ESTUDIOS DE ECONOMÍA APLICADA VOL. 36-1 2018 PÁGS. 181 – 194

Some Risk Analysis Problems in Cyber Insurance Economics*

DAVID RÍOS INSUA [a], AITOR COUCE-VIEIRA [a], KRESHNIK MUSARAJ [b]

[a] *Instituto de Ciencias Matemáticas, Consejo Superior de Investigaciones Científicas, Calle Nicolás Cabrera 13-15, Campus de Cantoblanco, 28049 Madrid, Spain. E-mail:* david.rios@icmat.es, aitor.couce@icmat.es

[b] *AXA Technology Services, AXA, Place de l'Iris 2 5-6, La Défense, 92400 Courbevoie, France. E-mail:* kreshnik.musaraj@axa.com

ABSTRACT

Cyber threats affect all kinds of organisations with frequent and costly impacts worldwide. Cyber insurance products have recently emerged with the potential of lowering the impact of cyberspace risks. However, they have yet to mature. In this paper we present several risk analysis models that may facilitate the implementation and adoption of cyber insurance. These models, described in terms of influence diagrams and bi-agent influence diagrams, provide a framework for estimating the economic impact of cyber risks that may face insurers and insurees as well as calculating their optimal risk mitigation and transfer strategies.

Keywords: Cybersecurity, Cyber insurance, Risk analysis, Adversarial risk analysis, Security Economics.

Algunos problemas de análisis de riesgos en Economía de los ciberseguros

RESUMEN

Las ciber amenazas afectan a todo tipo de organizaciones, causando frecuentes y costosos impactos globalmente. Recientemente, han surgido productos de ciberseguro con el potencial de reducir el impacto de los riesgos en el ciberespacio. Sin embargo, aún tienen que madurar. En este artículo presentamos varios modelos de análisis de riesgos que podrían facilitar la implantación y adopción de ciberseguros. Estos modelos, descritos como diagramas de influencia y diagramas de influencia bi-agente, aportan un marco para estimar el impacto económico de los ciber riesgos a los que se enfrentan aseguradores y asegurados, así como también para calcular sus estrategias óptimas de mitigación y transferencia del riesgo.

Palabras clave: Ciberseguridad, Ciberseguros, Análisis de riesgos, Análisis de riesgos adversarios, Economía de la Seguridad.

JEL Classification: C44, C73, D81, G22

* *Work supported by the EU's Horizon 2020 project 740920 CYBECO (Supporting Cyberinsurance from a Behavioural Choice Perspective). The work of DRI is supported by the Spanish Ministry of Economy and Innovation program MTM2014-56949-C3-1-R and the AXA-ICMAT Chair on Adversarial Risk Analysis.*

Artículo recibido en noviembre de 2017 y aceptado en noviembre de 2017
Artículo disponible en versión electrónica en la página www.revista-eea.net, ref. ə-36112

ISSN 1697-5731 (online) – ISSN 1133-3197 (print)

1. INTRODUCTION

A defining feature of our society is its almost pervasive digitalisation as reflected in the information systems that store confidential information and process valuable data; the social networks that host an important part of our personal information and activity; the cyber-physical systems that operate industries, vehicles or infrastructures; or the electronic services for shopping, banking, administration or politics, to name but a few. All kinds of organisations, from corporations to governments to SMEs[1], may be critically impacted by cyber attacks (Andress and Winterfeld, 2013). Indeed, their economic impact is outstanding and, consequently, cybersecurity has become an issue of major importance, both technically and financially.

Furthermore, attacks, espionage, insiders and breaches appear to increase in frequency, impact and sophistication (Lloyd's, 2017). For instance, the industry estimates that attacks costed as much as $ 450 billion globally in 2016, causing an impact over the global GDP[2] (0.8% in 2014) of a similar magnitude to drug trade (0.9%) or international crime (1.2%) (McAfee, 2017). There are, even, well-functioning black markets in the 'dark web' (Herley and Florêncio, 2010) that exchange attack tools or stolen information, providing incentives to skilled people to develop new hacking products and services. Cybersecurity is emerging as one of the major global concerns (World Economic Forum, 2017), as reflected in legislation and other initiatives to protect the digital infrastructure. Although some experts criticize an excessive hype about the potential disruptive capability of large-scale cyber attacks, cybersecurity is a truly relevant problem, due to the persistence, frequency and variety of cyber threats.

