Article

Cyber Risk Contagion

Arianna Agosto * and Paolo Giudici *

Posted Date: 23 August 2023

doi: 10.20944/preprints202308.1018.v2

Keywords: Cyber risk; Contagion; Autoregressive models

Article

Cyber Risk Contagion

Arianna Agosto [1,†,‡] **and Paolo Giudici** [2,*,‡]

[1] Department of Economics and Management, University of Pavia; arianna.agosto@unipv.it
[2] Department of Economics and Management, University of Pavia; giudici@unipv.it
* Correspondence: giudici@unipv.it
† Current address: Via San Felice 5, 27100 Pavia, Italy.
‡ These authors contributed equally to this work.

Abstract: Financial technologies, stemming from the application of artificial intelligence to big data in finance, are continuously expanding, across different markets and financial services. While financial technologies bring many opportunities, such as reduced costs and extended inclusion, they also bring risks, among which cyber risks, which are constantly increasing and are difficult to measure. Among the difficulties in measurement lies the existence of interdependence among different cyber risks. The study of interdependence and possible contagion channels between cyber attacks to different institutions and economic sectors is indeed increasingly important to ensure economic and financial sustainability. Against this backdrop, this paper proposes a multivariate model for count time series of cyber risk events, in which the time-varying intensity parameter determining the probability that a cyber attack occurs evolves according to general autoregressive score models, taking both time and sectorial dependence into account. The model is particularly suitable for studying how the behaviors of different markets or sectors are interconnected and it constitutes a new approach to the multivariate analysis of count time series of cyber loss events.

Keywords: cyber risk; contagion; autoregressive models

1. Introduction

The Financial Stability Board defines Financial Technologies as "technologically enabled financial innovations that could result in new business models, applications, processes, or products with an associated material effect on financial markets and institutions and on the provision of financial services". While innovation in finance is not a new concept, the focus on technological innovations and their pace has increased significantly. Fintech solutions that use big data analytics, artificial intelligence and blockchain technologies are currently being introduced at an unprecedented rate. These new technologies are changing the nature of the financial industry, creating many opportunities that offer more inclusive access to financial services. On the other hand, FinTech solutions leave the door open to many risks, that may hamper consumer protection and financial stability. Relevant examples of such risks are underestimation of creditworthiness, market risk noncompliance, fraud detection and, as a possible major source of risks, cyber-attacks (see e.g. [11]).

Across the world, there is a strong need to improve the competitiveness of the fintech sector, introducing a risk management framework, and cyber risk management in particular, to prevent and mitigate cyber attacks.

Cyber risks can be defined as "any risk emerging from intentional attacks on information and communication technology (ICT) systems that compromises the confidentiality, availability, or the integrity of data or services". According to this definition, cyber risk does not strictly coincide with IT operational risks, as it relates only to intentional attacks, on the one hand; and it deals not only with monetary losses, but also with reputational losses, on the other.

In the last few years the number of cyber attacks on information technology (IT) systems has surged and, therefore, the need to measure cyber risks has considerably increased.

While the scientific literature on the measurement of operational risks based on loss data constitutes a reasonably large body, that on cyber risk measurement is very limited. The lack of

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 23 August 2023 doi:10.20944/preprints202308.1018.v2

literature on cyber risk measurement may be due to the limited availability of cyber loss data, which are typically not disclosed, to avoid reputational consequences. [8] showed how to solve this problem, treating loss data as the levels of an ordinal variable.

Another problem that hampers the availability of correct cyber loss data is the interdependence among cyber losses, due to the fact that cyber attacks have often multiple targets (see e.g. [4]).

This motivates the work of this paper, in which we aim to contribute to cyber risk measurement by means of a methodology able to capture interdependencies (contagion) among cyber losses.

Over the past decade, especially after the global financial crisis in 2008, the study of financial risks arising from interconnectedness between individuals and institutions has attracted the attention of researchers and regulatory authorities. From a statistical viewpoint, the assessment of vulnerabilities originated by contagion channels was supported by the use of financial networks [2,5].

Most existing analytical works used balance sheet and other financial statements to extract financial links [10], while a second group focused on co-movements of security prices [1,7].

