Economics, Security and Innovation

Massimo Felici

Security and Cloud Lab
Hewlett-Packard Laboratories
Long Down Avenue
Bristol BS34 8QZ
United Kingdom
massimo.felici@hp.com

Abstract. This paper takes into account an economic perspective of security and innovation. In particular, it discusses aspects of economics that may be relevant in order to assess and deploy security technologies. At the micro level of analysis, as an example, this paper highlights discussions on the economics of security in the cloud. *Do we really understand the economics of security in the cloud? Are there economic models that capture operational security in the cloud?* Early work at HP Labs on trust economics underpins a systematic approach to information security decision-making and risk management. The results on trust economics highlight how economics may drive operational security and the deployment of security technologies. At the macro level of analysis, drawn from ongoing work within the Security and Trust Coordination and Enhanced Collaboration, this paper links economics to innovation in cyber security and privacy. Despite the R&D investments in cyber security and privacy, the general perception is that security and privacy technologies are deployed ineffectively. This paper also presents an integrated framework taking into account market perspectives that may support identifying suitable R&D strategies and assessing their impact.

Keywords: Economics · Innovation · Cyber Security and Privacy

1 Introduction

Despite the continuous investment in cyber security and privacy, continuous threats and attacks remind us that the Internet is a vulnerable ecosystem (or cyberspace). This section recalls some economic drivers for innovation in cyber security and privacy. In particular, this section highlights three main perspectives: economics of information security, economic barriers for information security, and innovation in cyber security and privacy – *How much does information security cost? How complex is information security? How to support innovation in cyber security and privacy?*

Recent trends in information security highlight a situation that is no longer sustainable [1]. On the one hand, the spending on information security has been increasing constantly. On the other hand, the severity and impact of data breaches are getting bigger too. This somehow exacerbates the economic risk of information security. Simply,

the increasing spending in information security combined with bigger data breaches make the (economic) risk of information security quite severe.

Further analysis of the economics of security for the Internet points out some economic barriers to information security [2]. From technical and organisational viewpoints, two major issues arise: information asymmetry (that is, one party to a transaction has better information than another one) and lack of diversity in platforms and networks. However, these issues also suggest information security as a market differentiator. From an impact viewpoint, externalities are still unclear. Effects (positive or negative) on third parties of economic transactions are often questionable and quite subjective. Future research should advance the understanding of the economic impact of security technologies (breaches). From a legal viewpoint, liability dumping practices and fragmentations of legislation and law enforcement create mistrust. This stresses the need for legal cooperation supporting a free market and trustworthy cyberspace.

Unfortunately, despite the investment in information security the Internet is still vulnerable to various security threats – the perception is of untrustworthiness. A critical analysis of research and development (R&D) activities in cyber security points out that efforts towards innovation have been ineffective in deploying those security mechanisms that are needed for a trustworthy Internet [3]. This problem is characterized by the *"valley of death"*, as shown in **Fig. 1**, faced by research and development initiatives in cyber security [4]. A critical analysis of such problem points out various issues (e.g. insufficient awareness of complexity of technology transfer, misalignment between market and threat environment) and success factors (e.g. customer and market needs, early involvement, value creation) [4].

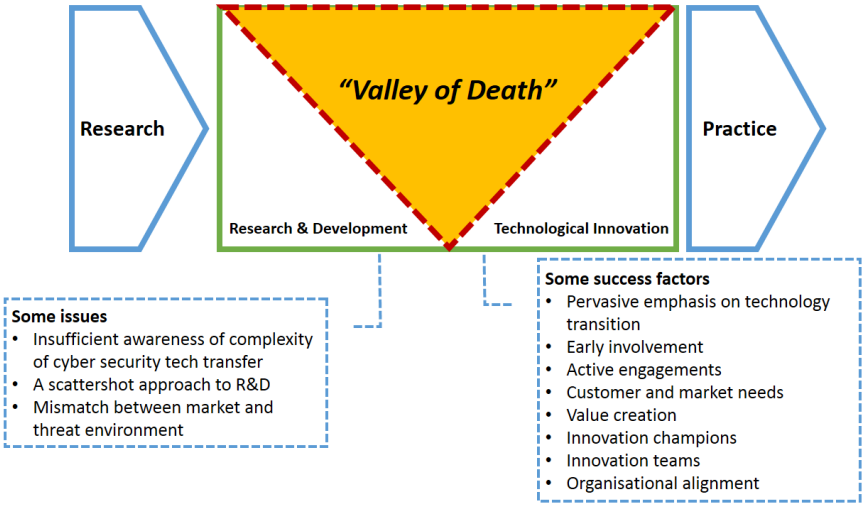

Fig. 1. Transitioning Cyber Security Research into Practice

This paper is concerned with the economic and market aspects of innovation in cyber security and privacy. It takes into account two perspectives. At the micro level of analysis, it looks at the problem of economics of security in the cloud. Understanding the

