An Integrated Framework for Innovation Management in Cyber Security and Privacy

Dharm Kapletia(✉), Massimo Felici, and Nick Wainwright

Security and Cloud Lab, Hewlett-Packard Laboratories, Long Down Avenue, Bristol BS34 8QZ, UK
dharmendra.kapletia@hp.com

Abstract. This paper is concerned with increasing the impact of publicly funded research and development (R&D) in cyber security and privacy. In the context of a high level of threat, there is a pressing need for firms and institutions to implement innovative and robust cyber security and privacy technologies. This particular challenge requires a systematic coordinated approach across both the public and private sectors. The innovation ecosystem involves complex interactions between key actors such as policy makers, incumbent service providers, and new innovators, each with their own view of how to increase the impact of R&D in cyber security and privacy. Drawing on R&D literature and roadmapping theory, this paper presents a framework and research tool for establishing an integrated view of innovation management in cyber security and privacy.

Keywords: Innovation management · Impact · Cyber security · Privacy

1 Introduction

Research in security and trust like other domains faces difficult transition from research into practice [1]. Recent work on cyber security research highlights the main factors (i.e. *"insufficient awareness of the complexity of cyber security transfer"*, *"a scatter-shot 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]. That is, most of research outcomes will 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 [4].

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 [5, 6]. Another technological aspect to be considered is the maturity of developments.

F. Cleary and M. Felici (Eds.): CSP Forum 2014, CCIS 470, pp. 135–147, 2014.
DOI: 10.1007/978-3-319-12574-9_12

The NASA Technology Readiness Levels (TRLs) are often used to assess the maturity of technology to be delivered in operational environments [7, 8]. 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) [9]. Moreover, it also requires a commitment of resources beyond the affordability of many research and development contexts, in particular, of publicly funded research [10, 11]. 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 how 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. Specific application domains have developed and adopted validation processes (collecting evidence) to assess the readiness of technology to be deployed in operational environments in order to minimise the risk of innovation (e.g. see the EUROCONTROL E-OCVM [12, 13]). At the national level, the innovation index is widely adopted as a measure to assess the level of innovation in different countries [14]. 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.

With the aim of supporting evidence-based policy making and increasing the impact of R&D decision-making, this paper sets out the method for conducting a comprehensive and systematic empirical investigation of stakeholder experiences in cyber security and privacy innovation. This includes both demand side views as well as technology and innovator views, across the end-to-end spectrum of innovation management. Insights generated are expected to capture authoritative snapshots of the health of innovation ecosystems. This paper is structured as follows. Section 2 introduces an integrated innovation management framework. Section 3 outlines a systematic procedural method for capturing the views and experiences of cyber security stakeholders. Section 4 applies the proposed framework on a case study based on a literature review. This is to further explain the framework itself and its application on a concrete example. Section 5 highlights some concluding remarks and discusses the application of the proposed framework for roadmapping R&D initiatives in cyber security and privacy.

2 An Integrated Framework for Innovation Management

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 [6]. 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 [15, 16]) can support innovation at various stages [17], 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) [18]. The European Commission, for instance, is supporting the adoption of pre-commercial procurement in order to deliver innovation in public sectors in Europe [19]. The pre-commercial procurement has been successfully adopted and used across different services [20, 21].

Initial findings from SecCord research [22] combined with insights drawn from critical aspects of R&D, as discussed, highlight three discrete primary areas of investigation: (I) R&D policy and market, (II) technology readiness, and (III) technology transfer (also referred to as transition). Figure 1 illustrates these areas of investigations forming together the integrated framework for innovation management underpinning empirical investigations and roadmaps in cyber security and privacy.

