Yet Another Cybersecurity Roadmapping Methodology

Davide Ariu, Luca Didaci, Giorgio Fumera,
Giorgio Giacinto, Fabio Roli
University of Cagliari
Piazza d'Armi, 09123 Cagliari, Italy
Email: {davide.ariu,didaci,fumera,giacinto,roli}@diee.unica.it

Enrico Frumento, Federica Freschi
CEFRIEL - ICT Institute Politecnico di Milano
Via Fucini 2, 20133 Milano, Italy
Email: {enrico.frumento, federica.freschi}@cefriel.com

***Abstract*—In this paper we describe the roadmapping methodology we developed in the context of the CyberROAD EU FP7 project, whose aim is to develop a research roadmap for cybercrime and cyber terrorism. To this aim we built on state-of-the-art methodologies and available guidelines, including related projects, and adapted them to the peculiarities of our roadmapping subject. In particular, its distinctive feature is that cybercrime and cyber terrorism *co-evolve* with their contextual environment (i.e., technology, society, politics and economy), which poses specific challenges to a roadmapping effort. Our approach can become a best practice in the field of cybersecurity, and can be also generalised to phenomena that exhibit a similar, strong co-evolution with their contextual environment. We aim to describe here the roadmapping methodology that will lead to the roadmap but not the roadmap itself (this one being, incidentally , still under construction at the time of writing this paper).**

I. Introduction

CyberROAD[1] is a project funded by the European Commission under the 7th Framework Program. It aims to develop the research roadmap for Cyber Crime (CC) and Cyber Terrorism (CT), thus providing a categorisation of CC and CT, identifying the major challenges, gaps and needs, and finally proposing desirable solutions and methods to evaluate them in practice. Such points are being addressed providing a thorough and comprehensive analysis, which will encompass the technological, social, economical, political, and legal aspects of CC and CT. The project spans for a period of 24 months (June 1st, 2014–May 31st, 2016), and is implemented by a consortium of 20 members from 10 different EU countries, representing all the key players (Defence and Law Enforcement Agencies, research and academia, private and public companies) involved in the fight against CC and CT.

The task of CyberROAD is known as "science and technology roadmapping" (S&TRM). S&TRM has been adopted since mid-1980s by corporations and industries as a tool for strategic planning of S&T resources toward a well defined goal, which usually consists of supporting the development of new products or technologies, with a focus ranging from a single product to a technological sector. Since mid-1990s, S&TRM has been increasingly exploited also by research institutions and think-tanks for providing intelligence to policymakers, with the aim of optimising public R&D investments and ensuring their relevance to society [5], [12]. The CyberROAD roadmap belongs to the category of policy-oriented roadmaps.

It is commonly acknowledged that a S&TRM project must be based on a principled methodology to be successful accomplished [11], [5], [12], [13]. So far, several roadmapping methodologies have been proposed in the literature; several guidelines are also available from public and private organisations that promoted roadmapping efforts in fields as different as industry and government, as well as many useful case studies. This means that a novel roadmapping effort can exploit and build on a considerable body of knowledge, possibly adapting existing methodologies to the characteristics and needs of the specific project. Accordingly, we started from a thorough analysis of S&TRM literature, focusing on policy-oriented roadmapping, and analysed recent S&TRM projects in the cybersecurity and related fields. We then developed a methodology that takes into account the specific application field of our project (the fight against CC and CT), as well as its contextual environment, which encompasses societal, political and economic issues beside technological ones.

After a survey of the relevant literature on S&TRM and of related projects in Sect. II, in Sect. III we describe the specific roadmapping methodology we developed for CyberROAD. We then give an illustrative example of its application in Sect. IV. We finally discuss the proposed methodology in Sect. V; in particular, we point out that it can be exploited not only in a cybersecurity context, but also in other S&TRM projects that, analogously to CyberROAD, involve different fields, and thus require the integration of different domain expertise.

II. State of the Art on S&T Roadmapping

S&T roadmaps can be broadly categorised as either *normative* (*goal-oriented*) or *exploratory* [5], [12], although hybrid roadmaps also exist [1]. The choice between these two kinds of roadmaps is among the first ones to be made in a roadmapping project, based on its context, goal and target audience. Normative roadmaps are commonly used by corporations and industries. They define the paths to attain a well-defined, desired future state from the present one, on a relatively short time horizon (usually, 6 months up to 5 years). The desired state is defined in detail by high-level decision makers, e.g., the end users, or policymakers. Exploratory roadmaps aim instead at enhancing future outlook or foresight of the evolution of an industrial, technological or social landscape, over a usually longer time span (up to 20 years), and taking into account various alternative futures, including rupture scenarios and major technological breakthroughs. Accordingly, *scenario building* (see below) plays a key role in this kind of roadmap, as well as the investigation of non-technical fields of influence [7].

