A COMMUNITIES-OF-PRACTICE APPROACH FOR POLICYMAKING IN THE FIELDS OF SECURITY AND RESILIENCE

Georgios Kolliarakis[1]

German Council on Foreign Relations, kolliarakis@dgap.org

Philippe Quevauviller[2]

European Commission, DG Migration and Home Affairs, Philippe.QUEVAUVILLER@ec.europa.eu

Abstract

Policymaking in highly salient, 'wicked' public policy fields, such as those related to societal resilience and citizens' security, faces a number of challenges with regard to the R&D knowledge production, circulation, and uptake. A number of mismatches at the interface between research and policy impact upon both the *reactive capacity* and the *anticipatory readiness* of actors to prevent, mitigate, and recover from threats and risks: For example, there is *loss of key knowledge* through disconnect between distributed 'sensory' intelligence (practitioners), and centralised 'brain' intelligence (policymakers); *Value conflicts* in prioritizing political agendas along the multi-layered decision regimes at regional/local, Member-State-, and EU-level; *Lock-in* into 'Hammer-Nail' biases, where available solutions dictate problem diagnoses; Not least, an *overstretch* of operational capabilities relating to traditional institutional mandates and obsolete threat assessments.

Major objective of this paper is to provide insights about how to change the modalities of *knowledge production* and *knowledge circulation*, so that promising new technologies 'trickle down' and make a difference in practice. We will explore the linkage between EU-level *security research* and its impacts upon *security policy delivery* on the ground (downstream). Vice versa, we will also point to the untapped potential of end-users' insights for informing future *security policy design* (upstream).

This paper sketches out the value-added and the untapped potential of cross-pollinating a 'Communities-of-Practice' (CoP) approach with anticipatory governance in the field of European Security R&D. The CoP approach aims at *cumulating* and *circulating* emerging knowledge, contributing thereby to better *uptake* of cutting-edge R&D for policy, enhancing *trust* and *fitness-for-purpose* in policy implementation (*reactively*), as well as boosting readiness in anticipatory policy design (*proactively*). The 'Communities-of-Practice' approach allows through problem-driven, semi-formal networks a silo-transgressing flow of knowledge, otherwise bottlenecked through formal, hierarchical administrative procedures, the promotion of shared visions, and the establishment of mutual commitment. The advantage of loosely-coupled, theme-centred CoPs lies into promoting a more inclusive, demand-driven exchange about R&D needs and requirements. Although this is far from being a sufficient condition, or a panacea, it is nevertheless a necessary prerequisite for *effective delivery*, and more *responsive design* of security and resilience policies.

---

[1] Dr Georgios Kolliarakis is advisor for research strategy at the German Council for Foreign Relations. He is one of the principal investigators in the *'Mediterranean Practitioners' Network & Capacity Building for Effective Response to Emerging Security Challenges'* (MEDEA, 2018-2023). The views expressed in this paper are his own and do not necessarily coincide with the views of the German Council on Foreign Relations, or the MEDEA network.

[2] Dr Philippe Quevauviller is a policy officer at Directorate General ‚Migration and Home Affairs', where, among others, he has been responsible for building up the *'Community of Users'* platform. The views expressed in this paper are his own and do not necessarily coincide with the views of the European Commission.

Two pilot endeavours, currently in-the-making, the 'Community of Users on Safe, Secure and Resilient Societies' (CoU), and the 'Mediterranean Practitioners' Network & Capacity Building for Effective Response to Emerging Security Challenges', located at programme and at project level respectively, will serve thereby as examples. This paper should highlight some of the achieved as well as some of the expected impacts of those pilots: First, *establishing 'Knowledge Brokers'* in order to facilitate timely flow of relevant evidence and requirements, both upstream and downstream; Second, *fostering shareholdership, trust, and commitment* among involved actors, including practitioners and the civil society, across the value chain from research production to policy application; Third, facilitating the *passage from Early-Warning to Early-Response*, by raising awareness for organisational, institutional, technological and cultural barriers and opportunities; Fourth, *promoting more robust future-oriented knowledge* for anticipatory policy design, minimising blind spots, and maximising stakeholder-inclusive scenario planning.

Keywords: Communities of Practice; Anticipatory Policymaking; Wicked Public Policy Problems; Security; Resilience

Introduction

The main motivation for this paper has been the rather frustrating observation of *knowledge getting lost*, namely knowledge which is produced by R&D actions, and may become neither accessible to policymakers nor practitioners, failing to contribute to better policy in order to benefit citizens. Loss of knowledge relevant for policy may take different facets. It can be new technological products or new insights about organisational processes which never transform to 'innovations' because stakeholders do not get early enough or properly engaged into the R&D value chain from *production* to *application*. Consequently, the missing link here seems to be R&D *circulation*. Lost knowledge can refer to readily available, robust solutions (technologies, methods) which get ignored because they do not align with vested interests, political agendas, or bureaucratic routines of the potential users. It can also take the form of ill-directed knowledge production, in the form of research actions, which are not responsive to documented needs and requirements of the ultimate end-users. Not least, knowledge may be lost due to organisational silos, lack of inter-institutional cooperation, or interoperability standards and procedures.