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

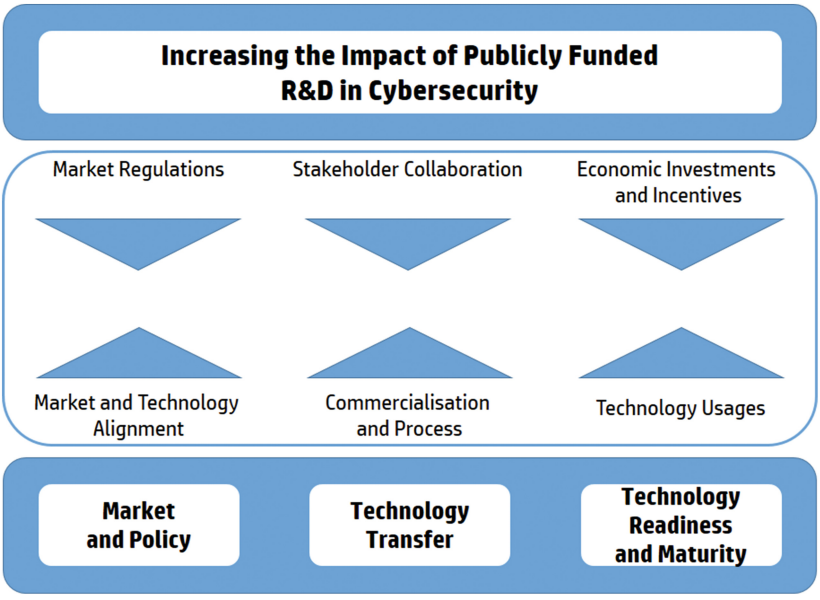

Fig. 1. An integrated framework for innovation management

can provide expert views and experiences across more than one process (e.g. innovators). The framework in Fig. 1 thus outlines the scope and focus for capturing, integrating and systematically analysing all stakeholder views of cyber security R&D impact.

3 Capturing Stakeholder Views and Experiences

There are a variety of tools available to capture stakeholder views and experiences. The use of roadmaps have been used for decades, offering a powerful visual representation of stakeholder views on where they want to go to achieve their desired objective [23]. In both academic and practitioner literature, they are reported as a recognised and proven tool, used extensively to ensure the right capabilities are in place at the right time. The process of roadmapping is said to require the simultaneous consideration of markets, products, technologies and interaction between them over time [24]. Much of the documented cases focus on the development and use of roadmaps at the firm-level, and advocates the importance of gaining cross functional views (across silos) and helping staff to see the impact they have on other parts of the organisation [25]. Roadmaps have also been used in similar fashion by governments looking at the industry level – bringing together a wide variety of stakeholder views from private and public sectors as well as other bodies such as educational institutions. The US government has developed such industry-based roadmaps for cyber security strategy and planning [26, 27].

Fellow colleagues and researchers across various European institutions, including other ICT projects[1] in Trust & Security funded by the European Commission's Framework Programme 7 (FP7), are actively investigating where investments need to be made in specific cyber security technologies and are also developing *technology roadmaps* for the security and privacy domains. At the level of individual technologies, technology roadmapping can offer a valuable stakeholder appraisal of early stage technologies and help strengthen value propositions and routes to market [28]. This research however will employ a *strategic roadmapping* approach – where the emphasis is more on characterising policy and practice related to R&D impact. This might for example include a focus on cross-boundary development processes, business models, security ecosystem dependencies, and involvement of end users [29]. While much has been reported recently on their use, roadmapping methodologies are continually evolving and can be customised in various ways [30, 31].

3.1 Roadmap Dimensions

The primary areas of investigation outlined in the integrated framework (Fig. 1) have been used to make up the three main layers of the roadmap architecture template for this research, as laid out in Fig. 2. They align well with typical layers found in generic roadmaps where the top is usually concerned with trends and drivers ('know why'); the

[1] http://cordis.europa.eu/fp7/ict/security/projects_en.html

middle contains products, services, systems, requirements ('know what'); and the bottom includes resources (includes technology) to be marshalled and integrated to develop the delivery mechanisms [32]. From an emerging typology of roadmaps, the proposed architecture for this research combines the 'strategic appraisal' and 'business reconfiguration' types [31]. This is based on the need to credibly establish and review evidence of the 'as-is' (current position in Fig. 2) in cyber security and privacy R&D. This can be compared and contrasted the desired 'to-be' end-state (vision in Fig. 2), which will lead to a gap analysis and initiate discussion of routes to address the gap.