economics of security (within a specific domain such as the cloud) enables risk-mitigation and deployment strategies for the cloud. At the macro level of analysis, it looks at the problem of road mapping innovation strategies by identifying contingencies between research, technology and market. This paper is structured as follows. Section 2 is concerned with the economics of security in the cloud. It identifies different issues faced by researchers and practitioners. Understanding and addressing such issues would enable risk mitigation and deployment strategies driven by economics. Early work at HP Labs on trust economics underpins a systematic approach to information security decision-making and risk management. Section 3 focuses on innovation in cyber security and privacy. It presents an integrated framework for innovation management. It also discusses some preliminary trends drawn from consultations with stakeholders. Section 4 points out some concluding remarks.

2 Economics of Security in the Cloud

This section takes into account a micro perspective of economics. With micro in this case we mean aspects of economics that may be relevant for operational deployment of information and communication technology (ICT). In particular, we analyse the cloud computing domain as one of the most relevant shift in the way ICT is deployed across differ industries. Recent studies forecast *"worldwide public IT cloud services spending to reach nearly $108 billion by 2017 as focus shift from savings to innovation"* [5]. Despite the potential market, further adoptions of cloud computing would require also to take into account also the necessity, hence the cost, of securing the cloud itself [6]. Hereby we are not questioning the benefit of cloud computing or its security, but make sure that the cost associated with securing the cloud is not overlooked (e.g. this may involve various changes in organisational practices too). Cost-benefit analyses are central to the adoption of any technology.

2.1 Modelling the Economics of Security.

We argue that the better our understanding of the economics of the cloud the better security itself. Unfortunately, despite the research effort in modelling the economics of cyber security, results are yet patchy [7]. Various models have been proposed capturing the economics of cyber security, although they often provide very different analytical results [7]. It is also difficult to assess the validity of modelling results due to a continuous evolving landscape in cyber security (e.g. new threats, new attacks, etc.). Information about cyber security threats and attacks are continuously updated by surveys and new data, which at the same time 'invalidate' (or make irrelevant) previous studies. It is therefore necessary to assess the effectiveness of implemented security measures. Unfortunately, operational information about security measures are seldom available.

Various studies (models) on economics of security provide different account of cyber security. However, in order to benefit from such studies we need first to understand and to compare the underlying economic models of cyber security [7] – *Is the*

model complete? Is the model consistent? Is the model transparent? Is the model accurate? Is the model conservative? Does the model provide insight? – Answering such questions is necessary in order to interpret any aspect of economics of security.

We discussed similar points at a dedicated workshop on the Economics of Security in the Cloud (ESC workshop, collocated with the IEEE CloudCom 2013 conference, Bristol, UK). The discussions with presenters and participants at the workshop gave rise to interesting insights:

- ***What is the cloud?*** There exist, as we know, multiple deployment models and operational scenarios [8]. Unfortunately, most models (on the economics of cyber security) often lack details of different deployments and cloud ecosystems.
- ***What are cloud offerings?*** There exist different business models (and costs associated with cloud services). However, cloud offerings may look similar, but (technical) details are important too.
- ***How do we assess cloud ecosystems?*** Cloud computing is a major shift in the way ICT is deployed. Emerging (business) relationships shape the cloud forming cloud ecosystems involving different actors (with different responsibilities). Risk and cost-benefit analyses need to take into account not just individual actors (e.g. the weakest link [9]), but how economics, benefits, risks and security threats propagate throughout the cloud supply chain.
- ***How do we address cloud governance?*** Adopting the cloud involves a shift in the way ICT is deployed across industries. This also requires new governance models that intend to guarantee compliance with relevant regulatory regimes. Moving to the cloud often involves data transfer from cloud customers to cloud providers [10]. Accountability is emerging among critical requirements in cloud ecosystems. There exist alternative governance models [11] – e.g. centralised, decentralised, delegation of responsibility, third party certification – which are difficult to assess in terms of economics. Economic models (although generic) are then used to characterise alternative governance models, but result difficult to link to operational ones or to transfer into operational environments (e.g. see [12, 13] for examples of economic models concerned with operational aspects of the cloud).
- ***Do we understand cost/benefit of security investment?*** Despite the effort in assessing security operationally, security metrics tend to be tailored to the specific cases and difficult to generalise. Generally accepted security metrics, across operational domains, are yet a problem requiring further investigations. Moreover, due to the continuous evolving cyberspace, assessing security (and related investments) is like pointing to a moving target (e.g. see [14] for examples of economic models of security investments).
- ***Do we understand economic and security models?*** The diversity of economic and security models makes their comparison difficult [7]. Unfortunately, they are quite often written for the modellers not for the users of such models. Therefore, they are difficult to adopt and transfer into practice.

These remarks provide critical insights about (modelling) the economics of security in the cloud. Next section discusses briefly how understanding economics may drive operational security and the deployment of security technologies in the cloud.

2.2 Cloud Stewardship Economics

As an example, we recall early work at HP Labs on *cloud stewardship economics* [15]. Cloud deployments involve benefits and risks beyond outsourcing [16]. Cloud services are ready-available. Market dynamics (rather than simply commercial agreements) determine the trust in such services and their consumption. Information management in the cloud requires a broader notion than security, specifically a theory for stewardship. Stakeholders in cloud ecosystems are affected by the choices and actions of others (throughout cloud supply chains). Cloud providers manage data on behalf of cloud customers (or other providers too), who trust and depend on third parties to manage information in the cloud. Beside such responsibilities, there is also a dependence on the robustness, resilience and sustainability of the whole cloud ecosystem. Cloud stewardship involves notions of assurance, trust, obligation, incentives, utility, preference, hence *economics*. Cloud stewardship economics, on the one hand, explores the concept of information stewardship in the context of cloud ecosystems, on the other hand, applies economic and mathematical modelling techniques to help stakeholders make strategy and policy decisions. The work conducted by the project on cloud stewardship economics [15] developed system and economic models (based on the utility theory) tailored to the cloud. Simulations of different scenarios (e.g. security and reputation dynamics, information asymmetries, etc.) supported discussions of such models with stakeholders. This helped to validate with stakeholders various behavioural assumptions about cloud ecosystems as well as to promote a shared understanding of cloud stewardship economics among them. The results on trust economics highlight how economics may drive operational security and the deployment of security technologies. Cloud stewardship economics underpins a systematic approach to information security decision-making and risk management [17, 18].

3 Innovation in Cyber Security and Privacy

The economics of security in the cloud, discussed in the previous section, is concerned with analysis of the contingencies between economics and security. This section takes into account different viewpoints of analysis concerned with security research and innovation. Research in security and privacy like other domains faces difficult transition from research into practice [3]. Recent work on cyber security research highlights the main factors (i.e. *"insufficient awareness of the complexity of cyber security transfer"*, *"a scattershot approach to R&D"* and *"mismatch between market and threat environment"* [2]) that jeopardise transferring security technology from research to practice – *"many research investments lead to security technologies that never see the light of the day"* [2]. This difficulty that research outcomes have to transition into real world applications and markets is often depicted as the *"valley of death"* [3].

Research outcomes may fail to have any industry impact. Whilst this usefully serves to filter out poorly conceived propositions, the challenge therein is to identify and support technologies that are valued by the market and of importance to end users [19]. This problem can be analysed from two different viewpoints: *technological* and *contextual*. On the one hand, research outcomes may not be ready or mature enough to be

deployed into practice. On the other hand, application domains may not be ready to adopt new technological developments due to low levels of innovation intakes.