Lost knowledge always comes together with high opportunity costs, particularly in the salient policy fields of civil security and societal resilience. The price for failing to prevent, mitigate or recover form threats, ranging from natural hazards and accidents to attacks, might well be unacceptably high for a society or a national political system, or the European Union as a whole. At the same time, a non-negligible amount of national and EU resources is invested to mission-

driven research and innovation actions which ought to deliver on making a positive difference in practice.

The principal objective of this paper is to provide insights about how to change the modalities of knowledge production and knowledge circulation, so that promising new technologies 'trickle down' and make a difference in practice. We will explore the linkage between EU-level security research and its impacts upon security policy delivery on the ground (downstream). Vice versa, we will also point to the untapped potential of end-users' insights for informing future security policy design (upstream). In the following we will try to showcase the potential of the Communities-of-Practice approach, originating in the organisational studies from the end of the 1990s, within the current context of European security research. We will briefly illustrate a pilot case, the 'Community of Users on Safe, Secure, and Resilient Societies', as a stakeholder-driven platform facilitated by the European Commission's DG 'Migration and Home Affairs'.

The paper offers an outlook about the value-added out of transferring such formats for research & innovation actions to security practitioners' networks, and how these may offer better threat assessments, minimising the 'blind spots' of individual organisations, but also helps transgressing inter-institutional barriers to communication and concerted action, for delivering security and resilience on the ground in a more responsive, effective, and sustainable manner.

The Challenge

In public policy fields that regularly trigger public controversies, such as in those related with societal security and resilience, decision makers cannot conclusively "solve" problems, but, at best, cope with them for a period of time and in a certain geographical context. Security qualifies as an archetypical *wicked policy problem*. Wicked problems are generally defined as the result of *interest and value divergence* among competing stakeholders, institutional *complexity* due to multi-level, inter-organisational governance, and, not least, of scientific *uncertainty* due to the lack of reliable cause-effect relationships (Rittel & Weber 1973; Head & Alford 2015). Stakeholder disagreement about framing the problem due to incompatible interests, and consequently, about which is the appropriate course for regulatory action, that will not cause more harm than good, are essential in grasping the dynamics of wicked problems in security policy.

Without the timely and targeted flow of evidence, solutions, trapped between bureaucratic inertia and interest-group politics, are most of the time 'clumsy', and result from "muddling-through" amidst contradictory or ambiguous goals (Lindblom 1979, Rainey & Jung 2015). The rise of public controversies in the past decade about what is effective, appropriate, legitimate, and accountable security policy, pays testimony to the above. This challenge is transferred, by default, from security policy to security research, and to the enabling conditions which should render it *useful, usable,* and *factually used* in order to deliver beneficial effects and ensure that it does not misfire, or backfire.

Security research as proactive form of security policy

In the field of science, technology and innovation, it is often the case that research generates not merely solutions to policy problems, but that such solutions often give rise themselves to new, 2nd-order problems in the form, e.g. of value-laden interest conflicts among different societal stakeholder groups (Biegelbauer & Hansen 2011). What additionally complicates the convergence on joint state-of-play diagnoses and on broadly supported policy remedies, is the issue of secrecy, and non-disclosure of sensitive information among Member States, or among agencies within a single Member State, or among researchers, practitioners, and policy makers. Besides the lack of transparency, which is a major obstacle to R&D knowledge transfer, is the lack of institutionalised, systematic and comparable data collection about implementation and performance of policy measures across national and international security agencies, and the practice of 'lamp-posting', looking for data where it is convenient, but not necessarily at the most relevant places that challenge the science-policy interface in the security field.

With the launch of the European Security Union in April 2015, a communication of the Commission to the Council and the Parliament, the 'European Agenda on Security' (European Commission 2015a) adopted an all-hazards, comprehensive-threat approach, making also a series of strategic recommendations for enhancing effectiveness and efficiency between the EU security research and the context of security policy implementation. Budgeted with almost 1.7 Bn EUR under Horizon 2020 for the period 2014-2020, the Challenge tasked with delivering on "Safe, Secure, and Resilient Societies" aims at responding to Critical Infrastructure Protection, Disaster Resilience, Fight against Crime and Terrorism, Border Security and External Security, and Digital Security.