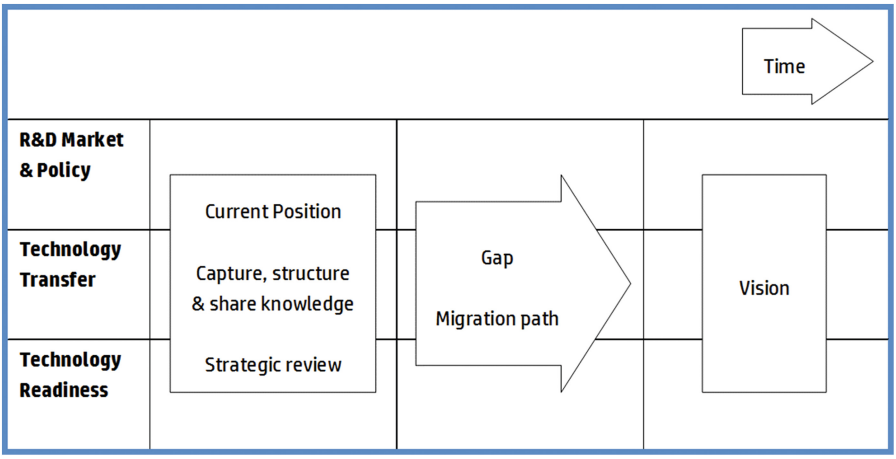

Fig. 2. Proposed roadmap architecture, incorporating the research framework

Following a robust and systematic method, this research project will develop an initial desk-based roadmap based on empirical data from semi-structured interviews and an online survey of cyber security stakeholders across stakeholders in Europe. The results will inform future activities towards a consolidated roadmap in cyber security and privacy. Future activities may include local and national roadmapping workshops. A judgement will be made as to when to best share the desk-based roadmap with other stakeholders. On the one hand, sharing the results after completion of all data gathering activities may help achieve triangulation using various sources of data. On the other hand sharing an emerging roadmap with stakeholders at key stages might validate key findings over time. Either way, a comparison of desk based and workshop based roadmaps at any stage in the research will provide interesting insights about the perceived reasons for similarities and differences.

3.2 Process for Building a Strategic Roadmap

The format and process of developing a strategic roadmap will adopt a customised approach based on extensive learning from practitioner and academic expertise and experience [29, 30]. Source materials have been modified slightly to fit the roadmap architecture in Fig. 2 and an industry-based level of analysis (rather than firm level).

The research will adopt a three stage process, moving from (1) *visioning key stakeholder end-states*, (2) *identifying problems and prioritising opportunities*, and (3) *establishing pathways forward*. Figure 3 outlines the specific empirical activities of mapping and analysis associated with each of the three stages.