From a technological viewpoint of analysis, it is necessary to identify and understand the barriers that inhibit technology transitions to practice, and how to address them [4, 20]. Another technological aspect to be considered is the maturity of developments. The NASA Technology Readiness Levels (TRLs) are often used to assess the maturity of technology to be delivered in operational environments [21, 22]. Moving from one technology readiness level to the next one (and above TRL 3 and TLR 4) requires dealing with a "research and development degree of difficulty" (that is, probability of success of R&D objectives) [23]. Moreover, it also requires a commitment of resources beyond the affordability of many research and development contexts, in particular, of publicly funded research [24, 25]. The assessment by TLRs is now being adapted for use in European Horizon 2020 funded research. This represents a significant shift affecting how funding decisions are reached and post-funding evaluations are carried out. From a contextual viewpoint of analysis, it is necessary to understand whether specific domains are ready to adopt new technologies. Validation processes, collecting evidence to assess the readiness of technology to be deployed in operational environments in order to minimise the risk of innovation, may vary across application domains. At the national level, the innovation index is widely adopted as a measure to assess the level of innovation in different countries [26]. The Global Innovation Index (GII) takes into account composite indicators ranking innovation performances.

The combination of these two perspectives, i.e. technological readiness (that is, how mature technology is) and contextual innovation (that is, how ready the innovation environment is), identifies a readiness-innovation space to discuss strategies to support research impact. It highlights two critical situations: 1) high-readiness of technology and low-innovation context, 2) low-readiness of technology and high-innovation potential context. The former characterises situations where technology has been extensively developed and used, but the deployment context is unable to benefit from innovation for different reasons (e.g. lack of innovation culture, unsuitable supporting mechanisms). The latter characterises situations where technology is under-developed for an innovation ecosystem. These two perspectives have been discussed with industry stakeholders in order to identify *innovation pathways*.

3.1 Technological Innovation Pathways

Cyber security and privacy are increasingly important topics for the competiveness of European economy and the current trend of investments in legal, technical or research areas related to these topics illustrate this importance. However, it is also necessary to address emerging and future cyber security and privacy threats and challenges that span multiple organisations, crossing domains and boundaries between companies, sectors, or countries. Unlike other research domains, which also deal with common and global challenges, cyber security and privacy domains are characterised by volatile dynamics – what is secure today might not be tomorrow, what is an unknown threat or vulnerability today might be on the news tomorrow. While threats and challenges are common

and global, the solutions and responses are often too fragmented, which yields not only to the waste of resources, but brings also danger of inadequate response.

Technological innovation pathways provide a means to identify research and development strategies that will be most effective. Research and development challenges in cyber security and privacy are diverse and ambitious. No single strategy is going to address all emergent issues in cyber security and privacy. Technological innovation pathways take into account challenges of developing and deploying research innovations. Innovation pathways identify alternative research and development strategies. Which may rely on different methodologies, mechanisms and processes. Technological innovation pathways identify those situations faced by research and development activities. Industry stakeholders, we consulted, identified four different types of technological innovation pathways:

- **Demand-driven Innovations:** research and development initiatives focusing on innovations required by clients or sector representatives. This is the case for those technologies and services with existing and recognised markets. Therefore, the relevant topics are identified within such markets focusing on specific clients (end users) and stakeholders (demanding further improvements in existing products and services).
- **Market-shaping Innovations:** research and development activities focusing on new technologies and services that are disruptive to current markets. Innovations that have the potential of creating new market opportunities, but that need the 'multiplication' of the impact in order to create 'hype' or market trend. That is, research and development initiatives that deploy ground-breaking innovations and establish new markets and trends.
- **Cross-fertilisation Innovations:** research and development initiatives supporting cross-fertilisation between different research disciplines as well as industrial sectors (different contexts addressing similar problems in alternative ways, e.g. dependability and security in hardware and software research). This would require acquiring multi-disciplinary skills and thinking programmatically (e.g. like for standardisation initiatives).
- **Grand Challenges:** large scale initiatives bringing Industry and Research in order to address complex problems in cyber security and privacy. This would involve the identification of a list of challenges and the coordination of relevant projects (e.g. clustering initiatives) in order to focus resources strategically.

