project." *Security Engineering and Intelligence Informatics*, A. Cuzzocrea, C. Kittl, D. E. Simos, E. Weippl, and L. Xu, eds., Springer Berlin Heidelberg, Berlin, Heidelberg, 269–287.

Schmidthaler, M., and Reichl, J. (2014). "Economic Valuation of Electricity Supply Security: Ad-hoc Cost Assessment Tool for Power Outages." *ELECTRA*, (276), 10–15.

Setola, R., and Porcellinis, S. D. (2009). "Critical Infrastructure Dependency Assessment Using the Input-Output Inoperability Model." *IJCIP*, 2, 170–178.

Svendsen, N. K., and Wolthusen, S. D. (2007). "Analysis and Statistical Properties of Critical Infrastructure Interdependency Multiflow Models." IEEE, 247–254.

Theoharidou, M., Kotzanikolaou, P., and Gritzalis, D. (2011). "Risk assessment methodology for interdependent critical infrastructures." *International Journal of Risk Assessment and Management*, 15(2/3), 128–148.

Turoff, M. (1971). "An alternative approach to cross impact analysis." *Technological Forecasting and Social Change*, 3, 309–339.

Turoff, M., Bañuls, V. A., Plotnick, L., Hiltz, S. R., and Ramírez de la Huerga, M. (2016). "A collaborative dynamic scenario model for the interaction of critical infrastructures." *Futures*, 84, 23–42.

US Government. (1996). "Executive Order, 13010. Critical Infrastructure Protection." *Federal Register*, 138(61), 3747–3750.

Wang, Z., Scaglione, A., and Thomas, R. J. (2012). "A Markov-Transition Model for Cascading Failures in Power Grids." *2012 45th Hawaii International Conference on System Sciences*, 2115–2124.

Yan, Z., Haimes, Y. Y., and Wallner, M. G. (2006). "Hierarchical coordinated Bayesian model for risk analysis with sparse data." Baltimore, USA.