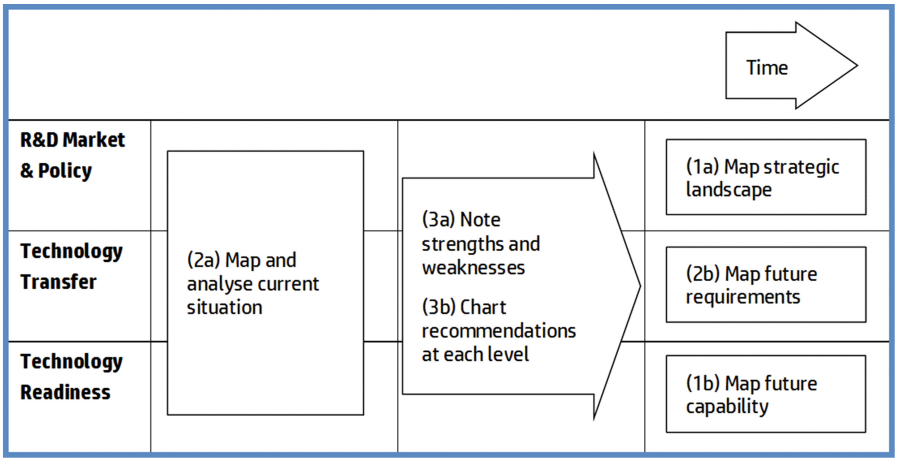

Fig. 3. Proposed roadmapping workshop method

Stage 1 – Visioning

(1a) Map strategic landscape – This involves developing a collective understanding of high level strategic goals related to R&D market and policy. This may include policy objectives, regulation, market maturity, national strategic initiatives, and future industry threats and challenges. Whilst there may be considerable differences in ideas between stakeholders, this activity can conclude by restating the common thread of increasing impact. This is an opportunity to create an appetite for change.

(1b) Map future capability – This relates to how future publicly funded R&D capability can be transformed at the operational level. Capability includes how organizations go about (individually or collectively) increasing the potential of their new security technologies. TRLs may be used in this context to frame how future capabilities relate to advancing through levels of maturity to a desired outcome.

Stage 2 – Opportunities

(2a) Map and analyse current situation – This will likely involve the greatest amount of time, whereby stakeholders involved in R&D market and policy, technology transfer and technology readiness articulate existing issues, challenges, enablers, and barriers associated with delivering impact. This will culminate with a process of ranking both problems and opportunities against Stage One findings.

(2b) Map future requirements – The focus at this point turns towards bridging the so-called 'valley of death' and may draw on problems and opportunities raised in 2a. Broadly speaking, this is likely to establish future positions related to business model choices, ecosystem needs, roles of intermediary entities, alternative/optimal forms of collaboration across boundaries, use of commercial vehicles, and different approaches to managing intellectual property rights.

Stage 3 – Pathways

(3a) Note strengths and weaknesses – This involves an in-depth collective discussion of the gaps identified from an analysis of Stage One and Stage Two. Gaps may be ranked against a scale to indicate the level of investment that is likely to be required to address them. If possible, broad indications of short, medium and long term timings associated with levels of investment may also be captured.

(3b) Chart recommendations at each level – This is the final activity of the workshop, which is designed to generate a final set of recommendations for increasing the impact of publicly funded R&D. The output of this activity may generate an execution roadmap to guide stakeholder decision-makers and research sponsors. This is where the importance of having participation from all stakeholder groups to help ensure recommendations have a greater chance of being implemented.

During roadmapping workshops, within each activity, stakeholder ideas will be captured using sticky notes against large wall charts, and then grouped into swim lanes (horizontal rows) where common themes exist, creating new categories. This may involve 'walking the wall' and critiquing ideas, filtering high-value trends via a voting process, and storytelling experiences through small group exercises [29].

3.3 Innovation Ecosystem

Past research also points out the importance of or securing committed and diverse stakeholders groups across disciplines, and ensuring their fully engagement with the process to avoid producing superficial roadmapping results [25]. Our research proposes the following stakeholder groupings and will seek participation from each one:

1. **Research and development** (individuals and organisations seeking to bring new technologies to market, e.g. University spin-outs and R&D labs in an enterprise)
2. **Security and privacy technology/service provider** (of ICT based systems, e.g. anti-virus security service provision)
3. **Technology owner or operator** (of ICT based systems, e.g. internal IT service within an organisation)
4. **Consultancy or industry support** (institutional associations, standards bodies, technology and market analysis, e.g. think tanks and incubators)
5. **Funders and Investors** (individual or entity responsible for sponsoring or investing in R&D, e.g. venture capitalist investment)

6. **Policy and regulation** (Government department, agency or appointed body, e.g. innovation policy development)
7. **Dependent third party** (those who might be compromised by a security breach, e.g. end user in an organisation).

