Anders Sandberg, Phd
James Martin Fellow,
Oxford Martin Programme on the Impacts of Future Technology
& James Martin Fellow
Future of Humanity Institute
Oxford University
anders.sandberg@philosophy.ox.ac.uk

Feng Zhou, Phd
Research Fellow Future of Humanity Institute
Oxford University
feng.zhou@philosophy.ox.ac.uk

Corresponding Author:
Pythagoras Petratos, Phd
Departmental Lecturer
Said Business School
Oxford University
Pythagoras.petratos@sbs.ox.ac.uk

Title of Contribution: Cyber Risks and Cyber Insurance

Keywords: Cyber Risks/Uncertainty/ Ignorance, Cyber Insurance, Insurable and Uninsurable Cyber Risks, Catastrophic Risks, Development of Cyber Insurance Markets, Incentives.

Abstract: This chapter is an introduction to cyber insurance. We describe the different types or risks as well as uncertainty and ignorance related to cyber security. A framework for catastrophes on the cyber space is also presented. It is assessed which risks might be insurable or uninsurable. The evolution and challenges of cyber insurance are discussed and finally we propose some thoughts for the further development of cyber insurance markets.

Acknowledgements: This work was supported by the FHI-Amlin Research Collaboration on Systemic Risk of Modelling in pursuing better understanding and management of the systemic risks associated with modelling in the insurance industry through the strategic collaboration between the Future of Humanity Institute and Amlin. We are grateful for comments and suggestions from numerous colleagues and insurance industry participants from Amlin plc, the Lloyd's of London and the Bank of England in several meetings and discussions among working parties.

1 Introduction

Cyber insurance has a broad definition and has been continuously evolving over time. It was defined as insurance for the damages to "physical" computer equipment in 1970s, but nowadays it has been changed to be a cost-effective option of risk mitigation strategies for IT/cyber related losses. According to Association of British Insurers (ABI), it "covers the losses relating to damage to, or loss of information from, IT systems and networks". Anderson et al. (2007) argue that cyber insurance in an ideal situation promotes users to implement good security. However, some barriers are currently preventing insurers to achieve this goal, and innovations in the cyberspace introduce new types of loss. For example, "Internet of Things" is shifting cybersecurity from protecting information assets to physical goods that were traditionally un-related to computers.

At present, cyber insurance has a small share in overall non-life insurance market and represents just 0.1% of the global Property & Casualty insurance premium pool (Marsh, 2015), but it is one of the fastest-growing new lines of insurance business and the cybersecurity is recognized as one of the top global risks in the World Economic Forum's report recently (WEF, 2015). Meanwhile, more and more traditional insurance contracts exclude specific losses that are linked to cybersecurity, it is necessary to develop a standalone cyber-insurance market. New technologies and innovations in the cyberspace are also spurring the development of cyber-insurance market, as well as the current trend of government requiring high standards on protecting sensitive information and enforcing financial punishments relating to information security breaches.

Both the complexity of cyber risk and the current immaturity of cyber-insurance market bring challenges for industry practitioners and regulators to fully understand potential future systemic risks in this kind of complex system. Not surprisingly, the recent Risk Nexus Report from Zurich Insurance Group argues that the global aggregations of cyber risk is analogous to those risks that were overlooked in the U.S. sub-prime mortgage market (Zurich, 2014). Its nickname "cyber sub-prime" intends to describe the interconnected nature of systemic cyber risk and the challenges for individual insurers to address the complexity. They believe that the existing research on systemic risk in the financial markets that aims to address recent crises should be helpful to understand the dynamics of future cyberspace.

2 Development of insurance for cyber risks

According to 2015 Information Security Breaches Survey (PWC, 2015), 90% of UK large organizations and 74% of small businesses reported that they had suffered at least one security breach in the past one year. The average cost of the worst single breach suffered by these businesses has gone up sharply. For instance, the average cost to a large organization is around £1.5m-£3m up from £600k-£1.15m a year ago. The survey also indicates that the majority of UK businesses surveyed expect breaches will continue to increase. Thompson (2014) estimates that the total cyber insurance currently amounts around US$2 billion, whereas the total cost of global security breaches could be more than US$400 billion. For more about the effects of cyber-attacks on UK companies, see (OxfordEconomics, 2014). For a more detailed history and evolution of cyber-insurance products, see (Majuca et al.,2006).

2.1 Economics of information security

Together with both the growth of ICT (Information and Communication Technology) and the growing impact of cyber risks to the real-world business increase the demand for insurance-related risk mitigation strategies. The following factors also play key roles in the development of cyber insurance:

A list of key factors affecting either demand for or supply of cyber insurance:

Mitigating cyber residual risks: Organizations have three basic cyber risk management strategies: self-protection, self-insurance, and transfer of risk via cyber insurance (Kesan et al., 2005). While organizations are increasing their information security spending on improving IT system, cyber residual risks still require insurance to mitigate unexpected events. Lelarge and Bolot (2009) find that cyber insurance is a powerful incentive mechanism that motivates organizations to invest in self-protection, so these three strategies are complementary to each other. Pal and Golubchik (2010) analyze the Internet users' investment in self-defense mechanisms when insurance solutions are offered in either full or partial cyber-insurance coverage models.

Promoting and aligning economic incentives: Organizations who have insurance as a last resort of risk management attract customers and business partners, especially for small businesses who are parts of a large/long supply chain in order to avoid being the weakest link of cyber-attacks. In the supply-demand model of cyber-insurance market, Pal (2014) argues that cyber insurance has the potential to jointly align the incentives of different stakeholders in the cyberspace, such stakeholders or players as security vendors, cyber insurers, regulatory agencies and network users. Anderson et al. (2007) also suggest that cyber insurance in an ideal situation promotes users to implement good security.

Protecting exclusions in traditional insurance: Cyber cover was mainly embedded in other traditional insurance products (e.g.: business interruption or professional liability insurance), but nowadays more and more traditional insurance contracts intend to exclude the cyber-related risks due to the complexity of cyberspace and potentially catastrophic consequence, as well as requiring different actuarial methods to preform data analysis (Siegel et al., 2002). As a result, standalone cyber-insurance policies are emerged. However, there is a gap between insurers and insured parties to explain the differences/exclusions among both standalone cyber-insurance contracts and traditional products. It is necessary to have cyber-insurance brokers to reduce the gap (Marsh, 2015).

Providing professional advice and delivering experienced cyber incident response: Insurance companies themselves collect a huge amount of customers' personally identifiable information and corporate clients' business confidential/financial information, so they must follow and have rich experience to deal with many regulations of protecting data information and cyber security (e.g.: HIPAA Health Insurance Portability and Accountability Act to protect the privacy of individual patients/customers, GLBA Gramm Leach Bliley Act to secure the private information of clients) (Appari and Johnson, 2010). Insurers also accumulate the updated knowledge and relevant experience from clients globally and communicate with other security professionals, in order to provide technical and legal assistance (as well as financial compensations) to manage cyber-related breaches and incidents (Marsh and Zurich, 2015).

Training cybersecurity awareness and building information security culture: Security managers often find difficulties to communicate with non-technical internal staff or external clients about security policies and technologies who have no formal security background, but insurance is an easy way to explain the (financial) impact of cybersecurity to the business. The insurance premium that has been reduced (or increased) year-by-year due to a better (or worse) security implementation in this year relative to other previous periods, it is a good indication and consistent comparison to define proper cyber risk metrics and to educate staff or clients. However, at this early stage of cyber insurance, there is still a lag for insurers to implement premium differentiation on the cyber insurance that reflects the insured security improvement precisely due to the immaturity of the cyber insurance market (Mukhopadhyay et al., 2013; Moran et al., 2015).

Government supports: A free-market approach is traditionally popular to manage risks in the financial system, since it increases motivation and efficiency of stakeholders in the system. As Anderson et al. (2007) suggest that one option to spur demand for cyber insurance is to make it compulsory (as it is common in motor insurance), but it may lead a deadweight on competitiveness and productivity growth. The role of government is to encourage and support the insurers to overcome the barriers of supplying cyber insurance (The barriers will be discussed in the cyber-insurance market section as followed). Recently, UK government launched its "10 Steps to Cyber Security" (CESG, 2012) and "Cyber Essentials Scheme" (BIS, 2014), both aiming to assist insurers to evaluate the security assessment of small and medium-sized enterprises.

Sharing data of cyber incidents (data pooling): It is necessary to form partnerships from different industries that share data in order to better understand cyber risks, as suggested in the UK Cyber Security Strategy (Cabinet, 2011). The recent launched Cyber Security Information Sharing Partnership (CiSP https://www.cert.gov.uk/cisp/) aims to collaborate with insurers to analyze emerging threats, disaster scenarios and trends in the cyberspace. The cyber insurance will be more affordable and its purchasing cost is expected to be lower than current level based on more relevant actuarial data in the near future, and a higher degree of price differentiation across different policies and individual firms will be feasible (Marsh, 2015). However, Bohme (2006) states and explains that information sharing is socially beneficial, but it is not efficient to rely on a trusted third party only (as a "social planner") to arrange data collection.

2.2 Insurable and uninsurable cyber risks

In terms of a specific insurance policy, the potential losses related to cyber-attacks or non-malicious IT failures can be currently grouped into 11 categories in the London Insurance Market (Marsh, 2015) that is also similar to the US market (Majuca et al., 2006).