Such diversity of menaces may be classified according to their motivation, skill and constraints (Dantu *et al.,* 2007), and their ability to exploit, discover or create vulnerabilities on the targeted systems (DSB, 2013). The most formidable threats are the military units maintained by global powers; although they are constrained by the possible military, economical, and political repercussions of their attacks. Other sources closely related with social institutions or movements are 'hacktivists', a wide profile that could cover from hackers trying to prove their ability to those closely related with terrorist organizations. Insiders are important cyber threats and, indeed, the biggest source of incidents (Cardenas *et al.,* 2009), but they are also the easier to handle through a sound cybersecurity program. Additionally, profit-oriented cyber criminal groups are now mature as professional organizations, some of them employing dozens of hackers and managing large financial resources (Sastry *et al.,* 2008), carrying on a wide range of targeted and non-targeted attacks (Cardenas *et al.,* 2009). When it comes to

[1] Small and medium enterprises.

[2] Gross domestic product.

malware, they are usually developed with a goal-oriented behaviour (Li *et al.*, 2009) and, consequently, a sound approach is to treat them as adversarial actors and counter-attack them with behavioural approaches (Li *et al.*, 2009).

Furthermore, the concept of Advanced Persistent Threat has arisen to name the most sophisticated attacks (Command Five, 2011), which are patiently orchestrated operations seeking to stay hide while they consolidate their path for executing their final objective. Relevant cases (Command Five, 2011) include the 2007 Operation Aurora attacks against Google to obtain confidential data about their algorithms and Chinese dissidents; the 2011 Energetic Bear against European and US energy firms; the 2012 Shamoon attack that disabled 30.000 computers of Saudi Aramco (Brenner, 2013); and the 2013 credit card breach of 40 million customers of the US retailer Target (DeNardis, 2015); to name but a few. Attacks with physical consequences are also emerging, including the 2010 Stuxnet attack against an Iranian nuclear plant that disabled a fifth of its nuclear centrifuges (Brenner, 2013) or the attack on a German steelworks in 2014 that stopped their process (Lee *et al.*, 2014). Another notorious trend over the last years have been the indiscriminate ransomware attacks such as the 2017 Wannacry and Petya cases (Yaqoob *et al.*, 2017) that affected thousands of large and small organisations across the globe and for several hours.

Risk analysis (Cooke and Bedford, 2001) is fundamental for cybersecurity. With it, organizations can assess the risks affecting their assets and what safeguards should be implemented to reduce the likelihood of such threats or their impact, in case they are produced. Numerous frameworks have been developed to screen cybersecurity risks and support risk management resource allocation, including ISO 27005 (ISO, 2011), NIST SP 800-30 (NIST, 2012), or CORAS (Lund *et al.*, 2001). Similarly, diverse compliance and control assessment frameworks, like ISO 27001 (2013) or Common Criteria (2012) provide guidance on the implementation of cybersecurity best practices. These standards cover detailed security measures suggested for protecting the assets of an organisation against the cyber risks to which they are exposed.

Although they have virtues, particularly their extensive catalogues of threats and assets, much remains to be done regarding risk analysis: a detailed study of the main methodologies reveal that they often rely on risk matrices, which present shortcomings well documented in Cox (2008). Moreover, with counted exceptions like IS1 (HMG, 2012), such methodologies do not explicitly take into account the intentionality of some of the cyber threats, a key factor to forecast which threats would target the system. Given the variety of threats, as well as due to the specific complexity of factors affecting critical systems, we believe that, from the modelling point of view, not sufficiently sophisticated and detailed methods and processes are being used. Data is also a challenge in cybersecurity, a field with huge uncertainties (Anderson and Fuloria, 2010);

unlike other risky domains, it is difficult to obtain and analyse data, since organisations are reluctant to disclose data about intrusion attempts or consequences of attacks (Balchanos, 2012).

It is important to highlight how in recent years new cyber insurance products have been introduced, of very different nature and not in every country, by different companies. However, cyber insurance has yet to take off (Marotta *et al.*, 2017; Low, 2017), in spite that organizations are increasingly aware of their dependence on new technologies and on how information is a critical asset that must be secured so as to not incur in loss of customers, reputational damage and sanctions by regulators. Obstacles for researching and developing cyber insurance (Marotta *et al.*, 2017) include information asymmetry between agents that undermines trust, lack of data due to sensitivity concerns, and the difficulty of specifying rates of occurrence or damages.

