risks

MDPI

Editorial

Special Issue "Cyber Risk and Security"

Michel Dacorogna [1] and Marie Kratz [2,*]

[1] Prime Re Solutions Ltd., 6340 Zug, Switzerland; michel.dacorogna@prs-zug.com
[2] ESSEC Business School, CREAR Risk Research Center, 95021 Cergy-Pontoise, France
* Correspondence: kratz@essec.edu

1. Cyber Risk, a Topical Subject in an Ever Increasing Risk Landscape

The COVID-19 pandemic and now the war in Ukraine, have raised the risks to levels not seen in the last 30 years. This Special Issue of *Risks* was planned before these events, but comes at the right moment to contribute to the progress in our understanding of cyber risk. The last two years have demonstrated our acute dependence on IT systems and the weakness of our defenses against cyber attacks. With climate changes and pandemics, cyber risk constitutes one of the main challenges to building more resilience in our society. Thus, this Special Issue is very topical and will help us advance our knowledge on this emerging risk. As any emerging risk, cyber risk requires a big investment in research to cope with it. An important issue is how to balance between building up cyber security and developing cyber resilience. Cyber security is a concept that was born with computers, while cyber resilience is a new concept that is gaining importance as we realize more and more that whatever defense we are able to build, we will not prevent all attacks from being successful. As long as our systems are connected to the Internet, they are susceptible to attacks from hackers all over the world. Thus, we need to design our processes in such a way that our organizations can survive those attacks with as little harm as possible, as well as to keep companies and organizations functioning despite broken IT systems. This is what is generally called 'resilience'. This resilience includes the ability of fast detection and stopping of attacks (preparedness/protection), reducing their impact and fixing breaches (reaction and improvement), and ensuring the company's access to cash (insurance covers). Finding the right tradeoffs between investing in security and resilience is one of the challenges that management is confronted with. That is why coming up with an optimal resource allocation strategy requires a better understanding and quantification of cyber risk.

2. Cyber Risk Landscape: A Multidimensional World

Cyber risks are difficult to apprehend because they originate from an IT landscape that is rapidly evolving. Every day, new avenues for cyber attacks are opened up by the expansion of IT systems and the emergence of new widely distributed applications. Not only do the hardware and software change rapidly but also the reach of IT is constantly widening as we have experienced during the pandemic. Relying on IT solutions to maintain the possibility of working and communicating has become central during lock-down phases. Moreover, from the point of view of insurance, this risk is not easily quantifiable, particularly because it broadly affects intangibles such as data or reputation that make the losses difficult to measure. Adding to this the fear of systemic risks, it is easy to understand the reluctance of insurance companies to widely cover this risk. Indeed, the interconnection of systems, the wide use of the same software, and the ever increasing cloud storage are some of the elements that raise fears of strong systemic risks. A good example is the wide spread of operating systems such as MS Windows on PCs, whose weaknesses can be easily targeted on a wide range of machines. However, it would be important to scientifically study this problem and explore the extent to which this fear is

Citation: Dacorogna, Michel, and Marie Kratz. 2022. Special Issue "Cyber Risk & Security". *Risks* 10: 112. https://doi.org/10.3390/risks10060112

Received: 11 April 2022
Accepted: 12 April 2022
Published: 28 May 2022

grounded. Research on the subject of systemic risk has been fostered by the financial crisis of 2008/2009 and researchers have made progress in the field of banking and finance. Research on cyber risk could inspire itself from the avenues proposed in the latter. In particular, developing 'footprint' scenarios for accumulation, similar to stress test for banks, could be an interesting way to explore. Moreover, one of the necessary condition for the presence of systemic risk, the existence of extreme events have been widely acknowledge in cyber data Dacorogna and Kratz (2020); Eling and Wirfs (2019). This requires special statistics to model the tail of the distribution (see e.g., Embrechts et al. (2011); Kratz (2019) and references therein).

3. Towards a Pluridisciplinary Research?

Because IT technology is crossing all human activities, pluridisciplinary research is needed to fully grasp the various aspects of the risk. It would be a mistake to specialize too early and hamper our full understanding of the problem, or to limit ourselves to exploring security solutions. This Special Issue is an illustration of the variety of research angles that this field can take. It contains both quantitative and qualitative approaches that contribute to developing defense strategies. They both need access to data. Finding good data sources is one of the important requirements for progress in our knowledge. In this issue, the difficulty of accessing good data on cyber risk is evidenced by the fact that we only received two papers that use data to test their model, one coming from the communication industry (Dal Moro 2020) and one collected from cyber attacks at a large company (Bentley et al. 2020). Nevertheless, you will find papers tackling modeling issues as well as various aspects of cyber security, including new ways of developing criminal investigations into cyber crimes (Barlatier 2020).

