Societal Security – Modes of interaction of different stakeholders

S. Grigoleit, R. Schietke, J. Burbiel

1, 2, 3 Fraunhofer Institute for Technological Trend Analysis INT, Euskirchen, Germany

Abstract: This article describes the modes of interaction of the different domains concerned with societal security (social and human science researcher, technology developer, security technology end-user, security policy-maker and civil society organizations) and identifies obstacles and barriers which could hinder a successful interaction and cooperation of these actors to enhance societal security. The final result is a set of recommendations how to overcome these barriers and obstacles and how to enhance knowledge sharing and cooperation between the different domains. For these analyses two types of data were used: a survey among the different stakeholders of societal security as well as literature research about knowledge sharing in general and experiences as well as lessons-learned from other sectors (e.g. health, multinational firms) regarding preconditions, processes and methods to improve common understanding and knowledge transfer.

Keywords: Interdisciplinary collaboration, knowledge sharing, knowledge transfer, modes of interaction, security research, societal security.

I. INTRODUCTION

This research work is a part of the European research project SOURCE [1] which aim it is to establish and support a network linking researchers, actors, agencies and institutions most concerned with societal security in Europe. Security is widely recognized as a primary need and even a universal right. Yet there is widespread disagreement on what security is, which threats cause insecurity, and how we should best seek to increase security through research, policy, legal instruments, product design, industrial development, and practice on the ground. Differing aims, means, methods and assumptions between those domains involved in security research and development contribute to these diverging views.

In academics, security is studied as a social or political phenomenon, while industrial actors regard it as a technological challenge against the backdrop of the market for security products. Public policy-makers see security as a matter of government; civil society actors consider security as a common good, while security end-users are primarily concerned with the actual implementation. Thus, the challenge lies in the fact that though there are many actors concerned with societal security (see Figure 1), they are concerned in widely different ways. These factors influence how the different stakeholders communicate and collaborate. [1]
One of the aims of this research project is to learn about how the different actors concerned with societal security interact. Are there obstacles to a mutual understanding? Is there anything that hinders the actors to reach a common view? In summary, this research project aims to go to the core of what prevents the different domains from interacting and cooperating successfully.

In practice, if different stakeholders come together to discuss security issues, this might typically be about the implementation of a specific security measure or it might be about a more general strategic or policy direction in the area of security or it might be about the spending of money on security investments. In all of these cases a broad range of security aspects has to be taken into account.

It is downright typical for security issues that on the one side many different stakeholders are affected and on the other side many and sometimes contradictory aspects of security have to be considered. What are these aspects one has to take into account? First of all, there is the security value itself which could be represented as a level of (perceived) security or the risk of security incidents. Then, of course, moral and ethical aspects have to be considered. One has to make sure that no civil liberties are infringed and that actions or measures intended to improve the security of citizens are in line with human rights and the ethical principles of those people which are affected by these actions. Security actions also have to fit in the social norms and cultural ideals of the affected society, to make sure that the society will accept the measures and will benefit from them. Security actions also have to be compatible with the framework of the more general political priorities. Security actions should be the logical consequence of general democratic political decisions. And also economic impacts have to be taken into account – both economic costs like the costs for the equipment itself, R&D investments etc. as well as economic benefits, which for example might result out of a reduced crime rate.[2]

In the first part of this article the results of a survey will be presented, which sheds light on the type of interaction among different stakeholders in the area of societal security. In the second part, this article will present the results of literature research on knowledge sharing in general to learn about the general obstacles and barriers regarding the sharing of knowledge and also to learn about how to overcome these obstacles and set up a successful knowledge sharing network of societal security.

II. METHODOLOGY

To reach this objective a questionnaire [3] was developed and distributed. The questionnaire sets the focus on the experienced interaction of the different domains and aims to answer the following questions:

• Do the members of the different domains encounter difficulties in the cooperation with representatives of other domains?

