



Global Model and Observatory for International
Responsible Research and Innovation Coordination

D6.2 Policy Brief: RRI for Security



**“This project has received funding from the European Union’s Seventh
Framework Programme for research, technological development and
demonstration under grant agreement no 321489”**

D6.2 Policy Brief: RRI for Security			
Document No.		WP6.2	
Workpackage No.	WP6	Workpackage Title:	Dissemination and Awareness Raising
Start Date:	15 th June 2013	Revision Date:	24 th July 2014
Author(s)		Carolin Brieger (Fraunhofer), Dr. Lilian Mitrou (AEGEAN), Dr. Zaharya Menevidis (Fraunhofer)	
Editor		Dr Rohaya Mohd Nor (UNIMAS)	
Contributors			
Status		R, PU	
Date		24 th July 2014	

* **R = Report**, P = Prototype, D = Demonstrator, O = Other, **PU = Public**, PP = Restricted to other programme participants (including the Commission Services), RE = Restricted to a group specified by the consortium (including the Commission Services), CO = Confidential, only for members of the consortium (including the Commission Services).














No.	Partner Name	Logo
1	Fraunhofer IPK	
2	Signosis Sprl	
3	De Montfort University	
4	University of Namur	
5	Technical University of Berlin	
6	University of Oxford	
7	Geolmaging Ltd	
8	University Sienna	
9	University of the Aegean	
10	University Malaysia Sarawak	
11	Universidad de Chile	
12	Kyushu Institute of Technology	
13	Arbeiter Samariter Bund Wien Gesundheits und Soziale Dienste Gemeinnutzige GmbH	

Table of Contents

Abbreviations	5
Executive Summary	6
1 Security Policy Issues.....	7
1.1 Context and Importance	7
1.2 Aim and Scope.....	7
2 Security Matters and RRI.....	7
2.1 The Security Promise.....	7
2.2 Notion of Security	8
2.3 Urban and Cyber Security Challenges	9
2.4 RRI and Security Measures.....	9
2.5 RRI and the Role of Normative Principles and Legal Rules	10
2.6 RRI for Security Research and Innovation.....	11
3 RRI as Balancing Instrument.....	12
3.1 RRI and Impact Assessment	12
3.2 Privacy by / in Design	13
3.3 The International Context	14
4 RRI and Security Actors	15
5 Case: Security Research Programme in Germany.....	16
6 Conclusion and Recommendations.....	16
7 References.....	19

Abbreviations

Term	Explanation
CCTV	Closed-circuit television
ESRIF	European Security Research and Innovation Forum
EU	European Union
FP7	7 th framework programme of the European Union
ICT	Information and Communication Technologies
IT	Information technology
PACT	Public Perception of Security and Privacy: Assessing Knowledge, Collecting Evidence, Translating Research Into Action
PB	Policy Brief
PbD	Privacy by Design
PIA	Privacy Impact Assessment
PRISE	Privacy enhancing shaping of security research and technology – A participatory approach to develop acceptable and accepted principles for European Security Industries and Policies
RRI	Responsible Research and Innovation
SIA	Surveillance Impact Assessment
UN	United Nations

Executive Summary

This policy paper presents and discusses the gaps (or problems) in the security domain where RRI can serve as a valuable tool to effectively address these gaps. As the RESPONSIBILITY project focuses on the context of RRI from a civil security technologies perspective, the intended Policy Brief (PB) aims to contribute to the on-going public discourse and development of security policies and recommendations. This policy paper highlights the urgency of the new, emerging and complex security issues, and elaborates the importance of engaging RRI as balancing instrument. In this context, RRI should be integrated in the process (particularly related to security research and innovation) to clarify and handle the on-going tension between formulating and implementing security measures and policies, and the issues related to privacy protection. Several pertinent key recommendations are further highlighted at the end of the paper for further consideration and deliberation.

In the paper, pertinent security problems and challenges are discussed and scrutinized. To date, it is speculated that the possible adverse impact towards quality of life such as threats on critical infrastructures (i.e., water, telecommunication, etc.), natural disasters or crimes will be amplified in the densely populated cities. Due to this, there will be growing concerns worldwide about emerging security issues and challenges. This will necessitate a new and balanced security approach to respond to these emerging and new security challenges. At present, formulation and implementation of security measures are largely based, and also too dependent, on technology to offer possible solutions to respond to security needs and challenges. New technologies are being designed, deployed and assessed as part of initiatives in formulating good security measures. Yet, societies around the world continue to express their concerns about these new technologies, particularly on their intended and unintended impacts. The societies exert pressure and demand that these impacts have to be addressed in the early design stages of the technology. The emerging security problems and the wide availability of innovative security technologies and designs, in addition to the growing concerns from individuals and societies, pose great challenge to policy makers at various levels. Hence, re-examining systematically the security concepts and measures is more important than ever, and is vital to any initiative to formulate viable security policies to effectively respond to future security challenges and needs.