These technological innovation pathways need to be integrated in and supported by suitable funding mechanisms at the national as well as European level. They point to alternative directions (sometime crossing each other) for innovation requiring different levels of private and public interventions. Moreover, they help us discussing some issues concerned with innovation. In particular, the identification of contingencies between research and development activities (in terms of technological innovation pathways) and issues concerned with technological transfers into industry practice. **Fig. 2** shows the four technological innovation pathways. Demand-driven innovations require an alignment between markets and users (of technological innovations, e.g. other in-

dustries) and consumers' needs, otherwise they may result in users and consumers' dissatisfaction and mistrust in technological innovations. Market-shaping innovations require an understanding of the economics of R&D, otherwise they may result in unclear strategies for investment and decision making (e.g. security technologies often face this type of problem due to a lack of understanding of security economics). Moreover, national and international legal frameworks for innovation shape markets and create the conditions for technological innovations and collaboration (or competition) among stakeholders. Cross-fertilisation innovations are characterised by R&D solutions (already existing in some domains) searching for problems across domains. Grand challenges, like security and privacy, require international cooperation for innovation.

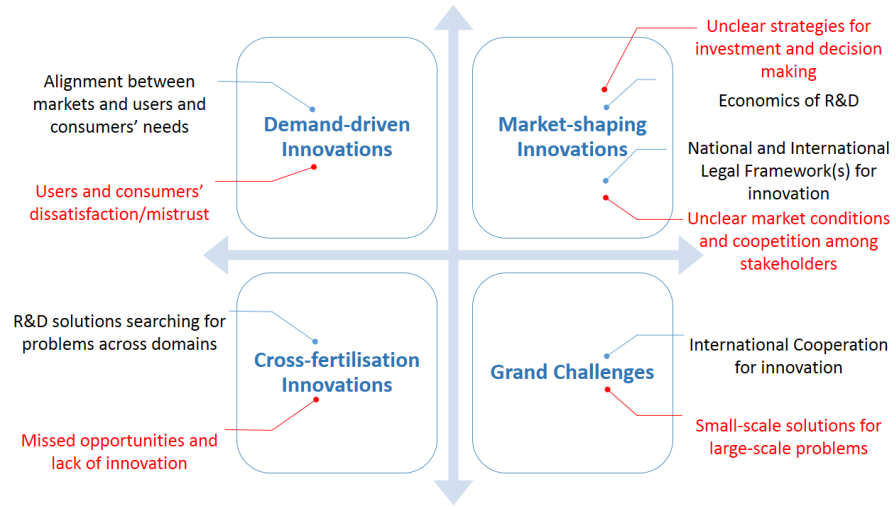

Fig. 2. Technological Innovation Pathways

The technological innovation pathways also supported discussing the barriers to innovation in cyber security and privacy. The aspects of R&D supporting innovation forms a basis for an integrated framework for innovation management [27].

3.2 Integrated Framework for Innovation Management

This section recall the integrated framework for innovation management we introduced in [27]. In order to support effectively the transition from publicly funded research to operation environments it is necessary to address different challenges, e.g. human resources, government regulations, deployment issues, and funding cycles [20]. Enhancing the readiness level of technologies requires not only dealing with such challenges but also using the suitable support at the right time. Different mechanisms may be suitable for early research developments but not so effective in supporting transition to operations. Other instruments may support effectively technology transfers and

adoption. In order to increase the impact of R&D in cyber security and privacy, different instruments – e.g. research projects, pilot projects, pre-commercial procurements [28,29] – can support innovation at various stages [30], from R&D initiatives enhancing the maturity and readiness of technology to the adoption of innovative technology. Similar considerations may arise in analysing the risk of technology (new or existing) with respect to market (new or existing) [31].The European Commission, for instance, is supporting the adoption of pre-commercial procurement in order to deliver innovation in public sectors in Europe [32]. The pre-commercial procurement has been successfully adopted and used across different services [33,34].

Initial findings from SecCord research combined with insights drawn from critical aspects of R&D, as discussed, highlight three discrete primary areas of investigation [27]: (I) R&D policy and market, (II) technology readiness, and (III) technology transfer (also referred to as transition). **Fig. 3** illustrates these areas of investigations forming together the integrated framework for innovation management underpinning empirical investigations and roadmaps in cyber security and privacy.