As stressed above, the *outcomes* of research actions, no matter how promising they are, may not automatically generate positive and innovative *impacts.* Turning research results into socially robust knowledge with transformative potential to make a difference takes considerably more effort, and the functional engagement of key stakeholders, since it raises thorny questions about whose knowledge is to be incorporated into official public policy, for which purposes, and for whose benefit (Nowotny 2007). The role of stakeholders in co-shaping security policy and also, by default, security research, lies at the core of this exploration. Substantial engagement, not to mistake with co-optation-disguised-as-integration, among the researchers', the technology developers', and the policy makers' communities, and, not least, citizens and civil society organisations, has not yet reached a satisfactory level. This might well be an explanation about the less-than-optimal uptake of research results by the relevant end-users' communities (European Commission 2015). Stakeholders' engagement early-on in the research cycle, should not only have a positive influence upon the quality and implementability of *results*, but, moreover, also a positive influence upon the relevance and responsiveness of the research agenda which then becomes better anchored into the practical realities of the ground (Kolliarakis 2017).

Methodological approach: The Communities-of-Practice model

If the point of entry to the EU security research/security policy ecology is not merely the threats and risks on the agenda, but predominantly the key stakeholders exercising influence, then we should direct our analytical focus elsewhere: Toward *stakeholder interactions* and their leverage in co-shaping the agenda, and toward enabling or constraining the search of appropriate solution. The "Communities-of-Practice" (CoP) approach aspired to differentiate the rather target-less and mission-indifferent 'Network' models of organisational analysis (Wenger 1998). The members of a CoP follow a *self-organising, informal* exchange logic, which is driven by *shared expertise* and a *commitment for joint enterprise* (Wenger 1998; Wenger et al. 2002). CoPs allow for better *flow of information* and knowledge within and across organisations, which allows for more creative and *innovative pathways toward problem-solving*.

What is more, the boundary-transgressing dimension of CoPs refers to geographically and temporally dispersed exchange among participating members, as exchange may well take place both in a face-to-face and in an on-line modus (Pattinson et al. 2016). CoPs are venues for *mutual learning and mobilisation*. This is based upon open sharing and targeted processing of

knowledge. It is the process of interaction that strengthens and consolidates trust and reciprocity among different actors, as *key intangible assets* which emerge bottom-up, in contrast to the *top-down compliance structures* of national and international administration. This furnishes CoPs with the unique ability to sidestep inter-blocking administrative frames, complement formal bureaucratic procedures, and even inspire inter-institutional cooperation (Pattinson et al. 2016). There is a series of strategic knowledge-management functions performed by members of a CoP, which range from *filtering out* key information from 'noise', *amplifying* not-yet-known innovative ideas, *gathering* the relevant stakeholders for each issue, *setting professional standards* and rules of procedure, up to *creating (political) traction* for an issue, advancing it to the top of the regulatory agenda.

A crucial feature of CoPs is the agile, *semi-permeable multi-layered engagement logic* of actors. This contrasts with the more rigid, hierarchical command & control structures in bureaucracies, which, while establishing process legitimacy of the outcomes when coping with day-to-day issues, are not so well equipped to provide timely and innovative solutions to complex, or unprecedented problems, adapt successfully to shifts in the environment of the organisation, or, even less, anticipate such shifts and act proactively. While formal hierarchies cause a lot of collateral losses in knowledge that does not fit in prescribed routines and mandates, the opt-in/opt-out mode of working together on an issue-driven basis within a CoP keeps only the competent and committed experts inside, which act both as problem-solvers and promoters.