RESPONSIBILITY views that RRI and security are always engaged in a dialectical process. Explicitly, every security research project/security tool should identify ethical, societal and legal issues to be faced, but at the same time, research and innovation co-define the aims, the scope and the outcome of security research and security policy. From the international context, RESPONSIBILITY acknowledges that matters pertaining to security and privacy will remain complex and challenging, and will be dealt with differently across countries, and even across different policy actors within a country. Nevertheless, RRI approach to security measures and policies will greatly benefit policy actors and decision makers at various levels of decision making. RRI as balancing instrument embeds with responsibility and regulatory values, as well as directions for framing research and assessing the impact of security technologies, measures and policies. In this view, RRI can transform regulatory choices into research outcomes. The Security Policy Brief, integrating principles of RRI serves the societal needs by addressing the growing security challenges and issues, and further contributes to security policy-making.

1 Security Policy Issues

1.1 Context and Importance

By 2050, seven out of every ten people will live in cities [1]. It is speculated that the possible adverse impact towards quality of life such as threats on critical infrastructures (i.e., water, telecommunication, etc.), natural disasters or crimes will be amplified in these densely populated cities. Due to this, there will be growing concerns worldwide about emerging security issues and challenges. This will necessitate a new and balanced security approach to respond to these emerging and new security challenges.

At present, formulation and implementation of security measures are largely based, and also too dependent, on technology to offer possible solutions to respond to security needs and challenges. New technologies are being designed, deployed and assessed as part of initiatives in formulating good security measures. Yet, societies around the world continue to express their concerns about these new technologies, particularly on their intended and unintended impacts. The societies exert pressure and demand that these impacts have to be addressed in the early design stages of the technology. This Security Policy Brief, integrating principles of responsible research and innovation, attempts to respond to this call. The Policy Brief serves the societal needs by addressing the growing security challenges and issues, and further contributes to security policy-making.

1.2 Aim and Scope

As the RESPONSIBILITY project focuses upon the context of RRI from a civil security technologies perspective, the Policy Brief (PB) aims to contribute to the on-going public discourse and development of security policies and recommendations. The Policy Brief encapsulates the following elements of security as a cross-sectorial theme: protection, reliability, certainty/assurance, confidence/faith, peace and safety. These security elements will further ensure that deliberations can feed into other policy areas. Hence, these deliberations constructively contribute to general discourse relevant to policy-making.

This policy paper provides a clear context about the importance of integrating a responsible research and innovation (RRI) perspective in the initiatives of formulating security policies. It clarifies the relationship between RRI policy (and principles) and policies focusing on security issues and concerns. Several recommendations are being put forward in this policy paper for deliberation.

2 Security Matters and RRI

2.1 The Security Promise

Security – and the absence of it – is part of the cultural and social self-concept of a community. A viable society is unable to exist without a minimum of security being put in place to ensure safety. When there is an occurrence of new threats, the society expects the state to deliver the “security promise”. Today, in large and densely populated cities, providing safety and delivering security promises pose great challenges, politically and socially.

At present, security approaches do not focus only on the defence of the nation state’s borders, but also, focus on protecting every human being [2]. The notion of security is

perceived to encompass the broader concept of “securitization” [3]. This broader view of security holds that security is existentially linked to survival, and goes beyond military conceptions and “traditional” military security (defence). Thus, security also encompasses civil security (fight against terrorism, protection and prevention against crime, prevention and detection of fraud, cyber security, energy security (in the face of geo-political threats to energy supplies and in the context of environmental concerns exacerbated by climate change), environmental security, food security (both in the context of food safety and food supply), health security (i.e. disease prevention and treatment) as well as social security.

2.2 Notion of Security

Security, in a nutshell, is the absence of danger [2]. *“Security is the condition (perceived or confirmed) of an individual, a community, an organization, a societal institution, a state, and their assets (such as goods, infrastructure), to be protected against danger or threats such as criminal activity, terrorism or other deliberate or hostile acts, [and] disasters (natural and man-made)”* [4].

The holistic view of security as a concept incorporates a range of factors and elements, from material assets to values such as hope, trust, confidence and resilience. The context of civil security, as an example of a cross-sectorial theme for security, covers processes and measures for protection, reliability, certainty/assurance, confidence/faith, peace and safety related to persons or to objects and conditions.

In practice, the public perception of security can be quite different than the state’s perception and understanding of security. These different perceptions are conditioned by several interpretations on relevant security principles or themes such as human security and personal security.

