Proceedigns of the 12th International Defense and Homeland Security Simulation Workshop (DHSS), 003
19th International Multidisciplinary Modeling & Simulation Multiconference

2724-0363 © 2022 The Authors.
doi: 10.46354/i3m.2022.dhss.003

ISIDOR: Analysing the Consequences of an Extensive and Prolonged Internet Outage with System Dynamics

Larissa Schachenhofer[1*], Manfred Gronalt[1] and Patrick Hirsch[1]

[1]Institute of Production and Logistics, Department of Economics and Social Sciences, University of Natural Resources and Life Sciences Vienna, Feistmantelstraße 4, 1180 Vienna, Austria

[*]Corresponding author. Email address: larissa.schachenhofer@boku.ac.at

Abstract

Our society is characterized by a high degree of digitalization as well as an increasing dependency on information and communication technology. Yet, redundancies in the critical infrastructure network are reduced for reasons of efficiency, which leads to a decreased system robustness, while internet outages and cyber threats are on the rise. This research is part of the research project ISIDOR, which aims to examine the consequences of a long-lasting and large-scale restriction of internet-based services or infrastructure. In contrary to cyber security related studies, the study at hand analyses the time span from the occurrence of an outage event. The methodology of System Dynamics is applied to create Causal Loop Diagrams, which visualize the cascade effects that are likely to occur during an outage event. The key findings expected from the research are the detection of relevant cause-effect relationships in respect to extensive internet outages. The value of the work is expected to consist of the identification of areas of activity, that should be strengthened in the future and to raise awareness in that field. The aim is to generate knowledge on how to deal with the complexity of interconnected crises in an informed manner.

Keywords: Internet outage, Critical infrastructure, Interconnected crisis, System Dynamics, Cascade effects

1. Introduction

Due to the high degree of digitalization and the growing dependency on information and communication technology, our society has to face an increasing risk in respect to the occurrence of interconnected crises. The temporal and areal extent of such an event is decisive for the number and severity of cascade effects, which can be expected from that. In this context, it is important to note that services provided by critical infrastructure are often interrelated. Yet, these interrelations are often not considered in risk analyses (Zabasta et al., 2012). Nevertheless, assuring functionality and safety within and beyond the different critical infrastructure sectors is of high importance for both the state and the population. In the event of a crisis situation, affected critical infrastructure elements can increase the risk for other related critical infrastructure sectors, too. These causalities can lead to detrimental domino effects, such as encountered in blackout events (Mrazek et al., 2019).

Supporting organisational decision-making by using simulation approaches is gaining more and more importance in the face of phenomena that involve a high level of uncertainty (Kulkarni et al., 2017). Internet outage events, one of the main modern risks, are part of such phenomena. A long-lasting and large-scale restriction of internet-based services or infrastructure could initiate a chain of supply bottlenecks that might pose a threat to public order. Consequently, interconnected crises constitute a relevant risk to modern societies. Known and so far unknown cause-effect relationships are important to get revealed in order to grasp the consequences that would affect organizations, corporations and society on a large scale. The topic of internet failures is often primarily looked at through the lens of cyber security which puts the time span before an event into focus. Conversely, our research as part of the research project ISIDOR examines the time span from the occurrence of such an outage event. We focus on the detection of cascade effects in relation to a long-lasting and large-scale restriction of internet-based services or infrastructure. We create causal loop diagrams to visualize the cascade effects, that are related to an internet outage event. Based on this, we identify critical areas of activity to increase the resilience and robustness of modern information and communication systems. Public authorities must be aware of this and must have plans in reaction to the increased risk of internet outages to not only be able to respond quickly but also to increase the general level of disaster preparedness by offering large-scale practical trainings on a regular basis for companies and organizations, that are part of the critical infrastructure, as well as broad parts of society. The relevance of Modeling & Simulation (M&S) for education and training purposes during crisis events such as pandemics or chemical, biological, radiological and nuclear threats is also shown by Bruzzone et al. (2020).

The paper proceeds as follows. Section 2 shows the state of the art of the research related to internet outages and a connection to the Modeling & Simulation literature is established. Section 3 is about the methods that were used for the analysis. In section 4 we present the results that can be reported so far from the research project. In the course of section 5, relevant conclusions are outlined and suggestions for future research are provided.

