Fictitious Crisis Scenario Development Related to a Bank Following a Breakdown in the Communication Network to Show Critical Infrastructure Digitization

J. J. Kohler, E. Fragnière, D. Konstantas, and E. Viganò

***Abstract*—The notion of critical infrastructure represents for states a vital asset for the functioning of society and the economy. These critical infrastructures cover many areas such as transportation, electricity, hospitals, and recently telecommunications which are taking more and more place in our economies due to the digitalization of our society. Business Continuity Plans (BCP) are often an obligation here to ensure the fastest possible recovery of these critical infrastructures in the event of a crisis. However, the scenarios that allow simulation exercises to be carried out remain very "logistically" oriented, while critical infrastructures linked in general to the digitization of the economy are poorly prepared for a major critical incident. To compensate for these weaknesses in the development of crisis scenarios linked to digitalization, we take the case of critical digital banking infrastructures and use counterfactual thinking to develop a crisis scenario that takes better account of the entire dematerialization dimension inherent in them.**

***Index Terms*—Counterfactual thinking, crisis scenario, critical infrastructure, digitalization.**

I. Introduction

Geneva State based in Switzerland is well-known for its financial center. It employs more than 35'000 people, 17'000 (circa 49%) working for the 92 banks. The evolution of the bank's activities has been facilitated by the development of Information Technology (IT). In the last 20-30 years, the banks became more and more interconnected to other banks, services providers, and their institutional and private clients moving the banking industry to a global scale. These financial institutions make extensive use of communication networks to exchange large amounts of information in increasingly short time frames, creating a strong dependence on communication network providers. Some financial companies have adapted the scope of their risk management to include risks related to communications networks, while others have had to resolve this issue under pressure from the financial regulator. Despite the integration of continuity and resilience plans, it is not uncommon for a service provider to experience problems, partially or totally impacting a service.

Manuscript received March 3, 2021; revised May 23, 2021.

J. J. Kohler and D. Konstantas are with the University of Geneva, Switzerland (e-mail: jean-jaques.kohler@etu.unige.ch, dimitri.konstantas@unige.ch).

E. Fragnière is with University of Applied Sciences Western Switzerland (HES-SO Valais), Switzerland (e-mail: emmanuel.fragniere@hevs.ch).

E. Viganò is with HES Professor, designing and directing the International Master in Information Systems Security Management within the HES-SO network, Switzerland (e-mail: enrico.vigano@vigilare.ch).

At the beginning of 2020, the telecommunications company Swisscom suffered three major outages on their fixed and mobile networks, the first two also impacting the emergency services. These cases of unavailability of communication networks put into perspective the importance and independence that the population in general, but also public or private companies and state and emergency services can have and the possible consequences. Repeated outages of mobile and fixed networks over a period of several weeks have prompted the Federal Office of Communications to take measures and conduct a thorough investigation.

The COVID-19 pandemic forced many employees to work remotely, for others to be confined to their homes for many weeks, and for key functions to continue working on company premises. This is the case for some banks that have decided to keep certain key functions (e.g. traders) on their premises for fear that the communication networks from the employee's home are not of good quality or that the bandwidth will not be able to handle the volume of data to be exchanged.

In the financial field, problems with communications networks can cause problems other than purely operational ones. Take for example a client who would place an order electronically to his relationship manager for the purchase of a security of a company listed on the European market. The latter would confirm the order and place it on the market (e.g. Euronext) directly in a banking system or through a trader. If the lines of communication between the bank and Euronext were to be disrupted, and the client's order was not finally executed as he wished, who would be held responsible for this incident and would have to bear any losses caused by this problem? To our knowledge, the question of legal liability for the improper execution of a client's order has not yet been decided.

Fig. 1 is not representative of the multitude of interactions and exchanges of information through multiple communication networks that a financial institution could have with its various actors and service providers, but it does allow us to understand the importance of communication networks for their proper functioning.

All the interconnections between the different actors in the world of finance, which are made possible by communication networks, raise serious questions for financial institutions not only in terms of risk analysis and management but also from the point of view of business continuity. The globalization of activities coupled with the development of services makes managing risks related to communication infrastructures increasingly difficult, as some incidents that ultimately have an impact on the financial institution may not have been

doi: 10.18178/ijfcc.2021.10.2.574

identified (for example, a failure of a computer server at the subcontractor of one of the service providers).