For example, it has been widely acknowledged that human security factors may include health, wellbeing, financial stability, welfare, civil liberties and human rights, as well as less tangible existential notions of home, place, freedom, respect, meaning and happiness. The concept of personal security, on the other hand, as explicitly emphasized in the Charter of Fundamental Rights and Freedoms, is about the protection of human rights that will require the state to take appropriate measures to safeguard these rights from violation by others (security measures as positive obligation of the State) [5]. These interpretations about security as an example, are inarguably contributing to the differences on security perception and expectation from the viewpoints of individuals and the state.

The Council of the EU stated that: “security means protecting people and the values of freedom and democracy so that everyone can enjoy their daily lives without fear” [6]. Such security approach must not focus only on the defence of the nation state’s borders but has to contribute to the protection of every human being [2].

In today’s globalized world, societies and nations are facing on-going and emerging security problems that pose great challenges to deal with. These new security problems and challenges will require a systematic inquiry to re-examine the security concepts and measures. This process is fundamental in any effort to formulate viable security policies to effectively respond to future security challenges. In the context of urbanized and networked societies for example, the new and emerging threats related to urban security or cybersecurity impose challenges on communities to exercise security rights and to propose effective security measures. Due to the nature of the security risks associated with this

modern way of living, one will argue that, if the safety and security of civilians, and their welfare, has traditionally been the responsibility of nation states, these states might no longer possess all of the means to deliver [7].

The following further elaborates the context of security challenges related to urban security and cyber security as good examples to demonstrate the importance of re-examining the security approach and measures for policy-making contribution.

2.3 Urban and Cyber Security Challenges

The trend of urbanization has imposed great challenges to many municipal governments to deal with in order to provide sufficient security to all urban residents [8]. Although urbanization is not a new phenomenon, yet in the past few years, the unprecedented speed and scale of demographic shifts due to the trend has caused great security concerns. At the beginning of the 19th century, it was just about three percent of the world urban population [8]. In 1990, fewer than 4 in 10 people lived in urban areas. However, in 2010, the world urban population has increased than ever before, and more than half was noted to live in cities. By 2050, it was speculated that the urban population would grow to 7 out of every 10 people. At the same time, the impact of adverse events such as contamination of the water supply, natural disasters or crimes is amplified in densely populated urban settings [9]. Further, the interconnectedness and agglomeration of infrastructures in urban areas, inarguably, are exposed to heightened risks of being attacked. Urban security has thus become one of the most challenging problems in a globalized and networked world.

Another security challenge, providing protection in the digital world or cybersecurity has been noted as another biggest concern facing by various countries and international institutions. Societies and individuals are becoming more and more dependent on networks and information communication and technologies (ICTs) in various aspects of life. This has led to people's live to become increasingly vulnerable to cyber threats and crimes, as well as other unintentional (or accidental) cyber incidents. In the European region, the increased of cyber-attacks and the sophistication of the methods use, as well as the growing scale of the targeted damage have made cybersecurity as a prioritized agenda for many European nations [10]. Cybersecurity incidents, either intentionally or accidentally, can disrupt critical infrastructures. Consequently, the taken-for-granted resources, services and supplies (such as water, gas, electricity, healthcare, public transportation or mobile applications) will be greatly affected. If the critical infrastructure disruptions and problems persist, possible chaos among the public will occur, and this in turn, can become a matter of national security.

2.4 RRI and Security Measures

Value-oriented approaches of security combine the protection of security with the protection of values of freedom and democracy [6]. As the focus has been shifted from the security of state to the security of people, hence without doubt, the security measures and approaches are inextricably bound to society's political, cultural and ethical values.

The European Security Research and Innovation Forum (ESRIF) underlines three major characteristics of security:

1. People — both as the source and the object of insecurity;
2. Society — in the knowledge that some threats will target people's identity, culture, and way of life;

3. Values – and which proactive and reactive measures can protect Europeans while reflecting their values and way of life [11].

In this context, one has to understand also that a common ground of systems for precautionary measures and surveillance is that they are accompanied by nuisance, incident, or annoying and irritating situations, or cases where the proportionality and adequacy determines the degree of acceptance.

The excessive use of security measures may impede social and personal development too. *This search for security is often conceived in tension with respect for fundamental human rights, especially the right to privacy* [12]. Surveillance research and technology for instance will support security forces in preventing criminal offenses, but contemporaneously it has ethical and legal implications. Individuals often consider those measures as infringement on their right of privacy. We will focus on privacy as it constitutes a key concern that RRI should address. At the same time privacy policy and protection demonstrate many of the problems that RRI faces.

Further, in view of the boundaries set by the need to serve both the social goods and interests and the fundamental rights, we identify the need to define what “we want science/research and innovation to do” [13], and how to respond to the aforementioned challenge/requirement and create value for society. This implies defining benefits, needs, impacts, threats and risks of any decision that is taken either in the context of security research or in relation to security/securing measures.