2. State of the art

According to Hansson et al. (2020) communication systems and technologies become increasingly interconnected with human communication overall. Already in 2013, Çetinkaya et al. (2013) stated that these communication networks have become part of the critical infrastructure and that these networks are more and more exposed to attacks and large-scale disasters as a consequence.

Today, critical infrastructures and with this also cyber physical systems are a popular target for cyber-attacks which aim at compromising critical systems. Such attacks have the potential to impact daily business operations, damage equipment and reputation and can also lead to intellectual property being at risk of theft. Furthermore, financial losses as well as health and safety risks can occur in relation to compromised systems (Settanni et al., 2017).

However, not only cyber-attacks lead to compromised or temporarily not accessible internet services. The causes for internet outages are manifold and can range from natural disasters, physical and software attacks, over accidental misconfiguration, network equipment hardware failures, software bugs to different forms of censorship and war (Aceto et al., 2018).

The threat of an internet outage event depends on the possible vulnerabilities of a system and the threat potential. The risk of an outage is comprised by these aspects, the probability of occurrence as well as the damage potential (Eckert, 2018). Already early studies show, that a profound understanding of challenges related to the internet network and related threats is indispensable. The challenges not only depend on the amount of network elements in the affected area, but also the criticality of the affected nodes and their relevance for the rest of the network. Another factor, that is decisive for the severity of the challenge imposed on the internet network by an outage event, is the duration of the impact (Çetinkaya et al., 2013).

Çetinkaya et al. (2015) state that the modeling of large-scale disasters and attacks against the physical internet infrastructure is of high importance and that there is only a small number of studies that provide holistic analyses from a multilevel perspective.

Also, Aceto et al. (2018) stress the importance to grasp the full extent of the problem by integrating the high complexity of the internet environment, that is resulting from the collaboration between different independent networks and hence a high coordination effort in the case of an outage event. The study further revealed a lack of methodologies, guidelines and best practices for analyzing internet outages. An underlying problem is that documented internet outages are difficult to compare and the metrics used may vary significantly.

According to Sterbenz et al. (2010) it is widely recognized that the resilience of the internet is not sufficient and that research and development actions are indispensable to improve the network resilience also in the face of the aforementioned challenges. This statement is supported by Aceto et al. (2018), who argued that the extent, to which the internet network is resilient against interruption, has to be evaluated in order to not only contribute to a comprehensive understanding of internet outages, but also to define essential mitigation strategies in the case of the occurrence of an outage event as a starting point. Also, this study reveals the paucity of studies on outage events and the necessity for more research on outage analyses, mitigation and prevention strategies, models for risk assessment as well as best practices.

Thus, in the face of the outlined research gaps found in the related literature, the research done in the course of the research project ISIDOR aims at contributing to a better understanding of internet outage events and underlying cascade effects from the impact perspective. While in previous studies internet outage events were primarily analyzed from the perspective of cyber security and the time span before an event, the innovative contribution of this paper is that our research focuses on the time span from the occurrence of such an event. For this, a system dynamics (SD) approach is used. SD goes back to Forrester (1961) who developed this methodology for the analysis of complex systems. The interdisciplinary SD approach is designed to identify causalities and feedback processes of dynamic real-world problems, that lead to a high dynamic complexity (Sterman, 2009). The behaviour of a dynamic system over time is pre-defined by its inherent structure. In the study of Longo et al. (2016) causal loop diagrams are used to discern the complexity of an emergency response system. It shows the major variables as well as important feedback loops in response reactions. Also, for the analyses of disasters in industrial plants Bruzzone et al. (2014) state that the application of Modeling & Simulation is highly relevant. The research aim of ISIDOR is to analyze the consequences of an extensive and prolonged internet outage starting with the occurrence of such an event. Based on that, recommendations for action will be provided as well as measures for the simultaneous restarting processes of the system after the outage event. One challenge in respect to modeling an internet outage was to define how it manifests itself. Internet blackouts become evident by digital services such as cloud-sharing services, digital communication services and digital data storage and access being temporarily not available, which serves as a starting point for the models.

We also refer to the DIN EN ISO 22301 for business continuity management systems, which provides generic requirements for security and resilience. Business continuity measures play a key role for the recommendations for action in respect to internet outages, and thus, will be included as well.