In particular, exploratory roadmaps are believed to be a useful tool for providing intelligence for policymakers in areas where science and technology play a prominent role, e.g., to highlight emerging S&T issues and to anticipate long-term

[1] http://www.cyberroad-project.eu/

978-1-4673-6590-1/15 $31.00 © 2015 IEEE
DOI 10.1109/ARES.2015.87

needs. Policy-oriented roadmaps, which is the category the CyberROAD roadmap belongs to, are currently considered to be still emerging [9]. They exhibit several distinctive features from corporate-/industry-oriented ones: (i) Their scope and goals are wider and less well defined; e.g., they can address far-reaching societal challenges. (ii) They usually involve also social, cultural, political, legal and economical dimensions, and cover a longer time span. (iii) Their target audience is made up of "generalists" rather than "experts". (iv) They are built by *multiple* organisations, and are aimed at an an *external* target audience (usually government, and often different organisations/departments). (v) Their main goal is *political persuasion* about actions to be implemented toward some objective.

Another crucial issue is the definition of a principled roadmapping methodology. To this aim, different resources are currently available. So far, several roadmapping methodologies have been proposed in the academic literature, as well as guidelines for successfully constructing and *implementing* roadmaps, in many different contexts such as company, industry and government [11], [13]; in particular, policy-oriented roadmaps have been analysed in [5], [9], [12]. Guidelines and best practices have also been defined by private and public organisations; a relevant example in the policymaking context is the roadmapping process developed by the International Energy Agency for the energy technology sector [8]. From our analysis of S&TRM, focused on policy-oriented roadmapping, the following five key issues emerged (see also Fig. 1).

1) Identifying the target audience. Since policy-oriented roadmaps are not aimed at the same organisation than produces them, a wide set of target stakeholders from different domains has to be effectively and evenly considered.

2) Data sources. The main data sources are the scientific literature in the field of interest, the stakeholders, and the domain experts. Their careful selection is critical, due to the wide scope of policy-oriented roadmaps and to the usual involvement of a number of stakeholders and domain experts from different fields, including non-technological/scientific ones. Effective and efficient information/knowledge elicitation techniques must also be defined.

3) Roadmap representation and visualisation. Policy-oriented roadmaps are targeted to the generalist view of policymakers. A clear, focused synthesis and presentation of their core issues is thus crucial. This can be attained by suitable graphical representations, which allow decision-makers to focus on the most relevant elements and relations in complex systems involving scientific, technological, economic, political and social dimensions, rather than on low-level details.

4) Roadmap validation and quality assessment. Early actions must be carried out to this aim, since the roadmapping planning stage. It is widely acknowledged that evaluating the quality of a roadmap during its construction is not sufficient: clear criteria and metrics have to be defined to evaluate a roadmap during its *implementation*. For instance, the following issue related to guaranteeing the roadmap reliability and replicability is particularly relevant in the context of CyberRoad: "To what degree would a roadmap be replicated if a completely different development team were involved in its construction?"

5) Roadmap construction technique. Last but not least, a sound methodology for developing the roadmap should be

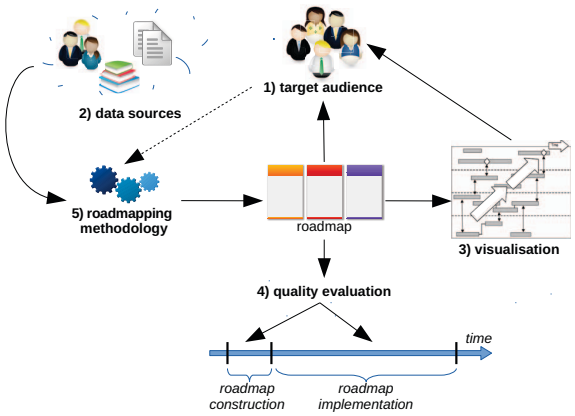

Fig. 1. Five key issues to be addressed to guarantee a successful roadmap.

applied. As mentioned above, several methodologies have been proposed so far, due to the widespread usage of S&TRM. Therefore, no unique paradigm or standard for roadmap construction exists, neither a single definition of S&TRM, even in the specific case of policy-oriented ones. Nevertheless, as argued in [5], defining a unique, general roadmapping methodology is not a practical nor a desirable goal: instead, "the approach should be based on a light and modular process using a 'methodological toolbox' with different modules depending on the roadmapping areas, issues, context and objectives." This is witnessed by recent, policy-oriented S&TRM projects in fields related to CyberROAD, such as:

- Time2Learn[2], Sept. 2002 – Nov. 2003, FP5
- eGovRTD2020: Roadmapping eGovernment Research – Visions and Measures towards Innovative Governments in 2020, January 2006 – May 2007, FP7 [4]
- iCOPER[3]: Interoperable Content for Performance in a Competency-driven Society, 2008–2011, *e*Content*plus*
- EHR4CR[4]: Electronic Health Record for Clinical Research, 2011–2015, partially funded by Innovative Medicines Initiative (IMI)

Their roadmapping methodologies are similar at a high level, but their implementation has been devised ad hoc, according to the specific characteristics and goals of the project.