2.5 RRI and the Role of Normative Principles and Legal Rules

Respecting and preserving fundamental rights and freedoms while guaranteeing security reflects a major goal, and at the same time a major challenge of a functioning democratic society.

Both the governance of science and technology (research and innovation) and the governance of security policies should be based on normative values and targets that are democratically agreed. Research and innovation policies, like other policies, have also to be driven by the EU Charter, the Treaties and the law, which are legally binding. It is noteworthy that the European Treaty on the European Union (Article 3) provides normative anchor points that in their mutual relationship provide a legitimate basis for defining the type of impacts, or the “right” impacts research and innovation should pursue [14].

Normative principles and legal rules serve RRI as they define whether a particular type of research and innovation is desirable or acceptable [15]. Regulatory values as well as rules as such (can) provide concrete anchor points both for framing research and assessing the impact of security policies. At the same time RRI, transforms regulatory choices into research outcomes.

The issue of responsible research and innovation creates a certain institutional ambiguity in relation to security. Explicitly, every security research project/security tool should identify ethical, societal and legal issues to be faced but at the same time research and innovation co-define the aims, the scope and the outcome of security research and security policy. In this way, RRI and security are engaged in a dialectical process. Values, principles and legal provisions (are attempting to) define the range of research and innovation.

However we should not ignore the driving force of technology. Institutional values and principles do acquire and foster their content also through the opinions and expectations that are formulated and formed in the society. The availability of innovation products and the promises of technological progress and goods for the well-being of the individuals may slightly, but definitely influence or even change their position on certain core fundamental values and consequently the interpretation thereof. The wide availability of (cheap) CCTV or biometric/face recognition systems, and respectively their increasing use also in the private sector and by private citizens change slightly but steadily the social perception of what is acceptable or excessive in relation to security measures, while influencing inevitably the regulatory content of core principles such as the principle of proportionality.

Furthermore, responsibility requires agents engaged in research and innovation to adhere to principles, rules and norms. Compliance with regulatory standards seems to be the simplest (necessary but eventually not sufficient) way to demonstrate and assure responsibility [16] as regulatory standards in democratic societies (should) crystallize the core perceptions, principles, balances and boundaries. However, even the way of compliance differs depending on the concrete perception about the conflicting and prevailing values and interests and the perception of the role and aim of RRI.

2.6 RRI for Security Research and Innovation

Moreover, what seems to be required with regard to the concept of responsibility is more and more an anticipatory and reflective function and approach of RRI. Both compliance and anticipation requires that researchers and actors engaged in innovation are aware of the broader social, legal and ethical contexts of their work [17], as research and innovation are not ends in themselves but they are (or in any case they should be) linked to social welfare and individual well-being.

For instance, after the terrorist attacks in the United States and Europe, an immense state-investment in security technologies has been created. The increased number of cyber-attacks against information systems and critical infrastructures, sometimes at the boundaries of (cyber) war as in the case of Estonia have led to an enhancement of relevance and consequently of investments in cybersecurity, which presupposes security research.

Security technologies often incorporate the aims and functions of the present holistic coherent security strategy: pre-emption, detection and enforcement. Security and surveillance technologies' core function is the monitoring of people and assets either in the physical or the electronic world, each on a different level of detail and scope.

The technology used for security purposes is not value neutral; it may serve to support or reinforce some values and principles at the expense of others [18]. For example a (video) surveillance system may be designed and deployed in a way that responds to privacy requirements while deploying Privacy Enhancing Technologies, i.e. by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data (for example by scrambling the face of persons), all without losing the functionality and efficiency of the information system [19].

Responsibility, as imperative, is an emergent issue that incorporates, reflects and influences social values. Responsibility is obtaining "some characteristics of a coercive force that attempts to shape actions" [16]. In this perspective, Responsibility may function as a

defining balancing instrument to support security research and policies being in line with ethical and legal requirements.

One of the biggest challenges to consider is about the need to reconcile the right of any person to security (Article 6 of the Charter of the Fundamental Rights and Freedoms) with the right of private life (Article 7) and data protection (Article 8).

RRI cannot and should not substitute social and political choices. The ideal of RRI derives from the combination of some elements that are equally relevant, if not crucial, for security research and policies, i.e. (ethical/ legal) acceptability, risk management and human/social benefits (gained through/from achieving the goals set). Either in the form of “ethical technology assessment” [20] or anticipatory impact assessment, researchers and innovators do carry the responsibility to identify, describe and assess the (intended or unintended) impacts and effects of research and innovation as well as recognize and provide indicators of ethical/legal implications.

3 RRI as Balancing Instrument

The tension between security and privacy highlights the role of RRI in respective social dispute and conflicts. Policies designed for security (surveillance, controls, access controls, online and offline tracking, extensive communications data retention) represent an intrusion into individuals’ informational/communicational privacy and personal autonomy and may result in an infringement of the said rights. Security research policies and measures need to consider aspects of privacy and data protection.