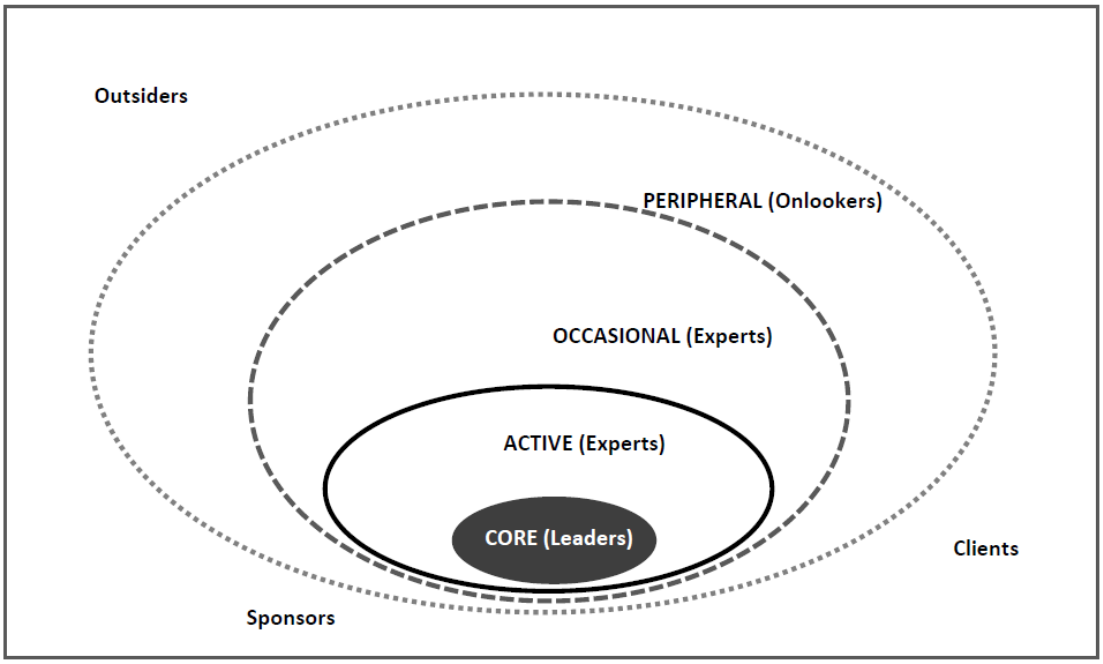

Figure 1: Levels of Participation in a CoP (modified after Wenger et al. 2002)

The layered geography of a CoP, as adapted from Wenger et al. (2002) (see Figure 1), comprises 'roles' within the community, which may continuously be shifting among actors, related to the proximity to the 'core' of the thematic domain. The 'domain' is the area of knowledge which provides the issues that bring the members together. The *core* comprises the *leaders* or *drivers*, who might have a co-ordinating activity within the crucial layer of the *active* experts. Around that circle there is a more permeable network of *occasional* experts who hop-in and out from the activity, depending upon themes and topics. The boundaries are permeable in both directions and define the identity of 'experts' in a peer-controlled way. They are part of that unique self-managed learning architecture, which transgresses sectors and disciplines, hierarchies, or national borders. There is a periphery of *tangential stakeholders* who are observers with the potential to move to the inner circles. Outside the domain of the CoP may reside the sponsors, clients and diverse institutions with similar repertoires.

The value of transforming tacit ('sticky') knowledge, embedded in organisational routines and practices performed by people, into explicit, codified ('leaky') knowledge which can 'travel' around organisations and benefit many more (Brown & Duguid 2001) cannot be overestimated. Knowledge and good practice spill-overs are then the beneficial symptoms of that 'open

innovation' setting provided by CoPs. The virtual or physical venue enabling this crucial "thinking together" as key performance of the CoP (Pyrko et al. 2017) allows for informal and fast exchange of competent and committed professionals. An illustrative example of the launch and the evolution of a CoP is given below.

A Pilot in-the-making: The Community of Users on Safe, Secure, and Resilient Societies

Most policies dealing with Disaster Risk and Crisis Management have established operational links with research. However, while interactions among research and policies are high on the policy agenda, much remains to be done to improve the way information flows from the different communities involved in implementation of both research outputs and policies. This includes capitalizing on past research and enhancing cooperation among EU Member States organisations. The complexity of the security sector stems from the wide variety of actors involved and the lack of coordination mechanism at EU and national level regarding the transfer of information and their actual use by implementers and decision-makers.

The need for enhanced coordination and information sharing, following a mapping of EU-funded projects to better understand the complex science-policy working environment at EU and national levels, formed the basis for the development of the so-called *"Community of Users on Safe, Secure and Resilient Societies"* (referred to as CoU below) (European Commission 2017). The CoU was created in 2014 and has developed since then into a powerful exchange platform followed by more than 1.500 members. What is at stake here is to create a mechanism involving different levels (EU, national and regional) by which different actors, and primarily the "users", will be able to *rapidly trace back information and experiences issued from research, capacity-building and training projects*, giving them the possibility to identify and contact right persons at the right time to get the feedback that they are looking for via a CoU dedicated website.[3]

Regular information exchanges and debates orchestrated by the CoU enable to better channel the information to security providers at local level, which has a direct effect a) on *research programming* (identification of gaps), b) *policy implementation* (direct support to technical needs) and c) *policy update* (regular reviews of the legislative requirements). The CoU thus turned into a useful complementary supporting group on research-related activities to EU security policies (not duplicating existing advisory groups dealing with policy implementation but rather

[3] See under http://securityresearch-cou.eu/.

channelling information about research outputs). It has also the capacity to *collect returns of experiences from industry and practitioners* to the EU level, and to identify the most promising technologies, tools and methods in order to support their access to the market.