In the rest of this section we focus on the key issue 5, which is the subject of this paper. In our survey we identified some specific, potentially useful roadmapping approaches, as a starting point toward the definition of a methodology suitable to CyberROAD. In particular, two interesting examples of normative and exploratory roadmap construction techniques are the ones of [10] and of [7], respectively. The normative approach of [10] is tailored to the implementation of government policies which define the high-level, future vision for a given public service. As a case study, the Royal Australian Navy's fleet plan along the time horizon of 2010–2030 was considered, based on the 2009 Australian Government's Defence White

[2]http://www.cordis.europa.eu/project/rcn/64013_en.html
[3]http://nm.wu.ac.at/nm/icoper
[4]http://www.ehr4cr.eu

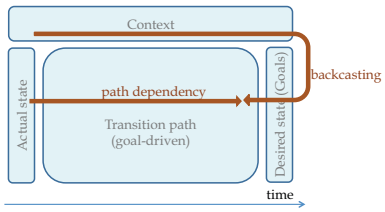

Fig. 2. Sketch of the normative roadmapping approach of [10].

Paper. In this kind of application, high-level objectives exists, defined by policymakers, and the setting is mainly static and under their control. The goal of roadmapping is to prescribe actions to reach such objectives. The proposed roadmapping approach consists of the following steps (see also Fig. 2). (i) Defining the **Context**, i.e., the trends and drivers that govern the overall, high-level goals of the roadmapping activity; e.g., in the case study mentioned above, they include the defence policy, the strategic interests, and the military capability. (ii) Based on the Context, a **Backcasting** process is applied to define in detail the **Desired state** at the end of the roadmap time span; then, reasoning backwards in time up to a medium-term period, the actions to be done to attain the Desired state must be defined. (iii) Since the **Current state** influences what can be attained in the future, it is necessary to define the **Path dependency**, i.e., the actions to be carried out from the current state to enable the ones identified through Backcasting.

In [7], an approach for scenario-based, exploratory TRM is proposed. It is based on the observation that technology is often influenced not only by *endogenous* factors, like market trends and standards, but also by *exogenous*, non-technical factors related to the evolution of society, economy and politics. As a consequence, technology does not follow an evolutionary path, making it very difficult to predict its development, and preventing the use of a normative roadmapping approach. In this context, exploratory roadmapping is useful as an instrument of technology forecasting, i.e., to understand how a technology may evolve, and forms the basis for subsequent planning activities. The approach of [7] consists of the following main steps (see Fig. 3, right): (i) identifying the exogenous and endogenous influencing factors of the technology under investigation (see, e.g., Fig. 3, left); (ii) projecting the possible evolution of the most relevant exogenous factors in one or more time steps during the roadmap time span (several alternative projections are usually possible); (iii) combining alternative projections into a few, consistent and alternative scenarios (even just two "extreme" scenarios); (iv) analysing how the influencing factors interact with each other, to identify the "driving factors" exhibiting the highest impact on the considered technology; (v) envisioning how the latter may evolve under each scenario; (vi) developing a roadmap for each scenario.

We finally discuss scenario building (aka scenario thinking or planning), which is a key component of exploratory roadmaps. It was introduced in a corporate R&D context in the 1950s [2], and is nowadays a strategic planning tool for supporting decision-making in complex and rapidly changing environments. It is widely used in business, industry and government. Its main purpose is to explore *different* potential evolutions of a given field (including non-technological issues) under the influence of some *driving forces*, to support proactive development and planning, and to cope with future challenges [16]. For instance, scenario building can allow recognising technological discontinuities or disruptive events, and include them into long-range planning, making an organisation better prepared to handle new situations as they arise [15].

Broadly speaking, a *scenario* can be defined as a coherent and concise description of a possible future, often in a narrative form, in which the underlying driving forces are pointed out. In practice, a number of different scenario building methodologies have been proposed so far, and, as pointed out in [14], they still lack of a solid conceptual foundation, and are usually adapted by the users to suit their needs. This is witnessed as well by the ad hoc scenario building techniques used in the roadmapping projects mentioned above. In [2] three main methodological "schools" are identified and analysed: Probabilistic Modified Trend (PMT), *La Prospective* (LP), and Intuitive Logics (IL). The PMT methodology mainly provides probabilistic forecasting tools, involving the analysis of historical data. The LP approach is more complex and mechanistic, and heavily relies on computer-based mathematical models and simulations. Both the above approaches aim at producing the *most probable* scenarios. The IL methodology is more flexible instead, as well as more subjective and qualitative. This makes it suited to a wider range of scenario purposes, including CyberROAD. Another feature of such a methodology is that it produces a small number of scenarios which are considered to be *equally probable*. We point out that the scenario building approach used in [7] (see above) mainly follows the IL methodology. The main steps of the IL methodology are the following: (i) determining two main driving forces affecting the subject of scenario building, characterised by the highest impact and the highest uncertainty in their evolution; (ii) defining two extreme but possible outcomes for both driving forces; (iii) developing a scenario for each of the four combinations of outcomes.