In this perspective, security may reconcile security and fundamental rights by making fundamental rights the primary asset to be protected through security policies and actions without turning up the notion of security into a fundamental right itself, as security should continue to be conceived as a condition of freedom.

Security measures must be legitimate and proportionate in order to gain societal acceptance and always applied in accordance with the rule of law. There can be no security measures without taking into account the respect for the rights and freedoms of individuals, especially for the protection of citizens' privacy and data protection.

Privacy protection in the context of security strategy provides a paradigm of how RRI and technology can be dealt with. Legislation pertaining to protection of personal data reflects on the other side the role and range of regulation to address a core requirement of RRI, i.e. the regulation of contested technology related issues [21].

Moreover, with regard to the protection of individuals’ rights and freedoms, methodologies have been developed that aim at integrating regulatory requirements into research and innovation, with the most relevant example being the idea of “privacy by design” [15]. Privacy protection is more and more relied on assessment and foresight.

3.1 RRI and Impact Assessment

As already underlined, both compliance and anticipation requires that researchers and actors engaged in innovation understand the social, legal and ethical contexts and impacts of their work. Compliance and anticipation presuppose identification, consideration, assessment and where necessary control of risks and impacts. Impact assessment

represents a tool of/for technology and research governance, being an element of responsibility.

Security technologies in themselves embed the ambiguities and tensions which are also constitutive of the very concept of security. Security technologies have to be assessed with regard to their effects on society and individuals' rights. In the case of privacy implications of a security measure, a double assessment is usually and more specifically required/proposed, this case: Privacy Impact Assessment (PIA) and Surveillance Impact Assessment (SIA). Taking into account the security gains and benefits, unwanted and/or unanticipated consequences have to be framed.

Researchers and innovators are required to pay serious attention to social and other implications, and to improve risk management techniques. Speaking about research, it is interesting to consider here the notion of 'research as policymaking'. The European Group on Ethics in Science points out, that surveillance policies have begun their life as research projects. The group emphasizes that the funding of security and surveillance technologies and projects sometimes evades having an open debate which takes into consideration the politically sensitive nature of the problems that these technologies are intended to solve.

More importantly also, Privacy Impact Assessment has also been suggested as a useful tool for engineers and software developers to help them to consider potential negative consequences of particular elements of a technology design. The PRISE project has developed criteria for performing a privacy impact assessment to be used in the FP7 security technology proposal evaluation and other research funding programmes as (part of the) basis for funding decisions. Therefore, they can be an important safeguard to ensure that public money is only spent on technologies in line with human and fundamental rights, and European values. The responsibility of the assessment based on the criteria should be given to special privacy evaluation teams with the relevant (legal, organisational, technical) abilities for the task [22].

However, this should not mean that RRI actions are to be judged solely on their consequences. Forecasting is not an easy task because assessments are made on the basis of known or potential applications of the technology. Moreover, it has to be taken into account that there is often a significant time delay between the emergence of technology and the understanding of its consequences.

3.2 Privacy by / in Design

Decision-making for undertaking security technology investments is a complex and multi-dimensional process. Hence, it is imperative for decision makers to consider the implications of the decision not just in the short run but also in the long run. Decision makers will need to holistically assess the impact of security measures and technologies that are being considered, from the early phase of the design and development of the idea or technologies. In reflecting to the importance of integrating RRI approach to formulate security policy and undertake decision making, we put forward two examples of concepts - Privacy by Design and Privacy in Design – to further discuss the RRI approach relevant to security research and innovation.

Privacy by design, which was developed in 1990s, could illustrate the interplay between security and RRI concepts, from both regulatory and technological perspectives. Privacy by Design (PbD) asserts that privacy has to be "designed" into systems from the beginning of

the system design. PbD is not a new concept; it embraces a practical approach that orientates the entire life cycle activities pertinent to a technology or system- from research, design, development, implementation, use and disposal – towards the embedment of privacy and data protection into the design of the technology or system.

Another concept, Privacy in Design is closely related with Privacy by Design. Privacy in Design emphasizes on raising awareness about the processes through which values and norms become embedded in the technological architecture. According to the European Group on Ethics, privacy in design refers to the Constructive Technology Assessment (CTA), which was developed in the Netherlands and Denmark. CTA focusses on broadening design, development, and implementation processes. This model emphasizes the early involvement of a broad array of actors to facilitate learning about technology and its potential impacts [5].