In this paper, we have considered the consequences that a bank-type financial institution in Geneva could suffer if the communication networks in the Geneva state were to be unavailable for more than 4 hours during an ordinary working day. To do so, we will rely on a counterfactual analysis and develop a theoretical model that will allow us to evaluate the risks faced by this bank about incidents impacting the communication infrastructures.

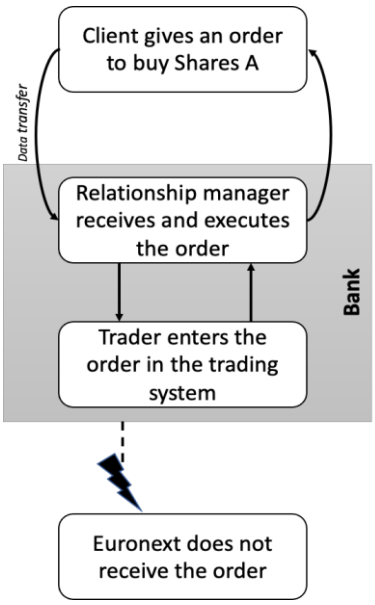


Fig. 1. Simplified scheme of exchange of data between the client, the Bank and the counterparty.

This paper is organized as follows. In Section II, we present a brief literature review related to critical infrastructure and its inherent link with communication infrastructures. In Section II, we present the classical approach to develop a crisis scenario and how it can be enriched by counterfactual thinking. In Section IV, we propose a new kind of crisis scenario related to a digitalized critical infrastructure in the banking sector. In Section V, we conclude and provide directions for further research.

II. Literature Review

Over the last few decades, several academic papers have been published on risk management, business continuity, crisis committees, and resilience. During the same period, society has continued to evolve, moving to a more globalized model with transnational interdependencies on multiple aspects allowing the massive and wide transportation and distribution of people, materials, products, services as stated by [1]. But this globalization of society creates some new risks that the current risk management practices have sometimes difficulties to identify and manage such as cyber risks, social engineering, social exclusion, or the decline in work commitment. [2] highlight the importance of combining risk and resilience analysis, especially for complex systems. [3] defines resilience as the ability of an ecosystem to integrate a disturbance into its functioning without modifying its qualitative structure. Resilience approaches require preparation for the unexpected, while risk analysis assumes that risks are known [4]. The scientific literature on resilience is abundant [5]-[10].

We notice a shift between the classical physical and modern digital notion of critical infrastructures of a state. This is the case for example for the broadband network or cyberspace. The shift of some critical infrastructures creates new risks that should not be ignored.

When a significant risk occurs, it is usually referred to as a disaster or a crisis. [11] describe disasters and catastrophes as events for which a society is in danger and suffers such impacts and losses that the social structure is disrupted and the performance of all or some of the essential functions of the society is prevented. In case a disaster or a crisis hits infrastructures considered as critical that its destruction or degradation could hurt the essential functions of a government, the national security, the national economy, or public health a described by [12]. The event could have a negative impact on other infrastructures as explained by [13].

In this paper, we have taken an interest in the role that the governments should play in the identification and the management of the risks of its critical infrastructures with the increased interdependencies of the GAFAM and in particular in the need to include such crucial elements in the elaboration of a crisis scenario.

III. Counterfactual Methodology to Improve the Relevant Crisis Scenarios

The development of new crisis management scenarios deserves special attention, especially in areas related to cyber risks. Indeed, the classical crisis scenarios used for training usually rarely include new threats such as cyberattacks. Consequently, the scenarios used to date to train crisis committees no longer necessarily correspond to reality. These scenarios are often linked to problems related to buildings such as an incident, a flood, a power outage, for example. Of course, it is important to train on logistical risks, but we must not forget the risks related to information systems or suppliers, thus related to information security.