III. The Proposed Methodology

The choice of a suitable roadmapping methodology has been guided by the characteristics of the CC and CT phenomenon. Under this viewpoint, the main feature of CC and CT is that they *co-evolve* with their contextual environment, i.e., technology, society, politics and economy, beside being also driven by internal forces. This in sharp contrast with the *independent* evolution of crime and information security before 2000. In particular, the emergence of new technologies, as well as novel social habits and issues (like social networks and privacy issues) can generate new opportunities for CC and CT, enabling novel kinds of attacks. In turn, CC and CT are among the forces that influence the evolution of technology (in the broadest sense of the word) and society. At the same time, the evolution of CC and CT is also driven by *internal* forces, which recently mostly coincided with market trends and laws. A clear example can be seen in the evolution of marketing and consumer profiling techniques, and in the corresponding evolution of social engineering techniques, both based on the same methodologies; other similar examples can be found in linked open data, psychology and personality profiling, cyber sociology, modern sentiment analysis techniques, and

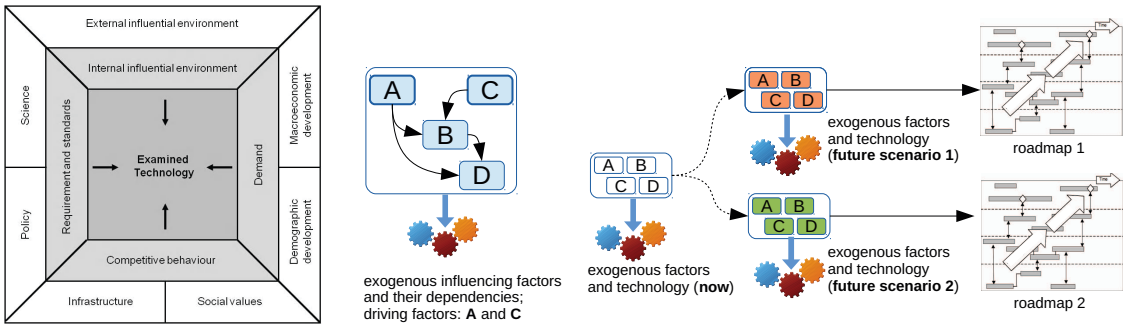

Fig. 3. Left (taken from [7]): high-level view of the exogenous and endogenous factors influencing a given technology. Right: sketch of the exploratory roadmapping approach of [7].

anonymising techniques (see, e.g., [6][5]).

The above considerations imply that the evolution of CC and CT can not be understood by considering them as "black boxes" influenced only by their contextual environment; instead, their peculiar, internal driving forces must be taken into account as well, like the cyber logic and cyber economy (see, e.g., the Hacker Profiling Project). Accordingly, a project like CyberROAD requires a specific roadmapping methodology; in particular, it must be different from methodologies adopted in projects like those mentioned in section II, whose subjects (e.g., e-government and health services) are related to phenomena that mainly evolve under the influence of external driving forces, and do not exhibit any significant co-evolution behaviour.

A. *Toward the CyberROAD methodology*

As pointed out in Sect. II, the first choice related to the roadmapping methodology is between a normative and an exploratory approach. Given the characteristics of CC and CT discussed above, this choice is not straightforward. On the one hand, the fact that the contextual environment, including long-term government policies, influence the evolution of CC and CT (e.g., enabling new attacks), is in principle a characteristics that allows a policy-oriented, normative approach, like the one of [10]. This would allow one to apply a Backcasting process to define a Desired state, and the main actions required to attain it; for instance, one could exploit existing, high-level EU policy objectives (e.g., white papers), to derive more specific, technical goals, such as hypothesising specific policies against CC and CT at the end of the roadmap time span.

On the other hand, the peculiar co-evolution of CC and CT with its contextual environment makes it infeasible to predict their evolution with a degree of certainty as the one required by the Path dependency step of [10], even in the short term. Therefore, even if specific objectives can be defined in the Backcasting step, defining specific actions to reach them in the Path dependency is not possible under such a dynamic setting. This implies that a purely normative approach is infeasible for analysing the evolution of CC and CT from the Current state. Accordingly, a scenario-based, exploratory approach appears better suited to define the Path dependency. To this aim, the approach of [7] is appealing. In particular, we point out that this approach is based on analysing the evolution of the roadmapping subject as a function of two distinct kinds of influencing factors, the "exogenous" and "endogenous" ones; in the context of CyberROAD, such a distinction closely resembles the one between the external driving forces of CC and CT (e.g., their contextual environment) and the internal ones.

Based on the above rationale, we initially developed a hybrid normative-exploratory approach by combining the ones of [10] and [7]. This approach is sketched in Fig. 4. The Backcasting step starts from a Context to be derived from long-term, high-level EU policies. For instance, they can refer to strategic interests and assets (like critical infrastructures), and to future EU roles in the cybersecurity field. This should lead to hypothesising more specific goals (the Desired state), as explained above. Subsequently, starting from the Current state of CC and CT and of their contextual environment, their possible evolution has to be envisioned in the Path dependency step through a scenario-based, exploratory approach. In particular, several "vertical" roadmaps can be developed to investigate the evolution of different, specific environment/business scenarios of interest, like social networks and mobile workforces. In the end, the outcomes of these exploratory roadmaps will be compared with the desired state, which allows one addressing questions, e.g.: What goals can be achieved, given the transition path? How to change the scenarios (technology, legislation, etc.) so that also the other goals can be achieved? What are the research priorities during the transition path?