Due to both the difference in severity/frequency of cyber events and the complexity of cyber risks, some of these losses are insurable while others are not available at present. Johnson et al. (2014) study the complexity of estimating systematic risk in cyber networks, which is an essential requirement to provide cyber insurance to the public. The following discussion explains the insurability and exposure for different cyber risks (Marsh, 2015).

Insurable cyber risks

Privacy events: Many privacy issues are related to managing regulatory requirements on information security. Insurers can collaborate with lawyers to provide different levels of services and protections to their clients. Since the losses from these events are handled and measured by a third-party professional lawyer, there is less information asymmetry or moral hazard problem between insurer and insured.

Crime and fraud: Police force often involves in the investigation of cyber-crime and fraud, therefore the financial losses related to such cyber events are measured by third parties such as police or lawyers. Insurers can not only offer insurance cover, but also provide professional advice on preventing these events or reducing the cost based on their experience from other customers.

Network security liability: Third-party liabilities related to certain security events occurring within an organization's IT network can be insured, mainly due to the scope of incidents can be clearly defined by the insurers and IT system engineers can also collaborate with insurers to improve mitigation strategies.

Software and data damage: Insurers can provide indemnity for the costs arising from the damage of data or software (e.g.: help recovering or reconstituting the damaged data), this is mainly because insurers are able to require the policy holders to follow necessary procedures of data backup or redundancy.

Cyber extortion: Traditionally, insurers have the necessary knowledge and experience of dealing with extortion in the physical world and conduct ransom negotiations (particularly in the London Market, such as the Lloyd's of London), extortion in the cyberspace is not much different from that. Cover is provided for both the cost of handling the incident and the ransom payment.

Uninsurable (or insurable but with constraints) cyber risks

Reputational loss: Although insurance cover is available for the losses that are directly linked to reputational damage (e.g.: cost of recovering public image or loss revenue from existing customers), it is difficult to measure the value of the compensation and the linkage between the cyber incident and the intangible asset if without certain constraints.

Network business interruption (e.g.: due to Denial of Service attacks): In the traditional insurance sector, it is common to offer full coverage for business interruption arising from natural disasters or man-made events. However, in the early stage of cyber insurance, insurers are concerned about the potential aggregate exposure from a single cyber event but interrupts many insured policy holders.

IP theft or espionage: These types of losses are extremely difficult to prove and quantify, since the value is changing quickly over time and trade secret is priceless before an incident but (likely) worthless if being public. It is also hard to define whether the incident was incurred in the insured period. Moreover, these attacks are often state-sponsored with a large amount of resource.

Physical asset damage: The interconnection between physical world and cyberspace is increased by the development of the so-called "Internet of Things (IoT)", therefore more and more cyber incidents will directly have impacts on the physical assets. At this stage, the complexity of these interconnections is

not well-understood by insurers, therefore it is difficult to combine cyber insurance with traditional property insurance or have such physical asset damage cover in the standalone cyber insurance.

Death and bodily injury: Similar to the physical asset damage, it is more and more likely that certain cyber related incidents may cause harm to the human (e.g.: medical devices, large scale industry equipment, driverless cars, etc.). Although it is uninsurable at the current stage of cyber insurance, it is covered by traditional insurance products such as general liability and employers' liability products.

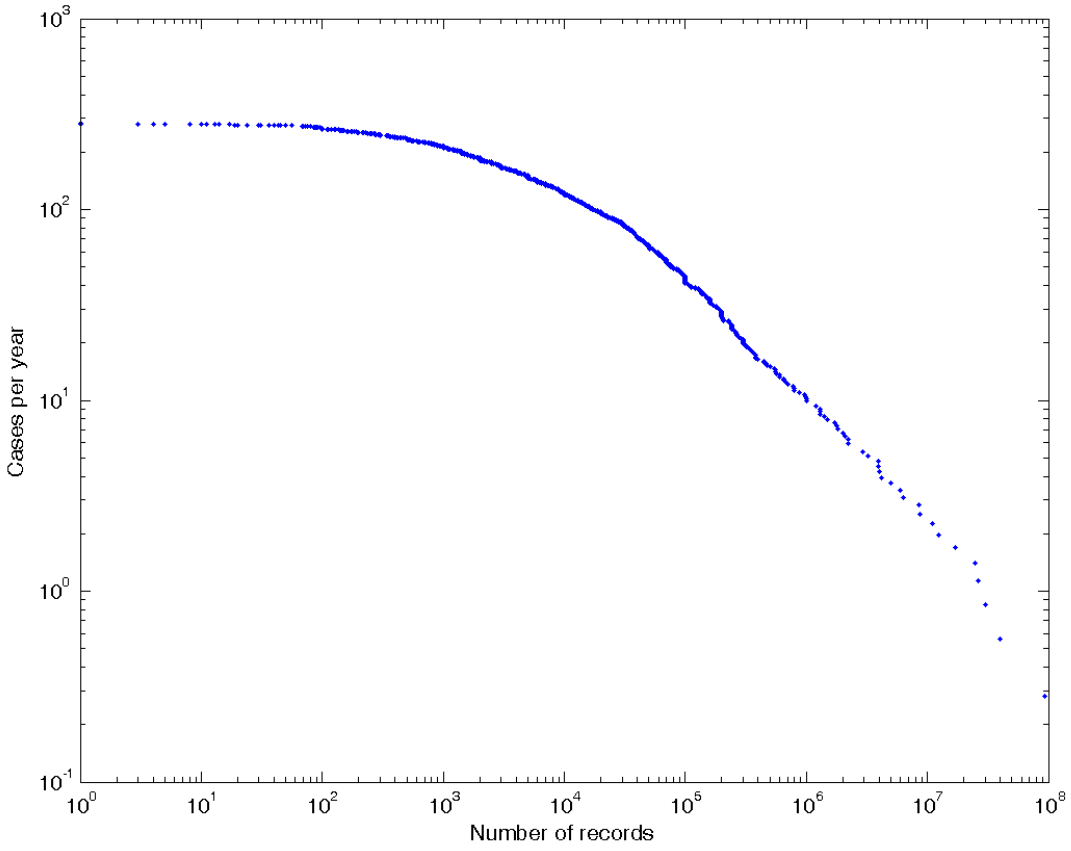

Figure 1: Size distribution of data losses (based on data from datalossdb 2000-2005). Expected number of losses per year larger than a certain size as a function of number of records lost. Note the power-law heavy tail for larger losses (exponent ≈ -0.66, consistent with the results in (Overill & Silomon 2011, Mailart & Sornette 2010)). This tail may be dominated by more targeted events and organized crime, including financial fraud, insider abuse and theft, as well as malware (Overill & Silomon 2011).

2.3 Challenges and developments

Even if insurers are able to offer cyber insurance to mitigate certain types of cyber-risk events, they must face and learn to overcome some challenges in order to maintain and expand their businesses. Not surprisingly, there are progresses and developments to address these challenges recently.

Challenges for insurers

External attackers are evolving over time: Information Security Breaches Survey (PWC, 2015) shows that outsiders are using more sophisticated methods to affect organizations.

Staff-related breaches are unique in individual cases: Whether inadvertent human error or not, the consequence from insiders' mistakes or misconducts is difficult for insurers to measure.

Lack of understanding and communication: Recent surveys indicate that a majority of CEOs believe their organizations have relevant insurance to cover cyber risks (PWC, 2015) whereas in fact only around 10% actually do (Marsh, 2015).

Increasing IT system collaboration and social network: Cyberspace is moving towards an ecosystem, which has more and more heterogeneous players collaborate and interact to each other.

New technologies and innovations: The ICT sector is attractive to capital markets with large amounts of capital to support new businesses and innovations. However, due to the nature of this fast evolving sector and heavy competition, ICT vendors focus more on the short process of introducing their products and services to the market and less on the security. It is challenging for insurers to follow these fast developments and potential risks involved in the process (Friedman, 2011).

Recent developments

Government: Organizations are increasingly using Government alerts (e.g.: the UK HMG Cyber Essentials scheme) to inform their awareness of threats and similar vulnerabilities (PWC, 2015). Insured firms can get discount on insurance premium if they follow these certification requirements, so it offers motivations for insured users to follow security procedures and policies.

Insurance cyber gap analysis: Marsh (2015) also suggests that it is necessary for insurance brokers to provide cyber gap analysis (determining which cyber risks are covered by existing traditional insurance or need to be covered in a standalone cyber insurance) when communicating with customers.

Insurers' data protection regulations: Insurance industry itself collects sensitive personal, financial and healthcare data from their policy holders (e.g.: personally identifiable information PII, protect health information PHI and business operation private information) in order to measure the customers' risks more precisely. As a result, the National Association of Insurance Commissioners NAIC (2015) recently adopts cybersecurity guidance for the insurance industry and regulators to follow. The expertise and experience of insurers' information security practice is also applied to advice their customers.

Understanding the benefits of cyber insurance: The growing amount of literature starts to support the benefits of cyber insurance as a market-based solution to cybersecurity. Kesan et al. (2005) state, when certain obstacles to a full market solution are fully worked out, several positive outcomes will occur. In general, cyber insurance market will result in higher overall social welfare.

3 Evolution of cyber-insurance market

It is still too early to know the structure of the future, mature cyber-insurance market. In the existing literature, both competitive (Shetty et al., 2010b) and monopolistic (Lelarge and Bolot, 2009; Hofmann, 2007; Pal and Golubchik, 2011) market structures are studied.