3. Material and methods

A comprehensive desk research and twenty-one expert interviews with representants from different sectors serve to create preliminary versions of the causal loop diagrams, which are the starting point for all further iterative processes. For this, the relevant results from related literature and the interviews are categorized systematically according to factors, that constitute potential system variables for the different sectors (internet service providers, public sector, health sector, transport sector, energy sector etc.). The structure of a system is characterized according to Ford (2009) by

- endogenous
- exogenous
- and excluded factors.

Thus, also the position of the variables in the system is derived from the available information. Further, the interrelations of the considered system variables are of interest in order to create the causal loop diagrams. Paragraphs or sentences, that validate the linkages, are written down in the course of the categorization. The variables are divided into start and end variables for the respective feedback processes. The relationship types in the models are either positive or negative and the analysis serves as the starting basis to create the causal loop diagrams.

In the models, the cause-and-effect interactions are illustrated with arrows. Figure 1 demonstrates an example of a positive and a negative interaction between system variables related to internet outages. The positive interaction between the internet bandwidth and the availability of digital services is shown by an arrow, that is supplemented with a "+" sign. It indicates, that the increase (decrease) of the internet bandwidth leads to an increased (decreased) availability of digital services. The negative interaction between the extent of failure of internet cables and the internet bandwidth becomes evident by a "-" sign. It shows that an increased failure of internet cables leads to a decreased internet bandwidth, while a reduction of faulty cable connections leads to an increase. Causal Loops can be balancing, if they are characterized by an underlying, self-correcting systemic behavior. In the opposite case, the Causal Loops are reinforcing and therefore strengthening change.

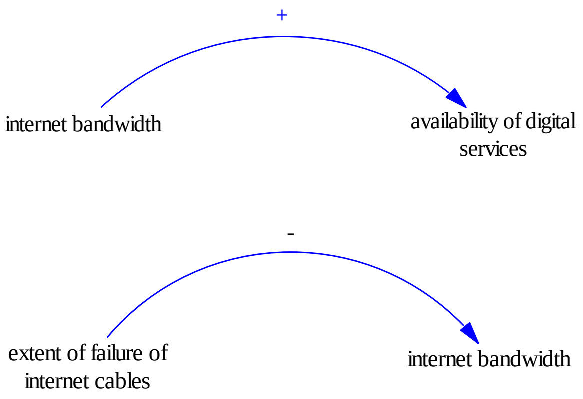
+
internet bandwidth
availability of digital services
-
extent of failure of internet cables
internet bandwidth

Figure 1. Positive and negative interdependencies in Causal Loop Diagrams

One created causal loop diagram is the building block model, which is sector-independent and visualizes general cause-effect relationships that can be expected in the case of an internet outage. This model can be applied to various sectors and adapted to specific needs. Parts of the models can be added or excluded. Further, two sector-specific models are created. One sector-specific model is applied to the health sector, while the other one is created for the transport sector. Both sector-specific models show sector-specific characteristics derived from the expert interviews as well as related literature in the first step.

The next step in the modeling process is the model validation. The iterative validation of the models is conducted through workshops with representants from different sectors held by the Austrian Federal Ministry of the Interior. The first workshop series consisted of seven workshops with approximately 240 participants from different sectors such as the information and communication technology sector, the energy sector and the transport and health sectors. The scenario of the first workshop series was the failure of DNS servers. The acronym DNS stands for Domain Name Service, which is used to translate domain names to numerical internet protocol (IP) addresses (Gupta et al., 2017).

The second workshop series started with a theory part and ended after three practical workshop parts. The scenario of this workshop series was an earthquake, which has led to a damaged digital communication infrastructure. In total, approximately 260 participants including

- public authorities
- regulators
- businesses that are part of the critical infrastructure
- and professional associations

attended.

A third workshop is planned, which will be the last workshop in the course of the research project ISIDOR.

Furthermore, the models are the object of various discussions within the project team. The project meetings, that take place on a regular basis, foster the iterative learning process within the project team further and serve to expand the created models and adapt them to recent insights and developments. These discussions are supplemented with bilateral talks between project partners, whenever the need for detailed reviews or a revision of the models arises. The iterative feedback process used is visualized in Figure 2.