The above hybrid solution is coherent with methodologies proposed in the roadmapping literature, as well as conceptually elegant. However, its normative component turned out to be infeasible in the specific CyberROAD context. The main reason is that CC and CT are worldwide phenomena. This implies that defining a normative "desired state", limited to EU, is nearly infeasible. Moreover, in a field like cybersecurity, a cooperation between research teams from very different fields (such as social sciences, economics, computer security, etc.), as well as government, law enforcement agencies and private companies, is required. We therefore chose to retain, and further develop, only the explorative part of the above approach. In particular, we let the final scenarios emerge in a bottom-up fashion from an aggregation of distinct, "vertical views" of the contextual environment of CC and CT; each view

[5] Available at http://www.sicherheitsforschung-magdeburg.de/uploads/journal/MJS_033_Frumento_Assessment.pdf

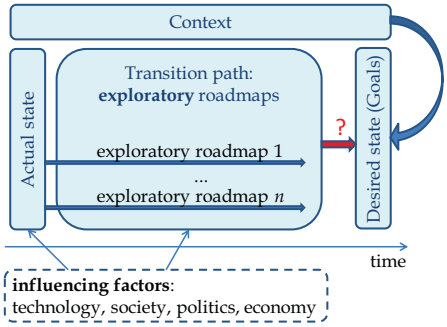

Fig. 4. Sketch of the preliminary roadmapping methodology developed for CyberROAD, as a hybrid normative-exploratory approach that combines the ones of [10] (see Fig. 2) and [7] (see Fig. 3).

is autonomously developed by experts in the different domains involved, without reference to a desired state. This approach is described in the rest of this section.

B. Outline of the proposed methodology

The roadmapping methodology we finally developed builds on the one of [7] and, partly, on the methodology followed in the eGov2020 project [4]. Our methodology is based on scenario analysis, coherently with the chosen exploratory approach. In particular, in the CyberROAD context the final aim of scenario building consists of identifying the resulting CC and CT threats, and the corresponding desired defences. To this aim, the wide contextual environment of CC and CT has to be taken into account, i.e., the technological, social, economical, political, and legal aspects that can influence the evolution of CC and CT. Accordingly, we defined a *scenario* as a concise, internally consistent and coherent sketch of a possible future state of CC and CT and of their context. In particular, the state of CC and CT consists of the threats that may arise under a given scenario, and of the corresponding desired defences. The roadmap is then obtained after a *gap analysis* step, aimed at identifying *research gaps* emerging from the comparison between the threats and the defences in the actual state, and the ones in each future scenario.

Our roadmapping approach consists of four main steps, which are described in more detail in the following, and are summarised in Fig. 5):

- Representing the actual state as a scenario, to allow a direct comparison with future scenarios
- Scenario building
- Gap analysis
- Roadmap construction

1) Actual state scenario: The actual state has to be described as a scenario, using the template shown in Table I. It consists of a short summary of the contextual environment, followed by the existing CC and CT threats and the available defences. In particular, each threat has to be characterised by the following information, in order to allow quantifying its *risk* in the subsequent roadmapping steps: the assets targeted by the threat, its likelihood, and its consequences.

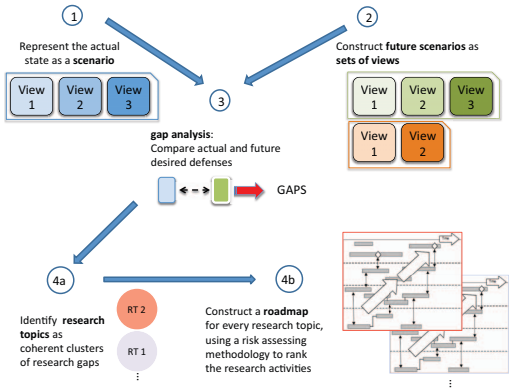

Fig. 5. Outline of the proposed methodology.

TABLE I. SCENARIO/VIEW TEMPLATE

View title
Summary (one page)
Key driving factors (only for the actual state)
Threats • description • targeted assets • threat likelihood • consequences
Defences

Given the multidisciplinary nature of this subject, we chose to subdivide the actual state scenario into several coherent, vertical *views* of the contextual environment. Each view focuses on a specific, sectorial aspect, like payment systems, driverless vehicles, mobile devices and services. This allows each view to be defined by *different* domain experts.

Finally, the *key driving factors* of each view must be identified, i.e., the ones that are expected to exert the highest influence on the evolution of future scenarios.

2) Scenario building: The goal of this step is to produce a set of possible future scenarios, which should explore a range of potential evolutions of CC and CT and of their contextual environment as wide as possible, highlighting the threats that can emerge, and the corresponding, desirable defences. For the same reason above, we chose a bottom-up scenario building approach, in which the final scenarios emerge by aggregating several vertical views of the contextual environment. This can be attained with three sub-steps (see Fig. 6):

1) Domain experts on each of the subjects that compose the contextual environment (society, politics, economy, and technology), build a set of *initial* views.
2) Coherent initial views are then combined to obtain a small set of broader, *final* views of the contextual environment, which must be *alternative* to each other (i.e., contradictory). To this aim, the most relevant and interesting groups of initial views should be identified, using the following guidelines:
   - a final view can be obtained by merging initial views that are coherent (non-contradictory), and contain elements which can interact, resulting in specific CC and/or CT threats;
   - the same initial view can be included into more than one final view, provided that such

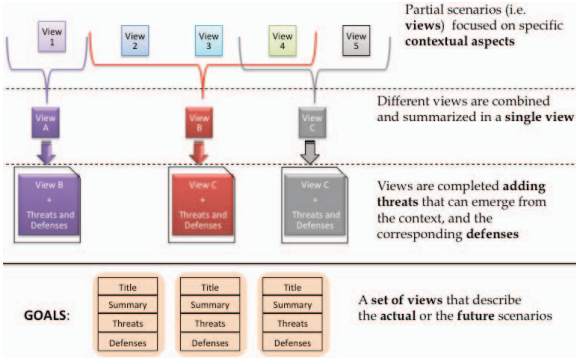

Fig. 6. Scenario building.