• What type of difficulties do they encounter (different professional background, technical language, organizational issues, etc.)?

• Do they have suggestions how to overcome these difficulties?

• Which of the aspects of security (security value, political priority, social norms, cultural ideals, morals, and economy) is an especially touchy and conflictual issue to discuss with representatives of other domains?

The questionnaire [3] was sent to the members of the SOURCE Primary Network [4] and was also promoted on the SOURCE homepage and social media as well as by the homepages and social media of the consortium partners.

Thus, in summary this questionnaire aims to identify conflictual aims of different actors of societal security which could lead to barriers between the different domains involved. It also sheds light on other obstacles the domain representatives experience in their day-to-day interaction.

III. ANALYSIS OF THE QUESTIONNAIRE

In total, 51 questionnaires were completely filled-in. The majority (66.6%) of the completed questionnaires were sent in by social and human scientists and to a lesser extent by security industry actors/technology developers (19.6%). The remaining domains (end-users (4%), policy makers (4%) and others (6%)) were rather underrepresented in the survey.
This result is completely understandable as also in reality this research area is dominated by technology developers and social and human scientists. Thus in the following only the overall accumulated answers of the questionnaire will be analyzed. Possible differences between the individual domains won’t be compared due to the low number of policy maker and end-users in the survey.

In the first question, the participants were asked how they would evaluate the type of interaction with representatives of other domains. They were invited to think of their day-to-day business with members of other domains, e.g. cooperation projects, meetings, workshops or whenever they do business with representatives of other security domains. In the questionnaire they could choose between “Easy interaction; no difficulties; interaction runs smoothly”, “Sometimes problematic interaction; the interaction has its ups and downs”, “Difficult or conflictual interaction” and “There is no professional contact”. It was also possible to choose with which of the other domains the encounter easy or difficult interactions (by checking the box of the respective domain).

Figure 2: Answer to the question how the participants of the survey would evaluate the interactions with other domains.

In Figure 2 the summed up answers of all participants of the survey is presented. It shows that the majority of the participants of the survey experience the quality of interaction with representatives of other domains as negative. Most of them (45%) rated the interactions as problematic, having ups- and downs, while 17% of them perceived the interactions even as conflictual. However, 28% of the participants see no difficulties while interacting with representatives from other domains.

Figure 3: Assessment of the interactions between social and human sciences actors [n=34] and representatives from the five security domains.
Due to the high number of social and human scientist in the survey it was also analyzed how this domain assesses the interaction with other specific security domains (see Figure 3). As expected – the interaction with representatives from the same domain seems to run much easier as the interaction with participants from other domains.

In a further question, the participants were asked, which were the most common difficulties they experience regarding the interaction and cooperation with other domains (see Figure 4) Interestingly, a more technical reason why the representatives might encounter difficulties in the interaction is by far not the most important one. Thus a formal education of e.g. social scientists in technology or vice versa of technology developers in sociology or ethics would not be enough to overcome the difficulties.

On the contrary, one reason for difficult interaction most of the participants mention is an incompatible ideology or philosophy of life. Thus beyond different technical knowledge or a professional background there is something else which hinders a smooth interaction and cooperation between the different domains. It seems to be the case that the different domains have opposing priorities and aims. That is also supported by the fact that many participants agree that there are (wide) discrepancies between the different professional needs and requirements. Around 20% of the participants even state that their discussions with other domains get heated and emotional.

On a more formal or technical level there are around 35% of the participants who encounter difficulties according to organizational conditions or different time horizons. More personal reasons like the proficiency in foreign languages, differing cultural backgrounds or personal dislikes do not seem to play a major role regarding difficulties in the interaction.

In the next question, the participants were asked to assume that they have been invited to a round table or panel discussion about the implementation of full-body scanner at European airports together with representatives of other domains. They were asked to check those topics they consider to be the most conflictual or touchy issues in the discussion (see Figure 5).