A crisis linked to a cyber-attack regarding a distributed denial-of-service (DDoS) with a key supplier is managed in a different way than a loss of a building. In the case of a cyber-attack, reaction times are very short, i.e. a few hours or even a few minutes. In a hospitality environment where companies are increasingly dependent on digital technologies and interconnected with other companies, the scenarios employed in simulation exercises must be adapted to their realities to be effective in the context of business continuity planning (BCP) simulation exercises.

These scenarios underpin any stress testing exercise. It is the chosen scenario that will allow the integration of all the precepts presented in this section. It shows the different dimensions that need to be integrated into a crisis management scenario. Thus, a good scenario integrates the following elements as shown in Fig. 2:

- The actors ("Actor")
- The time dimension ("Time")
- A Threat type ("Threat type")
- An event ("Event")
- The resources to be used ("Asset/Resource")

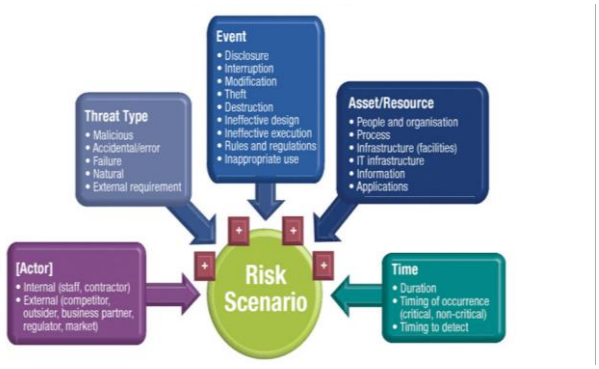


Fig. 2. Cyber risk scenario components (Risk IT framework, ISACA, 2009).

In Fig. 3, another ISACA model helps to develop the story related to the crisis scenario.

Fig. 3. Risk scenario development (Risk IT framework, ISACA, 2009).

With these classic approaches to scenario writing, you quickly get bogged down in fairly classic event sequences. However, this is appropriate when it comes to a major critical incident associated with critical physical infrastructure, such as the explosion of a company building, for example. If we now consider a major critical incident associated with a digital critical infrastructure such as a fiber optic cable that is severed by a terrorist group, cause and effect chains are much harder to imagine here, as the configuration of such a digital infrastructure is unfortunately not well known (so common sense cannot be applied here) and completely dematerialized. Applying mental simulations [14] such as counterfactual thinking can be very useful.

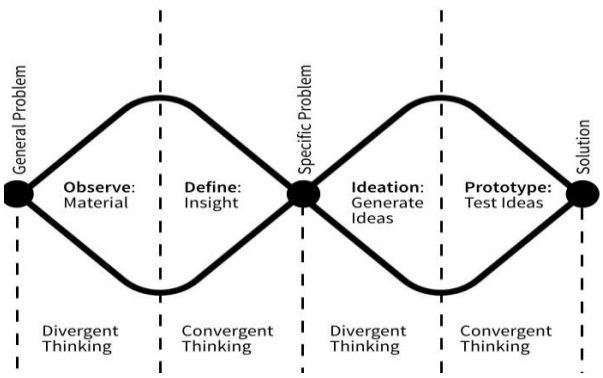


Fig. 4. Source: Change by design, [15].

The logic of the counterfactual approach is to start from a turning point that has not necessarily arrived yet. It is then a matter of imagining a whole series of previous steps (backward-looking) and successive steps (forward-looking).

The use of counterfactual thinking differs from one scientific field to another. In history, it is used to "better reconstruct historical narratives among other things (e.g. what if Germany had won the Second World War). In the medical world, counterfactual thinking helps to digest a defeat, by telling oneself things could have been much worse. In crisis management, which is the focus of this research, counterfactual thinking helps us to move away from simple problem solving as advocated by the double diamond model (see Figure 4) in innovation. The double diamond forces us to leave our comfort zone, through the two successive stages of divergence, but it also forces us to assume that the two stages of convergence remain in an identical context.