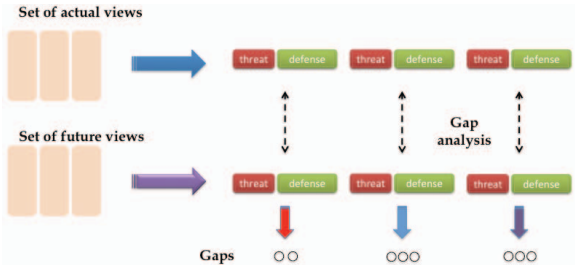

Fig. 7. Gap Analysis.

final views are alternative to each other (i.e., they must contain also contradictory initial view, as explained above).

3) Each final view has to be completed by adding the specific aspects related to CC and CT, i.e., by envisioning the possible, corresponding threats and defining the desired defences.

Each final view must be described according to the same template used for the actual state scenario, excluding only the key driving factors (see Tab. I).

3) Gap Analysis: The goal of this step is to identify the research gaps that emerge from the comparison of each of the future views with the actual state views (see Fig. 7). We define a research gap as a specific research issue that needs to be addressed, to enable a desired defence against a specific threat. Research gaps have thus to be identified by tracking the changes of the threats from the actual to the future scenarios, and comparing the corresponding existing and desired defences. In particular, a given threat in the actual state can increase, decrease, remain unchanged, or disappear in a future scenario. Novel threats can also appear in a future scenario. The outcome of gap analysis must be summarised in a table in which each row contains a single threat from a future scenario (either a known or a novel threat), the defence existing or pursued in the actual state (only for known threats), the desired defence in the future view, and the identified research gaps (see the example in Table IV).

4) Roadmap construction: The final roadmap, aimed at addressing the identified research gaps, is defined through the following sub-steps (see Fig. 8):

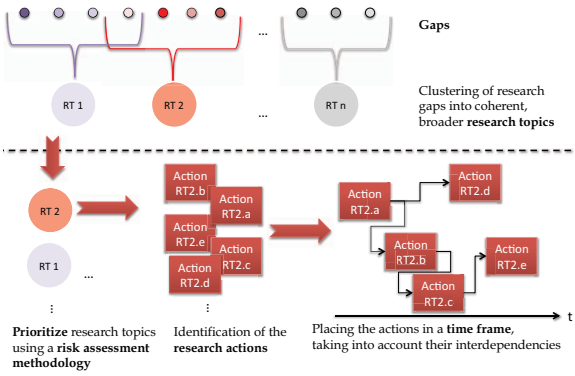

Fig. 8. Roadmap Construction.

a) Defining a set of broad *research topics*, as coherent clusters of related research gaps, that can be addressed by a suitable sequence of research actions, i.e., EU projects.

b) The identified research topics are prioritised using a suitable risk assessment methodology, taking into account the relevance of the threats they address. In particular, this will be attained by evaluating the **risk** of each threat (using the information mentioned in Sect. III-B1), as well as the following **non-risk** (cost) factors that have to be defined for each research action: distance to the market (in terms of Technology Readiness Level[6]), cost of the action, estimated in terms of the number of projects the EU should fund for getting proper results, and availability of competences in Europe.

c) A distinct, "vertical" roadmap is defined for each research topic. This is attained identifying the specific research actions required to address the corresponding gaps, and putting the actions into a clear time frame, taking into account their interdependencies.

IV. An Example

Here we give an example of the application of the above methodology, focused on the definition of a vertical view of the current state and of a possible future state, and on the subsequent gap analysis. The topic of both views is the evolution of the *workforces*, i.e., how the people are accustomed to work. This is one of the aspects arising from the wide adoption of the mobile technologies. The digital devices have strongly shaped the way people are working and collaborating. The everyday working activity can be seen as a continuous process of updating user's personal data space through an enabling technology, selected among several with the usability in mind. Private and professional lives blend, due to the flexibility to work at any time from different locations and consequently physical and virtual encounters seamlessly merge.

Tables II and III summarise respectively the current and a possible future state of workforces, including threats and defences. Table IV shows a possible outcome of gap analysis.