As commonly expected, the cyber-insurance market will soon become a complex dynamic system (Anderson and Moore, 2009; Halse and Hoemsnes, 2013). As a result, the market not only provides one option of risk mitigation strategies, but also builds an eco-system together with other sectors in cyberspace that can influence heterogeneous stakeholders' behaviors and business strategies (Hall et al., 2011). This is similar to other financial systems, such as stock or credit markets (Gracie, 2015). Therefore, the existing research in other financial systems will be relevant to understand the future cyber-insurance market (Zurich, 2014).

3.1 Obstacles of developing cyber-insurance market

Shetty et al. (2010a) and Bohme and Schwartz (2010) argue that the underdeveloped cyber insurance market is mainly due to: (1) Interdependent security (externalities) (Ogut et al., 2005; Bolot and Lelarge, 2008; Zhao et al., 2009); (2) Correlated risk (Bohme and Kataria, 2006); and (3) Information asymmetries (Bandyopadhyay et al., 2009). Furthermore, Bohme and Schwartz (2010) argue that "it appears that the market failure can only be overcome if all obstacles are tackled simultaneously". Meanwhile, Marsh (2015) states that a well-developed reinsurance market for cyber insurance is also one of necessary conditions to expand the business.

The four key obstacles are explained as follows:

Interdependent security (externalities): Kunreuther and Heal (2003) ask the question: "Do firms have adequate incentives to invest in protection against a risk whose magnitude depends on the actions of others?". One of the differences between cyber and traditional insurance (e.g.: property or motor) is the close interconnections among players in cyberspace. The security in cyberspace is dependent on all players in the system, but heterogeneous players have different preferences about cybersecurity and the "free rider problem" occurs when those who benefit from other players' security investment don't have to pay for it (Varian, 2004). As Naghizadeh and Liu (2014) argue that security is a non-excludable public good, so users can stay out and still enjoy spill-overs from others' contribution without paying. As a result, even insurers help their insured customers to increase their overall security, those un-insured players in the system still can weaken these insured customers.

Correlated risk: Bohme and Kataria (2006) define two tiers of correlated cyber risks: (1) internal correlation, which they define as "the correlation of cyber-risk within a firm (i.e.: a correlated failure of multiple systems on the internal network), and (2) global correlation, as "the correlation of cyber-risk at a global level, which also appears in the insurer's portfolio." The growing development of Cloud computing platform may accelerate the two tiers to be integrated together. For example, an internal incident in a cloud service provider will lead systematic risks in both its internal system and its customers' systems.

Information asymmetries: Bohme and Schwartz (2010) define "asymmetric information" as environment where some players have private information to take advantages on something that are not available to other players. The common issues in the conventional insurance literature due to "asymmetric information" are: adverse selection (Akerlof, 1970) and moral hazard (Arrow, 1963). They are also relevant to the cyber-insurance market and other obstacles (e.g. the interdependent security) may exacerbate its problems (Shetty et al., 2010a). Furthermore, Bohme and Schwartz (2010) also identify specific forms of information asymmetries in cyber insurance. Meanwhile, Pal (2012) proposes three mechanisms (premium differentiation, fines, security auditing) to resolve information asymmetry in cyber insurance

Lack of reinsurance market: It is still in the early stage for reinsurers to re-insure cyber risks from primary insurers, but several proposals have been put forward to build such reinsurance function (Toregas and Zahn, 2014), such as to establish government regulated funds similar to US Terrorism Risk Insurance Act or UK Financial Service Compensation Scheme. Anderson et al. (2007, 2009) discuss that one possible option is for government to provide reinsurance, but they emphasize that "while government re-insurance can create insurance markets where otherwise there would be no supply, such measures must be carefully designed to avoid a regime in which profits are private (to the insurers' shareholders), losses are socialized (born by the tac-payer), and systems remain insecure (because the government intervention removes the incentive to build properly secure products)."

3.2 Technologies spur the cyber-insurance market

Many new technologies have been developed in recent years will spur the cyber-insurance market. We identify some of these technologies and group them into 3 main categories: (1) IT technologies assist insurers to manage and discover cyber incidents, as well as attract more customers demand for cyber insurance; (2) Technologies and methods that are helpful for insurers to perform actuarial modelling and data analysis; and (3) Technologies that are useful to better understand the complexity of cyber-insurance market.

IT technologies

Some standalone technologies: Such as Intrusion Detection Systems (IDS), firewalls, digital forensic technology, Microsoft Photo DNA, encryption tools have become more advanced and relevant for insurers to investigate cyber incidents.

Trusted computing infrastructure: Although the opponents of trusted computing argue that users will lose their freedom and privacy (Anderson, 2003a,b), the technology provides insurers an opportunity of identifying insurable events and defining claims more precisely.

Cloud platforms: Cloud service providers can reduce the issues of misaligned incentives between insurers and cloud users, if they can collaborate with insurers to attract more customers. Meanwhile, automated systems reduce human errors in the computing process. However, on the other hand, the cloud platform may lead to systemic risk since they are connected to other IT systems.

Anonymous communication and transactions: The anonymity network that is currently represented by e.g. Tor software makes cyber criminals "anonymous" and untraceable. Anonymous digital currencies

allow sophisticated markets for illicit goods and services (Juels, Kosba & Shi 2015). As a result, there is a deep/dark web that provides a cyber black market for attackers to trade sensitive information (e.g.: selling stolen credit card information to other parties, etc), so the attackers' motivation of attacking any organizations become larger.

Mobile devices: Nowadays, more and more business activities and collaborations are based on mobile devices (e.g.: Bring Your Own Devices). This leads more cyber incidents that require cyber insurance, since such as devices are lost or stolen easily and users do not have sufficient skills to manage the security on these mobile devices.

Leaking technology: ICT enables rapid copying and dissemination of information, making information leaks harder to contain. In the past a sizeable leak of proprietary information (such as the more than 40 gigabytes of internal data released in the 2014 Sony hack) would have been limited by the need to transmit it by sending hard drives (expensive) or setting up a website (legally traceable and blockable); by 2014 it could be distributed anonymously using bittorrent in a way that makes it impossible to trace and block. In addition, leaks are potentiated by the appearance of search tools making released data more accessible.

Actuarial modelling methods

Network simulator: Similar to stress and scenario testing that are commonly used in the financial markets (e.g. banking system), insurers can use various applications and services to run network simulation in an artificial environment in order to test the stability and resilience of insured network under different conditions.

Actuarial data analysis (big data analytics): More and more professional consulting service firms have been investing and offering advanced actuarial pricing and risk management services based on big data analytics to assist insurers uncovering hidden patterns and unknown correlations in cyber risks.

Data pooling platform (data anonymization): Technologies of information sanitization that aim to encrypt or remove sensitive information from data sets are becoming more feasible, this encourages more data to be shared in the pooling platform in order to help government and insurers to better understand cyber risks from aggregated data sets.

Machine learning and Bayesian networks: More and more applications from these sub-fields of computer science are used in understanding the cyber risks. Insurers will hopefully gain insights about managing the cyber risks from these developments. Yang and Lui (2014) apply Bayesian network to analyze the influence of cyber-insurance market to security adoption in heterogeneous networks.

Data visualization: According to the "digital detectives" website of Microsoft, advances in data visualization technology assist Microsoft Digital Crimes Unit (uses Microsoft PowerMap) to understand the pattern of Citadel botnets better and remove the malware from infected machines more efficiently (Constantin, 2013). The same technologies will help insurers to identify cyber incidents from different malware or causes, so they can distinguish the incidents in order to reduce specific claims (similar to distinguish different risk events in natural catastrophe insurance) or issue insurance-linked securities

based on specified triggers (cyber incident) earlier. Anderson et al. (2007) consider one of potential strategies to promote cyber insurance is to develop financial instruments for risk sharing similar to "Cat Bonds" and "Exploit Derivatives" in the traditional insurance business operations (e.g.: flood and natural-disaster insurance). As Anderson et al. (2007) explain "Exploit Derivatives are vehicles for insurers to hedge against the discovery of vulnerabilities that causes significant loss events across their portfolios. "

Socio-technical systems

Security awareness training and behavioral games: Toregas and Zahn (2014) mention a growing consensus that cyber security is not achievable by solely focusing on technological aspects, but also requiring to understand both technologies and their users' behaviors. The importance of understanding human-computer interaction has been studied widely since the works of Adams and Sasse (1999) and Sasse et al. (2001). Recently, some behavioral digital games based on computer simulations are introduced to train the users' behavior and awareness of using technologies securely (Cone et al., 2007).

Existing interdisciplinary research in financial systems: Bohme (2010b) argues that some key obstacles causing cyber-insurance market failure are due to a lack of understanding information economics. An interdisciplinary and integrated research that focus on a cyber eco-system is better than targeting each individual technological elements alone (Bohme, 2010a). This idea is similar to recent progress of understanding systemic risks in the financial markets. Schneier (2002) and Anderson and Moore (2007, 2009) state that a combination of economics, game theory and psychology is necessary to understand and manage cybersecurity in the modern and future networked environment. Johnson et al. (2011) model security games with market insurance to inform policy makers on adjusting incentives to improve network security and cyber-insurance market. Baddeley (2011) applies some lessons from Behavioural Economics to under issues of information security. More papers on the economics of information security and privacy can be found in the book of Moore et al. (2010).