This paper applies the network approach in the context of cyber risk analysis and contributes to the study of interconnectedness in the financial and economic system by proposing a multivariate model for count time series of cyber risk events. The model was introduced by [3] in the credit risk contagion context and has a score-driven specification: the time-varying intensity parameter determining the probability that an extreme market event occurs follows the specification of general autoregressive score (GAS) models, also known as dynamic conditional score models [6,9]. In the GAS framework, time-varying parameters depend on their lagged values and on the scaled score of the conditional observation density. GAS models belong to the class of observation-driven models and are found to perform comparably to parameter-driven models in terms of predictive accuracy. From a computational point of view, they can be easily estimated through maximum likelihood optimization.

We apply the model to the daily count of cyber events in different economic sectors, from 2018 to 2021, and find significant time dependence, along with some cross-sector effects.

2. Materials and Methods

A well-known distribution for non-negative integer variables is the negative binomial, which generalizes the Poisson distribution. The negative binomial distribution is derived from the Poisson-gamma mixture and is characterized by a location parameter μ - also defined as the intensity of the count process - and a dispersion parameter α. The higher α, the higher the overdispersion in the data. Indeed, when $\alpha = 0$, the negative binomial distribution reduces to the Poisson one, where the variance is equal to the mean.

Following [3], we assume that the observations in each count time series of cyber events i follow a negative binomial distribution with a time-varying location parameter $\mu_{it} > 0$ and a static dispersion parameter $\alpha_i \geq 0$:

$$X_{it} \sim NB(\mu_{it}, \alpha_i) \tag{1}$$

First, we reparametrize the location parameter through an exponential link: $f_t = \log(\mu_t)$. This is a common choice in the specification of generalized linear models, as it ensures strict positivity of the time-varying parameter without imposing restrictions on the coefficients. Then, to model the time-varying location parameters $f_t = \log(\mu_t)$, we use a Generalized Autoregressive Score (GAS) specification [6,9]. In the general GAS specification, the dynamics of filtered parameters $f_{t+1} = (f_1, ..., f_t)$ are captured by an autoregressive term and by the scaled score (gradient) of the conditional observation density through the recursions

$$f_{t+1} = C + Bf_t + A\, S(f_t)\nabla(x_t, f_t) \tag{2}$$

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 23 August 2023 doi:10.20944/preprints202308.1018.v2

where $f_t = (f_{1t}, ..., f_{kt})$ is the vector of time-varying parameters, $C = (c_1, ..., c_k)$ are the constant parameters, $B = \text{diag}(b_1, ..., b_k)$ is the $k \times k$ diagonal matrix of autoregressive parameters, A is the $k \times k$ matrix of coefficients associated to the scaled score and $S(f_t)$ is a scaling function for the score $\nabla(x_t, f_t)$. Moreover, we assume:

$$A = \text{diag}(e) + \gamma\delta' \tag{3}$$

where e, γ, $\delta \in R^k$ are column vectors. In addition, to be able to estimate the values of γ and δ, we impose $\delta_k = 1 - \sum_{i=1}^{k-1} \delta_i$.

The score $\nabla(x_t, f_t)$ corresponds to the first derivative of the negative binomial log-likelihood function:

$$\nabla(x_t, f_t) = \frac{x_t - \exp(f_t)}{\alpha \exp(f_t) + 1} \tag{4}$$

Without loss of generality, we use a unit scaling, that is we assume $S(f_t) = I_k$.

In the context of our cyber risk application, the coefficients in the A matrix express in-sector and cross-sector dependence through the score. Being the latter calculated as the scaled difference between the observed and expected number of events (i.e. the shock) at the previous time, the A coefficients determine the impact of unexpected cyber losses occurred in $t-1$ on the expected cyber losses in t in the same sector (diagonal effects) and in other sectors (off-diagonal effects). Formulation (3) gives further insight into the interpretation of parameters: e measures the own effect of shock events in sector i, while the γ and δ vectors act as multipliers of the off-diagonal elements of A. The B coefficients express, instead, the dependence of the expected number of cyber losses on past expectations, while the C constant parameters determine the unconditional and long-term mean of the number of events.