In this paper, we sketch three major decision problems relevant in cybersecurity economics around the concept of cyber insurance. The first one outlines a more rigorous framework for risk analysis in cybersecurity. It serves an organisation to decide its best resource allocation strategy in terms of cybersecurity controls and cyber insurance. It also helps an insurance company to design their cyber products based on parametric variations. The second model serves an insurance company to decide their reinsurance portfolio. Finally, the third one supports also an insurance company in deciding whether to grant a given insurance product to a company.

We describe all three models in terms of influence diagrams (ID) and bi-agent influence diagrams (BAID), see Ortega *et al.* (2017). Square nodes refer to decisions; oval nodes to uncertainties, modelled as random variables; and hexagonal nodes to evaluations, modelled as utilities. We use different colours when we refer to nodes owned by different agents and mixed colours when referring to nodes shared by several of the involved agents. Arrows have the same interpretation as in Shachter (1986). For each model we sketch the corresponding economical problem and outline its general solution.

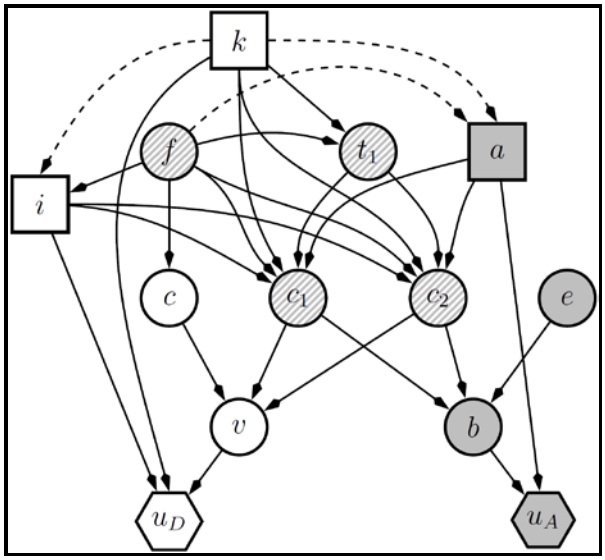
2. A CYBERSECURITY RESOURCE ALLOCATION MODEL

We first present an integrated risk analysis approach to facilitate cybersecurity decision-making. Our initial goal is to improve current risk assessment frameworks introducing a scheme that incorporates all relevant parameters, including decision-makers' preferences and risk attitudes (Clemen and Reilly, 2013) and the intentionality of adversaries. Moreover, we introduce decisions concerning cyber insurance adoption to complement risk reduction with risk transfer.

The problem is represented in Fig. 1 as a BAID. There are two agents involved: the Defender (*D*, she) who represents a company that needs to decide

its security resource allocation and the Attacker (*A*, he), who aims at attacking the Defender to obtain some benefit. White nodes refer to *D*; grey nodes refer to *A*; striped nodes are shared by both agents.

Figure 1
Cybersecurity resource allocation model



Source: Own elaboration.

The Defender is characterised by certain features *f*. She has an ICT[3] infrastructure evaluated against a performance measure *c* which we assimilate with a cost. Such performance is essentially uncertain. We simplify here by assuming that we integrate out all sources of external uncertainty within it. The system is exposed to a set of threats. Some of the threats are traditional (e.g., fire, energy blackout); other threats are cyber but may be seen as random because of their very nature (as with most computer virus); finally, others are intentional, both cyber (like DDoS attacks) or physical (like a bomb). Here we assume that there are just a generic random threat t_1 and an intentional cyber threat *a*. These threats have impacts over certain assets, which we limit here to two and designate them, respectively, c_1 and c_2. We integrate the results under normal circumstances and the impacts with a value function $v(c, c_1, c_2)$. Additionally, the features will usually influence the performance and eventual occurrence and impacts of the threats.