Multi-agent technique: Agent-based approach of modelling a complex system is becoming popular in the financial markets, but it is not commonly used by researchers to model cyberspace or perform stress testing on particular cyber events. Recently, a few researchers start to apply this technique to model network resilience (Sifalakis et al., 2010; Baxter and Sommerville, 2011; Sommerville et al., 2012).

4. General Categorization of Cyber Risks

In the previous analysis we presented the literature related to the evolution of cyber-insurance. It is our intention to further examine the challenges for the development of a cyber-insurance market. ''An understanding of insurance must begin with the concept of risk—that is, the variation in possible outcomes of a situation'' (Zeckhauser, 2008). We embark on a theoretical and empirical analysis, using examples of cyber security events, in order to better understand cyber risks and relate them to cyber security.

The first crucial observation is that numerous different things can be included under the term ''cyber risks''. A more precise definition of ''cyber risks'' would result if we break them into three distinct elements.

- (Cyber) *Risk*, can be defined as a measurable quantity, according to Knight (1921). In that sense probability distributions could be assigned to cyber threats. It is thus it is feasible to quantify the (cyber) risks and consequently estimate insurance premiums.
- (Cyber) *Uncertainty*, can be considered to be the unmeasurable quantity related to cyber events. Therefore, we do not know the states of the world and he precise probabilities would not be known. It is also known as Knightian Uncertainty, based on the classic distinction by Frank Knight (1921).
- (Cyber) *Ignorance* can be considered a third category, when we may not have the ability to define what states of the world are possible (Zeckhauser and Viscusi, 2008). It can be considered one step further from uncertainty, when some potential outcomes are unknowable or unknown (Zeckhauser, 2006). There are two important types of ignorance. *Primary Ignorance* concerns situations in which one does not recognize that is ignorant and *Recognized Ignorance*, when one perceives that ignorance (Roy and Zeckhauser, 2013). For example the financial meltdown of 2008 can be considered such an event. It can also be argued that many catastrophic risks are subject to ignorance.

4.2 Catastrophic Risks and Insurance

4.2.1 General Description of Catastrophic Risks

The above general categorization brings us to further types of risk that influence cyber insurance. ''Catastrophes provide the predominant conceptual model of what insurance is about. One pays premiums to secure financial protection against low-probability high consequence events – what we normally call catastrophes.'' (Zeckhauser, 1996, a, b). The main problem is that private markets are facing difficulties in providing coverage for catastrophic risk and thus they can be deemed ''uninsurable risk''. (Jaffee and Russell, 1997).

The timing and consequence of catastrophic events may largely vary. We have already identified the frequency/severity spectrum used for cyber events. In other words the catastrophic risks fall within the Low Probability – High Consequence class (Kleindorfer and Kunreuther, 1999). However the probabilities and consequences are not clearly defined, particularly towards the upper end of losses.

In this chapter we are more interested about the insurers' perspective on assessing such risks. The Actuarial Standard Board defines ''Catastrophe – A relative infrequent event of phenomenon that produces unusually large aggregate losses''. More precisely, ''An event is designated a catastrophe by the industry when claims are expected to reach a certain dollar threshold, currently set at $25 million, and more than a certain number of policyholders and insurance companies are affected.''(Insurance Information Institute, 2015). In that sense, numerous cyber events, as we would examine later, can have the rarity and loss magnitude of catastrophic risks.

However, catastrophes can involve a loss much greater than $ 25 million. The *Swiss Re sigma study* describes catastrophe losses. In 2014, total insured and uninsured losses due to disasters were estimated at $ 110 billion (Swiss Re, 2015). This number is below the inflation adjusted 10 year average

of $ 200 billion and lower than $138 billion in 2013. However the number of natural disaster catastrophes was at a record high reaching 189, and in total there were 336 disaster events.

This variation in total losses and the number of catastrophes, partly displays their unpredictability as well as their severe consequences. By doing simple calculations, we can observe that the average loss per catastrophe is much higher than $25 million (insurance covered claims of USD 28 billion of losses from natural catastrophes and USD 7 billion from man-made disasters). There are two major categories regarding the causes of catastrophic risks:

- Natural disasters, including georisks (like earthquakes) and Climate induced Risks (as hurricanes and floods)
- Man-made Catastrophes can be considered a broader category and it includes industrial accidents and terrorist attacks (Zurich, 2013).

Earthquakes can have devastating effects for insurers but also situations where thousands of women claim to be damaged by breast implants or individuals harmed by asbestos (Zeckhauser, 1996, a, b). This example, except making the distinction between natural and man-made disasters, presents some interesting features that could be used for some initial comments about cyber risks.

A feature is that natural disasters are usually localized (geo specific). The same can apply to cyber events. A system failure in an energy grid can have local effects. Nevertheless there are many cases, let us say a computer virus, that can have regional or global impacts. Cyberspace is by its nature fairly nonlocal, and there are fewer "natural boundaries" that constrain the size of an impact. This makes these breaches rather easily diffuse around the world, therefore resulting in widespread damage.

Also, it seems that a disproportionately larger number man-made breaches and disasters occur in cyberspace (PWC, 2015): actually it can be argued that there are very few cases in which the human factor is not involved. While the majority may be unintentional, intentional incidents have the potential for particularly expensive damage.

4.2.2 Aggregate Catastrophes and Systemic Risks

''Aggregate catastrophes occur when many similarly situated people, all subject to common risks, suddenly find that they have suffered a loss, and the total losses exceed expectations''. (Zeckhauser, 1996, a, b). The *single worst* incident suffered by an organization might be considered to be a measure for informing us about catastrophic risks, especially in large corporations. Infection of viruses or malicious software remains the largest single worst incident causal factor (PWC, 2015). As argued above, viruses and malware have the ability to propagate rapidly and cause harm to various people and organizations.

In that sense, we can further decompose the High Consequence characteristic. One dimension is the number of individuals and organization that a cyber event might affect. Another dimension is the geographic location where the cyber event takes place. Some cyber events might have global reach, enlarging the consequences.

An additional critical parameter is the importance of the individuals and organization for the economy and society. A cyber attack on Critical Infrastructure can further enlarge the consequence by generating losses to other operations. For example, the failure of VISA or MASTERCARD systems would not only result in losses for these companies but it would likely generate significant losses to other businesses. This would apply to other Critical (Information) Infrastructure, and the losses could be identified according to the importance of the system for the operations of other individuals and organizations.

4.2.3 Global Aggregations of Cyber Risk

A report by Zurich and the Atlantic Council attempts to expose ''global aggregations of cyber risk'' as analogous to the risks associated with the U.S. sub-prime and 2008 financial crisis. ''Governments and forward looking organizations need to take a holistic view and look beyond these issues to broader risks, including the increasing danger of global shocks initiated and amplified by the interconnected nature of the internet'' (Zurich, 2014). An illustrative analogy between the financial markets and the Information Technology of organizations is over-leverage (Zurich, 2014). Over-leverage of companies in financial markets was created due to excessive debt, while organizations can over-leverage in IT due to overreliance on technology solutions. In both cases leverage is used to maximize their returns, however it is likely that the associated risks were underestimated, as it was proved by the financial crisis.

There are two crucial elements in this discussion. The first is a ''Lehman moment'', a catastrophic event that would spread in the web and cause major losses. Nevertheless a ''Lehman moment'' would encompass ignorance. While it was anticipated that Lehman Brothers could go bankrupt, none could foresee the chain of events that it triggered and led to the global financial crisis of 2008. In that sense even catastrophic events that seem to have a specific impact might actually end in unpredictable outcomes. The original ''Lehman moment'' can be regarded a global shock due to the scale of Lehman Brothers operations across the world. However, the channel that initially cascaded this global shock was rather localized; the U.S. subprime market.

The other element comprises of the propagation mechanism. The complexity and interconnections of financial products and markets, eventually transmitted this shock around the globe. The complexity of financial products might be a useful analogy to the increasing complexity of IT systems. It has been argued that the 2008 financial crisis is a demonstration that the causes of risks were camouflaged by excess complexity (Zurich, 2014). Even if this complexity is not excessive, it is still difficult to understand and predict the cascading risks and channels. Another analogy of the internet with the financial markets is that risks were assumed not to be correlated with each other. Nevertheless this is far from true: financial products and markets can be highly correlated. The same applies to Information Technology operations and systems.

In that sense it is not only complexity *per se* but also complexity due to the interconnected nature of risks that add to the uncertainty (Zurich, 2014). Thus, complexity and interconnections can facilitate systemic problems when 'extreme events', as global shocks, occur. ''Connecting to the internet means exposure to nth-order effects – risks from interconnections with and dependencies on'' other risk aggregations (Zurich, 2014). The report by Zurich identifies seven such aggregations (Internal IT enterprise, Counterparties and partners, Outsourced and contract, supply chain, disruptive

technologies, upstream infrastructure, external shocks) It can be however argued that due to ignorance they can be more common, or more severe, than expected (for example external shocks). An addition issue is a possible ''perfect storm''. Especially if a cyber ''Lehman moment'' coincides with other events, this interaction could cause losses of much larger scope, duration and intensity, similar to the series of events of the 2008 financial crisis (Zurich, 2014). It is even more difficult or rather impossible to identify and define the interconnections between other events and a ''Lehman moment'' before it happens, since it is principally unpredictable. In the worst case, catastrophic events would coincide and can significantly multiply the damage. This makes mitigation of risks increasingly difficult, if the outcomes are unknown or unknowable.