Mobilizing researchers from various disciplines for this Special Issue has been a challenge. It illustrates the difficulty of approaching the problem in a multi-dimensional way. We specifically looked for contributions also coming from disciplines other than statistics and actuarial mathematics, to enlarge the perspective and provide distinct, complementary, and sharp insights to researchers of actuarial mathematics or risk analysis and management. It should help improve the understanding of cyber risk, which by nature requires a pluridisciplinary approach if we want to tackle this complex risk in an innovative and relevant way. Research is generally focused on narrow specialization and people choose to concentrate on highly rated or specialized journals. This Special Issue is an effort to break these barriers and we thank the researchers who have taken the courage to contribute to this unusual special volume. Readers will see how rich those various approaches are and how creative research on cyber risk can be. In this Special Issue, there are few papers dealing directly with insurance, such as Dal Moro (2020), where the problem of building an index for a parametric reinsurance cover is studied, or Antonio et al. (2021) where authors explore a way of insurance rate making using a network approach through graph mining. Cyber risk modeling is also covered by Bentley et al. (2020) based on a multivariate model of various attacks, and by Orlando (2020) who deals with the problem of quantifying the cyber risk for investment decisions. Two papers treat special aspects of the risk of IT systems in cloud data storage Franke and Hoxell (2020) and the risk of Intelligent Transportation Systems (ITS) Zeddini et al. (2022). There is one paper focused on developing new techniques of criminal investigations using the example of cyber crimes Barlatier (2020). The simple list points out to the wide scope of research that is needed to tackle cyber risk.

4. Some Research Perspectives Tackled in This Special Issue

This foreword is not aimed at writing a literature review on the cyber topic; the reader may simply turn to references given in the few recent papers mentioned within this foreword. Instead, we focus on the contributions in this issue. Franke and Hoxell (2020) address the growing concerns about both oligopolies in digital services and cyber security and market concentration. The authors propose a way to analyze the tradeoffs between the marginal costs of storage and those of security. They show that there is no straightforward

answer. Depending on certain choices of parameters, it could go both ways. They propose to extend their research on the subject empirically to determine what type of function (convex or concave) is the most appropriate for the production and/or cyber risk costs. At the moment, the data to calibrate their model is not available. In Zeddini et al. (2022), the authors use a qualitative approach based on the TVRA (Threat, Vulnerability, Risk Analysis) methodology, in order to assess the risk of ITS, which is one of the challenges of the coming years in transportation. They show that we are facing a difficult trade-off between the need of increasing the efficiency and safety of ITS through more communication between systems, and cyber security, since connections will open up the possibility of cyber attacks. The authors conclude by providing a risk assessment of various types of typical attacks on ITS.

In view of offering good insurance covers, in Dal Moro (2020), the author explores the possibility of building an index of cyber risk. Such an index could become the basis for proposing parametric reinsurance covers. Based on a dataset provided by Symantec about the IT activity (i.e., the number of virus or intrusions being blocked by Norton on end-user computers), he studies the activity across various geographical locations and confirms that there is no geographical limitation to cyber risk. Performing preliminary statistical analysis, he concludes that a cyber loss risk index could be built based on those IT activities when partnering with cyber security firms. Antonio et al. (2021) proposed a somehow unusual way, in an actuarial sense, to quantify the cyber risk and come up with an insurance premium. They propose a graph mining approach (GMA) and show that this approach leads to heterogeneous rating as a function of the communication activity. They obtain lower rates than if not considering GMA and communication. The network approach has been extensively used to estimate cyber risk in absence of claims data (see, for instance, Fahrenwaldt et al. (2018); Hillairet and Lopez (2021); Nagurney et al. (2017); Xu and Hua (2019) and references therein), but this paper adds the GMA component. In the field of modeling, Bentley et al. (2020) propose a multivariate loss model for different, dependent types of attack and the effect of mitigation strategies on those attacks. This model is based on a dataset of six years of tickets submitted by security engineers at a large (anonymous) company. They explore various mitigation strategies with their model. They show that, choosing VaR as risk measure (recall that the so-called Value-at-Risk (VaR) corresponds to quantiles of the associated loss distribution), they can reduce it significantly by using their model for deciding on strategies to follow. Orlando proposes an approach to assess the unexpected cyber loss at a specified confidence level over a given period of time. She calls it Cy-VaR and explores three key components of the Cy-VaR, vulnerability of the systems, the assets exposed, and the profile of the potential attackers, in order to help investment decisions on cyber-security. She calls for access to data to better calibrate her model. Finally, in Barlatier (2020) we learn about another important component of the fight against cyber attacks, which is the criminal investigation. The author searches for what the most appropriate means of crime prevention and crime repression are. He questions the social role of investigation as a useful tool of production of evidences. He describes a paradigm shift towards a knowledge management of crime control. In the words of the author:'criminal intelligence provides solutions that are considered promising for mass delinquency management instead of investigation'. It is another argument for research on cyber risk, which is becoming a central tool for crime prevention and repression.