The CoU establishes "horizontal" dialogues and interactions among different disciplines and actors. However, enabling operational links with users, is a more challenging and time-consuming exercise which can only be done through the nurturing of "Communities of Practice" as described above. In the context of security and crisis management-related research, CoPs within the CoU perform comprehensive overviews of leading projects in their respective domains, helping integrating free-floating knowledge, otherwise lost, so that synergies and a critical mass may be built-up. Through *interfacing and bridging the different "worlds*", there are more opportunities that users will get better-channelled information. This is depicted below for the sub-community dealing with natural disasters focusing on climate-related extreme events. The same principle of course applies to the many other security fields mentioned in this paper and covered by the Secure Societies Programme in the areas of *Disaster Resilient Societies, Fight against Crime and Terrorism, Border Security,* and *Digital Security*.

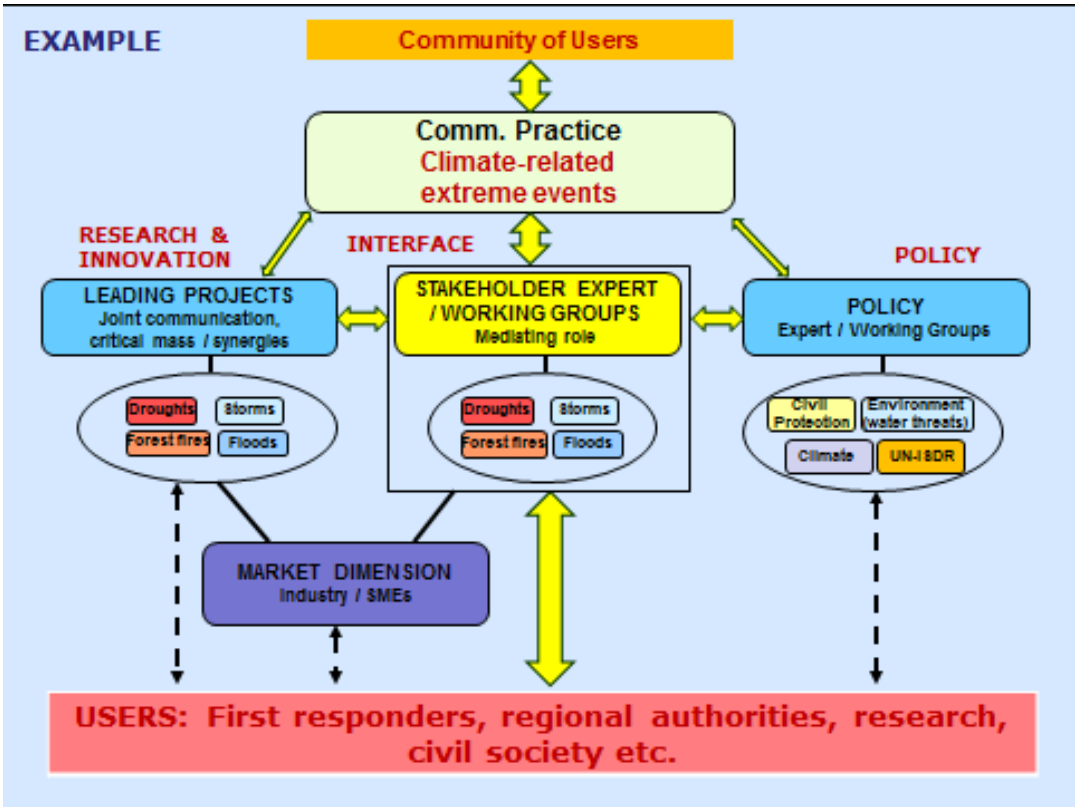

Figure 2: Channelling information in the Natural Hazards area

For scaling up the knowledge transfer by the Natural Hazards Communities of Practice, they are linked both upwards and downwards with the policy level, other research programmes, and relevant pubic authorities and the civil society. In this broad context, the CoU does not directly interfere with policy development and implementation, but rather uses contacts with different policy bodies to inform end-users about policy updates, and, vice versa, to facilitate the flow of R&D insights toward policy actors. This is illustrated in Figure 3 below:

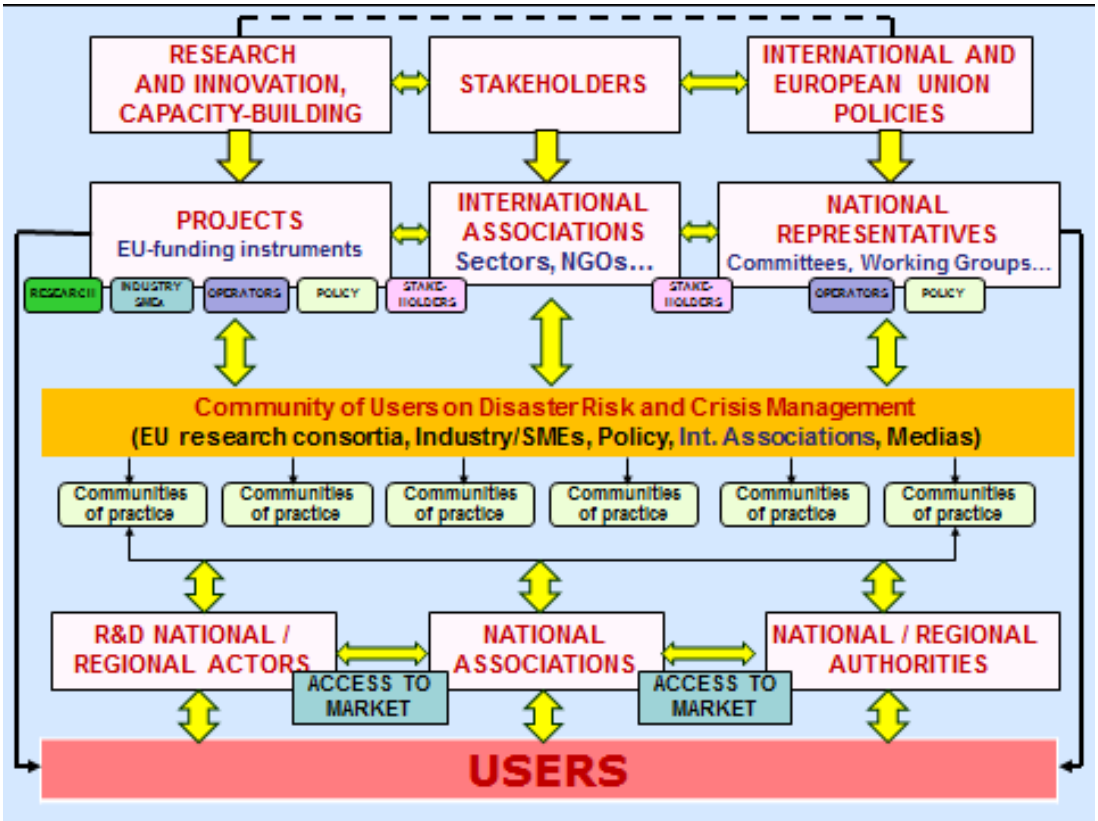

Figure 3: Linking CoU Levels to Communities of Practice

In conclusion, the Community of Users has the vocation to act as a facilitating platform, creating links and dialogues among different actors / disciplines ("horizontal level") and among different levels (from EU-to-local). Discussions are now on-going to identify and foster CoPs in different areas and ways to ensure sustainability of the overall CoU exchange platform.[4]

[4] This will be debated at the annual Security Research and Innovation Conference that will be held in Brussels on 5-6 December 2018.

Discussion and Implications

It should be clear by now that the Communities-of-Practice model as a *mechanism of multi-stakeholder knowledge production and circulation* does not merely have a reactive dimension – to respond to existent problems – but, moreover, it generates capabilities for anticipating and coping with emerging problems in a forward-looking way. That may entail defining the challenges for security R&D, or establishing robust threat assessments by drawing upon the broad expertise of the CoP members. Anticipatory governance from a CoP perspective is an inclusive exercise, involving societal stakeholders reflecting about undesirable and desirable futures, in order to *mobilize political, institutional, and epistemic resources* in the present, and if necessary correct and complement deficient governance arrangements. Following David Guston, anticipatory governance is

> "… a broad-based capacity extended through society that can act on a variety of inputs to manage emerging knowledge-based technologies while such management is still possible. … (A)nticipatory governance motivates activities designed to build subsidiary capacities in foresight, engagement, and integration."
>
> (Guston 2014, p. 219)

A major objective of an anticipatory governance regime in the security and resilience field is to diversify sources of knowledge, minimize 'blind spots' in strategic policy vision, and foster via innovative technology R&D, as well as better regulation and standards a higher adaptive potential of institutions and organisations to the evolving risk environment. Knowledge production in mutual dialogue with policy practice can address emerging techno-social challenges in a timely way, without suppressing controversies. Ethical, legal, and societal assessments, along with variants of participative and constructive technology assessments, can be key components of such a reflexive anticipation, and integration of science and technology in policy and society.