Another study, undertaken by Stahl [15], is worth to highlight here as it presents an interesting case study that illustrates the close connection of privacy (including the application of PbD) and RRI concepts. The case study is about a collaborative research project on a mobile biometric security device for online banking applications. The case further reveals the tension between cybersecurity and privacy (implications) in a sector that is expected to be “secure” with regard to individual customers (privacy, confidentiality of economic transactions) and the protection of accuracy, trustworthiness, confidentiality and security from the context of economic activities. Based on his study, Stahl further indicates that actors with responsibility for privacy include: policy-makers who approved a call; funders who administer the budget; researchers who adhere to professional standards; and end user organisations which represent user interests. All these actors should commit themselves to legal requirements laid down by the respective laws while implementing value-sensitive design or privacy by design with a view to minimise the potentially negative impact on end users’ acceptance of the technology.

3.3 The International Context

From the international standpoint, security and privacy can be highly contextualized concepts. Whilst globalization integrates government of different nations, and permits interaction at various levels, yet matters pertaining to security and privacy will remain complex and challenging, and will be dealt with differently across countries, and even across different policy actors within a country.

Pressing global issues such as rapid urbanization trends and threats related to cybersecurity will continue to dominate the national agenda of many nations as the digital economy now becoming the backbone of many nations’ economy to grow and sustain. In China for example, which has the world’s largest urban population, security is crucial in the national agendas. The frequent natural disasters as well as other forms of incidents and threats that can affect civil security have led to the establishment of cooperation between China and Europe in the fields of civil security and civil protection¹. Further, in the context of participating in the digital economy, government of different nations, businesses, industries, communities and

¹ See for example http://europa.eu/rapid/press-release_SPEECH-12-449_en.htm and http://www.uaces.org/events/conferences/cork/papers/abstract.php?paper_id=572#.VAodz_lDVVI

individuals worldwide are highly connected and interact daily to transact. Cybersecurity hence has been an important national agenda for many of these countries. Whilst the digital world has created new spheres of freedom, it also has created spheres of insecurity and makes many countries to be vulnerable and exposed to various forms of security risks particularly those related to civil security and cybersecurity. Formulating effective security policy hence has pose challenges greater than ever for many nations to deal with the emerging and new security issues and problems.

Reflecting on RRI for security measures, approaches and policy making, no doubt, RRI can become an important conceptual tool that can be extremely beneficial for the international stakeholders in area concerning security and privacy matters. The important element of RRI - 'responsibility' – is value that is already embedded within various national cultures. From the international context, RRI as a tool can be utilized by policy makers and decision makers in the area of security policy making to sensitize the pertinent contexts and elements crucial for formulating effective security policy that can function within the institutional and legal framework of a particular country.

4 RRI and Security Actors

Social and decision making processes have to be scrutinized and assessed while taking into consideration the actors (to be) involved.

In view of the increasing number of threats from natural disasters or crime, every level of government, in multi-level governance system, is required to be able to demonstrate it has a security policy [23]. States, in this context, play a key role in formulating, implementing, coordinating and supervising policy initiative [24], which combines proactive actions to encourage competitiveness and attractiveness with corrective measures, directed toward the solving of – mostly traditional -security challenges [23].

The deployment of security and surveillance technologies was once considered the prerogative of the State and/or its agencies. This is no longer the case considering commercial entities and individuals who utilise technologies to monitor other individuals in public accessible or private spaces for security reasons, and act proactively or collect evidence to enforce the law or private security policies. Design and implementation of security policies, as well as RRI, comprise a broad range of actors, namely: legislators, public bodies (from local authorities to regional structures), civil society actors, policy-makers at different levels, researchers and research organisations (both publicly and privately funded) and individuals-research users [15].

It seems that especially in some sectors, such as Cybersecurity-strategies, responsibility for security lies with all players of the global information society, from citizens to governments [10]. According to the EU, Cybersecurity strategy needs to properly define and analyse vulnerabilities, and also, to reduce and mitigate risks. The strategy should represent as shared responsibility of both public authorities and private actors. The respective Joint Communication underlines that due to the multifaceted nature of threats, synergies between civilian and government security approaches in protecting critical cyber assets should be enhanced, being supported by research and development and closer cooperation between governments, private sector and academia in the EU.

This “shared responsibility” for cybersecurity, which actually - due to the networked character of almost every activity - affects every other aspect of security, draws a parallel

with the roles and tasks associated with RRI. Since security (and security policies) will challenge individuals and communities in an unforeseen manner, national and regional governments and (especially public) organisations have to work together. They have to engage in this dialogue in order to constantly re-examine the notion of security and clarify and debate the security problems and issues in relation to fundamental rights, especially privacy. Governance, in this context, implies that private and governmental actors are involved in a (non-hierarchical) regulatory process. To encourage a balanced approach between the autonomy of research and the state's regulatory and coordinator roles, new coordination mechanisms have to be considered. The local governments should work together with the community to enable them to be more responsive to the needs, and respond effectively to the security needs of their citizens; the local governments should further engage civil society actors in participatory, transparent decision-making process to help to find socially acceptable solutions to security challenges [8].