5. Challenges Ahead

This brief description of the content of this Special Issue shows the wide spectrum of subjects covered and the interest and need of putting together various approaches to gain a better understanding of this risk, which is bound to grow with the dissemination of IT solutions in every dimension of our life. Nevertheless, there are still many questions to be answered and fields to be explored. In the future, researchers will need to look for or have access to more data to challenge, calibrate, and test their models. This should advance the understanding of cyber attacks properties and help find a better evaluation of this risk. The

academic world must work with companies to make them aware of the need to develop common databases accessible to research. In many papers, the presence of systemic risk in the cyber space is put forward. It is one of the research target for the years to come, as was discussed earlier. Another avenue of research is the links between IT systems and a wide range of catastrophic risks such as floods, earthquakes, windstorms, or pandemics, without forgetting financial crashes and failure in electricity supply. This exploration goes along with the development of methods for avoiding systemic failures and for structuring hedging solutions in order to ensure cash flow when needed. This program is vast and ambitious. We are not going to lack work in the coming years, which will be a necessary step for increasing the cyber resilience of society.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

Barlatier, Jérôme. 2020. Criminal investigation and criminal intelligence: Example of adaptation in the prevention and repression of cybercrime. *Risks* 8: 99. [CrossRef]

Bentley, Mark, Alec Stephenson, Peter Toscas, and Zili Zhu. 2020. A multivariate model to quantify and mitigate cybersecurity risks. *Risks* 8: 61. [CrossRef]

Dacorogna, Michel, and Marie Kratz. 2020. Moving from uncertainty to risk: The case of cyber risk. In *Cybersecurity in Humanities and Social Sciences: A Research Methods Approach*. Edited by Hugo Loiseau, Daniel Ventre and Hartmut Aden. Montreal and New York: ISTE Scientific Publsihing and Wiley, pp. 123–52.

Dal Moro, Eric. 2020. Towards an economic cyber loss index for parametric cover based on it security indicator: A preliminary analysis. *Risks* 8: 45. [CrossRef]

Eling, Martin, and Jan H. Wirfs. 2019. What are the actual costs of cyber risk events? *European Journal of Operational Research* 272: 1109–19. [CrossRef]

Embrechts, Paul, Claudia Klüppelberg, and Thomas Mikosch. 2011. *Modelling Extremal Events for Insurance and Finance*, 2nd ed. Berlin/Heidelberg and New York: Springer.

Fahrenwaldt, Matthias A., Stefan Weber, and Kerstin Weske. 2018. Pricing of cyber insurance contracts in a network model. *ASTIN Bulletin* 3: 1175–218. [CrossRef]

Franke, Ulrik, and Amanda Hoxell. 2020. Observable cyber risk on cournot oligopoly data storage markets. *Risks* 8: 119. [CrossRef]

Hillairet, Caroline, and Olivier Lopez. 2021. Propagation of cyber incidents in an insurance portfolio: Counting processes combined with compartmental epidemiological models. *Scandinavian Actuarial Journal* 8: 671–94. [CrossRef]

Kratz, Marie. 2019. Introduction to Extreme Value Theory. Applications to Risk Analysis & Management. In *2017 MATRIX Annals—Mathematics of Risk*. Edited by David R. Wood, Jan de Gier, Cheryl E. Praeger and Terence Tao. Berlin/Heidelberg and New York: Springer, pp. 591–636.

Nagurney, Anna, Patrizia Daniele, and Shivani Shukla. 2017. A supply chain network game theory model of cybersecurity investments with nonlinear budget constraints. *Annals of Operations Research* 248: 405–27. [CrossRef]

Orlando, Albina. 2020. Cyber risk quantification: Investigating the role of cyber value at risk. *Risks* 8: 184. [CrossRef]

Xu, Maochao, and Lei Hua. 2019. Cybersecurity insurance: Modeling and pricing. *North American Actuarial Journal* 23: 220–49. [CrossRef]

Antonio, Yeftanus, Sapto Wahyu Indratno, and Rinovia Simanjuntak. 2021. Cyber insurance ratemaking: A graph mining approach. *Risks* 8: 224. [CrossRef]

Zeddini, Besma, Mohamed Maachaoui, and Youssef Inedjaren. 2022. Security threats in intelligent transportation systems and their risk levels. *Risks* 10: 91 [CrossRef]