3. Results

3.1. Data

We apply our modelling approach to the daily cyber attack data collected by an international data provider in an agnostic and independent manner, which essentially involves transforming each news of cyber attacks into a severity scale that goes from "low" to "high" values. The data, which can be publicly visualized at www.hackmanac.com, consists of daily times series of cyber losses, categorized by severity and by economic sector of belonging of the attacked company. The time series covers a full three years period, from 2018 to 2021.

The data has already been analyzed by means of rank regression models, in [8]. Here we extend the work taking into account time and sectorial dependence.

For each day in the analyzed time period, we count the number of cyber attacks in each of the following sectors: Education, Government, Healthcare, Financial, Information and Communication Technology (ICT), Trade. We consider only high-severity events, corresponding to "high" or "critical" losses. Thus, we end up with six count time series of extreme events.

In particular, the companies included in our analysis belong to the following industries: Financial (FIN), Information and Communication Technology (ICT), Manufacturing (MFG), Energy (ENG), Trade (TRD).

We remark that all the considered series show a high frequency of zeros and are overdispersed, i.e. their variance is higher than the mean. These features motivate the use of count data models for rare events allowing for possible zero-inflation and overdispersion.

3.2. Empirical findings

We now present results of fitting the negative binomial score-driven model presented in Section 2 to the time series of cyber attacks to different economic sectors in the 2018-2021 period (see Section

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 23 August 2023 doi:10.20944/preprints202308.1018.v2

3.1). By letting the α coefficients equal to those estimated at the univariate level and maximizing the log-likelihood, we estimate the parameters entering the score-driven dynamics and obtain predictions for the counts.

The coefficients - estimated through likelihood maximization - for the proposed score-driven model are shown in Table 1, together with the corresponding standard errors. Table 1 indicates, along with the presence of a significant constant parameter (the c coefficient), the presence of significant time dependence (expressed by the b autoregressive coefficients) for all sectors and, particularly, for the Education one. This is in line with the observation that, during the COVID-19 period, on-line educational services have substantially increased and, along them, cyber attacks to educational institutions.

On the other hand, Table 2 captures the sectorial dependence among cyber attacks. In particular, coefficients in row i in Table 2 express the impact that shocks to the number of cyber attacks in other sectors (along the columns) have on sector i, while coefficients in column j measure the extent to which cyber attacks in sector j affect the others (along the rows). The value of the off-diagonal elements, capturing cross-sector dependence, is determined by the γ and δ parameters entering specification (3). The diagonal elements of the A matrix can be instead interpreted as in-sector channels of contagion, that is the impact of shocks to the number of cyber attacks in a sector on the expected number of cyber attacks in the same sector. Their value is determined by the estimated e parameters in (3).

Based on our results, the sector which affects others most strongly turns out to be ICT, followed by Government, both impacting particularly on the Educational sector. The result is in line with the intuition that the ICT sector, being more dependent on technology, is also more subject to attacks; whereas the Government sector, being strategic for a country, plays a rather central role. Looking instead at "in-strength" centrality, the sector most impacted by cyber attacks in other sectors is the Educational one. This is in line with the intuition that the Educational sector is often among the most open to innovations and the least protected. The Educational sector is also the one showing the highest in-sector dependence.

Table 1. Maximum likelihood estimates of parameters for the multivariate negative binomial score-driven model applied to the daily count of "High" and "Critical" severity cyber risk events in the 2018-2021 period (*** denotes statistical significance at the 1% level).

Sector	c	b
Education	-1.9443***	0.1547***
	(0.0639)	(0.0202)
Government	-0.3891***	0.1086***
	(0.0417)	(0.0963)
Healthcare	-0.3833***	0.1086***
	(0.0504)	(0.0619)
Financial	-0.3864***	0.1085***
	(0.0952)	(0.0707)
ICT	-0.3881***	0.1086***
	(-0.0612)	(0.0906)
Trade	-0.3868***	0.1085***
	(0.0345)	(0.0504)

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 23 August 2023 doi:10.20944/preprints202308.1018.v2

Table 2. Maximum likelihood estimate of the A matrix, expressing the in-sector and cross-sector impact of shocks on the expected daily number of cyber risk events (EDU = Education, GOV = Government, HLT = Healthcare, FIN = Financial, ICT = Information and Communication Technology, TRD = Trade). The bold numbers denote statistical significance at least at the 10% level.