[3] Information and communications technology

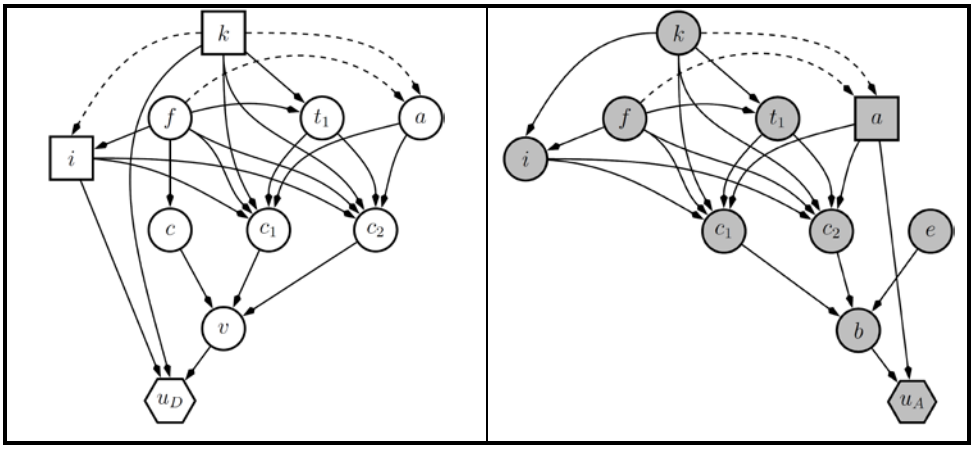
In order to reduce such impacts, the Defender may implement a portfolio k of security controls (e.g., fire detectors, firewalls, administration procedures) to reduce risk (probability and impact), as well as acquire an insurance i to transfer risk. The insurance product may come from several providers, cover traditional or cyber threats, among other defining features. The insurance cost, likewise, will also depend on the assets and architecture to be protected. Note that we could include the cyber insurance within the portfolio of security controls. However, it is recommendable to separate them, since premiums will typically depend on the security controls deployed (and the value of assets at risk). There would usually be constraints regarding the decisions to be made, legal, financial or technical. The Defender aims at maximising expected utility, where her utility u_D caters for her preferences and risk attitudes.

The Attacker also makes decisions. He has to choose what attack a to implement. We assume here that prior to making such decision he is capable of probing the defender and, therefore, observing what defences and features are in place. Depending on the impacts, the actions he implements and other external uncertainties e affecting him, like whether he is detected or not, he obtains his consequences b. We also assume that the Attacker aims at maximising expected utility, where his utility u_A caters for his preferences and risk attitudes, which depends also on the cost of his actions.

The Defender aims at solving her problem reflected in Fig. 2a.

Figure 2
Cybersecurity risk analysis

Figure 2a: Defender problem *Figure 2b: Attacker problem*



Source: Own elaboration.

To solve it, we need to assess:

- The probabilities of the threats happening, given the portfolio of security controls implemented as well as the organisation's features, which, under convenient conditional independence conditions, are $p(t_1|k,f)\ p(a|k,f)$.
- The impacts of the threats, should they happen, given the portfolio of security controls implemented and the insurance product adopted which, again, under suitable conditional independence conditions is $p(c_1|t_1,a,i,k,f)\ p(c_2|t_1,a,i,k,f)$.
- The performance of the system given by $p(c|f)$.

The insurance product will typically have a cost which is a function of the security control portfolio adopted and the features of the company $c_i = g(k,f)$. Once we have assessed all these quantities, we would need to find the portfolio of security controls and insurance that maximise expected utility. When portfolio *k* is implemented together with insurance *i*, the expected utility is

$$\psi(k,i|f) = \int\ldots\int u_D\left(v(c,c_1,c_2),c_i\right) p(t_1|k,f)\, p(a|k,f)\, p(c_1|t_1,a,i,k,f) \times p(c_2|t_1,a,i,k,f)\, p(c|f)\, dt_1\, da\, dc_1\, dc_2\, dc.$$

We seek, then, the maximum expected utility portfolio-insurance pair under the relevant restrictions, that is,

$$\max_{k\in K,\, i\in I} \psi(k,i|f),$$

where *K* represents the constraints over the portfolio and *I*, the insurance catalogue. The pair (k,i) could be further restricted jointly, e.g. by a common budget constraint or certain legal or technical requirements. In principle, all the above elements are standard, and may be modelled through statistical methods (if data are available) and/or expert judgement (Cooke and Bedford, 2001), except for $p(a|k,f)$ which entails a strategic element: it describes the probability that the Defender gives to receiving the attack a from the Attacker had portfolio *k* been adopted when the features are *f*.