We should point, for that, to the pilot project *'Mediterranean Practitioners' Network & Capacity Building for Effective Response to Emerging Security Challenges'* (MEDEA, 2018-2023), integrating practitioners from EU Member States' public authorities, and R&D communities. MEDEA's design follows the CoP logic in order to bridge the mismatch among threat assessments and operational capabilities, inter-institutional cooperation, and strategic planning at regional, national and EU levels. Practitioner-driven knowledge production takes place along four domains/Communities of Practice, dealing respectively with Migration Flows, Border Management, Fight against crime and terrorism, and Natural hazards and technological

accidents. A most crucial aspect of that experiment is that a *triple knowledge interface is activated*, streamlining information and knowledge flows among policy makers from national ministries and International bodies, researchers, and security providers on the ground, in order to co-create strategies and action plans, advise on future policy agendas *(upstream)*, but also inform future R&D requirements *(downstream)*. The value-added arising, along the challenges to be encountered by the CoPs in the course of this endeavour include:

1/ *Boosting the Quality and Validity of Foresight Knowledge*:

Inclusiveness of stakeholders reduces the risks of conformity 'groupthink' and minimises blind spots in horizon scanning. It may also prevent the suppression of *"inconvenient truths*" which may lead to dangerous "Unknown Knowns" in security planning (Kolliarakis 2018). What is more, the quality criteria of *relevance, fitness-for-purpose, and reliability* of the source of knowledge, are boosted through the practitioners' access to the ground. The validity of foresight knowledge goes beyond plausible future-oriented visions: It links *transformative action* with *feasibility tests* and *scientific plausibility* (Guimaraes Pereira et al. 2007), recasting thus the Science-Policy-Society nexus. Forward-looking activities become, thus, more responsive to *constraints*, but also *to windows of opportunity* situated in specific institutional, organisational, and socio-cultural contexts on the ground.

2/ *Moving Outside the Institutional Zones of Comfort:*

Despite the joint endeavour and objective, actors involved as stakeholders and experts within a CoP are exposed to the diverging logics and languages of the others, to the differing capacities and time frames for action, and, not least to the different institutional mandates. Coming and thinking together about a joint problem does not change much of the fact that the members of a CoP may have *different institutionally prescribed primary tasks*, other than R&D. This is bound to create friction and disagreement. Yet, it appears to be an opportune way in order to move outside their respective zones of comfort and *appropriate new repertoires and skills*, inspired by the best practices of other members. This is the path to *turn capacities into capabilities* in security & resilience policy planning and provision. What is more, the channelling and contextualising of *new* security technology R&D into the respective local contexts of application is the non-plus-ultra frame condition for enabling *innovative* security technology R&D, useful, usable, and factually used on the ground.

3/ *Educating Knowledge Brokers to mediate between the 'Brain' and the 'Sensors':*

The role of the intermediary/translator among different communities of stakeholders is one of the most demanding and less rewarding 'cross-over' tasks within and among CoPs. However, this is a function of major strategic importance for effective knowledge circulation across boundaries, which cannot be found in handbooks, but be appropriated through active collaboration in CoPs. Lost knowledge and 2nd-order risks emerge out of disconnect between the *distributed 'sensory' intelligence* residing with practitioners from the implementation ground, and the *centralised 'brain' intelligence* by public administrators, policy planners and politicians. Integrating them will streamline threat diagnoses with capabilities and policy priorities. CoP brokers facilitate both *policy delivery*, in terms of effective and efficient implementation, but also future *policy design*, in terms of more responsive and anticipatory planning. The paramount challenge here is not merely to improve *Early Warning* by facilitating the transfer of evidence from the practitioners' *'sensory organs'* to decision makers' *'brains'*, but, most crucially, to pass over to *Early Response* by removing barriers and bottlenecks and allowing timely, effective, and accountable crisis management in emergencies, re-connecting the 'brain' to the executive 'organs' in the periphery.

4l *Fostering Sustainability via Transaction Capital and Trust:*

The conditions which influence CoPs' self-sustainability, that is, whether CoPs will *fly* or will *flop* in the middle term, relate almost exclusively with the *transactional social capital* their members develop in situ. This is a key intangible asset in the form of informal relationships and trust-building, which needs to absorb conflict and failure in joint endeavours, and takes time to consolidate. The promotion of *shared visions* and the establishment of *mutual commitment* is an invaluable 'side effect' of the above. Yet, *coming together* in order to exchange about specific R&D aspects of, e.g. Critical Infrastructure Protection, or Border Controls, is less demanding than *staying together* in a CoP collaborative setting, which needs to be based upon a series of mutually rewarding experiences that pay testimony to the value-added of the investment. Should in this process the vested interests of a group of members take capture of the CoP agenda, this would alienate the community and endanger its functionality. The role of the CoP leaders in the core group ought to safeguard impartial fact- and evidence- oriented exchange, but also avoid that management undermines the future self-sustainability of the CoU.