This research incorporates learning from past roadmapping initiatives [31] to ensure a successful outcome. This includes a robust framework and roadmap architecture that is aligned with future developments of the European cybersecurity strategy [33], and a systematic process for empirical data collection and analysis through various sources, drawing on the support of a wide variety of stakeholders in cyber security and privacy.

4 Increasing the Impact of Cyber Security R&D in the US

This section assists in establishing proof of concept for the selected roadmap architecture (as set out in Sects. 2 and 3). Observations from industry leading developments in the United States presented an opportunity to conduct a desk-based roadmapping exercise. Various published US policy sources were analysed mainly from the 'regulator' stakeholder viewpoint [27, 34–40]. The US roadmap presented in Fig. 4 reflects data captured for activities 1a, 1b and 2b, which essentially outlines the future vision. It is possible to take this exercise further through desk-based research by investigating other documented stakeholder perspectives. This would help construct a more integrated view of innovation management in the US.

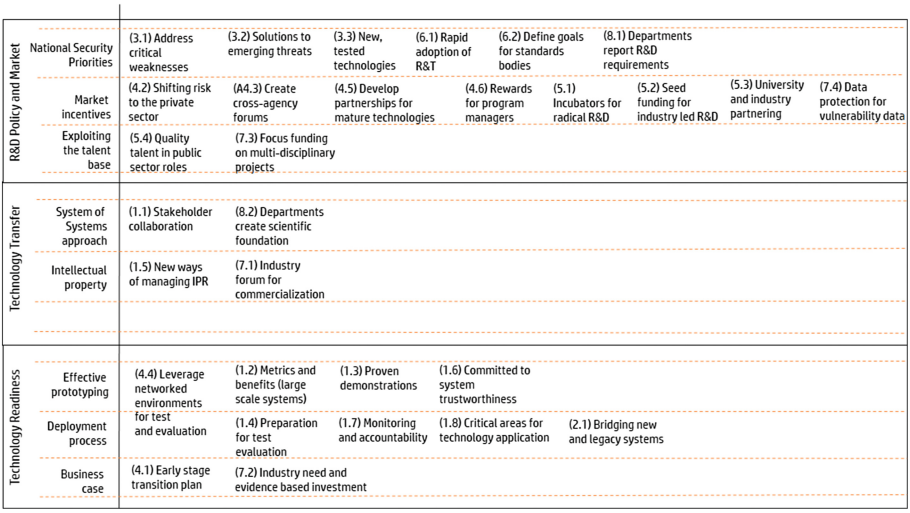

Fig. 4. US example roadmapping exercise

A more detailed breakdown of the original data can be viewed in the appendix. As expected, common themes across source documents are represented by swim lanes and new category labels have been generated. For example, categories under technology readiness include: effective prototyping, deployment process and business case.

5 Discussion and Concluding Remarks

It is clear that measures must be taken to ensure that investments in promising cyber security and privacy technologies survive the valley of death and are given the opportunity to deliver high value impact. Given the complexity associated with cyber security research-to-practice transfer, it is vital to collect and analyse the views of key stakeholders (involved in the end-to-end process of innovation) when devising recommendations that could lead to future policies, strategies and interventions.

This paper has outlined a framework and research tool for developing an integrated view of innovation management in cyber security and privacy. Most importantly, it provides a robust and systematic approach for collecting and analysing industry-level stakeholder views using tried and tested strategic roadmapping methodology. This will be implemented to characterise views of the cyber security innovation ecosystem in the United Kingdom and Europe. The research tool also can be applied to conduct a historical desk-based roadmapping exercise. In this regard, other future applications might include an impact assessment of past European funded R&D projects, the findings of which could inform planning for future research programmes. It may also be possible to repeat the process for other industries, particularly where similar complexities exists.