In order to assess it, as in adversarial risk analysis (ARA), (Banks *et al.*, 2015), we may consider the Attacker problem reflected in Fig. 2b. Then, the Defender should analyse such problem. Specifically, for a given portfolio *k* and features *f*, assuming that the Attacker maximizes expected utility, he would compute for each attack *a* the corresponding expected utility

$$\psi(a|k,f) = \int\ldots\int u_A(a,b)\, p_A(t_1|k,f)\, p_A(c_1|t_1,a,i,k,f) \times p_A(c_2|t_1,a,i,k,f)\, p_A(b|c_1,c_2,e)\, p_A(e)\, dt_1\, dc_1\, dc_2\, db\, de.$$

where u_A and p_A are, respectively, the utility function and probability distributions of *A*. He would then find the attack $a^*(k,f)$ that maximises expected utility, through

$$\max_{a \in A} \psi_A(a|k, f)$$

where A is his attack set. However, the Defender will not typically know u_A and p_A. Suppose we are capable of modelling her uncertainty about them with random probabilities P_A and a random utility function U_A (Banks *et al.*, 2015). Then, the optimal random attack, given the defence k and the features f, is

$$A^*(k, f) = \arg\max_{a \in A} \int \ldots \int U_A(a,b) P_A(t_1|k, f) P_A(c_1|t_1, a, i, k, f)$$
$$\times P_A(c_2|t_1, a, i, k, f) P_A(b|c_1, c_2, e) P_A(e) dt_1 \, dc_1 \, dc_2 \, db \, de.$$

Finally, the distribution over the attacks we were looking for satisfies

$$p(a|k, f) = P\left(A^*(K, f) = a\right),$$

assuming that A is discrete (when referring to attack options). Such distribution would be typically estimated by simulation by sampling from the random utilities and probabilities

$$F = \left(U_A, P_A(t_1|k, f), P_A(c_1|t_1, a, i, k, f), P_A(c_2|t_2, a, i, k, f), P_A(b|c_1, c_2, e), P_A(e)\right)$$

assess the corresponding optimal attack and, finally, estimate the attack probabilities through the Monte Carlo frequencies.

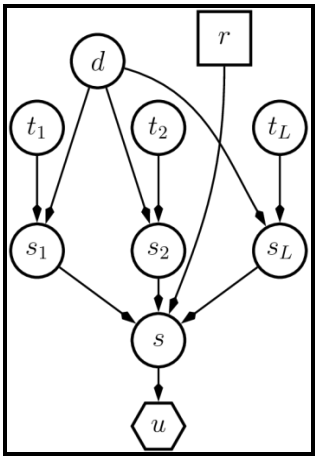
This model can be viewed as a template that can be extended further to include bigger numbers of threats, of attackers or assets; it can also contain additional types of costs or other system performance objectives say, referring to safety, reputation or legal aspects. It may be adapted to model attackers who do not rely on probing the defender or other interactions between the agents (e.g., the sequential defence-attack-defence). Finally, several utility nodes can be incorporated to describe the preferences and risk attitudes for multiple stakeholders.

The model has been introduced to support a company in deciding the best security portfolio and insurance combination given certain constraints. It may be also used in a parametric manner to set cyber insurance prices and coverages as well as to segment the market, as we briefly outline. First, the insurance product prices were c_i, and their impact was reflected in the utility function $u_D(v(c, c_1, c_2), c_i)$. Consequently, we could determine the optimal portfolio and insurance product $(k^*, i^*(c_i)|f)$ to make decisions about the optimal investment and insurance product, given the prices, for a company with features f. This would inform the pricing process: for a given profile f, we could determine the maximum prices that a customer would be willing to pay to acquire a certain insurance product. Moreover, we could define the set $F(i) = \{f: i^* = i\}$ which comprises all companies (as characterised by their features f) such that their optimal insurance product is i. This could constitute the basis to segment a cyber insurance market.

3. CYBER REINSURANCE

We describe now another major problem for an insurance company referring to reinsurance, described in Fig. 3 through an ID.

Figure 3
Cybersecurity reinsurance model



Source: Own elaboration.

Suppose that an insurance company has segmented the market in several sectors, possibly as outlined in Section 2. To fix ideas, in the ID in Figure 3 we have included three segments referring to standard SMEs S_1; ICT SMEs S_2; and, finally, large enterprises S_L. In standard SMEs, ICT is just a support function and they rarely employ dedicated staff. In ICT SMEs, this technology is critical and core; they typically employ dedicated staff, possibly even focusing on cybersecurity. Large enterprises maintain an important ICT infrastructure and usually have in-house ICT, security and information departments. Each of them would have their own specific threats, which we, respectively, summarise through t_1, t_2 and t_L. Moreover, there will typically be common threats which we summarise through d. This allows us to induce the potential accumulation effect that may hold in this application area.