It is here that counterfactual thinking is certainly more powerful than the double diamond as regards the elaboration of a crisis scenario arising from a major critical incident of the digital type. Indeed, by postulating that the major critical incident is a turning point, the worst-case scenario result will represent a drastic direction different from the normal and must be "plausible" recontextualized as it goes along to be able to be managed and therefore rehearsed. A business continuity plan without exercise is not used at all. Within the framework of this short paper, this is what we have done. We started from the classic ISACA models for crisis scenario development that we have enriched with counterfactual thinking, we imagined a whole series of more or less probable developments to end with the narrative scenario proposed in the following section. The aim of such a scenario is not to make predictions (the predictive power is indeed nil), but rather to open up the fields of possibilities and in this new context of critical digital infrastructure to elaborate plausible scenarios.

IV. Script

To present our analysis using the counterfactual methodology, we have voluntarily decided to base our analysis on a fictitious private bank whose main characteristics could be similar to those of small or medium-sized private banks implemented in the canton of Geneva in Switzerland, with activity both in Switzerland and internationally.

A. ABC – A Fictitious Private Bank

ABC is a recognized and respected name in Switzerland since 1930. This private bank offers customized investment solutions to international private and institutional clients from its headquarters in Geneva. This long-standing success is due to the strong relationships it maintains with each of its clients as well as the expertise and professionalism of its staff. As the accounts are based in Switzerland, they are governed by Swiss banking law. Also, Switzerland offers economic and political stability, which is favorable to the smooth running of ABC's business.

The main services offered by the bank are:

- Discretionary management (investment management based on strategies agreed with clients)
- Consulting Services
- Transaction execution and custody services
- Wealth Management

- Credit solutions
- E-banking access

The bank is headquartered in Geneva and has 4 branches (Gibraltar, Luxembourg, Miami, and Monaco) as well as 4 representative offices (Dubai, London, Montevideo, and Zurich).

At the end of 2020, ABC employed no less than 1'000 people worldwide, 450 of whom were in Geneva. Most of the bank's activities are centralized in Geneva for legal reasons, but also the reputation of the Swiss financial center and its pool of highly qualified manpower.

The headquarters in Geneva is spread over 2 buildings of almost identical size (usable surface area). The first building is in the city center and mainly accommodates senior management, asset managers, financial analysts, financial advisors, documentation, marketing, and asset managers. The second building, located in the Geneva countryside, houses the finance, risk, operations, IT, general services, middle office, and human resources teams.

The distribution of employees among the buildings is almost identical. Thus, there are approximately 225 employees per building. As far as possible, no IT outsourcing is intended. The bank pays great attention to the confidentiality of its data. The "master" servers are in building 2 while the "slave" servers are in building 1. Building 2 is equipped with a generator capable of powering the entire building and the computer server room for several days (> 7 days). The servers are directly connected to a UPS continuously (battery autonomy without the generator, 45 min.).

B. Incident Description

In this part, we have imagined a disruption of the fixed telephone network of the ABC Bank for an unknown duration at 9 am. The incident was detected a few minutes later by bank employees who could not reach their customers, but also by unhappy customers who finally managed to reach their relationship managers by calling them directly on their cell phones. As the telephone exchange was impacted by the disruption of the fixed-line network for an unknown length of time, the telephone manager informed the crisis management committee.

After a quick analysis of the available information, the committee decided to activate the Business Continuity Plan and to switch the telephone exchange to the GSM network to be able to receive and make calls to customers. Following this decision, the switchover of the telephone exchange was carried out immediately and successfully thanks to clearly established and previously tested protocols. Customers and bank employees can now exchange information with each other again, for example, transmit and confirm stock exchange orders or payments.

In the case described above, the impact on ABC Bank of an indefinite interruption of fixed telephone lines is difficult to quantify because many external factors are involved, such as the day of the week, the time of day, and market volatility.

C. Worst-Case Scenario

We imagined that we are on a Tuesday morning at the end of the year, a few days before the New Year. A serious fire in a technical room of the City of Geneva has destroyed several telecommunication optical fibers. These are the property of several telecommunication companies. The particularity of this technical room is that all the optical fibers of the City of Geneva transit through this room.

Once the fire alarm was triggered, the fire department intervened quickly and massively to overcome the flames. Despite this, the technical room was damaged. For safety reasons, the fire department did not allow anyone to enter the premises.