5 Case: Security Research Programme in Germany

The security research programme, launched in 2007 by the German Ministry of Education and Research, aims at the development of innovative solutions, which increase civil security while maintaining the balance between security and freedom. In an open dialogue with experts, key topics were identified and the research agenda was established. The programme applies multidisciplinary research by including the whole innovation chain. Scenario-oriented research ensures that the needs of end users are taken into account throughout the entire project phase. International cooperation is also part of the programme. Joint research focuses on harnessing the various potential synergies to shape research and innovation in order to improve public security. During the implementation of the programme, social issues will also play a role. Therefore aspects of data protection, the acceptance of specific technology developments and questions concerning security culture and architecture will be examined [25].

6 Conclusion and Recommendations

In this policy paper, RESPONSIBILITY puts forward several key arguments to illuminate the importance of engaging RRI in the complex process of devising security measures and approaches, and formulating security policies to manage new, emerging and difficult security challenges and problems. RESPONSIBILITY asserts that RRI should be employed as balancing instrument to effectively deal with the on-going tension between formulating and executing security measures and policies, and the issues concerning privacy protection.

The interplay between RRI and security approaches and measures, in addition to political, economic and cultural elements, has been explored in this paper to demonstrate how complex is the security issues, particularly the challenges and risks associated with civil security. Also, the dynamic of the innovative design of security technologies is derived from the complex relationship between these elements. It has been further emphasized in the paper that technological innovations generate substantial impacts to society. Hence, its intended and unintended impacts and effects should be considered at the early design stage.

Framing the problem context within this understanding, RESPONSIBILITY further asserts the importance for dialogues and discussion between scientific experts, political actors, and

other well-informed participants to ensure all concerns and interests are being considered in the process of formulating security policies. The political actors have a task to retain the deliberations' democratic credentials and the interests of its citizens [26]. Also, this approach can further accommodate the context of undertaking security research and innovation where various issues and factors such as cost, method, feasibility, impact, risk, ethics and legal must be considered and assessed at the early stage of any security related project. As generating good decision making process is an integral part of policy-making, hence the public and other stakeholders need to be involved in establishing research agenda, and debate about what should be the outcomes of research and innovation in the security field. This is aligned with the general understanding that: for policy solutions to be implemented, problems have to be defined first, then decisions need to be made and resources must be found and allocated. RRI in this context can serve as a reflective tool and promote participatory approach in security related project and decision making.

RESPONSIBILITY puts forward the following recommendation in the context of engaging RRI and security policies for consideration and deliberation:

- Policies need to foster a multi-disciplinary research approach; researchers from different disciplines have to learn to work together.
- This multi-disciplinary approach has to be inclusive and participatory. More explicitly, this approach has to be opened for all relevant stakeholders and participants that may shape the research agenda. These stakeholders can permit all views and concerns to be considered at the early stage of the research. An Inclusive and participatory approach does not necessarily imply that participants will find a common acceptable consensus. But RRI will bring the contradictory positions to the surface [15]. Thus, RRI will contribute to define clear positions and consequently promote solutions and enhance governance.
- The decision-making processes for security technology investments for policy making in the area of security is a complex, multi-dimensional problem. The processes must consider the implications of such decisions, not only in the short term but in the longer term, and simultaneously, consider also the whole life-cycle of security measures. In this sense, responsible decision making and implementation should be aimed at enhancing decision-making at the strategic level (i.e. security technology investments or policies that affect significantly security infrastructures) rather than the operational level that are more related to real-time optimisation of capacities [27].
- Security policies and measures should be addressed from their inception in terms of their impact on privacy and other fundamental rights (privacy by design and by default) and taking into consideration the imperatives of acting responsibly both in ensuring security and guaranteeing fundamental rights and freedoms.
- Referring to security research protection of fundamental rights and freedoms, ethical reflection and social deliberations should form part of an ongoing research process

- A multi-disciplinary assessment of a research project has to consider not only possible benefits and detriments of the innovation but also public acceptance and risks. The impact assessment should address the potential implications of the proposed technology for fundamental rights and freedoms and if risks are identified, measures should be taken to identify processes to mitigate the risk or to determine alternative methods. [5]
- Privacy and data protection is a key issue both with regard to security policy and in the context of RRI. Therefore, research projects need to be guided by officials, who are experts on the field of data protection.
- Findings – whether they are of scientific or social nature – need to be communicated to the wide public transparently. Comprehensive information and open debates may reduce public concerns and reservations.