The effects of these threats in the insurance claims of each segment is established through s_1, s_2 and s_L. For assessing them, we would consider the size of each segment and aspects such as ICT systems, cybersecurity and financial resources, features, assets and threats at each segment, much as we did in the first model. Nodes s_1, s_2 and s_L summarise all of this for each segment.

Node s aggregates the effects s_1, s_2 and s_L over various segments, but are also compensated by the reinsurance decision r, so that $s = g(s_1, s_2, s_L, r)$. The

reinsurance decision could be restricted by, say, financial, legal or compliance requirements. It could actually refer to a portfolio referring to several reinsurers. Then, once we are capable of building $p(d)$, $p(t_i)$, $p(s_i|t_i, d)$ – with $i = 1,2, L$ - and the utility function u, for the insurance company, we would aim at maximising

$$\max_r \int \ldots \int u\left(g\left(s_1, s_2, s_L, r\right)\right) p\left(d\right) \times \prod_i p\left(t_i\right) \prod_i p\left(s_i|t_i, d\right) ds_1\, ds_2\, ds_L\, dt_1\, dt_2\, dt_L.$$

to find the optimal reinsurance decision of the insurance company.

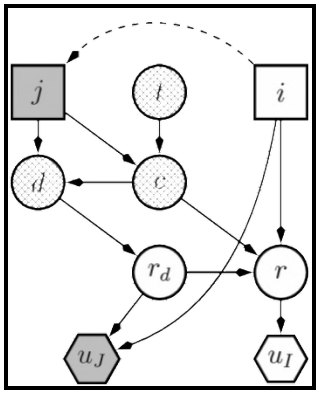
Again this model serves as a template in that it can be extended to include further details. The number of common and specific threats can be extended, for instance, to include the most common threats for each segment, information that could be derived, e.g., from the claims history or cybersecurity industry reports. Segments could be extended, too, for instance, differentiating by sector or country, or between medium and microbusiness (less than nine employees). Moreover, a dynamic model could be constructed, replicating the threats and effects nodes over several periods, typically years. This could be interesting as cyber insurance presents two very relevant dynamic aspects. First, cybersecurity is continuously evolving, with some types of attacks becoming more frequent or harmful for a number of years or some sectors suffering more attacks. Second, cyber insurance is an emerging market so the size of insuree segments could rapidly grow over time.

4. GRANTING INSURANCE PRODUCTS

In our third and final model, we consider a problem relevant for an insurance company which refers to the decision of granting or not an insurance product to a potential customer. We describe the problem as a BAID in Fig. 4. There are two agents involved: the insurance company (*I*, white nodes) and the customer (*J*, grey nodes). Striped nodes are shared by both agents.

The insurance company needs to decide whether to grant or not an insurance product (*i*) to the customer which, in turn, faces threats, summarised in *t*. These threats determine the likelihoods and sizes of claims, as discussed in previous sections. However, the claim likelihood (*c*) is also affected by costumer decisions regarding cybersecurity compliance and care in terms of insurance liability (*j*). This involves behaviours that could reduce cybersecurity effectiveness (e.g., adherence to security policy, security control maintenance, misuse) or, worst case, committing fraud. Should a claim happen, the insurer or a supporting cybersecurity auditor would typically perform a forensic investigation on the claim, aimed at detecting fraud. The claim finally awarded to the insuree by the insurance company (*r*) would depend on the initial claim and the result of the detection report (r_d). Both the insurance company and the insuree would aim at maximising their respective utilities (u_I and u_J).

Figure 4
Insurance granting decision



Source: Own elaboration.

This is again an ARA problem, structurally resembling that in Section 2. Then, the process would go through two stages: the adversarial problem first (costumer), and the insurance company one, second. The decision faced by the insurance company is a standard decision analysis problem with the extra ingredient of having to forecast whether the client decisions.

To do so, we consider the customer problem; as in the Attacker problem of Section 2, we model his decision as uncertain and use random utilities and probabilities to build the customer expected utility and find his random optimal decision which we use to estimate the desired fraud probabilities, that would be estimated through Monte Carlo simulation. This, in turn, feeds the expected utility of the insurance company to finally decide whether to grant or not the product. Finally, we seek the maximum expected utility decision for the insurance company.