![Figure 4: Most common difficulties encountered regarding the interaction and cooperation with other domains.](image)

![Figure 5: Conflictual issues in a discussion with representatives of different security domains about the implementation of full-body scanners at European airports.](image)
It is most interesting that the participants experience moral and ethical issues followed by social implications to be the most conflictual issues to discuss with representatives of other domains. This underlines the finding that the problem is not mainly about different technical or specialized knowledge and is probably not solved by the exchange of facts and figures. Instead the differences are affected by our own moral concepts and our personal beliefs what security aims we should pursue.

An issue which is also mentioned quite often is the security value of the security measurement itself. It seems to be the case that questions like “will the security measure increase or decrease the perceived security value” are not easy to answer in an interdisciplinary team.

The issue which is at the bottom of the scale in Figure 5 is the economic dimension. When dealing with facts and figures it seems to be easier to reach a common understanding.

Additionally, the participants were asked to make suggestions on how to overcome the encountered difficulties and obstacles. This question was not answered by all participants. However, in total 23 free text answers were received.

The answers show that most of the participants are aware of problems existing between different actors and their different ways of dealing with societal security topics. Although not all of them formulated it explicitly, it seems that the main reason for the difficulties among different security domain representatives is a lack of a common understanding regarding societal security in general and a missing mutual understanding and acceptance regarding different perceptions, perspectives, arguments, and attitudes.

A minority of the participants (3 out of 23 responses) of the questionnaire seem to be pessimistic that the discrepancies between the different domains can be overcome. These participants experience different domains to be in incompatible thought-worlds and see deep-rooted discrepancies between professional needs and perspectives. They have “no suggestion regarding how to overcome the fundamental difficulties with ‘hardliners’”.

Most of the participants suggest having more face-to-face meetings between representatives of different domains. They state that “more dialogue is needed” and that we should “reserve time-slots for interactive-discussions and comparison of how minor and mayor aspects are perceived and understood”. It was also stated that “language is an ongoing challenge” and that we should use plain language and make an effort to “ensure clarity of understanding, reduce jargon, acronyms and ‘insider’ language”. It was also generally suggested to present results in “popular and easy to understand formats”.

To reduce this lack of mutual understanding it was also demanded to educate the representatives of the different domains about the approaches, processes and needs of other domains. Participants wrote that it would be “useful that the researchers recognized the processes and routines of the policy-makers and that the policy-maker understood the principles of research and the “freedom of thinking”. This requires more communication and/or collaboration between the actors concerned with societal security in order to promote the dialogue between them. Knowledge should be shared to improve the understanding of each other, to make points of view comprehensible and to facilitate learning from each other.

IV. KNOWLEDGE SHARING IN SOCIETAL SECURITY

The first part of this article has shown how different stakeholders of societal security experience there interaction and has identified common obstacles to a fruitful communication and successful collaboration like different ideologies, discrepancies in professional needs, different views on morals & ethics or social implications.

The second part of this article presents the results of a literature review in the area of knowledge sharing. The published experiences and lessons-learned from other sectors (e.g. health, business enterprises) have been compiled and translated to the societal security sector. The final result is a set of recommendations how to overcome the experienced obstacles and barriers to a successful interaction and cooperation in societal security.
WHAT IS KNOWLEDGE SHARING?

Knowledge sharing is an activity through which knowledge is exchanged among people or organizations.[6] Davenport and Prusak have distinguished knowledge from information and information from data on the basis of a value-adding process, which transforms collected facts and figures into communicable messages and then into knowledge: [7]

- **Data** is a set of discrete, objective facts about events.
- **Information** can be described as a message, usually in the form of a document or an audible or visible communication. As with any message, it has a sender and a receiver.
- **Knowledge** consists of experience, values, contextual information and expert insight that provide a framework for evaluating and incorporating new experiences and information. It originates and is applied in the minds of knowers.

In general, there are two types of knowledge: tacit knowledge and explicit knowledge.