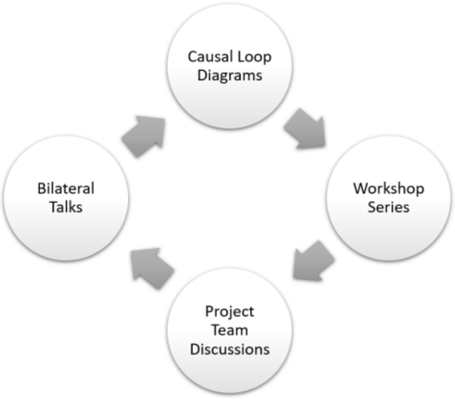

Figure 2. Visualization of the iterative feedback process in ISIDOR

4. Results and Discussion

The two key parameters, with which we model the internet outage, are (1) the decrease of the internet bandwidth and failure of internet-based services and (2) compromised cloud-sharing services and digital communication channels. Our analysis of the system variables and the underlying systemic behavior, we were able to derive from certain patterns revealed during our empirical research, show that two archetypes are of high relevance for the understanding of the consequences resulting from internet outages. The first one is the archetype "*Shifting the Burden*" and is shown in Figure 3. It represents the processes initiated when the internet bandwidth decreases due to an internet outage and the impact this has on the digital order transmission at site (1). Orders are redirected to site (2), if the internet connection in this area is still available. This increases the utilization level at site (2), which again results in a decrease of resources that could be used for the fault removal of the original cause at site (1). The disruption of the digital order transmission constitutes the symptom of the outage event and the redirection of orders is simply the reduction of this symptom. The increased utilization level is a resulting side effect, leading to a disadvantage for fault removal as the actual problem resolution variable. Two balancing "B" (=self-correcting) and one reinforcing "R" (=strengthening) loop are part of this archetype pattern. The balancing loops show countermeasures to cope with the situation while the reinforcing loop visualizes the fact that the more resources are bound or redirected to site (2) in order to cope with the increased number of orders there, the less resources are available for actual troubleshooting at site (1) in order to remove the origin of the problem. This archetype shows the criticality that goes hand in hand with the symptom treatment, when leaving the origin of faults unnoticed or untreated. This can often be the case when the underlying problem requires a longer period of time to get resolved due to a high complexity level. The longer time period, that is claimed by the resolution of the actual issue, is also shown by the delay mark in Figure 3.

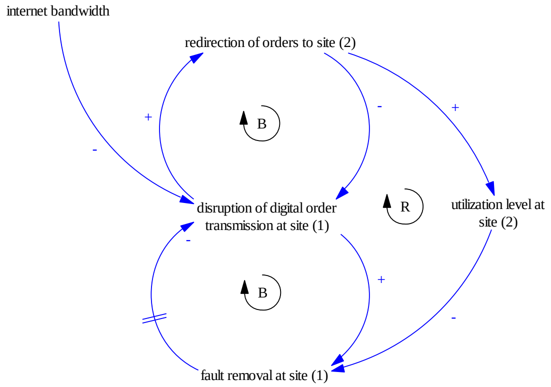
internet bandwidth
redirection of orders to site (2)
+
-
-
+
B
disruption of digital order transmission at site (1)
R
utilization level at site (2)
-
B
+
-
fault removal at site (1)

Figure 3. Archetype "*Shifting the Burden*" during an internet outage

The second archetype identified as relevant for internet outages is called "*Eroding Goals*". This archetype is characterized by a discrepancy between the desired and the actual state and can lead to a downwards goal alignment, in this case indicated by a reduction of the order fulfillment rate. Another option is to take corrective actions that lead to a decrease in the discrepancy. An example applied to internet outages is presented in Figure 4. It visualizes how the goal alignment action leads to an increased discrepancy between the target and the actual state. In contrast to this, the corrective measures, that would demand more time than reducing the order fulfillment rate which is again shown by a delay mark, would lead to a decrease in the discrepancy between the target and the actual order fulfillment rate.