Insights generated by the research tool may assist identifying a mismatch between stakeholder views and recommendations, and current R&D policies and strategies. Having stakeholder engagement across the groupings identified in Sect. 3 will allow for a greater understanding of connections and dependencies in the ecosystem. For instance ‘regulators’ and ‘investors’ can learn more about challenges faced by ‘innovators’ or the impact of their decisions on established ‘ICT owners and operators’. The risks are that the quality of the insights will depend heavily on the commitment and expertise of selected stakeholders. The end product of the roadmapping process should be regarded as a snapshot in time, unless maintained and updated. All findings and analysis will be presented in a white paper to the European Commission and disseminated widely to stakeholders, networks and forums in cyber security and privacy.

Acknowledgments. This work has been partly funded by the Seventh Framework Programme (FP7) of the European Commission, Security and Trust Coordination and Enhanced Collaboration (SecCord) – http://www.seccord.eu/ – grant agreement 316622.

Appendix

Increasing the impact of publicly funded R&D in the United States – Desk-based roadmapping			
Source	Roadmap label		Documented evidence
A roadmap for cybersecurity research [34]	1.1	Stakeholder collaboration	Public-private collaboration among government, industry, and academia, + extraordinary economic, social, and technological forcing functions
	1.2	Metrics and benefits (large scale systems)	Metrics need to be experimentally evaluated and benefits to large scale systems clearly demonstrated
	1.3	Proven demonstrations	Proven demonstrations of effectiveness are required, this would help roll-out adoption in practice
	1.4	Preparation for test evaluation	Design mechanisms, policies, and plans for test evaluation that can be incrementally deployed
	1.5	New ways of managing IPR (Intellectual Property Rights)	Innovative approaches to licensing and sharing intellectual properties for global scale technologies
	1.6	Committed to system trustworthiness	Overarching commitment to system trustworthiness, going beyond past approaches
	1.7	Monitoring and accountability	Recognition of the pervasive needs for monitoring and accountability
	1.8	Critical areas for technology application	Understanding critical areas suitable for technology application
Cross sector roadmap for cybersecurity of control systems [27]	2.1	Bridging new and legacy systems	Encourage R&D into tying legacy systems into upcoming security solutions
Homeland Security – cybersecurity R&D priorities [35]	3.1	Address critical weaknesses	Driving security improvements to address critical weaknesses
	3.2	Solutions to emerging threats	Discovering new solutions for emerging cyber security threats
	3.3	New, tested technologies	Delivering new, tested technologies to defend against cyber security threats
Trustworthy cyberspace: Strategic Plan for the Federal Cybersecurity R&D Program [36]	4.1	Early stage transition plan	Early stage transition plan in place, that includes commercialization pathways, tech transfer coordination, proactive program management, and resources to reward success in transitioning
	4.2	Shifting risk to the private sector	Private sector is willing to take on significant risk-taking and shepherd research through the commercialization process
	4.3	Create cross-agency forums	Participation in cross-agency security entrepreneur forums, PI meetings, laboratory expos, and defense venture catalyst initiative
	4.4	Leverage networked environments for test and evaluation	Cross-agency activities designed to leverage available operational and next generation networked environments to support experimental deployment, test and evaluation in public and private environments
	4.5	Develop partnerships for mature technologies	Cross-agency activities designed to develop partnerships for mature technologies, through open system integrator forums (VCs, SIs, government), and small business innovative research conferences
	4.6	Rewards for program managers	Government funded R&D to build-in rewards for government program managers and principal investigators for commercial success

(*Continued*)

(*Continued*)