Again, this model serves also as an extendible template. Insurer decisions could include alternative insurance products. Other behaviours of random nature (e.g., errors) or features of the customer could be added as uncertain nodes that precedes the claim node. Additionally, more companies could be added (replicating the grey and shaded nodes). The claim node could be bifurcated in different types of claims. Indeed, an adversarial threat could substitute or complement the random threat node to enable the assessment of the potential impact in claims of a specific cyber attack (this could be relevant during a surge of a type of cyber attack or during a notorious incident like WannaCry).

5. DISCUSSION

Risk analysis and management frameworks used in current cybersecurity practice provide thorough knowledge bases for understanding cyber threats, security policies and technologies and the consequences over the assets that depend on digital infrastructures. However, these frameworks provide risk analysis methods that are not sufficiently formalised, neither comprehensive enough. Indeed, most of them suggest risk matrices as their main analytic method, which provide a fast but limited analysis of risks. In addition, the frameworks do not contemplate, for example, methodologies to analyse the adversarial aspects of risks or the incorporation of cyber insurance.

We have presented three decision making models in relation with cybersecurity and, specially, cyber insurance. The first one refers to cybersecurity resource allocation. On one hand, it allows companies to decide their best security portfolio, including the corresponding cyber insurance contract. On the other, it allows a cyber insurance company to design its products. Once with them, we may formulate the cyber reinsurance problem, which allows a company to decide how to allocate its reinsurance portfolio. Finally, we have illustrated the insurance granting decision.

In companion papers we shall illustrate in detail and numerically the subtleties of various models. There are other relevant applied economics problems in the field. Specially relevant is the behaviour of agents in the cybersecurity arena. The effective implementation and maintenance of a cybersecurity program and culture is key for minimising risk and, thus, the mechanisms that incentivise adherence to such program or the economics of its implementation are relevant aspects to be studied. When it comes to threat agents, the study of the strategic interaction of adversarial threats could be further extended, as many hackers, more profit-oriented, face a choice problem when selecting their targets. A third interaction, on the protection side, is between governments establishing cybersecurity regulations and the organisations at risk, which could be enriched with the incorporation of cyber insurance companies. Other interesting interactions could be between threat sources (i.e., the agent that wants the attack) and threat perpetrators (i.e., the agent that undertakes the actual attack). Other cybersecurity economic problems, more present in the literature, could be the study of deep web markets related with cyber attacks, models for the economic impact analysis of cyber risks at a macroeconomic or market level or, less analysed, the socioeconomic conditions that incentivise becoming a hacker.

BIBLIOGRAPHY REFERENCES

ANDERSON, R. and FULORIA, S. (2010). "Security Economics and Critical National Infrastructure". In MOORE, T., PYM, D. and IONNIADIS, C. (ed.): *Economics of Information Security and Privacy* (pp. 55-56). Boston (MA, USA): Springer.

ANDRESS, J. AND WINTERFELD, S., (2013). C*yber Warfare: Techniques, Tactics and Tools for Security Practitioners*. Waltham, MA (USA): Syngress.

BALCHANOS, M.G. (2012). *A Probabilistic Technique for the Assessment of Complex Dynamic System Resilience*. Ph.D. Thesis, Georgia Institute of Technology (USA).

BANKS, D., RÍOS INSUA, D. and RÍOS, J. (2015). *Adversarial Risk Analysis*. New York (USA): Chapman and Hall/CRC.

BRENNER, J.F. (2013). "Eyes Wide Shut: The Growing Threat of Cyber Attacks on Industrial Control Systems". *Bulletin of the Atomic Scientists*, Vol. 69, No. 5, pp. 15-20.

CARDENAS, A., AMIN, S., SINOPOLI, B., GIANI, A., PERRIG, A. and SASTRY, S. (2009). "Challenges for Securing Cyber Physical Systems". *Workshop on Future Directions in Cyber-Physical Systems Security*.

CLEMEN, R. T. and REILLY, T. (2013). *Making Hard Decisions with Decision Tools*. Independence. KY (USA): Cengage Learning.

COMMAND FIVE PTY LTD, Australia (2011). *Advanced Persistent Threats: A Decade in Review*.

COOKE, R. and BEDFORD., T. (2001). *Probabilistic Risk Analysis: Foundations and Methods*. Cambridge (UK): Cambridge University Press.

COX, L. A. (2008). "What's Wrong with Risk Matrices?". *Risk Analysis*, Vol. 28, No. 2, pp. 497–512.