Sector	EDU	GOV	HLT	FIN	ICT	TRD
EDU	**0.9548**	**0.0097**	0.0015	0.0067	**0.0105**	0.0434
GOV	0.0039	**0.3834**	0.0000	0.0034	0.0052	0.0217
HLT	0.0061	0.0075	**0.3798**	0.0052	0.0081	0.0336
FIN	0.0123	0.0152	0.0023	**0.3910**	0.0164	0.0680
ICT	0.0000	0.0000	0.0012	0.0000	**0.3788**	0.0000
TRD	0.0016	0.0020	0.0000	0.0014	0.0021	**0.3890**

We now evaluate the performance of the proposed model. Figures from Figure 1 to Figure 6 compare, for each time series, the observed counts against the 95% confidence bands for the fitted ones. It can be seen that the model well predicts the actual number of cyber attacks in the Education, Government, Healthcare, Financial and ICT sectors. Indeed, the observed value is nearly always included in the predicted interval. For the Trade sector, instead, the model constantly overfits the count of attacks, probably due to the limited number of observed events.

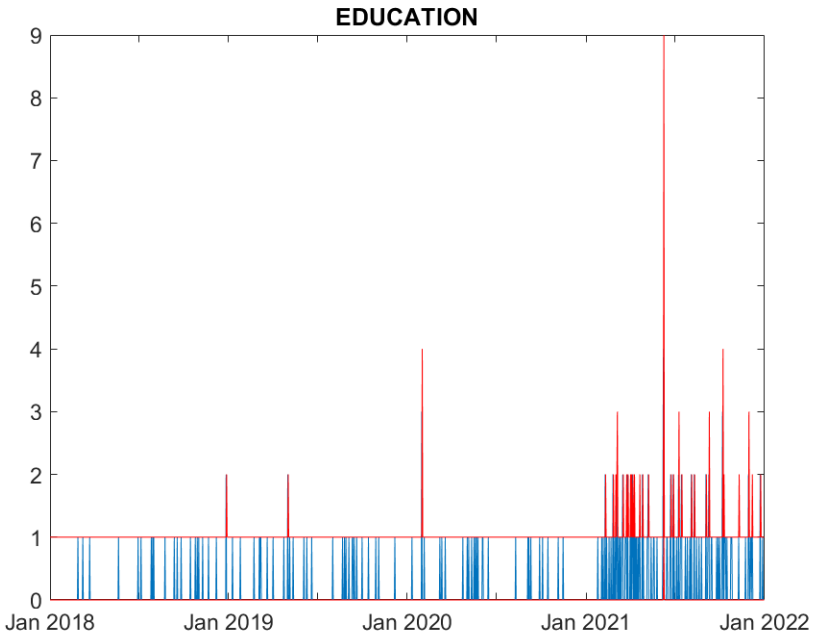

Figure 1. Real (blue) and predicted (95% confidence interval, red) cyber attack counts to Education counterparties.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 23 August 2023 doi:10.20944/preprints202308.1018.v2