Increasing the impact of publicly funded R&D in the United States – Desk-based roadmapping			
Source	Roadmap label		Documented evidence
Cybersecurity game-change R&D recommendations [37]	5.1	Incubators for radical R&D	Support game-changing R&D using incubators and Federal start-up funding
	5.2	Seed funding for industry led R&D	Support industry-based research consortia to lead and direct focused R&D using seed funding
	5.3	University and industry partnering	Support universities to create industrial partner programs designed to stimulate pre-competitive cooperation among industrial partners
	5.4	Quality talent in public sector roles	Recruit experienced high quality talent into government program manager roles, supporting technology transfer
Cyberspace policy review: assuring a trusted and resilient information and communications infrastructure [38]	6.1	Rapid adoption of R&T (Research and Technology)	Federal government to work with industry to develop migration paths and incentives for rapid adoption of research and technology development, including collaboration between academic and industrial laboratories
	6.2	Define goals for standards bodies	Federal government, in collaboration with private sector and other stakeholders, should use the infrastructure objectives and R&D framework to help define goals for national and international standards bodies
Roadmap to achieve energy delivery systems cybersecurity [39]	7.1	Industry forum for commercialization	Develop a matchmaking forum to connect researchers, vendors, and asset owners to accelerate research from concept to commercialization
	7.2	Industry need and evidence based investment	Develop mechanisms for utility and vendor engagement for pilot research studies to address the business case up front. Create a forum for industry to detail and request R&D topics
	7.3	Focus funding on multi-disciplinary projects	Require diverse (academic, lab, industry) participation to receive funding
	7.4	Data protection for vulnerability data	Support legislation that protects entities who disclose vulnerabilities in good faith to the appropriate parties
Federal R&D strategic plan [40]	8.1	Departments report R&D requirements	Required to provide Congress with a strategic plan based on an assessment of cyber security risk to guide the overall direction of Federal cyber security and information assurance R&D for IT and networking systems
	8.2	Departments create scientific foundation	Through existing programs and activities, support research that will lead to the development of a scientific foundation for the field of cyber security, including research that increases understanding of the underlying principles of securing complex networked systems, enables repeatable experimentation, and creates quantifiable security metrics

References

1. Maughan, D., Balenson, D., Lindqvist, U., Tudor, Z.: Crossing the "Valley of Death": transitioning cybersecurity research into practice. IEEE Secur. Priv. **11**(2), 14–23 (2013)
2. Anderson, R., Boehme, R., Clayton, R. Moore, T.: Security Economics and the Internal Market. ENISA (2008)
3. Downey, F.: Bridging the "valley of death": Response to the House of Commons Science and Technology Select Committee Bridging the "valley of death": Improving the Commercialisation of Research Inquiry from Engineering the Future. The Royal Academy of Engineering, London (2012)
4. Auerswald, P.E., Branscomb, L.M.: Valleys of death and Darwinian seas: financing the invention to innovation transition in the United States. J. Technol. Transf. **28**(3–4), 227–239 (2003). (Kluwer Academic Publishers)
5. Benzel, T.V., Lipner, S.: Crossing the great divide: transferring security technology from research to the market. IEEE Secur. Priv. **11**(2), 12–13 (2013)
6. D'Amico, A., O'Brien, B., Larkin, M.: building a bridge across the transition chasm. IEEE Secur. Priv. **11**(2), 24–33 (2013)
7. Mankins, J.C.: Technology readiness levels: a white paper. NASA (1995)
8. NASA: HRST technology assessments technology readiness levels, chart
9. Mankins, J.C.: Research & Development degree of difficulty (R&D3): a white paper. NASA (1998)
10. ENISA: Security economics and the internal market: evaluation of stakeholder replies (2008)
11. ENISA: Security economics and the internal market: ENISA conclusions on follow-up activities (2008)
12. EUROCONTROL: European operational concept validation methodology, E-OCVM version 3.0, volume I (2010)
13. EUROCONTROL: European operational concept validation methodology, E-OCVM version 3.0, volume II annexes (2010)
14. INSEAD: The global innovation index 2012: stronger innovation linkages for global growth. INSEAD and WIPO (2012)
15. ENISA: EP3R 2012 activity report. European Public+Private Partnership for Resilience (2012)
16. ENISA: EP3R 2013 work objectives. European Public+Private Partnership for Resilience (2013)
17. NIST: Between invention and innovation: an analysis of funding for early-stage technology development. NIST GCR 02–841, November 2002
18. Hartmann, G.C., Myers, M.B.: Technical risk, product specifications, and market risk. In: Branscomb, L.M., Auerswald, P.E. (eds.) Taking Technical Risks: How Innovators, Executives, and Investors Manage High-Tech Risks. MIT Press, Cambridge (2003)
19. European Commission: Pre-commercial procurement: driving innovation to ensure high public services in Europe. European Communities (2008)
20. European Commission: Opportunities for public technology procurement in the ICT-related sectors in Europe, final report (2008)
21. 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)
22. Felici, M., Wainwright, N.: Deliverable 6.4 – Future Internet Initiatives Year 1. SecCord Project No. 316622, November 2013