DANTU, R., KOLAN, P., AKL, R. and LOPER, K. (2007). "Classification of Attributes and Behavior in Risk Management Using Bayesian Networks". *IEEE Intelligence and Security Informatics, 2007*, pp. 71-74.

DENARDIS, L. (2015). "Five Destabilizing Trends in Internet Governance". *I/S: A Journal of Law and Policy for the Information Society*, Vol. 12, No. 1, pp. 113-133.

DEFENSE SCIENCE BOARD, DEPARTMENT OF DEFENSE, USA (2013). *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat*.

HERLEY, C. and FLORÊNCIO, D. (2010). "Nobody Sells Gold for the Price of Silver: Dishonesty, Uncertainty and the Underground Economy". In MOORE, T., PYM, D. and IONNIADIS, C. (ed.): *Economics of Information Security and Privacy* (pp. 33- 53). Boston (MA, USA): Springer.

NATIONAL TECHNICAL AUTHORITY FOR INFORMATION ASSURANCE, UK (2012). *HMG IA Standard Number 1*.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (2013). *ISO/IEC 27001:2013, Information Technology - Security Techniques - Information Security Management Systems - Requirements*.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (2011). *ISO/IEC 27005:2011, Information Technology - Security Techniques - Information Security Risk Management*.

LEE, R. M., ASSANTE, J. and CONWAY, T. (2014). *ICS Defense Use Case Dec 301, 2014 - German Steel Mill Cyber Attack*. SANS Institute, USA.

LI, Z., LIAO, Q. and STRIEGEL, A. (2009). "Botnet Economics: Uncertainty Matters". In Johnson, M.E. (ed.): *Managing Information Risk and the Economics of Security* (pp. 245-267). Boston (MA, USA): Springer.

LOW, P. (2017). "Insuring Against Cyber-Attacks". *Computer Fraud & Security*, Vol. 2017, No. 4, pp. 18-20.

LLOYD'S, UK (2017). *Counting the Cost - Cyber Exposure Decoded*.

LUND, M.S., SOLHAUG, B. and STØLEN, K. (2010). *Model-Driven Risk Analysis: The CORAS Approach*. Heidelberg (Germany): Springer.

MANIMARAN, C.-C., TEN, G., and LIU, C.-W. (2008). "Vulnerability Assessment of Cybersecurity for SCADA Systems". *IEEE Transactions on Power Systems*, Vol. 23, No. 4, pp. 1836-1846.

MAROTTA, A., MARTINELLY, F., NANNI, S., ORLANDO, A., and YAUTSIUKHIN, A. (2017). "Cyber-Insurance Survey". *Computer Science Review*, Vol. 24, pp. 35-61.

MCAFFE (USA) (2014). *Net Losses: Estimating the Global Cost of Cybercrime*.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, USA (2012). *NIST Special Publication 800-30 Rev. 1 - Guide for Conducting Risk Assessments*.

ORTEGA, J., RIOS INSUA, D., and CANO, J. (2017). "Adversarial Risk Analysis for Bi-agent Influence Diagrams". *XXXVI Congreso Nacional de Estadística e Investigación Operativa*.

SASTRY, S., CARDENAS, S., and AMIN, A.A. (2008). "Research Challenges for the Security of Control Systems". *Proceedings of the 3rd Conference on Hot Topics in Security*: pp. 6:1-6:6.

SHACHTER, R.D. (1986). "Evaluating Influence Diagrams". *Operations Research* Vol. 34, No. 6, pp 871-882.

THE COMMON CRITERIA RECOGNITION AGREEMENT MEMBERS (2009). *Common Criteria for Information Technology Security Evaluation, Version 3.1 Release 4*.

ZHUGE, J., HOLZ, T., SONG, C., GUO, J., HAN, X., and ZOU, W. (2009). "Studying Malicious Websites and the Underground Economy on the Chinese Web". In Johnson, M.E. (ed.): *Managing Information Risk and the Economics of Security* (pp. 225-244). Boston (MA, USA): Springer.

YAQOOB, I., AHMED, E., UR REHMAN, M.H., AHMED, A.I.A., AL-GARADI, M.A., IMRAN, M., and GUIZANI, M. (2017). "The Rise of Ransomware and Emerging Security Challenges in the Internet of Things". *Computer Networks*, [In Press].

WORLD ECONOMIC FORUM (2017). *The Global Risks Report 2017*. Geneva (Switzerland): World Economic Forum.