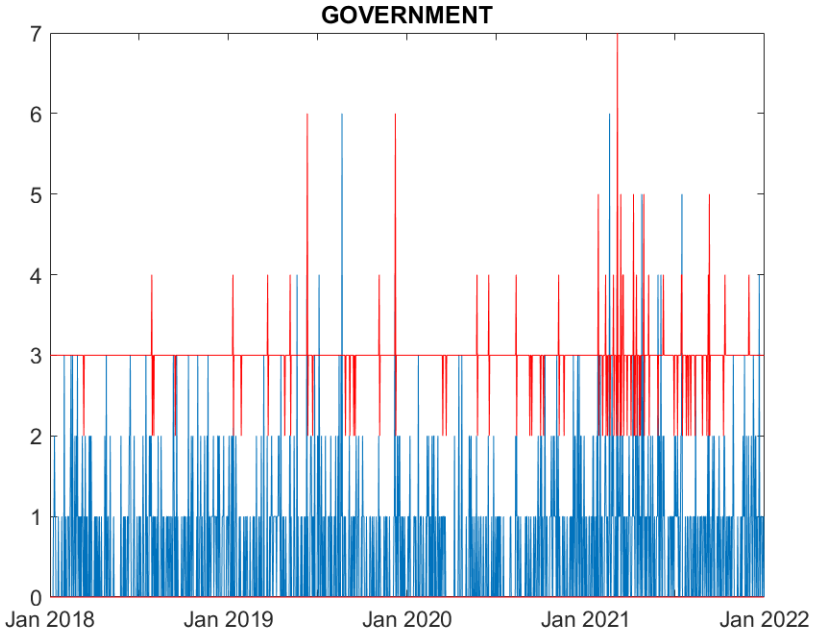

Figure 2. Real (blue) and predicted (95% confidence interval, red) cyber attack counts to Government counterparties.

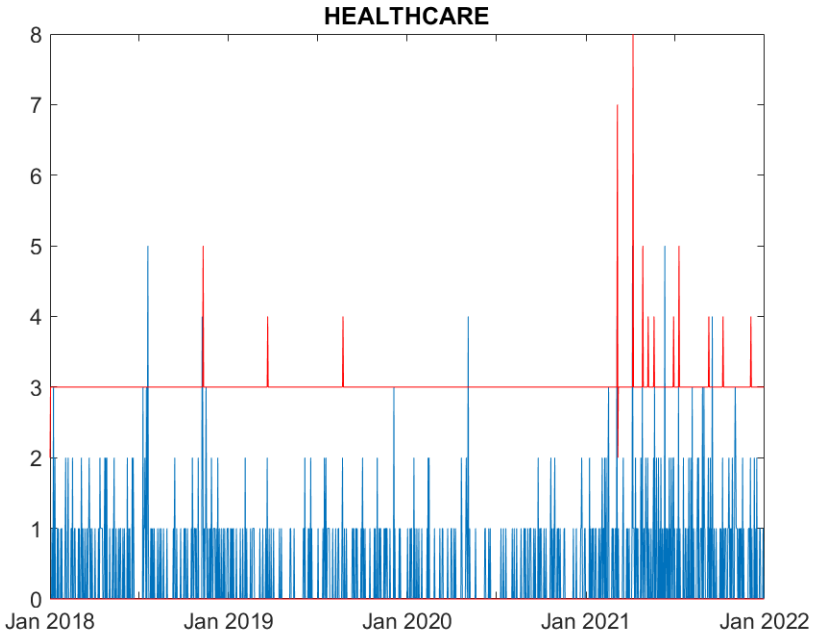

Figure 3. Real (blue) and predicted (95% confidence interval, red) cyber attack counts to Healthcare counterparties.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 23 August 2023 doi:10.20944/preprints202308.1018.v2

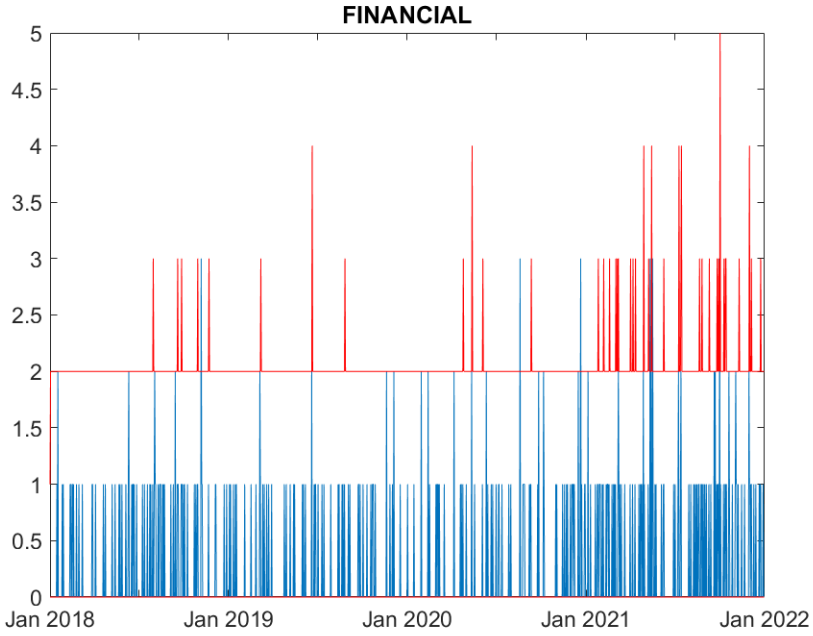

Figure 4. Real (blue) and predicted (95% confidence interval, red) cyber attack counts to Financial counterparties.