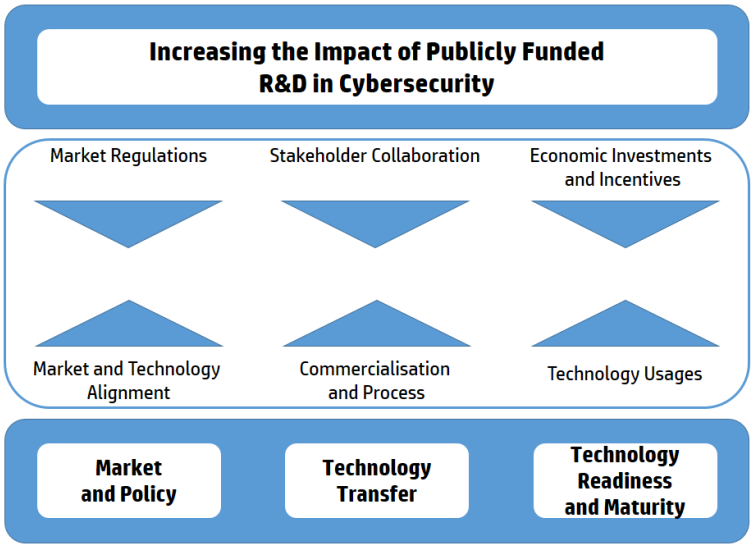

Fig. 3. An integrated framework for innovation management

Some stakeholders clearly operate within one particular area of investigation (e.g. regulators and funders within R&D Policy and Market, and Information Communications Technology (ICT) service providers within Technology Transfer), whilst others can provide expert views and experiences across more than one process (e.g. innovators). The integrated framework thus outlines the scope and focus for capturing, integrating and systematically analysing all stakeholder views of cyber security R&D impact. The integrated framework underpins a questionnaire on *Cyber Security and Privacy R&D Impact in Europe* we are using for gathering stakeholders' opinions in order to understand contingencies between different aspects of innovation. Next section discusses some initial indications based on stakeholders' responses.

3.3 Ongoing Stakeholder Consultation

The integrated framework identifies three dimensions – i.e. *market and policy*, *technology transfer*, *technology readiness and maturity* – influencing the impact of R&D in cyber security and privacy. These dimensions form the basis for a survey we are conducting with stakeholders. For example, **Table 1** lists the different statements (and questions) for the dimension concerned with technology readiness and maturity we asked stakeholders to rank (answer) according to their experiences. The other dimensions – i.e. technology transfer, market and policy – are investigated with other relevant statements (questions).

Table 1. Innovation Dimension: Technology readiness and maturity

Technology usages	
Statements	1. Cyber security technologies with a strong business case still lack opportunities to access capital to follow through into application 2. Further support mechanisms are needed to help demonstrate utility in large scale systems environments 3. Access to actionable test feedback from end users is hard to achieve for new cyber security technologies
Question	4. What factors are critical to the development of competitive business models for new technologies in cyber security and privacy?
Economic incentives and investments	
Statements	5. Industry recognised metrics specific to cyber security and privacy are already widely used in commercial documents to demonstrate the efficacy of new technologies against threats 6. Large enterprises should play a greater technical and economic role in supporting new cyber security technology ventures in the wider marketplace 7. 3. The effective application of new cyber security technologies is significantly affected by exogenous factors, such as legal frameworks, insurance and taxation
Question	8. What can be done to decrease risk to investments for technologies that have demonstrated potential in laboratory environments?

We will now discuss some initial indications for each of the dimensions identified by the integrated framework for innovation management (a full study of stakeholder feedback is due once we have completed the survey). The initial indications identified by stakeholders point out insights about R&D in cyber security and privacy.

- **Technology Readiness and Maturity.** Stakeholders indicate the need for further support mechanisms are needed to demonstrate the utility of research and development outcomes in large scale environments. Unfortunately, they also point out that it is difficult to get feedback by end users of security and trust technologies. In terms of economic incentives and investments, stakeholders stress the lack of commonly adopted security (privacy) metrics. Interestingly, despite there is a strong emphasis on measures supporting SMEs, stakeholders recognise that large enterprises should play a leading role in advocating technology innovation.

- **Technology Transfer.** Looking at processes and dynamics of technology transfers, stakeholders indicate that the integration between new security and privacy technologies into current infrastructures presents a significant barrier to technology transfer. This is probably due also to the fact that changes required by integrating new technologies represent often an organisational risk. Moreover, the lack of shared data on security incidents and industry benchmarks is a major obstacle to technology transfers. Another interesting point is that stakeholders recognise the need for effective marketing supporting technology transfers.
- **Market and Policy.** This dimension highlights various contingencies concerned with innovation in cyber security and privacy. In general, these stress the misalignment between the expectations of stakeholders how are responsible for research and development activities (and technology transfers) and the innovation environments (shaped by governmental stakeholders who define relevant policies and economic incentives). Other interesting results point out conflicting views on the effectiveness of publicly-funded research (we will analyse whether or not there are different opinions across stakeholder groups) and well as of stakeholder forums in identifying requirements for security and privacy technologies.