[6]See the definition of TRL proposed by the European Commission in the Horizon 2020 context: http://ec.europa.eu/research/participants/data/ref/h2020/wp/2014_2015/annexes/h2020-wp1415-annex-g-trl_en.pdf

TABLE II. EXAMPLE OF A VIEW OF THE ACTUAL STATE RELATED TO WORKFORCES

Title: Workforces

Summary: The recent global recession directly influences the labour market, adding new paradigms, more flexibility and more mobility. Thanks to mobile and ubiquitous terminals, a user could complete a task in any possible place, home, public spaces or company office. The market is constantly offering new "methods" to access a users own data space like, for example, the expected revolution of the wearable electronic and IoT. We are working into a Digital ecosystem: a community of people and smart objects, who interact, exchange information, combine, evolving in terms of knowledge, skills and contacts. New Data spaces services are available moving toward a complete dematerialisation of the personal data space on centralised cloud services. Among cloud services is emerging the concept of federated cloud and clout, where common standards for both hardware and software companies exists.[7] The essence of cybercrime is to abuse the trust chains to steal assets. Within this scenario, what defines the security patterns are the trust chains, which are growing in number and are influenced by logical and physical contexts.
Possible key driving factors: Blending life, Evolution of privacy & Identity

Threats:

- Increased importance of the human element in the enterprise processes
- Heterogeneous attack surface for the enterprises
- Cybercrime market and cybercrime as a service (Cybercrime=marketing)
- Exploitation of the new sharing habits and changes in the perception of risk and privacy
- Legislation inconsistencies (hide between the cracks)
- Abuse of unnoticed trust chains also due to the increasing of disappearing computing or immersed human paradigms

Defences:

- Legal and Law Enforcement issues:
  - Privacy and data legislation is important to help defining which data of the personal data space a user can access, in a specific place to protect his identity, privacy or to respect some security policies[8]
  - Relevance of the Cybersecurity insurance and connection with the active defence systems[9]
- Technological issues:
  - New authentication methods (no password, behavioural, fuzzy security, ...)
  - New counterattack and prevention technologies[10]
  - Inclusion of human elements inside an holistic strategy of protection
  - Threat intelligence

[7] http://www.identity-tower.com/blogs/enrico-frumento/redefinition-digital-identity-through-evolution-modern-workforces-part-1, http://www.identity-tower.com/blogs/enrico-frumento/redefinition-digital-identity-through-evolution-modern-workforces-part-2
[8] http://www.identity-tower.com/publication/task-force-1-personal-information-space
[9] http://www.agcs.allianz.com/services/financial-lines/allianz-cyber-protect, http://www.bankinfosecurity.com/rsa-conference-rise-cyberinsurance-a-8153
[10] http://www.govtech.com/dc/articles/Will-DPM-5GL-save-cybersecurity.html

TABLE III. EXAMPLE OF A VIEW OF A POSSIBLE FUTURE STATE RELATED TO WORKFORCES

Title: Workforces, situation of distributed power

Summary: This scenario sounds like a world where individual rights are respected, and where people profit from the services delivered by machines without losing control over their personal information space. People generally seems to have some concerns about their privacy but have confidence in the technologies at issue. In a scenario where the integration of service largely uses a peer-to-peer decentralised approach, it is in general possible to have isolated service providers and isolated peers. Their business is to be disconnected from others for several reasons (privacy, independency, or hiding themselves from the others). People are less dependent on one service provider; interoperability is forcing services and platforms to compete in offering the best user experience. This scenario is characterised by the typical elements of "Blending life": a world where physical and virtual encounters seamlessly merge. There is a blending between private and professional lives due to the flexibility to work at any time from different locations and media. This kind of society has moves toward a complete dematerialisation of the personal data space on cloud services. The public services (e.g., health) can exchange the data they need to deliver proactive personalised alerts and reminders. All these elements combine to create an idea of growing service customisation. Another important aspect to be considered in this scenario is the revolution in automation field, which implies the diffusion of automatic transports.

Threats:

- New forms of abuses/new targets: Human, IoT, Infrastructures, Linked open data, Social, Connected things (smart card, IoT, wearable)
- Minor perception of information security risk because of people, finding themselves living in blending life, starts to take for granted the technological infrastructure and it becomes somehow "transparent" to the user
- Wide adoption of authentication behavioural methods and behaviour theft (like nowadays the identity theft)
- Extreme data broker, i.e., fake identity trading (see "Data Brokers A Call for Transparency and Accountability", American FTC, May 2014)

Defences:

- Legal and Law Enforcement issues:
  - Policies related to privacy are becoming less cumbersome, the central government establish the general directions and criteria
  - Term-of-service (ToS) are becoming more invasive and start to regulate more aspects of cyber lives than in the past. The users accepting them automatically comply to these set of "rules"
  - Cross-border legal problems with cyber entities complying with laws frameworks of a foreign country
  - Right to be forgotten evolved into something functional (see the book Delete, by Viktor Mayer Shörimberger)
- New protection systems:
  - Situational security authentication system (based on behaviour of humans and machines)
  - Protection systems that emulate humans as human honeypot
  - Personality virtual alter ego, etc.

TABLE IV. EXAMPLE OF GAP ANALYSIS ON THE VIEWS IN TABLES II AND III. THE SYMBOLS NEXT TO THE GAP NUMBER DENOTE WHETHER THE CORRESPONDING THREAT IS INCREASING (↑), DECREASING (↓), UNCHANGED (=), OR A NEW ONE (!), GOING FROM THE ACTUAL TO THE FUTURE VIEW.

