Strengthening the role of Social Sciences and Humanities (SSH) and end-users in security research

Investigating the position and role of SSH in security research, the informal ESSRO group, supported by the SOURCE project, drafted this position paper summarising the results from a multi-stakeholder consultation event.[1] This paper sets out to discuss specific roles for SSH in security research and define tasks and SSH-inspired research-based contributions to European security policy.[2]

European security *policy*, comprising dimensions of internal and external security, takes a threat-based approach, highlighting terrorism, radicalisation, organised and cyber-crime as well as climate change as key challenges to be addressed by targeted policy initiatives.[3] European security *research* is supposed to contribute in several ways: developing a better understanding of (root) causes and provide technological, societal and policy solutions to combat the abovementioned threats. Also, security research should increase the competitiveness of the European security industry.
The security research work programme[4] takes a *mission-oriented approach*, i.e. specific challenges are listed in the topic description and research is expected to create impact through the development of innovative solutions and/or better and improved understanding of causes of a given security threat. Challenges, threats and topics are defined in the realm of policy and any expected impact of research has to feed back into the policy arena. This framing is compatible with a type of research that has been labelled as techno-solutionism, where a process or technology is developed to address a pre-defined problem and the suggested solution is understood as a tool to be instrumentally applied by the relevant (public or private) security providers. Within this solutionist framework, SSH are introduced as a crosscutting priority in a number of topics addressing human factors, as well as social, societal and organisational aspects of specific security threats. SSH typically take on auxiliary roles, investigating legal and ethical aspects of (primarily technology-enabled) security solutions, conducting citizen surveys to assess the public's acceptance of specific security measures, researching psychological, social and cultural factors leading to crime and terrorism.

[1] The workshop took place in Brussels Oct. 9th and 10th, 2018. It was attended by representatives from different stakeholder groups and funded by the SOURCE project.
[2] The term SSH is used to cover a broad spectrum of disciplines from law to political science, anthropology, criminology, science and technology studies, history, psychology, economics and sociology. Each of these disciplines can add a specific perspective to understand a given security problem, broadening the scope of mission-oriented security research, supporting the development of solutions that are flexible and more targeted to end-user needs. As academic disciplines, SSH are capable of taking the reflexive position of the detached outside observer, asking for an occasional shift of perspective to critically reflect upon operational professional practices and refocus – opening unforeseen pathways to innovation.
[3] See e.g. The European Agenda on Security COM(2015) 185 final, or the 2016 policy document for a European Union Global Strategy: Shared Vision, Common Action: A Stronger Europe A Global Strategy for the European Union's Foreign And Security Policy
[4] See Horizon 2020 Work Programme 2018-2020, 14. Secure Societies – Protecting freedom and security of Europe and its citizens (EC Decision C (2018)4708 of 24 July 2018)

However, SSH have the capabilities to contribute beyond their role as service providers who respond to targeted questions of ethics, acceptance and causes of crime and terrorism that are relevant for law enforcement. Taking an SSH-informed look beyond the sequence of *problem-research-solution* can produce important insights for security policy and also help to improve the linear solutionist approach taken in security research.

SSH can help to better understand security challenges and threats, directing security research (a), they can add complexity to security problem description (b), develop suggestions on how to achieve sustainable impact of research output (c), and identify how these aspects are closely and reflexively interlinked.

(a) Assessing security threats from an SSH perspective

When identifying security threats, policy makers are constrained by public framings of security as a policy issue and often rely on briefings by experts and stakeholders lobbying for a specific cause or interest. This may restrict their analysis, defining and ranking security challenges within a narrow frame of reference. Taking the example of terrorism as one of the key challenges identified in European security policy, a critical look from an SSH perspective reveals some aspects that are not fully considered by policy makers when addressing security threats. First, in terms of damage to life and limb, terrorism would not qualify as a key challenge to the security of European citizens. Moreover, the few qualitative studies available on risk perception suggest that fear of terrorism is less pronounced among the population than media awareness would suggest. The social resilience to terrorism is still poorly researched, but may be greater than expected. Taking quantifiable indicators such as terrorist-related deaths to assess the threat posed by terrorist attacks, there are many other security risks producing a significantly higher death toll among European citizens. Secondly, the societal impact of terrorism has to be understood at the symbolical-political *and* at the operational law enforcement levels. The rationale of terrorist groups or predators is of a genuine political nature. Their goal is to spread fear and foster hostility, produce spectacular media-headlines and trigger robust reactions of public authorities. Violent attacks are a means to an end. Terrorism works first and foremost as a form of communication targeting the symbolical political order of society to elicit reaction and response. Security policy entering in this communication and taking terrorists' claims at face value runs the risk of playing into the hands of the predators.
Introducing such SSH-inspired considerations into the policy process where security threats are defined and ranked, can help to produce more balanced threat assessments and avoid counter-productive side effects of policy measures. As this case shows, a broader and more in-depth inquiry at the early stages of the policy cycle can also help to better conceptualise and target security challenges. We suggest establishing a new layer of security research supporting the definition of key challenges and threats, adding evidence-based input from SSH into the drafting of the security research programme. Traditionally, political representatives from Member States have been in charge of decisions about the annual European security research programmes, receiving non-binding advice from stakeholders, DGs and the security advisory group. This process could be improved through SSH theory and research.