4.2.4 Global Catastrophic Risks Framework

A very useful framework in order to qualitative describe globally catastrophic or existential catastrophes was developed by Nick Bostrom (Bostrom and Cirkovic 2011, Bostrom (2013)). This framework is based on three factors: *severity* (how badly the population would be affected), *scope* (the size of the population at risk) and *probability* (how likely the disaster is likely to occur, according to the most reasonable judgement given currently available evidence). This model uses the first two factors and presents many advantages and flexibility. The scope includes not just the spatial size of the risk variable that we descried earlier but also, generational effects that are important regarding the duration and aftermath of the catastrophe.

Nevertheless, the major advantage of this framework is the way it treats probability. ''Probability can be understood in different senses…The uncertainty and error-proneness…of risk is itself something we must factor into our all-things considered probability assignments. This factor often *dominates* in low-probability high-consequence risks – especially those involving poorly understood natural phenomena, complex social dynamics, or new technology, or are that difficult to assess for other reasons'' (Bostrom, 2013). Therefore, this facilitates our analysis since most of the factors discussed above can be adapted to this framework. Scope encompasses both geographic spread, number of affected actors, and the importance of the damage. Moreover, its flexibility allows adding other concepts. In the discussion that follows, because the uncertainty and ignorance surrounding the estimation of probabilities we would shortly discuss about plausibility. Plausibility can be used as a distinct alternative to probabilities (Ramirez and Selin, 2014).

Qualitative risk categories.

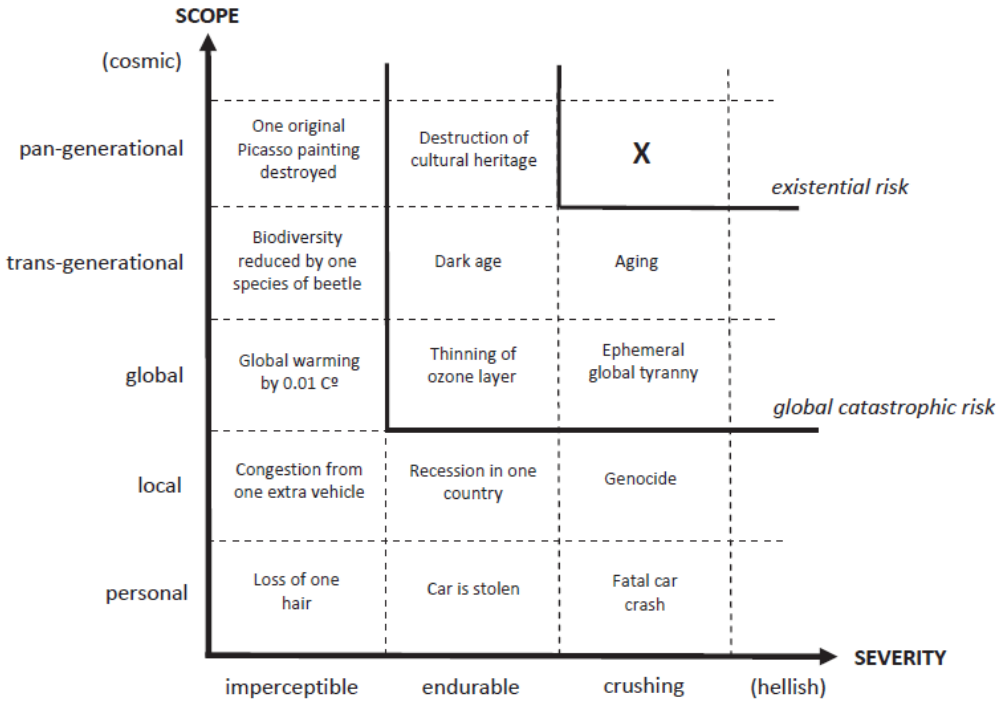

Figure 2: Qualitative risk categories from (Bostrom 2013).

4.3 Interdependencies and Asymmetric Threats

We have discussed correlations and interconnections. Special mention should be attributed to Interdependencies, a related concept and relevant to cyber risks. Often these concepts are used interchangeably and denote the same thing. However we would like to expand our analysis by focusing on complex interdependence (Keohane and Nye, 1977; Keohane and Nye, 1998), since it can provide an additional theoretical foundation. First of all, it should be emphasized that the context of international relations is central to insurance. Except political risk insurance, state relations influence numerous macro risk factors, as economic relations and defense and security. ''The information revolution alters patterns of complex interdependence by exponentially increasing the number of channels of communication in world politics'' (Keohane and Nye, 1998).

In addition, commercial and particularly, strategic information are valuable. The availability and confidentiality of such information in multiple channels increases the level of risk. Information can be used to convince and capture terrorists, prevent and resolve conflicts and enable countries to defeat adversaries (Nye and Owens, 1996). On the other hand because information reduces the ''costs, economies of scale, and barriers of entry to markets, it should reduce the power of large states and enhance the power of small states and non-state actors'' (Keohane and Nye, 1998).

This generates important asymmetries. A small group of hackers could disrupt, a relatively to their size and resources, large IT system. Another notable case is that of WikiLeaks: a single leak, amplified by a

single disseminating organization, has global consequences for a superpower. Asymmetric threats and the enabling of non-state actors adds even more complexity to the layers described before. The number of threats is therefore multiplied and consequently risks increase. Moreover, ambiguity regarding the nature and identification of these relative small actors makes the estimation of risks quite unpredictable.

4.4 Cyber Risks and Losses

Before 1989 the insurance industry did not experience a loss of more than $ 1 billion from a single event and since then catastrophes of the same magnitude have occurred (Kleinndorfer and Kunrether, 1999). As more and more people with larger insured wealth congregate in coastal areas this is to expect (even leaving out climate change). ''Megacatastrophes'', like Hurricane Andrew, seem therefore to happen more often and clearly demonstrate the limitations of relying on historical data in order to estimate future probabilities of losses (Actuarial Standard Board, 2000). Not only there are limitations to historical data but also cyber risks are new phenomena with continuously evolving technology and factors that are difficult to predict or even imagine. However, it is argued that there is likelihood for a global cyber catastrophic event (Zurich, 2014).

There are important methodological problems regarding probability estimation when assessing global catastrophic risks (Ord et al., 2010). Due to their high severity and scope even low probability risks need to be managed, but the probability of theory, model or calculation error in doing so is far higher than the risk probability itself, even when done carefully. This means that risk estimates should be regarded as suspect unless bounded by several independent estimates or other constraints.

A major concern for the private insurance industry is that it might not be able to provide coverage for some catastrophic events without the possibility of insolvency or a significant loss (Kleindorfer and Kunreuther, 1999). This is intensified when the scope and severity of the disaster are high. In the event of a 'cyber sub-prime' the losses can be massive and potentially result to insolvency. Even more worried would be the possibility of interconnected events that could amplify such crisis. The coincidence of catastrophes or a perfect storm would also have devastating effects. It is therefore essential to try and understand the cyber risks that can affect insurance. In this part to attempted to provide a theoretical analysis of risks in order to understand better cyber insurance. In the next part we attempt to put some flesh to this theoretical skeleton by providing real and imaginary examples.

5. Cyber Risks, Catastrophes and Ignorance

5.1 Identifying Cyber Risks

The discussion above indicated that the estimation of probabilities regarding cyber risks is in many cases difficult or impossible. The common methods are based on past events in order to define catastrophes and identify potential losses. These methods present significant limitations. There are various reasons for that. First of all cyberspace is a very dynamic environment. Information and Communication Technologies are continuously changing. The internet is constantly expanding. It is embedding existing devices and technologies, and is likely to integrate future innovations, generating the Internet of Things (IoT). The number of interconnected devices, individuals and organizations is therefore increasing. This

results in larger complexity and interdependence among devices with currently unknown functions and vulnerabilities.

In that sense if we assume that we know all the causes of potential losses then it might be a display of primary ignorance. On the contrary we can recognize our ignorance. We attempt to examine practical examples of cyber risks in three ways. The first is though the traditional approach on historic events. The second technique can be considered an expansion of that. We can infer based on historical events and develop potential cases, subject to uncertainty. Finally, we would build imaginary but plausible scenarios (Ramirez and Selin, 2014) in order to better understand cyber uncertainty and push the boundaries of ignorance. It can be said, that effective scenario formation and imagining might reduce ambiguity, enter the space of ignorance and therefore diminish it.

5.2 Existential and Global Catastrophic Risks

Bostrom's classification was developed in regard to threats to the entire future of the human species, or "merely" global disasters. The cyber counterpart would be risks that can escalate to such a level that they disrupt the global market or indeed current civilization. They are not merely uninsurably large, but terminal to most existing actors.

One possible example might be misuse of Artificial Intelligence (AI). Autonomous "smart" systems have already demonstrated potential for economically significant misbehavior such as the 2010 "Flash Crash", which at least in part was due to a systemic interaction of automatic trading agents. As technology advances AI is likely to become more powerful and ubiquitous, but there are significant control problems that remain to be solved. The fundamental issue is that superintelligent systems do not generally behave in human-compatible ways, and this can produce existential risk (Bostrom, 2013). More plausible scenarios involve unpredictable AI actions that are deliberate, autonomous and potentially very tenacious. It might include the paralysis of the internet globally by AI software embedded in the web infrastructure, or by automated adaptive hacking tools (e.g. descendants of the current DARPA Cyber Grand Challenge). In another scenario of endurable severity and local scope, AI systems can involve the disruption of operations in an organization. Of course severity may vary as well as scope. For example, if there is failure of ICT systems in a healthcare organization, it could result to loss of human lives. The disaster can diffuse globally if AI of a wide spread logistics database system decides not to allow access to information, or even worse, altering or destroying it (for example, because it interprets restoration or circumvention attempts as intrusion attempts). However, due to the fact that the capabilities of AI are very ambiguous, such scenarios are difficult to define.