While the activities of ABC Bank were in full swing, the bank's employees began to receive errors appearing on their screens. Other employees who were on the phone with customers or other colleagues suffered clean cuts in their communications. There was some unrest within the bank as banking applications began to display errors, and the telephone lines between the various buildings and the outside world were inoperative. Confusion within the various departments was growing. It was impossible to know if the banking operations had been executed correctly. From the front office to the back office, most activities were either stopped or severely slowed down.

Following all these events, the crisis committee met to analyze the situation and implement action plans to ensure minimum service. Based on information transmitted by the optical fiber suppliers, the source of the problems seems to have been identified, namely the destruction of the optical fiber in a technical room. The crisis committee decided to switch the telephone exchange to the cellular network to be able to answer calls from customers calling the main number. Concerning the electronic exchange of information between the bank and the various counterparties, it is impossible to use networks other than the fiber optic network given the volumes of data to be exchanged and the speed of execution required, particularly for trading floor applications.

Fortunately for ABC Bank, technicians from the various telecommunications providers were able to access the premises and repair the optical fibers within two hours. Thanks to this rapid intervention, data exchange between Bank ABC and its various counterparties was able to resume. The telephone exchange is now operational again. The restoration of the telecommunication lines now poses problems in reconciling banking transactions, i.e. whether orders have been transmitted and executed.

The example of a cut in the optical fibers in the Canton of Geneva allows us to put into perspective the operational, financial, and reputational impacts, both for institutions heavily dependent on communication networks and for the Canton of Geneva in general.

Cutting a communication line can have significant direct and indirect operational impacts not only for the financial sector but also for a large part of the economic system of the Canton of Geneva. Even though it is difficult to quantify the number of operational losses generated by our worst-case scenario, we believe it is important to identify the ins and outs to propose measures to manage this risk optimally.

V. Conclusion

Critical state infrastructures are more and more based on dematerialized processes. This is the case for most banks that offer their customers digitalized services and thus concentrate critical infrastructures making them increasingly

vulnerable. Indeed, a bank is considered critical infrastructure for the economy of a country. The same is true for the power grid and telecommunications networks that support these digital services. It is therefore sufficient for a major critical incident to affect only one of these three critical infrastructures (bank, power grid, telecommunication network) to create an immediate and cascading complete shutdown of the economy. Our contribution in this context is to develop new crisis scenarios that are better "contextualized" thanks to counterfactual thinking, which provides the basis for much more relevant simulation exercises to be better prepared for this type of crisis that is extremely complex to manage.

The next stage of this research will consist of developing BCPs and simulation exercises more adapted to the complete digital transformation of society by taking better into account network configurations. Indeed, the notion of orchestrating the crisis linked to a major "digitalized" critical incident takes on its full meaning.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

Jean-Jaques Kohler, Emmanuel Fragnière, Dimitri Konstantas and Enrico Vigano wrote the full paper together.

References

[1] S A. Terje and E. Zio, "Globalization and global risk: How risk analysis needs to be enhanced to be effective in confronting current threats," *Reliability Engineering and System Safety*, vol. 205, January 2021.

[2] J. Park, T. P. Seager, P. S. C. Rao, M. Convertino, and I. Linkov, "Integrating risk and resilience approaches to catastrophe management in engineering systems," *Risk Analysis: An International Journal*, vol. 33, no. 3, pp. 356–367, Mar. 2013.

[3] C. S. Holling, "Resilience and stability of ecological systems," *Annual Review of Ecology and Systematics*, vol. 4, pp. 1–23, 1973.

[4] T. Mitchell and K. Harris, "Resilience: A risk management approach" *Overseas Development Institute Background Note*, pp. 1–7, January 2012.

[5] A. Opdyke, A. Javernick-Will, and M. Koschmann, "Infrastructure hazard resilience trends: An analysis of 25 years of research," *Natural Hazards*, vol. 87, no. 2, pp. 773–789, 2017.

[6] G. Pescaroli, R. T. Wicks, G. Giacomello, and D. E. Alexander, "Increasing resilience to cascading events: The M. OR. D. OR. scenario," *Safety Science*, vol. 110, pp. 131–140, December 2018.