(b) Adding complexity to security problem description

The narrow description of security problems in abstract policy terms (e.g. terrorism, organised crime, etc.) needs to be expanded or contextualised in two directions to better inform and guide security research:
(a) as policy issues, security problems should be addressed in a broader context to avoid adverse effects of securitization. As briefly outlined above, a broader view, inspired by SSH based investigation can add important dimensions to security policy problem analysis. Broadening the conceptual framework and applying the idea of *societal security*, security problems can be described beyond a threat-based focus. This case can be made for many key security challenges, a good example being organised crime. Reframing organised crime from an SSH perspective as a form of profit-oriented collaborative economic activity, can yield important insights with regard to adequate security policy strategies. Efforts to improve prosecution of criminal actors in illegal markets run the risk of producing detrimental effects. This has been repeatedly demonstrated for drug markets.[5] Intervening at the supply side of the market through effective prosecution of drug traffickers can have the effect of increasing the price of the criminalised commodity (drugs) for end-users since demand shows almost no price elasticity. This will attract new suppliers, bringing the market back into a state of equilibrium. Broadening the scope and understanding organised crime as economic activity can help to reshape the security challenge from a problem of law enforcement to a challenge to be addressed by broader policy initiatives as well, and investigating e.g. strategies to reframe drug policy as public health issue or to legalise certain substances.
(b) Taking a bottom-up perspective and looking at the description of security problems as they are perceived by end-users, stakeholders, researchers and field operatives on ground level an SSH informed approach can help to *map and reconcile the different rationalities of involved communities*. With the introduction of practitioner networks, the European security research programme has taken a first step to strengthen the bottom-up stream in security research. Locating security problems in the context of routine operations of law enforcement, first responders or crisis managers can help to better understand what kind of problems have to be addressed, what type of innovations are needed and how solutions have to be designed to create expected and sustainable impact. This constitutes an important step to bridge the gaps between solution or technology providers, policy actors and the complexities of security work on ground level. End user needs and demands are often complex, contextually embedded and rarely presented in a well-structured fashion. Technology projects tend to over-simplify the characteristics of end-users. These characteristics are based on researchers and developers common sense.[6] Hence, local requirements of law enforcement, emergency services or first responders have to be translated or synthesized to better inform research activities and R&D strategies. End user needs are often met with generic (technology-enabled) solutions, developed and tested in simulation environments or laboratory settings by security researchers funded by the security research programme. While this problem has been acknowledged in principle and the participation of end-users has been made a mandatory requirement in several topics of the security research programme, the gap still

[5] Boivin, R. (2014). Risks, prices, and positions: A social network analysis of illegal drug trafficking in the world-economy. *International Journal of Drug Policy*, *25*(2), 235-243.
[6] https://www.mdpi.com/2071-1050/10/10/3738/htm

exists and only very few solutions are actually implemented, adding to frustration and disappointment on all sides. One way to address this problem is the use of public procurement in security research. This strategy, however, primarily supports the industry R&D side of the gap. Whether the needs of users are sufficiently met, remains an open question. Collecting and systematically investigating these needs, in close connection with 'actual' end users in their own settings and contexts, SSH can make important contributions[7]. It could demonstrate that emerging security problems at ground level often have to be addressed in real time and time critical decisions have to be taken in an environment shaped by a (legally enforced) division of labour, often hindering the seamless exchange of information. Currently and in the past, response to security problems has often utilized a centralised organisational model of command and control, which stems from military and Cold War civil emergency management. This organisational model has found particular appeal in situations where the social order is expected to break down, such as during various 'natural' and other disasters. However, empirical SSH research on disasters has suggested for a number of years that actually experienced disaster conform to this 'command and control' only to some extent, requiring real time decisions and creating emergent networks that cannot fully adhere to hierarchical structures. An important impact of SSH research on societal security could be interrogating these different kinds of models of response to security problems, asking what assumptions on humans and organisation underpin them, and unpacking how well they correspond with actual experiences of end-users in the security sector. Considering such contextual factors can yield a more realistic account of the way security threats are processed and handled under given organisational, operational, resource-dependent constraints shaping information processing among security professionals. In many constellations security work from an SSH perspective can be conceptualised as a process of turning unstructured information into actionable intelligence leading to practical action.[8]