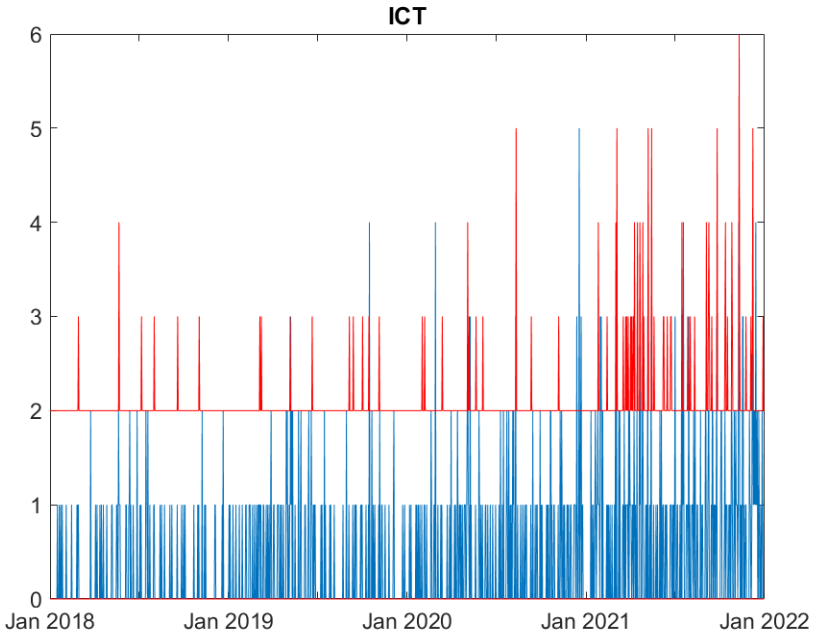

Figure 5. Real (blue) and predicted (95% confidence interval, red) cyber attack counts to ICT counterparties.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 23 August 2023 doi:10.20944/preprints202308.1018.v2

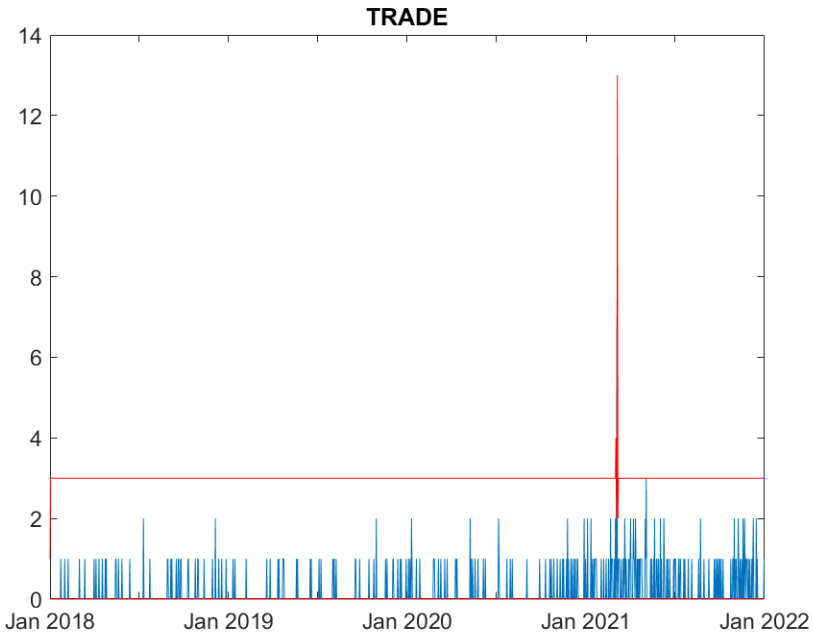

Figure 6. Real (blue) and predicted (95% confidence interval, red) cyber attack counts to Trade counterparties.