23. Probert, D., Radnor, M.: Frontier experiences from industry-academia consortia. IEEE Eng. Manag. Rev. **31**(3), 28 (2003)
24. Groenveld, P.: Roadmapping integrates business and technology. Res. Technol. Manag. **50** (6), 49–58 (2007). (Industrial Research Institute)
25. Cosner, R.R., Hynds, E.J., Fusfeld, A.R., Loweth, C.V., Scouten, C., Albright, R.: Integrating roadmapping into technical planning. Res. Technol. Manag. **50**(6), 31–48 (2007). (Industrial Research Institute)
26. Department for Homeland Security: A roadmap for cybersecurity research. United States Government (2009)
27. Industrial Control Systems Joint Working Group: Cross-sector roadmap for cybersecurity of control systems. Department for Homeland Security, United States Government (2011)
28. Dissel, M.C., Phaal, R., Farrukh, C.J., Probert, D.R.: Value roadmapping. Res. Technol. Manag. **52**(6), 45–53 (2009). (Industrial Research Institute)
29. Petrick, I.J., Martinelli, R.: Driving disruptive innovation: problem finding and strategy setting in an uncertain world. Res. Technol. Manag. **55**(6), 49–57 (2012). (Industrial Research Institute)
30. Radnor, M., Probert, D.R.: Viewing the future. Res. Technol. Manag. **47**(2), 25–26 (2004). (Industrial Research Institute)
31. Phaal, R., Farrukh, C., Probert, D.: Customizing roadmapping. IEEE Eng. Manag. Rev. **32** (3), 80–91 (2004)
32. Phaal, R., Farrukh, C.J.P., Probert, D.R.: Developing a technology roadmapping system. In: Technology Management: A Unifying Discipline for Melting the Boundaries, Portland International Conference on Management of Engineering & Technology (PICMET), pp. 99–111 (2005)
33. European Commission: High Representative of the European Union for Foreign Affairs and Security Policy, Joint Communication to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN (2013) 1 final, Brussels (2013)
34. Department of Homeland Security, Science and Technology Directorate: A roadmap for cybersecurity research, November 2009
35. Cybersecurity R&D priorities, United States Homeland Security (2014)
36. Trustworthy cyberspace: strategic plan for the federal cybersecurity research and development program. Executive Office of the President National Science and Technology Council (2011)
37. NITRD: Cybersecurity game-change research & development recommendations. The Networking and Information Technology Research and Development (NITRD) Program (2010)
38. White House: cyberspace policy review: assuring a trusted and resilient information and communications infrastructure. United States Whitehouse publication (2009)
39. ESCSWG: Roadmap to achieve energy delivery systems cybersecurity. The Energy Sector Control Systems Working Group (ESCSWG), Sept (2011)
40. Space Foundation: U.S. non-military cybersecurity research & development and related policies, Cybersecurity, Federal Research and Development Strategic Plan. Space Foundation (2014)