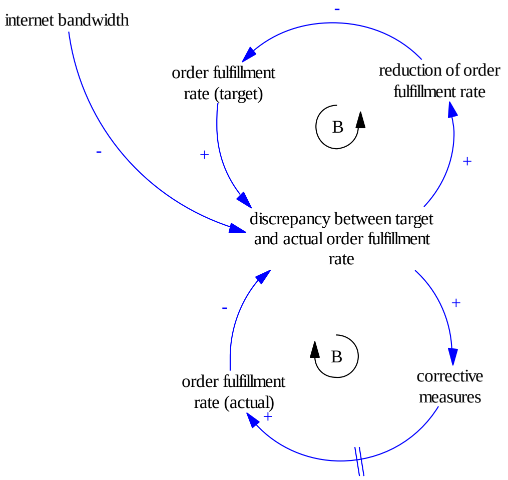
internet bandwidth
-
order fulfillment rate (target)
reduction of order fulfillment rate
B
+
+
-
discrepancy between target and actual order fulfillment rate
-
+
B
order fulfillment rate (actual)
corrective measures
+

Figure 4. Archetype "*Eroding Goals*" during an internet outage

Both archetypes constitute systemic behaviors, that can take place during an extensive and prolonged internet outage. The problem with such systemic patterns is the fact that, remaining unknown, they can lead to unexpected cause-effect relationships and domino effects, that could build up quickly and in the worst case even have the potential to initiate downward trends bringing the system or parts of it to a standstill. Thus, these hidden systemic patterns and especially the reinforcing Causal Loops are at the center of the analyses conducted in the course of ISIDOR.

The results, we can report so far, indicate that the shifting processes initiated by an internet outage entail that many communication and monitoring processes are, as far as this is possible, shifted to mobile communication. If corporations and organizations throughout all different sectors make use of this alternative strategy to compensate for the disrupted digital communication and other digitally performed monitoring and coordination processes, the cellular network is likely to get overloaded after a certain time span in the case of an extensive and prolonged internet outage event. If this is the case, the population in the affected area is completely disconnected from the communication network. Furthermore, Aceto et al. (2018) mention the increasing convergence of different communication networks and the questionable resilience of wide area networks as another issue in this regard in their work. These are open issues, that have to be considered carefully and integrated in the research on outage events. The consequences of a coincidence of the failure of multiple communication networks for the population in general and the challenges, this situation would impose on the public order, are currently very difficult to estimate and leave room for future research work.

5. Conclusions

Internet outage events are still not studied in the extent as their steadily increasing importance would require. In the course of the research project ISIDOR, systemic patterns behind an internet outage are detected and visualized using System Dynamics. The archetypes "Shifting the Burden" and "Eroding Goals" are found to depict the hidden patterns of an outage event in an adequate matter. Further, shifting certain processes from the digital to the cellular network increases the probability of an overload in the mobile network, which might lead to coinciding communication network system failures. The increasing convergence of the communication networks are imposing further challenges on the resilience of the majority of modern human communication processes.

The results of the research project will also encompass recommendations for action and significant restarting measures for a simultaneous system reboot in different sectors.

There were two important limitations to this research. First, interconnected crises are a highly complex object of study. Hence, no claim to completeness in terms of causalities can be made. Second, the scope of the research project did not foresee the application of a quantitative simulation tool. Future research could apply such a tool to carry out several simulation runs that will aid in adding quantitative results to our research.

Funding

The research leading to these results has received funding from the KIRAS programme. KIRAS is a research, technology and innovation funding programme of the Republic of Austria, Ministry for Agriculture, Regions and Tourism. The Austrian Research Promotion Agency (FFG) has been authorised for the programme management (FFG grant number: 879668).

Acknowledgements

We would like to thank the Austrian Federal Ministry of the Interior, Wolfgang Czerni and Helmut Pisecky for embedding our requests into the workshop settings and for providing us with the relevant insights. Also, the assistance provided by Nico Schlauf was greatly

appreciated.

References

Aceto, G., Botta, A., Marchetta, P., Persico, V., & Pescapé, A. (2018). A comprehensive survey on internet outages. *Journal of Network and Computer Applications*, *113*, 36–63. https://doi.org/10.1016/j.jnca.2018.03.026

Bruzzone, A. G., Frascio, M., Longo, F., Chiurco, A., Zanoni, S., Zavanella, L., Fadda, P., Fancello, G., Falcone, D., De Felice, F., Petrillo, A., & Carotenuto, P. (2014). Disaster and emergency management simulation in industrial plants. *26th European Modeling and Simulation Symposium (EMSS 2014)*, 649-656.