4. Conclusions

Within the context of fintech risk management, this paper has focused on one of the main risks that arise with the development of financial technologies: cyber risk. The paper has suggested a research direction to measure such risk, so to manage and mitigate it.

More precisely, the paper has proposed a model to measure contagion risk of (extreme) cyber losses. The model is based on a multivariate negative binomial score-driven model for count time series. The use of negative binomial distribution allows dealing with overdispersion, a common feature in count time series of rare events, such as cyber attacks.

The presented model is very suitable to study contagion in financial losses among different industries and markets. In the proposed specification, the interdependence between extreme event counts arises indeed from the effect of shocks in a sector on the probability that new events occur in others.

The application of the model to daily cyber loss data in the 2018-2021 period reveals high time dependence and significant cross-sector effects.

The study has focused on cyber risk deriving from ordinal loss data. A possible extension would be to consider continuous loss data, when available, as in [4].

Further research should take into account other types of extreme events, such as climate-change impacts.

We believe that this paper can contribute to encouraging the development and growth of financial technologies, making them sustainable and minimizing their possible negative impacts on consumers and investors. This by means of appropriate risk management methods, whose compliance burden can be limited by the technology itself.

A strict collaboration and open discussion between academics, fintech experts and regulators can help move in this direction, defining fintech risk management models that, while limiting the negative impact of disrupting technologies, encourage their development.

Author Contributions: "Conceptualization, A.A. and P.G.; methodology, A.A:; software, A.A.; validation, P.G.; formal analysis, A.A.; investigation, A.A.; resources, P.G.; data curation, A.A.; writing—original draft preparation, A.A.; writing—review and editing, P.G.; visualization, P.G.; supervision, P.G.; project administration, P.G.; funding acquisition, P.G.

Funding: "This research was funded by European Commission PERISCOPE project grant number 101016233."

Acknowledgments: The paper is the result of a close collaboration between the two authors. Both authors declare not to have any conflicts of interest. The authors would like to thank Sofia Scozzari, CEO and founder of Hackmanack, for having provided the data.

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

MDPI	Multidisciplinary Digital Publishing Institute
DOAJ	Directory of open access journals
TLA	Three letter acronym
LD	Linear dichroism

References

1. Adrian, T. and M. K. Brunnermeier (2016). CoVaR. The American Economic Review 106(7), 1705-1741.
2. Ahelegbey, D., Billio, M., Casarin, R. (2016). Bayesian graphical models for structural vector autoregressive models. Journal of Applied Econometrics 31(2), 357-386.
3. Agosto, A. Multivariate Score-Driven Models for Count Time Series To Assess Financial Contagion.Available at SSRN 4119895 (2022).
4. Aldasoro, I., Gambacorta, L., Giudici, P., Leach, T.. (2022) The drivers of cyber risk, Journal of financial stability, 60, 100989 (2022).
5. Billio, M., Getmansky, M., Lo, W.L., Pelizzon, L. (2012) Econometric measures of connectedness and systemic risk in the finance and insurance sectors, Journal of Financial Economics, 104(3), 535-559.
6. Creal, D., S. J. Koopman, and A. Lucas (2013). Generalized autoregressive score models with applications. Journal of Applied Econometrics 28, 777-795.
7. Diebold, F. and K. Yilmaz (2014). On the Network Topology of Variance Decompositions: Measuring the Connectedness of Financial Firms. Journal of Econometrics 182(1), 119-134.
8. Giudici P. and Raffinetti E. (2021). Explainable AI methods in cyber risk management, Quality and Reliability Engineering International, 1-9.
9. Harvey, A. C. (2013). Dynamic Models for Volatility and Heavy Tails: With Applications to Financial and Economic Time Series. Cambridge University Press, New York.
10. Minoiu, C. and J. A. Reyes (2013). A Network Analysis of Global Banking: 1978–2010. Journal of Financial Stability 9(2), 168-184.
11. Kopp, E., Kaffenberger, L. and Wilson, C: Cyber Risk, Market Failures, and Financial Stability, IMF Working Paper, WP/17/185, pp. 1-35 (2017).