The final results (once analysed in search for statistical correlations and arguments) of the questionnaire we are collecting will inform a road mapping exercise for identifying contingencies in current innovation strategies as well as recommendations for future research and development initiatives.

4 Concluding remarks

This paper has discussed various aspects of economics, security and innovation. The combination of both micro and macro levels of analyses highlights contingencies in the way the economics of security may affect (or, if understood, positively influence) innovation in cyber security and privacy. At the micro level, we discussed the economics of security in the cloud. Although different economic models of security have been proposed, there is still a lack of understanding of the economics of security in the cloud. Future activities intend to understand and discuss further the operational (and pragmatic) aspects of economics of security in cyber security – *What is new in the economics of cyber security and privacy?* At the macro level of analysis, stakeholder indicate various contingencies between innovation dimensions (i.e. technology readiness and maturity, technology transfer, market and policy). This paper discusses various contingencies between economics, security and innovation. Addressing the problem of the "valley of death" faced by R&D in security and privacy would require alignments of technologies, economic incentives and markets. This also would suggest defining innovation in terms of technology investments and deployments by taking into account economics, market opportunities and R&D strategies. In conclusion, economics, security and innovation characterise a complex problem space for R&D in cyber security and privacy – security (privacy) metrics (models) are yet unclear; assessing the economics of security (privacy) is even more complex; innovation in cyber security and privacy without understanding the economics of security (privacy) is probably a utopia.

Acknowledgements. I would like to thank colleagues at HP Labs, in particular, Yolanta Beres, Dharm Kapletia, Simon Shiu and Nick Wainwright, who supported me with different materials I further elaborated in this paper. Their work has provided me solid foundations for my research interests. The work on the *'economics of security in the cloud'* and the *'integrated framework for innovation management'* has been partially funded by the Security and Trust Coordination and Enhanced Collaboration (SecCord) – http://www.seccord.eu/ – grant agreement 316622 within the Seventh Framework Programme (FP7) of the European Commission. The section on technological innovation pathways has benefited from feedback by the SecCord's Advisory Focus Group.

References

1. The Economist: Defending the digital Frontier, Special Report on Cyber-Security (2014)
2. Anderson, R., Boehme, R., Clayton, R., Moore, T.: Security Economics and the Internal Market. ENISA (2008)
3. Maughan, D., Balenson, D., Lindqvist, U., Tudor, Z.:, Crossing the "Valley of Death: Transitioning Cybersecurity Research into Practice, IEEE Security & Privacy, March/April (2013)
4. Benzel, T.V., Lipner, S.: Crossing the Great Divide: Transferring Security Technology from Research to the Market, IEEE Security & Privacy, March/April (2013)
5. IDC: Worldwide and Regional Public IT Cloud Services 2013–2017 Forecast, (2013)
6. The Economist: Securing the Cloud (2002)
7. Pfleeger, S.L., Rue, R.: Cybersecurity Economic Issues: Clearing the Path to Good Practice, IEEE Software, January/February (2008)
8. Mell, P., Grance, T.: The NIST Definition of Cloud Computing, NIST Special Publication 800-145, September (2011)
9. Pieters, W.: Defining "The Weakest Link": Comparative Security in Complex Systems of Systems. In Proceedings of the 2013 IEEE International Conference on Cloud Computing Technology and Science (CloudCom 2013), IEEE Computer Society, pp. 39-44 (2013)
10. Felici, M., Jaatun, M.G., Kosta, E., Wainwright, N.: Bringing Accountability to the Cloud: Addressing Emerging Threats and Legal Perspectives. In M. Felici (Ed.), Cyber Security and Privacy (CSP EU FORUM 2013), Springer-Verlag, CCIS 182, pp. 28-40 (2013)
11. Prüfer, J.: How to Govern the Cloud? Characterizing the Optimal Enforcement Institution that Supports Accountability in Cloud Computing. In Proceedings of the 2013 IEEE International Conference on Cloud Computing Technology and Science (CloudCom 2013), IEEE Computer Society, pp. 33-38 (2013)
12. Díaz-Sánchez, F., Al Zahr, S., Gagnaire, M.: An Exact Placement Approach for Optimizing Cost and Recovery Time under Faulty Multi-cloud Environments. In Proceedings of the 2013 IEEE International Conference on Cloud Computing Technology and Science (CloudCom 2013), IEEE Computer Society, pp. 138-143 (2013)
13. Johnson, K., Wang, Y., Calinescu, R., Sommerville, I., Baxter, G., Tucker, J.V.: Services2Cloud: A Framework for Revenue Analysis of Software-as-a-Service Provisioning. In Proceedings of the 2013 IEEE International Conference on Cloud Computing Technology and Science (CloudCom 2013), IEEE Computer Society, pp. 144-151 (2013)
14. Tsalis, N., Theoharidou, M., Gritzalis, D.: Return on Security Investment for Cloud Platforms. In Proceedings of the 2013 IEEE International Conference on Cloud Computing Technology and Science (CloudCom 2013), IEEE Computer Society, pp. 132-137 (2013)