It may be that there are workable solutions or that AI will never be too powerful, but these are risky bets. It seems that it is easy for people to overestimate their knowledge regarding AI (Yudkowsky, 2011). ''It may be tempting to ignore Artificial Intelligence because, of all the global risk …AI is hardest to discuss. We cannot consult actuarial statistics to assign small annual probabilities of catastrophe, as with asteroid strikes. We cannot use calculations from a precise, precisely confirmed model to rule out events or place infinitesimal upper bounds on their probability, as with proposed physics disasters. But

this makes AI catastrophes more worrisome, not less.'' (Yudkowsky, 2011). In that sense AI qualifies for uncertainty and ignorance. AI represents a risk that could go all the way into the extreme upper right hand box of the framework, but is both extremely uncertain and largely a future risk: it can be dealt with by R&D aimed at safe and beneficial uses of AI.

However, cyber risk also has strong interconnections to traditional catastrophic risks. Such risks include major technical disasters, conflict and war, and particularly total war with the use of Weapons of Mass Destruction (WMD).

The threat of a nuclear disaster is the most notable case by far. This is due to Stuxnet, a complex piece of malware interfering with Siemens industrial control systems and speculated that it was used for Iran nuclear program (NATO, 2013). Based on this precedent it can be argued that a nuclear catastrophe can be realized. The scale of these risks could largely vary. Cirincione (2011) and Ackerman and Potter (2011) discuss the global catastrophic risks of nuclear war and catastrophic nuclear terrorism. In both cases cyberspace is ''enabling'' these risks. In addition, the internet could provide the most cost – effective opportunity for adversaries. It enables states and non state actors and enhances their power. They can transform their capabilities and become nuclear threats that was not imaginable in the past. These asymmetric threats impose great challenges to insurance.

Stuxnet is considered to be a government cyber weapon. Rogue states might dedicate more resources in attaining such capabilities. The same could apply with terrorist groups. It is interesting to notice the multiple channels and complexity surrounding them. States relations can deteriorate and governments might decide to pursue cyber weapons targeting at nuclear as well as other military and critical infrastructure targets. The emergence of terrorists groups is also subject to uncertainty and ignorance. The rapid emergence of Islamic State, raising considerable resources, was not forecasted. Hamas and Hezbollah were established terrorist organizations and it can be alleged that they were capable of using cyber space. Nevertheless, it was believed by Israeli officials that these organizations used a criminal organization based in a former Soviet State to attack Israel's internet infrastructure during the January 2009 military offensive in the Gaza Strip (NATO, 2013).

Cyber weapons can also easily be spread to other actors, through theft or leakage (such as the exploits revealed in the attack on the security consultancy Hacking Team in 2015), trade, or by imitation: once Stuxnet was out in the wild, many other groups could analyze it and copy its tricks into their toolkits. The market for zero day exploits, driven by governments and security companies seeking new tools, has both the effect of incentivizing search for more vulnerabilities and inhibiting public disclosure of them since discoverers can gain more by secretly selling their find and agencies using them do not wish to lose their advantage. Even when vulnerabilities are revealed removing them is sometimes hard since they might be embedded in systems that cannot easily be upgraded (such as industrial systems or implants); this means that use of some cyber weapons can lead to more subsequent attacks on targets unrelated to the original target.

This case highlights the complexity generated by multiple channels and agents. It is consistent with the concept of n-th order effects (Zurich, 2014). The potential cooperation of different agents enhances

complexity due to the exponential number of combinations. Nexuses of adversaries can be formed, pooling resources and capabilities and thus magnifying cyber attacks. Nuclear catastrophes can have regional or global consequences (Cirincione, 2011) according to their intensity. Similar cyber global catastrophic scenarios can involve other types of WMD (i.e. Biological Weapons) or conflict and war.

5.3 Catastrophic Risks

War and conflict enabled by cyber space can present variations in consequences and scale. They can be also interdependent to other complex events. The cyber attack on Estonia in April 2007 was caused due to political frictions with Russia. On August 2008 the conflict of Russia and Georgia was accompanied by hacking activity from unknown foreign intruders which appeared to coincide with Russian military actions (NATO, 2013). A crucial observation is that the manmade causes of these cyber attacks are still not known with certainty. Another critical remark is that there are interdependencies between traditional kinetic power and cyber capabilities. An analogous example to the above cases is the takeover of missiles systems by hackers (there are claims this briefly happened to a German Patriot anti-aircraft defense system in 2015 (Storm 2015)). An action by hackers launching missiles could escalate to conflict or war.

Now imagine that these missiles are stationed in South Korea. And that they are launched by unknown hackers just after the cyber-attack on Sony, that FBI blamed on Pyongyang (BBC, 2015). Sony was about to release the Interview, a comedy about the assassination of the North Korea's Leader, indicating that the tensions in North Korea were running high. This could trigger events that could escalate to a catastrophe involving even nuclear weapons. A crisis in Korea could also cause negative impact on global markets due to the importance of the South Korean economy and trade interconnections. This example presents just a small part of complex interdependencies.

This example could have been even worse. Imagine now that the aforementioned events coincide with a release on WikiLeaks that North Korea is abandoned and isolated (a previous WikiLeaks cable suggested that Chinese officials expressed the desire to relinquish support for North Korea (The Economist, 2010)). North Korea can increase its level of alertness and retaliate severely, if they feel that the balance of power has changed against them and the regime is under existential threat. If these events coincide, then it is more likely to have a catastrophe. It is also possible that these events are fabricated and lead to an 'accident'. It is important to realize the multiple layers of complex interdependencies, which in many occasions can be unpredictable. The "WikiLeaks paradigm" is noteworthy because it can generate the conditions and instability which can consequently trigger other disasters.

In January 2011 the Canadian government reported an attack against its Department of National Defense as well as the Finance Department and Treasury Board, causing the disconnection of the main Canadian economic agencies from the internet (NATO, 2013). Once again there is ambiguity regarding the identity of attackers, and in addition Canadian counter-espionage agents were left scrambling to find how much sensitive information was compromised (Weston on CBC News, 2011). In that sense, it is not only difficult to forecast cyber-attacks but it is also unclear how much loss they caused. This makes mitigation harder. A proof of that is that cyber-attacks disrupted again the Department of Finance and

Treasury Board (MacDonald and King on WSJ, 2015). Thus, cyber-attacks are repeated with frequency on the same Critical Infrastructure.

Although these cyber – attacks might not qualify for catastrophic risks, it is hard to estimate the losses and associated costs. A considerable loss is the opportunity cost for not using the economic infrastructure of the Department of Finance and Treasury Board. Except Stuxnet, earlier, in 2003 Slammer worm disabled safety monitors in nuclear facilities and later, in October 2011, the Duqu Trojan hit Iran's nuclear facilities (Vaidya, 2015). This is another indication of the frequency of cyber - attacks on nuclear facilities, that could easily lead to major catastrophes.

Not only nuclear facilities are targeted but also energy infrastructure has experienced cyber-attacks. A notable case is Shamoon malware which destroyed 30,000 computers of Saudi Aramco in August of 2012. Interestingly enough, 5 days later a similar attack forced RasGas, one of the largest producers of liquid petroleum gas, to shut down its website and e-mails (BBC, 2012). Despite that it was not reported oil and gas supply was not disrupted, inference to these cases points that in the future this is a plausible consequence. Especially similar cyber - attacks can create shocks to the global economy due to interconnections, if they coincide with other events affecting the price of energy.

We have mainly focused on cyber events that produce high consequence outcomes on a single or small number of organizations affected. Nevertheless another important category of cyber events is when they have impact on a wide range of individuals and organizations. This type of events is likely to generate systemic global catastrophes. There are numerous examples. In respect to losses some cases are distinct. Code Red Worm as early as July 2001 infected 359,000 computers in less than 14 hours and caused estimated losses of $ 2.6 billion, Mydoom in 2004 skyrocketed losses to $38.5 billion, Conficker in 2008 infecting 11 million hosts with an estimated loss of $ 9.1 billion and the list is long (Vaidya, 2015). It should be noted that these disasters are systemic and with correlated global effects. They can therefore be considered potential ''Lehman moments'' for cyber insurance.

6. Conclusion: Summary, Challenges and Future Directions, The development of the Cyber Insurance Market

Cyber risks are rapidly evolving due to technological change and the systemic and complex nature of the ICT world, producing fundamental uncertainty and ignorance. Cyber insurance typically focuses on the less uncertain risks or constrains uninsurable risks to make them more manageable. Tools or practices for handling interdependent security, correlation, and information asymmetries as well as the lack of reinsurance would help the market grow.