(c) Achieving sustainable impact from research output

As mentioned above, security research-based solutions fail to engage in dialogue with the end users concerning their own needs and requirements. Hence, research output fails to create a sustainable impact. Several obstacles have been identified, preventing the implementation of research results in practical security work. While the immediate impact of policy knowledge produced in security research projects is hard to assess, since knowledge diffusion is a complex process on different time scales, involving many different channels, fora and media, the case of technology-enabled solutions is different. Introducing a new element (e.g. an ICT-based process, a new surveillance tool or communication technology) in entrenched complex bureaucratic settings always entails an element of organisational reform and adaptation. Techno-solutionist thinking that strives for new tools, tends to ignore this dimension. Also, institutions endowed with security-related tasks, are tied into their regulatory frameworks and local environments (in cities, regions, countries). Internal organisa-

[7] Parallel to the technological readiness levels, social readiness levels could serve as an orientation for R&D.

[8] With the wisdom of hindsight, there is ample evidence that available forensic evidence about predators of major terrorist attacks was not properly processed in due time. Improving internal communication and working towards better cross-organisational and cross-national cooperation of security providers (law enforcement, first responders, etc.) could help to produce sustainable improvements, enhancing security and optimising processes.

tional and external environments not only shape the uptake of innovations, they also can be a source for the development of innovative solutions, improving security work. Improving the operation of law enforcement and other public security providers, often hinges on organisational changes, training and investment in human resources, strengthening of trust-based inter-agency or cross-border cooperation. A large number of challenges can be named to exemplify this. For example: How can police forces be sufficiently well positioned to do justice to the increasing diversification of society? How can the legal and organizational setting of critical infrastructures be shaped in order to, for example, adequately counter the cyber threat? In the face of increasing natural disasters, what is the extent to which not only professional rescue forces should be strengthened, but the population also be addressed as "first responders" in emergencies? It is in addressing these types of problems, that SSH research on security architecture could contribute to strengthening societal resilience.

Such innovations however, can hardly be successfully implemented within the existing framework of project-based security research. They do not follow the logic of *research-solution-implementation* but rather require a long-term commitment and recursive processes of testing, evaluating, learning and re-adaptation. The standard 24 or 36-month project format falls short of delivering a sustainable impact along these lines. Replacing the rigid logic of *problem-research-solution* with a more flexible model of a fuzzy *security field*, comprised of institutions, different stakeholder groups, technologies, regulations, discourses and practices to be addressed through hybrid and flexible project teams operating with some degrees of freedom over a longer period of time might be a more feasible approach here. Designing security research on the basis of the idea of security fields, the multiple and complex interrelations between policies, technologies, regulatory and organisational constraints, making up a specific security threat might be more adequately addressed. Similarly, the effectiveness of security research may be improved through the broadening of topics and calls within Horizon Europe, allowing for baseline studies of policy effects and practitioner needs, as well as research that is aimed at critically examining the current key security challenges and allowing for the identification of unaddressed threats to societal security. New measures along the lines of a *societal readiness level* could be developed, to strengthen the crosscutting integration of SSH in security research. The conceptual tool kit of SSH could be applied to design an adequate framework, exploiting the notion of *societal security* to map the links between heterogeneous elements and combining these into complex security challenges as described in European policy papers. Solutions then, would not be one-shot tools, but rather improvements that could be assessed over longer time spans as effects of incremental changes, innovations and adaptations as perceived by the different stakeholders involved. Putting the focus on inter-agency and cross-border cooperation can also create sustainable added European value, demonstrating good practices on ground level and spreading them through wider practitioner networks.

- SSH can fill the gap between supply and demand in security research
- SSH can act as a translator for complex end-user needs, better informing research activities and R&D strategies
- SSH can contribute to a better description of security problems in the policy cycle
- SSH can help to achieve a sustainable impact on societal resilience