EXECUTIVE SUMMARY

Probable maximum cyber loss: Empirical estimation and reinsurance design with private-public partnership

A society with a developed interconnected network system has been constantly exposed to the possibility of a super-extreme cyber loss over the last decade. An extreme cyber risk event could cost the society more than a major natural catastrophe can do. For instance, the loss amount by "Wannacry" attack in 2017 is expected to reach almost $4 billion across the globe and a potential economic damage by a next extreme cyber risk is estimated to be more than $120 billion based on an analysis by Lloyd's. This super-extreme cyber risk can potentially trigger a huge accumulation risk to insurance companies. A cyber disaster becomes more catastrophic, complex and rapidly evolving, hence one of the challenges for insurers and risk managers is to estimate the size of a next extreme loss possibly hitting many policyholders in other pools simultaneously, called silent cyber risk. This challenge keeps potential insureds from purchasing cyber-insurance, in which the cover limit is conservatively set at a low level.

In this regard, we suggest an alternative approach to a more accurate, widening prediction for the cover limit by focusing on maximum losses in certain blocks (time blocks) and investigating their statistical property based on the largest database (Private Rights Clearinghouse; PRC) of cyber risk from 2005 to 2018. Although a number of studies have attempted to estimate the size of an extreme cyber loss, particularly with a threshold-based model, there still exists a possibility of a black swan beyond their estimates, the size of the black swan that has been already experienced by the society over the last years. Hence, the aim of this paper is to capture the trend of worst case cyber losses and to provide an insight for feasible cover limit of cyber-insurance in response to increasing demand for a benchmark measurement of the limit in the current market. Consequently, we define the probable maximum cyber loss (PMCL), which stands for the worst cyber loss likely to occur, proved to be much larger than the existing measures of cyber risk.

To achieve the objective, we establish four steps illustrated in Figure 1 and identify that the series of cyber loss maxima in three time blocks (weekly, biweekly and monthly) are stationary, short-range temporal dependency exists and Fréchet type of generalized extreme value distribution (GEV) is well fitted with fat-tailedness of loss maxima. In the application to the PMCL estimation, we find that predicted losses likely to occur in the next five years are almost seven times larger than the estimate by the recent literature with a widely used Pareto-based

model. Particularly, the estimates for the more recent period show a dramatic increase compared to the ones for the older period with a significant structural break between pre-2014 and post-2014. We additionally consider a possible risk categorization by two factors (malicious risk vs. negligent risk) and model the dependence structure (extreme dependency), resulting in the PMCL estimates on average 3.27 times larger than the ones without the correlated risk.

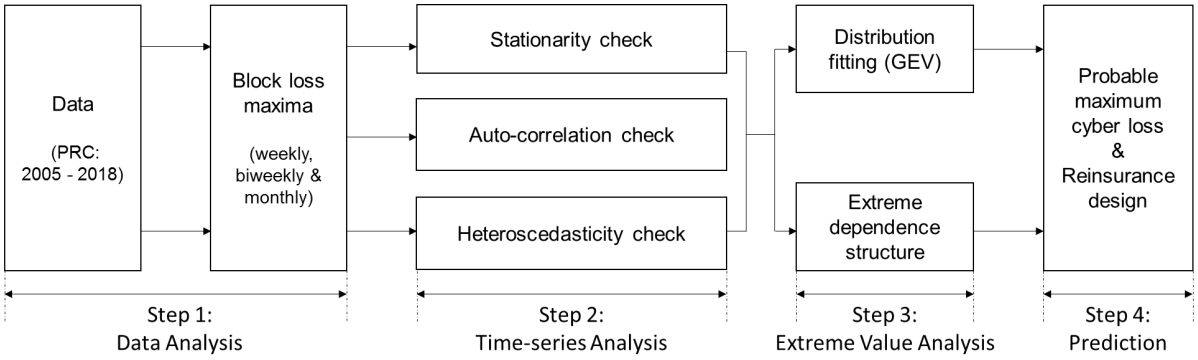


Figure 1. The methodological process for the empirical estimation on extreme cyber losses.

We conclude that the size of a catastrophe cyber loss possibly triggering a huge accumulation risk is practically uncontrollable for a private sector (e.g., for a single insurer). This conclusion implies that a super-extreme loss could lead a cyber-insurer to become insolvent by a single event, which can also cause a systemic risk in the industry. Therefore, we propose a reinsurance design with private-public partnership based on PMCL estimates. We set up a reinsurance portfolio of a potential cyber-insurer by suggesting 1) a quota share treaty with a reinsurer (or collective reinsurance from the market) up to our PMCL estimates as the cover limit and 2) a catastrophe Excess-of-Loss (CatXL) coverage with the government on the amount above the cover limit of CatXL.

The estimation on reinsurance pricing shows that the total annual premium based on PMCL estimates is twice larger than the estimated premium worldwide for 2019 by industry, revealing a need to increase the capacity of the cyber-insurance market. It further indicates that this increase in the capacity needs to be backed by the government with the financial support for on average $ 2.1 billion loss per exposure. This three-layer program with private-public partnership already implemented in several countries against terrorism risk should be considered against cyber risk. To sum up, this paper contributes to the literature on extreme cyber loss modeling in that maximum loss process for different time frames is analyzed with taking into account temporal dependency. This contribution is important for actuaries who are designing cyber-insurance policies in primary insurers and reinsurers, and for policymakers who are concerned about a social cost by a next super-extreme cyber loss as a New Normal in the digital era.