While there are some cyber risks for which we can have sufficient information for quantifiable estimates, in the majority of cases uncertainty and ignorance prevail. This reflects the very limited, if any, information regarding the nature and evolution of cyberattacks. There are two basic problems in obtaining information. The first concerns the identity of attackers. The agents responsible for cyber threats present a large variety. They can range from large nations and militaries to organized crime and activists. The second issue, somewhat related to the first, are the resources and skills of these agents. The skills and sophistication can also substantially vary.

There are examples of single hackers that managed to cause catastrophic damage – like Michael Calce aka “MafiaBoy” – who has caused an estimated $ 1.2 bn damage with attacks on CNN, Dell, e-Bay and Amazon (Niccolai, 2000; Harris, 2006). Organized Crime Groups (OCGs) are getting more involved in cyber crime, and trends suggest considerable increases in scope, sophistication, number and types of attacks, number of victims and economic damage (Europol, 2014). Nevertheless except traditional OCGs that leverage their existing criminal activity there are many new organized criminals focusing solely on cyber crime. They are capable of building sophisticated and complex systems for stealing money and intellectual property at a ‘’grand scale’’ and it has been reported that in former Soviet Union there are 20 to 30 criminal groups that have reached ‘’nation-state level’’ capabilities (Ranger 2014).

It has been argued that many governments are developing their cyber offensive and defensive capabilities, and most particularly cyber intelligence operations. U.S. is further ‘’aggressively’’ enhancing its cyber capabilities. This is because of claims by officials about serious cyber threats from China and occurrence of high magnitude attacks, for example on Sony from North Korea (Mason and Hosenball 2015). There is considerable uncertainty and ignorance regarding the nature and source of many threats. Often the perpetrating agents cannot be identified. On top of that, there are allegations that some governments might employ hackers or even organized cyber criminals. In this dynamic environment, threat agents can easily change identity and diffuse their knowledge and innovative technologies. At the same time much information regarding these threats or attacks might remain unknown. Finally cyberterrorist acts have been anticipated, but none can predict their potential scale. An analogy with the unexpected rise of Islamic State (IS) might be drawn.

In general it is very hard or in some cases seems impossible to have information and predict the frequency and magnitude of cyberattacks. At the same it is also difficult to estimate the potential losses from cyberattacks due to interdependencies that can propagate shocks and strongly correlated risks. These, along with limited information regarding the reputation loss, opportunity cost from operation interruptions, valuation of intellectual property, among others, impose significant barriers to the development of insurance markets. In that sense uninsurable risks can remain. Nevertheless building better insurance and financial models, as some actuarial models referred above, is a first step to better understand and estimate cybersisks and relate them to insurance premiums. On top of that, incentives, regulation and liability provisions, new technologies for better security and investment in secure infrastructure can diminish some risks and facilitate the further development of cyber insurance markets.

It may be that these barriers are insurmountable, or that currently undiscovered tools – whether technological, actuarial or social – are ready to be found. The challenge is extremely hard, involving management of systemic risks with elements of extreme uncertainty and ignorance, but the market rewards would be equally grand.

References

Ackerman G. and Potter W., (2011). Catastrophic nuclear terrorism. A preventable peril In Bostrom N., Cirkovic M. (editors) (2011) Global Catastrophic Risks. Oxford University Press.

Actuarial Standard Board (2000) Treatment of Catastrophe Losses in Property/Casualty Insurance Ratemaking Actuarial Standard of Practice No. 39

Adams, A. and Sasse, M. A. (1999). Users are not the enemy. Communications of the ACM, 42(12):40–46.

Akerlof, G. A. (1970). The market for" lemons": Quality uncertainty and the market mechanism. The quarterly journal of economics, pages 488–500.

Anderson, R. (2003a). Cryptography and competition policy issues with trusted computing. In Proceedings of PODC'03, Boston, Massachsetts, pages 3–10.

Anderson, R. (2003b). 'trusted computing' and competition policy – issues for computing professionals. Upgrade, IV(3):35–41.

Anderson, R., Bhme, R., Clayton, R., and Moor, T. (2009). Security economics and european policy. In Pohlmann, N., Reimer, H., and Schneider, W., editors, ISSE 2008 Securing Electronic Business Processes, pages 57–76. Vieweg+Teubner.

Anderson, R., Bohme, R., Clayton, R., and Moore, T. (2007). Security economics and the internal market. ENISA.

Anderson, R. and Moore, T. (2007). Information security economics and beyond. Advances in Cryptology - CRYPTO07.

Anderson, R. and Moore, T. (2009). Information security: where computer science, economics and psychology meet. Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences, 367(1898):2717–2727.

Appari, A. and Johnson, M. E. (2010). Information security and privacy in healthcare: current state of research. International journal of Internet and enterprise management, 6(4):279–314.

Arrow, K. J. (1963). Uncertainty and the welfare economics of medical care. The American economic review, pages 941–973.

Baddeley, M. (2011). Information security: Lessons from behavioural economics. In Workshop on the Economics of Information Security.

Bandyopadhyay, T., Mookerjee, V. S., and Rao, R. C. (2009). Why it managers don't go for cyber-insurance products. Communications of the ACM, 52(11):68–73.

Baxter, G. and Sommerville, I. (2011). Socio-technical systems: From design methods to systems engineering. Interacting with Computers, 23(1):4–17.

BBC (2015). Sony cyber-attack: North Korea faces new US sanctions. 3rd January http://www.bbc.co.uk/news/world-us-canada-30661973

BBC (2012). Computer virus hits second energy firm, August 31st http://www.bbc.co.uk/news/technology-19434920

BIS (2014). Cyber essentials scheme. Technical report, UK Department for Business Innovation and Skills.

Bohme, R. (2006). A comparison of market approaches to software vulnerability disclosure. In Emerging trends in information and communication security, pages 298–311. Springer.

Bohme, R. (2010a). Security metrics and security investment models. In Advances in Information and Computer Security, pages 10–24. Springer.

Bohme, R. (2010b). Towards insurable network architectures. Information Technology, 52.

Bohme, R. and Kataria, G. (2006). Models and measures for correlation in cyber-insurance. In WEIS.

Bohme, R. and Schwartz, G. (2010). Modeling cyber-insurance: Towards a unifying framework. In WEIS.

Bolot, J.-C. and Lelarge, M. (2008). A new perspective on internet security using insurance. In INFOCOM 2008. The 27th Conference on Computer Communications. IEEE.

Bostrom, N (2013). Existential Risk Prevention as Global Priority, Global Policy 4: 15–31.

Bostrom N. and Cirkovic M. (editors) (2011) Global Catastrophic Risks. Oxford University Press.

Cabinet (2011). The uk cyber security strategy: Protecting and promoting the uk in a digital world. Technical report, UK Cabinet Office.

CESG (2012). 10 steps to cyber security: information risk management regime. Technical report, UK Department for Business Innovation and Skills.

Cone, B. D., Irvine, C. E., Thompson, M. F., and Nguyen, T. D. (2007). A video game for cyber security training and awareness. computers & security, 26(1):63–72.

Cirincione J. (2011). The continuing threat of nuclear war, In Bostrom N., Cirkovic M. (editors) (2011) Global Catastrophic Risks. Oxford University Press.

Constantin, L. (2013). Fbi and Microsoft takedown program blunts most citadel botnets. Computer World.

Crowley J. (2011). 10 Most Costly Cyber Attacks in History. BusinessPundit.com http://www.businesspundit.com/10-most-costly-cyber-attacks-in-history/

Europol, (2014). The Internet Organised Crime Treat Assessment (iOCTA) 2014. European Police Office, 2014

Friedman, A. (2011). Economic and policy frameworks for cybersecurity risks. Center for Technology Innovation at Brookings.

Gracie, A. (2015). Cyber resilience: a financial stability perspective. Cyber defence and network security conference London.

Hall, C., Clayton, R., Anderson, R., and Ouzounis, E. (2011). Inter-x: Resilience of the internet interconnection ecosystem. ENISA.

Halse, H. R. and Hoemsnes, J. (2013). Cyber-insurance and endogenous network formation. Master's thesis, Norwegian Unievrsity of Science and Technology.

Harris, James K. (2006), "Ethical Perspectives in Information Security Education", Issues in Information Systems VII (1): 181

Hofmann, A. (2007). Internalizing externalities of loss prevention through insurance monopoly: an analysis of interdependent risks. The GENEVA Risk and Insurance Review, 32(1):91–111.

Insurance Information Institute (2015) Catastrophes and Insurance Issues http://www.iii.org/publications/insurance-handbook/insurance-and-disasters/catastrophes-and-insurance-issues

Jaffee, D. M. and Russell, T (1997) Catastrophe Insurance, Capital Markets, and Uninsurable Risks The Journal of Risk and Insurance Vol. 64, No. 2, Symposium on Financial Risk Management in Insurance Firms (Jun., 1997), pp. 205-230

Johnson, B., Böhme, R., and Grossklags, J. (2011). Security games with market insurance. In Decision and Game Theory for Security, pages 117–130. Springer.

Johnson, B., Laszka, A., and Grossklags, J. (2014). The complexity of estimating systematic risk in networks. In Computer Security Foundations Symposium (CSF), 2014 IEEE 27th, pages 325–336. IEEE.

Juels, A., Kosba, A., and Shi, E. (2015). The ring of gyges: Using smart contracts for crime. *aries*, *40*, 54.