The Expert Group report on the Global Governance of Science recommended [2]:

- The continuing promotion of ethical self-governance
 - The self-critical appreciation of relations between science and society
 - Making the results of research as widely available as possible
 - Enacting fundamental human rights
 - Promoting critical reflection and discussion with regard to both the means and ends of science
 - Extending EU leadership in helping to bridge divides
- RRI should be seen as a way to improve a qualitative debate and better decision making on the contested question of safeguarding security.

7 References

- [1] World Health Organization (WHO), "Global Health Observatory - Urban population growth," [Online]. Available: http://www.who.int/gho/urban_health/situation_trends/urban_population_growth_text/en/. [Accessed June 2014].
- [2] European Commission, "Ethical and Regulatory Challenges to Science and Research Policy at the Global Level," Directorate-General for Research and Innovation, Brussels, 2012.
- [3] B. Buzan, O. Weaver and J. de Wilde, *Security: A New Framework for Analysis*, 1998.
- [4] A. J. Sieber (Institute for the Protection and Security of the Citizens - IPSC), "Presentation on CEN BT/WG 161 - Standards for Security and Protection of the Citizens," in *Security Research Conference*, Ankara, 2008.
- [5] European Group on Ethics in Science and New Technologies to the European Commission, *Ethics of security and surveillance technologies - Opinion no. 28*, 2014.
- [6] Council of the European Union, "Internal Security Strategy for the European Union: Towards a European Security Model, 5842/2/10," Brussels, 23 February 2010, 2010.
- [7] R. McRae, "Human Security in a Globalized World," in *Human Security and the new Diplomacy. Protecting People, Promoting Peace*, Québec, McGill-Queen's University Press, 2001, p. 17.
- [8] Canadian Consortium on Human Security and Human Security Research and Outreach Programme of Foreign Affairs and International Trade Canada, "Human Security for an Urban Century. Local Challenges, Global Perspectives," 2007.
- [9] World Health Organization / United Nations Human Settlements Programme, "Executive Summary. Hidden cities - Unmasking and Overcoming Health Inequities in Urban Settings," 2010.
- [10] European Commission, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, Joint Communication to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions, 2013.
- [11] European Security Research and Innovation Forum (ESRIF), "Final Report," 2009. [Online]. Available: http://ec.europa.eu/enterprise/policies/security/files/esrif_final_report_en.pdf. [Accessed 9 July 2014].
- [12] IRISS-Project, *Increasing Resilience in Surveillance Societies - Deliverable D1.1: Surveillance, fighting, crime and violence*, 2012.
- [13] R. Owen, J. Stilgoe, P. Macnaghten, M. Gorman, E. Fisher and D. Guston, *A framework for responsible innovation. Responsible innovation: managing the responsible*

- emergence of science and innovation in society, 2013, pp. 27-50, p. 28.
- [14] R. v. Schomburg, "Prospects for Technology Assessment in a framework of responsible research and innovation," in *Technikfolgen abschätzen lehren: Bildungspotenziale transdisziplinärer Methoden*, VS Verlag.
- [15] B. C. Stahl, "Responsible research and innovation: the role of privacy in an emerging framework," *Science and Public Policy*, pp. 1-9, 2013.
- [16] K. Pandza and P. Ellwood, "Strategic and ethical foundations for responsible innovation," *Research Policy*, vol. 42, no. 5, pp. 1112-1125, 2013.
- [17] E. Fisher and C. Miller, "Contextualizing the engineering laboratory," in *Engineering in context*, Palo Alto, Academica Press, 2009, pp. 369-381.
- [18] A. Carusi and G. De Grandis, "The Ethical Work that Regulations will not do," *Information, Communication & Society*, vol. 15, no. 1, pp. 124-141, 2012.
- [19] European Commission, Communication: Promoting Data Protection by Privacy Enhancing Technologies (PETs), COM(2007) 228 final, 2007.
- [20] E. Palm and S. O. Hansson, "The case for ethical technology assessment (eTA)," *Technological Forecasting and Social Change*, vol. 73, no. 5, pp. 543-558, 2006.
- [21] European Group on Ethics in Science and New Technologies to the European Commission, Ethics of information and communication technologies - Opinion no. 26, 2012.
- [22] PRISE Project, "Concluding Conference Statement Paper," 2013.
- [23] OECD, "What Policies for Globalising Cities? Rethinking the Urban Policy Agenda," Campo de las Naciones, Madrid, Spain, 2007.
- [24] N. Brenner, *New State Spaces: Urban governance and the Rescaling of Statehood*, Oxford: Oxford University Press, 2004.
- [25] Federal Ministry of Education and Research, Security Research - Research for Civil Security, <http://www.bmbf.de/en/6293.php> (30.01.2014).
- [26] Miedema, Frank, *Science 3.0: Real Science, Real Knowledge*, Amsterdam University Press, 2013.
- [27] PACT project, D1.1 Report on Theoretical Frameworks and Previous Empirical Research, 2012.