**Tacit knowledge** is the kind of knowledge that is difficult to transfer to another person by means of writing it down or verbalizing it. For example, the ability to speak a language or knead dough requires all sorts of knowledge which is difficult or impossible to explicitly transfer to other users. Since tacit knowledge is highly individualized, the degree and facility by which it can be shared depends to a great extent on the ability and willingness of the person possessing it to convey it to others. [8–10]

Although the sharing of tacit knowledge is a great challenge, there are various activities and mechanisms which help sharing this kind of knowledge. They include conversations or workshops or the use of information technology tools such as email, groupware, instant messaging and related technologies.[10]

**Explicit knowledge** is knowledge that has been articulated, codified and stored in certain media. It can be readily transmitted to others. The information contained in encyclopedias and textbooks are typical examples of explicit knowledge. [10, 11]

WHY DO WE NEED KNOWLEDGE SHARING?

The different domains involved in societal security operate with fundamentally different understandings of security threats and societal security in general. They differ considerably in terms of their values, their means and their goals. This is because they stem from different “knowledge communities”, that is educational and training backgrounds, institutional foundations, different techniques and technologies, and different means for communication and dissemination of their work.

While there are many publications about the value of knowledge sharing in organizations and the need to share knowledge among the management and the staff in order to grow stronger and become more competitive, [10] there are relatively few publications about knowledge sharing between different domains and types of organizations.
However, in 2006 the European Commission identified the importance of improving knowledge transfer between research institutions, the industry and civil society organization in its broad-based innovation strategy for the EU as one of ten key areas for action. [12]

One of the basic models of knowledge management is the SECI model of knowledge creation. [10] It can be used to explain the process of knowledge creation in organizations on the basis of knowledge transfer activities. While it has been developed for the business sector, it can also be used to understand how knowledge creation could work in broader networks including different domains and disciplines.

The SECI model is based on a double spiral movement between tacit and explicit knowledge. Figure 7 shows the four modes of knowledge conversion: socialization (from individual tacit knowledge to group tacit knowledge), externalization (from tacit knowledge to explicit knowledge), combination (from separate explicit knowledge to systemic explicit knowledge), and internalization (from explicit knowledge to tacit knowledge): [10, 13]

**Socialization** is the process of sharing tacit knowledge of individuals. Sharing experiences is a key to understanding others’ ways of thinking and feeling.

**Externalization** requires the articulation of tacit knowledge and its translation into forms that can be understood by others. Dialogue supports externalization. In practice, externalization is supported by the use of metaphors and analogies.

**Combination** involves the conversion of explicit knowledge into more complex sets of explicit knowledge. Editing and systemizing such knowledge are the keys to this conversion mode.

**Internalization** means the conversion of newly created explicit into tacit knowledge of individuals. Learning by doing, training and exercises are important to embody explicit knowledge. Thus on-the-job training (OJT), simulations or experiments are used to induce internalization of new knowledge.

**Figure 7: Organizational knowledge creation model. [5]**

**WHAT ARE THE PRECONDITIONS FOR KNOWLEDGE SHARING?**

To establish this knowledge sharing culture in a network of societal security and to help create new knowledge, it is helpful to learn from the already established models and processes of knowledge sharing in the business sector and to use the approved tools of knowledge management.

There is no universally accepted definition of knowledge management. Put very simply, knowledge-management can be seen as an application of the SECI model of knowledge creation, i.e. as the conversion of tacit knowledge into explicit knowledge, combining and sharing it with others. It is useful to consider knowledge management as having three pillars. These pillars are: management and organization, infrastructure/content management as well as people and culture. [10]

**Management and organization:** In organizations the most important pillar of knowledge management is the commitment of the highest level of management.
Infrastructure/content management: An adequate ICT infrastructure is necessary in order to better create, organize, share and apply knowledge. In any knowledge management system, three principal technology infrastructures are needed: Firstly, the technology infrastructure needed to organize content (e.g. taxonomy or knowledge mapping); secondly, the technology infrastructure needed to search information, once organized; and thirdly, the technology infrastructure needed to locate appropriate expertise (e.g. people finders).