15. HP: Trust Economics: A systematic approach to information security decision making. HP Labs (2011)
16. Catteddu, D., Hogben, G. (Eds.): Cloud Computing: Benefits, risks and recommendations for information security. European Network and Information Security Agency (ENISA) (2009)
17. Baldwin, A., Pym, D., Shiu, S.: Enterprise Information Risk Management: Dealing with Cloud Computing. In S. Pearson, G. Yee (Eds.), Privacy and Security for Cloud Computing, Springer-Verlag, Computer Communications and Networks, pp. 257-291 (2013)
18. Lloyd's: Lloyd's 360° Risk Insight Managing digital risk: trends, issues and implications for business (2010)
19. Auerswald, P.E., Branscomb, L.M.: Valleys of Death and Darwinian Seas: Financing the Invention to Innovation Transition in the United States. Journal of Technology Transfer 28(3-4):227-239, Kluwer Academic Publishers (2003)
20. D'Amico, A., O'Brien, B., Larkin, M.: Building a Bridge across the Transition Chasm. IEEE Security & Privacy 11(2):24-33 (2013)
21. Mankins, J.C.: Technology Readiness Levels: A White Paper. NASA (1995)
22. NASA, HRST Technology Assessments Technology Readiness Levels, Chart.
23. Mankins, J.C.: Research & Development Degree of Difficulty (R&D3): A White Paper. NASA (1998)
24. ENISA, Security Economics and the Internal Market: Evaluation of Stakeholder Replies, (2008)
25. ENISA, Security Economics and the Internal Market: ENISA Conclusions on Follow-up Activities (2008)
26. INSEAD, The Global Innovation Index 2012: Stronger Innovation Linkages for Global Growth, INSEAD and WIPO (2012)
27. Kapletia, D., Felici, M., Wainwright, N.: An Integrated Framework for Innovation Management in Cyber Security and Privacy. In F. Cleary, M. Felici (Eds.), Cyber Security and Privacy, Springer-Verlag, CCIS 470, (2014)
28. ENISA: EP3R 2012 Activity Report, European Public+Private Partnership for Resilience, (2012)
29. ENISA: EP3R 2013 Work Objectives, European Public+Private Partnership for Resilience, (2013)
30. NIST: Between Invention and Innovation: An Analysis of Funding for Early-Stage Technology Development. NIST GCR 02–841, November (2002)
31. Hartmann, G.C., Myers, M.B.: Technical Risk, Product Specifications, and Market Risk. In Branscomb, L.M., Auerswald, P.E., Taking Technical Risks: How Innovators, Executives, and Investors Manage High-Tech Risks, MIT Press (2003)
32. European Commission, Pre-commercial procurement: Driving Innovation to Ensure high Public Services in Europe, European Communities (2008)
33. European Commission, Opportunities for Public Technology Procurement in the ICT-related sectors in Europe, Final Report (2008)
34. European Commission, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, Pre-commercial Procurement: Driving innovation to ensure sustainable high quality public services in Europe, SEC(2007) 1668, COM(2007) 799 final, Brussels (2007)