Gap #	Threat (future view)	Threat (actual view)	Defence (future view)	Research gap
1 (↑)	Abuses on new targets (Human, IoT, Infrastructure, linked open data, social, connected things ...)	Statistics and detection of preferred attacks patterns	Threat intelligence and detection of new opportunities before they are exploited; emulate human behaviour and creation of "human honey pots"	Threat and attack intelligence, attack simulation infrastructures
2 (=)	Abuse of unnoticed trust chains also due to the increasing of disappearing computing or immersed human paradigms	Identification of trust chains; extended testing; arm race with attackers in finding exploits	Identification of NEW trust chains before attackers with proper testing and developing CMMs	NA
3 (↓)	Legislation inconsistencies	New EU data privacy law	Policy related to privacy is less cumbersome; the central government establishes the central directions and criteria	More EU harmonisation; problems with non-EU entities handling EU data
4 (!)	Term-of-service (ToS) are becoming more invasive	NA	Market is becoming extremely aggressive in terms of what it can be done with released data	Monitor the ethical and legislative infrastructure for the ToS of non-EU entities

V. CONCLUSIONS

We described the methodology we developed for constructing a policy-oriented research roadmap for cybercrime and cyber terrorism, at the EU level. In the preparatory phase, we analysed the state-of-the-art of S&TRM methodologies, as well as the available guidelines and related projects, focusing on policy-oriented roadmaps. We also considered the peculiarities which distinguish CC and CT from other fields: one is that they require a multidisciplinary approach involving very different domains; the other, and most relevant one, is that they co-evolve with their contextual environment. This makes a roadmapping effort particularly challenging, and a normative approach infeasible. We finally chose an exploratory approach based on a bottom-up scenario building step, in which the possible, future scenarios are obtained by aggregating vertical views of the contextual environment, obtained by combining the contributions of the different domain experts involved.

We believe that the scope of our methodology, as well as its rationale, is not limited to the CyberROAD project, nor to its specific subject. On the one hand, it can become a best practice for future roadmapping projects in the cybersecurity field; on the other hand, it can be generalised to phenomena that exhibit a similar, peculiar behaviour as CC and CT, i.e., a strong co-evolution with their own contextual environment.

ACKNOWLEDGMENT

The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n 607642.

REFERENCES

[1] D.A. Beeton, R. Phaal, D.R. Probert, "Exploratory roadmapping for foresight," *International Journal of Technology Intelligence and Planning*, vol. 4, no. 4, pp.398–412, 2008.

[2] R. Bradfield, G. Wright, G. Burta, G. Cairns, K. Van Der Heijden, "The origins and evolution of scenario techniques in long range business planning," *Futures*, vol. 37, pp. 795–812, 2005.

[3] M.M. Carvalho, A. Fleury, A.P. Lopes, "An overview of the literature on technilogy roadmapping (TRM): Contributions and trends," *Technological Forecasting & Social Change*, vol. 80, pp. 1418–1437, 2013.

[4] C. Codagnone, M.A. Wimmer (Eds.), "Roadmapping eGovernment Research – Visions and Measures towards Innovative Governments in 2020," Results from the EC-funded Project eGovRTD2020, IST-2004-027139, 2007.

[5] O. Da Costa, M. Boden, M. Friedewald, "Science and Technology Roadmapping for Policy Intelligence. Lessons for Future Projects," in: Proc. 2nd Prague Workshop On Futures Studies Methodology, pp. 146–161, 2005.

[6] E. Frumento, R. Puricelli, "An innovative and comprehensive framework for Social Driven Vulnerability Assessment," *Magdeburger Journal zur Sicherheitsforschung*, Vol. 2, pp. 493–505, 2014.

[7] H. Geschka, H. Hahnenwald, "Scenario-Based Exploratory Technology Roadmaps – A Method for the Exploration of Technical Trends," in: [13], pp. 123–136, 2013.

[8] "Energy Technology Roadmaps – a guide to development and implementation," International Energy Agency, Paris, 2014. http://www.iea.org/roadmaps/

[9] H. Jeffrey, J. Sedgwick, C. Robinson, "Technology roadmaps: An evaluation of their success in the renewable energy sector," *Technological Forecasting & Social Change*, vol. 80, pp. 1015–1027, 2013.

[10] C.I.V. Kerr, R. Phaal, D.R. Probert, "Roadmapping as a Responsive Mode to Government Policy: A Goal-Orientated Approach to Realising a Vision," in: [13], pp. 67–87, 2013.

[11] R.N. Kostoff, R.R. Schaller, "Science and Technology Roadmaps," *IEEE Transactions on Engineering Management*, vol. 48, no. 2, pp. 132–143, 2001.

[12] H.M. Londo, E. More, R. Phaal, L. Wütenberger, L. Cameron, "Background paper on technology roadmaps," Report for United Nations Framework Convention on Climate Change (UNFCCC), 2013.

[13] M.G. Möhrle, R. Isenmann, R. Phaal (Eds.), *Technology roadmapping for strategy and innovation: charting the route to success*. Springer, 2013.

[14] G. Wright, R. Bradfield, G. Cairns, "Does the intuitive logics method – and its recent enhancements – produce 'effective' scenarios?" *Technological Forecasting & Social Change*, vol. 80, pp. 631–642, 2013.

[15] D. Mietzner, G. Reger, "Advantages and Disadvantages of Scenario Approaches for Strategic Foresight," , 2005.

[16] J. Ratcliffe, "Scenario building: a suitable method for strategic property planning?" *Property Management*, vol. 18, no. 2, pp.127–144, 2000.