Keohane R. and Nye J. (1977). Power and interdependence: world politics in transition. Little, Brown

Keohane R. and Nye J., (1998) Power and Interdependence in the Information Age, Foreign Affairs, Vol. 77, No.5, pp. NATO (2013). The history of cyber attacks - a timeline. http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm

Kesan, J., Majuca, R., and Yurcik, W. (2005). Cyberinsurance as a market-based solution to the problem of cybersecurity: a case study. WEIS.

Kleindorfer P. and Kunreuther H., (1999) Challenges Facing the Insurance Industry in Managing Catastrophic Risk in Kenneth A. Froot, editor The Financing of Catastrophe Risk University of Chicago Press.

Knight F., (1921). Risk, Uncertainty, and Profit. Boston, MA: Hart, Schaffner & Marx; Houghton Mifflin Co.

Kunreuther, H. and Heal, G. (2003). Interdependent security. Journal of risk and uncertainty, 26(2-3):231–249.

Lelarge, M. and Bolot, J. (2009). Economic incentives to increase security in the internet: The case for insurance. In INFOCOM 2009, IEEE, pages 1494–1502. IEEE.

MacDonald A. and King C., (2015). Canadian Government Servers Hit by Cyberattack, Minister Says Hacking group Anonymous takes credit for the attack, which appeared to have affected several government websites. Wall Street Journal June 17th http://www.wsj.com/articles/canadian-government-servers-hit-by-cyberattack-minister-says-1434565899

Maillart, T. and Sornette, D. (2010). Heavy-tailed distribution of cyber-risks. *The European Physical Journal B*, *75*(3), 357-364.

Majuca, R. P., Yurcik, W., and Kesan, J. P. (2006). The evolution of cyberinsurance. arXiv preprint cs/0601020.

Marsh (2015). Uk cyber security: the role of insurance in managing and mitigating the risk. Technical report, UK HM Government.

Marsh and Zurich (2015). Uk 2015 cyber risk survey report. Technical report, Marsh Insights.

Mason, J. and Hosenball, M. (2015) Obama vows to boost U.S. cyber defenses amid signs of China hacking. Reuters, June 8, 2015.

Moore, T., Pym, D., and Ioannidis, C., editors (2010). Economics of Information Security and Privacy. Springer US.

Moran, J., Beeson, B., Mulligan, C., Sage, O., and Menapace, M. (2015). Examining the evolving cyber insurance marketplace. Homeland security digital library.

Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., and Sadhukhan, S. K. (2013). Cyber-risk decision models: To insure it or not? Decision Support Systems, 56:11–26.

Naghizadeh, P. and Liu, M. (2014). Voluntary participation in cyber-insurance markets. In Workshop on the Economics of Information Security (WEIS).

NAIC (2015). Principles for effective cybersecurity: Insurance regulatory guidance. National Association of Insurance Commissioners.

NATO (2013). The history of cyber attacks - a timeline.
http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm

Niccolai, James (2000-02-10), Analyst puts hacker damage at $1.2 billion and rising, InfoWorld, archived from the original on 2007-11-12, retrieved 2007-04-22.

Nye J. and Owens W., (1996). America's Information Edge. Foreign Affairs Vol. 75, No. 2, pp. 20-3 81-94.

Ogut, H., Menon, N., and Raghunathan, S. (2005). Cyber insurance and it security investment: Impact of interdependence risk. In WEIS.

Ord T., Hillerbrand R., and Sandberg A. (2010). Probing the improbable: methodological challenges for risks with low probabilities and high stakes Journal of Risk Research Volume 13, Issue 2, Special Issue: The Philosophy of Risk.

Overill, R. E. and Silomon, J. A. (2011). Single and Double Power Laws for Cyber-Crimes. *Journal of Information Warfare*, *10*(3), 29-36.

OxfordEconomics (2014). Cyber-attacks: effects on uk companies. Technical report, Oxford Economics (A report for Centre for the Protection of National Infrastructure).

Pal, R. (2012). Cyber-insurance for cyber-security: A solution to the information asymmetry problem. In SIAM Annual Meeting. Citeseer.

Pal, R. (2014). Improving network security through cyber-insurance. PhD thesis, UNIVERSITY OF SOUTHERN CALIFORNIA.

Pal, R. and Golubchik, L. (2010). Analyzing self-defense investments in internet security under cyber-insurance coverage. In Distributed Computing Systems (ICDCS), 2010 IEEE 30th International Conference on, pages 339–347. IEEE.

Pal, R. and Golubchik, L. (2011). Pricing and investments in internet security: A cyber-insurance perspective. CoRR, abs/1103.1552.

PWC (2015). 2015 information security breaches survey. Technical report, UK HM Government.

Ramirez R. and Selin C., (2014). Plausibility and probability in scenario planning. Foresight, Vol. 16 Iss: 1, pp.54 – 74

Ranger, S. (2014) Organised cybercrime groups are now as powerful as nations. ZDNet. June 9 2014

Roy D. and Zeckhauser R., (2013) Ignorance: Lessons from the Laboratory of Literature. M-RCBG Faculty Working Paper Series 2010-11

Sasse, M. A., Brostoff, S., and Weirich, D. (2001). Transforming the weakest linka human/computer interaction approach to usable and effective security. BT technology journal, 19(3):122–131.

Schneier, B. (2002). Computer security: Its the economics, stupid. In WEIS. WEIS.

Shetty, N., Schwartz, G., Felegyhazi, M., and Walrand, J. (2010a). Competitive cyber-insurance and internet security. In Moore, T., Pym, D., and Ioannidis, C., editors, Economics of Information Security and Privacy, pages 229–247. Springer US.

Shetty, N., Schwartz, G., and Walrand, J. (2010b). Can competitive insurers improve network security? In Acquisti, A., Smith, S., and Sadeghi, A.-R., editors, Trust and Trustworthy Computing, volume 6101 of Lecture Notes in Computer Science, pages 308–322. Springer Berlin Heidelberg.

Siegel, C. A., Sagalow, T. R., and Serritella, P. (2002). Cyber-risk management: technical and insurance controls for enterprise-level security. Information Systems Security, 11(4):33–49.

Sifalakis, M., Fry, M., and Hutchison, D. (2010). Event detection and correlation for network environments. Selected Areas in Communications, IEEE Journal on, 28(1):60–69.

Sommerville, I., Cliff, D., Calinescu, R., Keen, J., Kelly, T., Kwiatkowska, M., Mcdermid, J., and Paige, R. (2012). Large-scale complex it systems. Communications of the ACM, 55(7):71–77.

Storm, D. (2015). Did hackers remotely execute 'unexplained' commands on German patriot missile battery? Computerworld, Jul 8 2015

Swiss Re (2015) 05/2015 Underinsurance of property risks: closing the gap. Swiss Re.

The Economist (2010) WikiLeaks embarrasses North Korea: A glimpse into the dark Nov 30th http://www.economist.com/blogs/banyan/2010/11/wikileaks_embarrasses_north_korea

Thompson, M. (2014). Why cyber-insurance is the next big thing. In CNBC Report.

Toregas, C. and Zahn, N. (2014). Insurance for cyber attacks the issue of setting premiums in context. Cyber Security Policy and Research Institute, The George Washington University.

Vaidya T., (2015) 2001-2013: Survey and Analysis of Major Cyberattacks Working Paper http://arxiv.org/pdf/1507.06673.pdf

Varian, H. R. (2004). System reliability and free riding. In in Economics of Information Security, Kluwer 2004 pp 115, pages 1–15. Kluwer Academic Publishers.

WEF (2015). Global risks 2015. Technical report, World Economic Forum, Geneva.

Weston G., (2011) Foreign hackers attack Canadian government: Computer systems at 3 key departments penetrated, CBC News Feb 16th http://www.cbc.ca/news/politics/foreign-hackers-attack-canadian-government-1.982618

Yang, Z. and Lui, J. C. (2014). Security adoption and influence of cyber-insurance markets in heterogeneous networks. Performance Evaluation,74:1 – 17.

Yudkowsky E. (2011) Artificial intelligence as a positive and negative factor in global risk In Bostrom N., Cirkovic M. (editors) (2011) Global Catastrophic Risks. Oxford University Press.

Zeckhauser R. and Visusi K. (2008) Discounting Dilemmas: Editors' Introduction, Journal of Risk and Uncertainty 37(2), 95-106.

Zeckhauser R. (2008) Insurance. The Concise Encyclopaedia of Economics http://www.econlib.org/library/Enc/Insurance.html

Zeckhauser R., (2006) Investing in the Unknown and Unknowable ," Capitalism and Society 1(2), 2006, Berkeley Electronic Press, http://www.bepress.com/cas/vol1/iss2/art5

Zeckhauser R. (1996a) The economics of catastrophes Journal of Risk and Uncertainty May 1996, Volume 12, Issue 2, pp 113-140

Zeckhauser R. (1996b) Insurance and Catastrophes Geneva Papers on Risk and Insurance: Issues and Practice 78, January 1996, 3-21

Zhao, X., Xue, L., and Whinston, A. B. (2009). Managing interdependent information security risks: A study of cyber-insurance, managed security service and risk pooling. ICIS 2009 Proceedings, page 49.

Zurich (2014). Beyond data breaches: global interconnections of cyber risk. Risk Nexus Report of Zurich Insurance Group and Atlantic Council.

Zurich Insurance Group (2013) Modeling natural catastrophes Annual Report 2013. Zurich Insurance Group. http://www.zurich.com/2013/en/annual-report/risk-review/analysis-by-risk-type/insurance-risk/modeling-natural-catastrophes.html