People and culture: People and culture as an enabler of knowledge management requires three important elements: Firstly, the redefinition of organizational structure, secondly, the corresponding human resource practices, and thirdly, a consistent organizational culture. For a network of societal security only the last two elements are relevant. This means that a network in the area of societal security should take care of inviting all relevant experts and that it is also important to create a climate of trust and an environment of openness.

On the basis of these general preconditions for knowledge sharing it has to be identified on a more detailed level, how knowledge sharing and collaboration in a societal security network could be advanced and how obstacles and barriers could be removed.

WHAT ARE THE BARRIERS AND PROMOTERS FOR KNOWLEDGE SHARING?

In a study about knowledge sharing among different stakeholders involved in the health sector (researcher, policymaker and end-user) several barriers due to different backgrounds and work conditions were reported. [14]

Firstly, academic researchers receive only few incentives from universities to participate in non-research activities beyond publishing in peer-reviewed academic journals and presenting at conferences. As knowledge sharing is often seen as something that occurs after the research is concluded, when resources may be exhausted, the knowledge sharing component is often neglected.

Secondly, policymakers are often faced with the daunting task of sorting through a mountain of information to isolate key knowledge. Research evidence is only one source of information among many others and may conflict with policymakers’ values and the current political climate.

Thirdly, end-users face a number of challenges that limit their participation in knowledge sharing. Often, time and resources are not available to engage in knowledge sharing. End-user may also see research evidence as contradictory with their practical experiences. Given that research evidence may be perceived as inaccessible or difficult to understand, it is not surprising that research evidence may be rejected in favor of professional experience.

In another study about knowledge sharing among scientists [15], Prescott Ensign analyses tacit knowledge transmission in the context of a multinational, multidivisional company. The main finding of Ensign’s research is that reputation matters a great deal in knowledge sharing among scientists, with a favorable reputation of the scientist asking for information resulting in a greater likelihood that the information will be transferred.

In more detail, his study shows that the duration of interaction between different scientists, the predictability of their behavior, the reciprocity (the expectation that the recipient would give help back to the source), the expertise of the recipient, the organizational connection and the uniqueness of the knowledge shared has a positive influence on knowledge sharing between scientists in multinational firms. On the other hand there are factors which influence the knowledge sharing in a negative way. These are a personal or professional relationship (co-work/co-locate), obligation (imbalance of exchange), physical distance and the time and effort required for knowledge sharing.[15],

A study conducted by DG Research in 2006 regarding transnational research cooperation and knowledge transfer between public research organizations and industry highlighted a number of key issues that should be addressed if closer linking between research and industry is to be achieved: [17, 18]

- The alignment of interests between a research organization and a private company within a given Member State is not always straightforward due to different agendas and expertise of the parties;
- Transnational collaboration is additionally hampered by three main factors: cultural differences (including language), legal differences, and difficulties in finding partners.
• Research organizations find it difficult to balance their researchers' desire for open access to research results with the need to protect them if they are to become part of commercially viable products.

• Although not being the sole factor, the differences between existing legal frameworks has a strong disincentive effect on transnational collaboration. The main research related barriers are the differences in IPR ownership regimes and joint ownership.

According to McDermott in knowledge sharing communities four key challenges must be overcome: [19]

• The technical challenge. Human and information systems must be designed to help community members think together, in addition to simply making information available.

• The social challenge. Communities must maintain enough diversity to encourage innovative thinking, yet still have common goals and interests.

• The management challenge. Environments that truly value knowledge sharing must be created and maintained.

• The personal challenge. Community members must be open to the ideas of others, be willing to share ideas, and maintain a thirst for new knowledge.