Conclusions and Outlook

Applying a CoP approach to research actions involving practitioners, policy makers, researchers, the industry/SMEs and Civil Society Organisations in security-related research actions for

serving policy, can be at best a *necessary condition* for opening up silo-transgressing channels of valid, timely, and relevant knowledge circulation. However, this should not be (mis-)taken with a guarantee or a *sufficient condition* for automatically generating positive impacts for the practitioners and/or the citizens. Many other barriers of legal, administrative, political, or cultural nature may still create bottlenecks or blockades to knowledge transfer. And yet, CoPs are better set to produce and promote *actionable knowledge* which is sensitive to frame conditions and more probable to lead to successful action and deliver desirable results (Argyris 1993). To pass from 'paper'-to-'practice' requires nevertheless a *paradigm shift for enabling a confidence-based sharing* among the above-mentioned actors across sectors and disciplines.

At the same time, there is enormous untapped potential to valorise exactly that aspect of the knowledge value chain: That is, *the aspect of circulation,* which is key to R&D impact. From the CoP vantage point, knowledge circulation might well be strategically more important even from that of *knowledge production*, in that it decisively boosts or undermines the linkages among key stakeholders in the context of security provision. Both new and promising products and methodologies need to be embedded within the specific, real, and often not welcoming institutional, organisational, and operational contexts in which they are supposed to be applied, if they are to become genuine *innovations* and make a difference.

All that could go wrong there, from failing technological standards, and missing ethical and legal provisions, to lack of resources, training, or political support can be 'sensed' within the CoP and tackled, if possible in advance. In other words, one major advantage of conducting security R&D within CoPs is the rise in *context awareness*. No matter how well technologies would perform in a lab or in a simulation test bed, reality out there is messy and fuzzy, and whether a potential solution will be absorbed or aborted in the end, is premised upon that, irrespective to its technological readiness. CoPs foster in this regard – in analogy to the Technology-Readiness-Level assessment model – the *institutional* and *organisational readiness* to promote legitimate, effective, and sustainable solutions for the benefit of the ultimate stakeholders of security and resilience policies, namely the citizens.

References

Argyris, C. (1993). Knowledge for Action: a Guide to Overcoming Barriers to Organizational Change. Jossey-Bass.

Brown J.S. and Duguid, P. (2001): Knowledge and Organisation: A social practice perspective. In: *Organisation Science 12*, p. 198-213.

European Commission (2017): A Community of Users on Secure, Safe and Resilient Societies (CoU) – Mapping EU policies and FP7 research for enhancing partnerships in H2020. Brussels. (edited by Ph. Quevauviller)

European Commission (2015). Ex-Post Evaluation of the FP7 Security Research Programme. Brussels.

European Commission (2015a): The European Agenda on Security. COM(2015) 185 final. Luxembourg.

Guimaraes Pereira, A. et al. (2007): Foresight Knowledge Assessment. *Int. J. Foresight and Innovation Policy* 3, p. 53-75.

Guston, D.H. (2014): Understanding Anticipatory Governance. In: *Social Studies of Science 44*, p. 218-242.

Head, B. W, and Alford, J. (2015): Wicked Problems: Implications for Public Policy and Management. In: *Administration and Society* 47, p. 711-739.

Kolliarakis, G. (2018, forth.): Anticipation and Wicked Problems in Public Policy: The creation of Unknown Knowns. In: Poli, R. (ed.) Handbook of Anticipation. Theoretical and Applied Aspects of the Use of Future in Decision Making. Springer.

Kolliarakis, G. (2017): In Quest of Reflexivity: Towards an Anticipatory Governance Regime for Security. In: Friedewald, M. et al. (Eds.): Surveillance, Privacy and Security: Citizens' Perspectives. Routledge.

Nowotny, H. (2007): How many policy rooms are there? Evidence-based and other kinds of science policies. In: *Science, Technology, & Human Values* 32, p. 479-490.

Pattinson, S. et al. (2016): In Search of Innovative Capabilities of Communities of Practice: A Systematic Review and Typology for Future Research. In: *Management Learning 47*, p. 506-524.

Pyrko, I. et al. (2017): What Makes Communities of Practice Work? In: *Human Relations 70*, p. 389-409.

Rainey, H.G., and Jung, C. S. (2015): A Conceptual Framework for Analysis of Goal Ambiguity in Public Organizations. In: *Journal of Public Administration Research and Theory* 25, p. 71-99.

Rittel, H.W.J and Webber, M.M. (1973): Dilemmas in a general theory of planning. In: *Policy Sciences* 4, p. 155-169.

Wenger, E. (1998): Communities of Practice: Learning, Meaning, and Identity. Cambridge University Press.

Wenger, E., McDermott, R. and Snyder, W. (2002): Cultivating Communities of Practice: A Guide to Managing Knowledge. Harvard Business School Press.