[7] C. Fox-Lent, M. E. Bates, and I. Linkov, "A matrix approach to community resilience assessment: an illustrative case at Rockaway Peninsula," *Environment Systems and Decisions*, vol. 35, no. 2, pp.209–218, June 2015.

[8] D. P. Aldrich and M. A. Meyer, "Social capital and community resilience," *American Behavioral Scientist*, vol. 59, no. 2, pp. 254–269, February 2015.

[9] S. Meerow, J. P. Newell, and M. Stults, "Defining urban resilience: A review," *Landscape and Urban Planning*, vol. 147, pp. 38–49, March 2016.

[10] C. Curt and J.-M. Tacnet, "Resilience of critical infrastructures: review and analysis of current approaches," *Risk Analysis*, vol. 38, no. 11, pp. 2441–2458, August 2018.

[11] C. E. Fritz and H. B. Williams, "The human being indisasters: a research perspective," *The Annals of the American Academy of Political and Social Science*, vol. 309, no. 1, pp. 42–51, January 1957.

[12] R. N. Hull, D. A. Belluck, and C. Lipchin, "A framework for multi-criteria decisionmaking with special reference to critical infrastructure: Policy and risk management working group summary and recommendations," *Ecotoxicology, Ecological Risk Assessment and Multiple Stressors*, pp. 355–369, 2006

[13] A. Löschel, U. Moslener, and D. T. G. Rübbelke, "Energy security – Concepts and indicators," *Energy Policy*, vol. 38, no. 4, pp. 1607–1608, April 2010.

[14] C. M. Gaglio, "The role of mental simulations and counterfactual thinking in the opportunity identification process," *Entrepreneurship Theory and Practice*, vol. 28, no. 6, pp. 533–552, November 2004.

[15] T. Brown and B. Katz, "Change by design," *Journal of Product Innovation Management*, vol. 28, no. 3, pp. 381–383, March 2011.

Jean-Jaques Kohler was born in Geneva, Switzerland, in 1980. He received a BSc in business management from the University of Applied Sciences and Arts Western Switzerland – Geneva and an Executive MBA from the University of Geneva. He has 15 years of experience in risk management, crisis management ,and business continuity.

He is a PhD student at the University of Geneva.

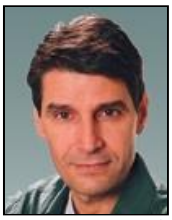
His current research interests include risk management, business continuity, and crisis management of critical infrastructures.

Emmanuel Fragnière is a professor of service design and innovation at the University of Applied Sciences Western Switzerland (HES-SO Valais). He is also a lecturer in enterprise risk management at the University of Bath, School of Management. Previously, he was a Commodity Risk Analyst at Cargill (Ocean Transportation) and a senior internal auditor at Banque Cantonale Vaudoise, the fourth largest bank in Switzerland.

Prof. Fragnière has published several papers in academic journals such as Annals of Operations Research, Environmental Modelling, and Assessment, European Journal of Operational Research, Interfaces, Management Science as well as Service Science.

Prof. Fragnière is the author (with Sullivan) of the book entitled Risk Management: Safeguarding Company Assets, Fifty-Minute Crisp Series, November 2006 (2015 new edition).

His research is focused on the development of design techniques for the service sector in general and more specifically applied to the energy and tourism markets.



Dimitri Konstantas is a professor at the University of Geneva, Switzerland and director of the Information Science Institute of the Geneva School of Economics and Management, and of the Continuous Education Master program on Information Security. He has been active since 1987 in research in the areas of object-oriented systems, agent technologies, Multimedia applications, e-commerce services, and mobile health systems, with numerous publications in international conferences and journals. His current interests are mobile services and applications with a special focus on the well-being services for the elderly and information security.

Prof. Konstantas has long participation in European research and industrial projects and is a consultant and expert to several European companies and governments.

Enrico Viganò holds a master's degree in electrical engineering and telecommunications and a University Certificate in Quality and IT Security. He began his professional career in multinational companies in South America in the fields of energy production and distribution and IT. He continued his professional career in Europe in the IT industry and with Swiss public administrations in the fields of information systems and information security as well as business continuity management. He also held the position of HES Professor, designing and directing the International Master in Information Systems Security Management within the HES-SO network.