Bruzzone, A. G., Sinelshchikov, K., Massei, M., & Pedemonte, M. (2020). Town protection simulation. *Proceedings of the 19th International Conference on Modeling & Applied Simulation (MAS 2020)*, 160-165. https://doi.org/10.46354/i3m.2020.mas.021

Çetinkaya, E. K., Alenazi, M. J. F., Peck, A. M., Rohrer, J. P., & Sterbenz, J. P. G. (2015). Multilevel resilience analysis of transportation and communication networks. *Telecommunication Systems*, *60*(4), 515–537. https://doi.org/10.1007/s11235-015-9991-y

Çetinkaya, E. K., Broyles, D., Dandekar, A., Srinivasan, S., & Sterbenz, J. P. G. (2013). Modelling communication network challenges for Future Internet resilience, survivability, and disruption tolerance: a simulation-based approach. *Telecommunication Systems.* Advance online publication. https://doi.org/10.1007/s11235-011-9575-4

DIN EN ISO 22301:2020-07, Security and resilience - Business continuity management systems - Requirements (ISO 22301:2019), German version EN ISO 22301:2019.

Eckert C. (2018). IT-Sicherheit: Konzepte - Verfahren - Protokolle: 1. Einführung. De Gruyter Oldenbourg.

Ford A. (2009). Modeling the Environment (Second Edition). Island Press.

Forrester, J.W. (1961). Industrial Dynamics. Cambridge, MA: The MIT Press. Reprinted by Pegasus Communications, Waltham, MA.

Gupta, V., Shah, S., & Shrivastava, S. (2017). Secure domain name service in software defined network. *2017 20th International Conference of Computer and Information Technology (ICCIT)*, 1–6. https://doi.org/10.1109/ICCITECHN.2017.8281791

Hansson, S., Orru, K., Siibak, A., Bäck, A., Krüger, M., Gabel, F., & Morsut, C. (2020). Communication-related vulnerability to disasters: A heuristic framework. *International Journal of Disaster Risk Reduction*, *51*, 101931. https://doi.org/10.1016/j.ijdrr.2020.101931

Kulkarni, V., Barat, S., Clark, T. & Barn, B.S. (2017) Supporting organisational decision making in presence of uncertainty. *29th European Modeling and Simulation Symposium (EMSS 2017)*, 34-43.

Longo, F., Nicoletti, L., Padovano, A., Cersullo, N., Zaccaro, B. , Massei, M., De Felice, F., Petrillo, A. (2016). A Combined Approach for Emergency Management using AHP and System Dynamics. *Proceedings of the 6th International Defense and Homeland Security Simulation Workshop (DHSS 2016)*, 61-66.

Mrazek J., Hromada M., Mrazkova Duricova L. (2019). Reactivity to crisis situations in the transport sector. *Proceedings of the 9th International Defense and Homeland Security Simulation Workshop (DHSS 2019)*, 47-50. https://doi.org/10.46354/i3m.2019.dhss.008

Settanni, G., Shovgenya, Y., Skopik, F., Graf, R., Wurzenberger, M., & Fiedler, R. (2017). Acquiring Cyber Threat Intelligence through Security Information Correlation. *2017 3rd IEEE International Conference on Cybernetics (CYBCONF)*, 1–7. https://doi.org/10.1109/CYBConf.2017.7985754

Sterbenz, J. P., Hutchison, D., Çetinkaya, E. K., Jabbar, A., Rohrer, J. P., Schöller, M., & Smith, P. (2010). Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. *Computer Networks*, 54(8), 1245–1265. https://doi.org/10.1016/j.comnet.2010.03.005

Sterman, J. D. (2009). Business dynamics: Systems thinking and modeling for a complex world (Reprint). Irwin/McGraw-Hill.

Zabasta, A., Nikiforova, O., & Kunicina, N. (2012). Application of UML for risk based interdependencies modelling in critical infrastructures. *Proceedings of the 2nd International Defense and Homeland Security Simulation Workshop (DHSS 2012)*, 85-90.