When these challenges are addressed, knowledge-sharing communities can provide opportunities for researchers, policymakers, and end-users to work together and learn from one another.

WHAT ARE THE LESSONS-LEARNED FROM OTHER DISCIPLINES REGARDING KNOWLEDGE SHARING?

The Handbook of Knowledge Sharing from the University of Alberta [14] formulated three main strategies to overcome common obstacles in knowledge sharing between different sectors:

• Consider the audience: Knowledge sharing is a process that requires guiding the audience in a particular way of thinking. To do so requires an understanding of the problems they face, the level of detail they need, and the style of thinking they use.[19] The message must be one that is valuable to an audience based on their needs, delivered by a messenger they can trust, in a language they are comfortable with.[20]

• Use Plain Language: If a community of people sharing knowledge spans several disciplines and contexts a common language is needed.[19] Thus, the use of plain language is highly recommended whenever possible in knowledge sharing.

• Tell Stories: Evidence itself is not sufficient; it must be communicated in ways that make it compelling. Telling stories may be one way to present research and other forms of knowledge in a way that is appealing to diverse audiences. [20]

The Knowledge Handbook further points out six characteristics of successful partnerships in research collaborations of partners with different backgrounds: [21]

• Cultural sensitivity: Differences between partners are respected.

• Trust. The investments researchers, policymakers and end-users make to engage in a partnership are recognized; disagreements are expected; and ways to resolve conflict are established prior to disagreements.

• Commitment: Partners are committed to solving a problem and see research projects as single steps towards the solution.

• Clear roles and expectations. All parties are clear about their intentions, assumptions, and limitations at the start of the process. In particular, written partnership agreements can be helpful in ensuring clarity.

• Partner with the organization, not the individual. Partnerships should be between organizations rather than individuals to protect against staff turnover and to increase the likelihood that project outcomes will be used.

• Organizational support. Resources such as time and money may be more accessible if employers are supportive of the partnership.
V. CONCLUSION

Firstly, we showed that barriers and disagreements between the different domains do not only depend on the different professional backgrounds or the technological or specialist knowledge of the actors. The main reason for societal security actors experiencing difficulties with other domains seems to be the feeling that they have incompatible ideologies or philosophies of life.

Secondly, we demonstrated that societal security actors experience moral and ethical issues followed by social implications to be the most conflictual subjects to discuss with representatives of other domains. This also shows that the different specialized knowledge alone is not the main reason for the encountered differences. Instead, it seems that it goes to the heart of our personal moral concepts, our ethical principles and our own priorities how societal security should look like.

So in a nutshell we need more debates about values, about ethical principles and moral concepts about how we want to live. We also need settled and commonly accepted guidelines and methodologies which lead us through the necessary discussions about security without experiencing the well-known obstacles and barriers of today.

On the basis of a literature research on knowledge sharing in general and the experiences and lessons-learned of other sectors as well as of the suggestions of the participants of the survey a list of recommendations and strategies for successful knowledge sharing has been developed:

(1) Commitment of all partners to advance the societal security network.
(2) All parties should provide time and resources for knowledge sharing and interaction; especially face-to-face meetings are highly recommended.
(1) Network members must be open to the ideas of others, be willing to share ideas, and maintain a thirst for new knowledge.
(2) The network must maintain enough diversity to encourage innovative thinking, yet still have common goals and interests.
(3) Use of plain language and a presentation adapted to the background and the needs of the audience.
(4) Education and training must be provided to learn about the background, approaches and needs of the other domains.
(5) The network has to provide for cultural sensitivity among its members.
(6) Ways to resolve conflicts are to be established prior to disagreements.
(7) Clear roles and expectations of all parties in the societal security network (e.g. on the basis of a Memorandum of Understanding).
(8) The organization should be a member of the network - not the individual (to protect against staff turnover).
(9) Capable IT tools should be implemented or designed to help the members of the network to share their knowledge.

REFERENCES


