Extended Abstract

Innovation, Inequalities, and Impacts: Countering non-anticipated effects of the European ICT Research

Georgios Kolliarakis

University of Frankfurt, Cluster of Excellence "Formation of Normative Orders"

Max-Horkheimer-Str. 2, 60323 Frankfurt, Germany

Kolliarakis@soz.uni-frankfurt.de

Tel.: +49 (0)69 798 31497

Accepted: 20 March 2015

Introduction

This paper addresses the European ICT research regime as an integral part of security research, as it emerged at EU level and also after 9/11. It focuses thereby on the unequal influence certain stakeholders from the high-tech development industry have on the biased directions of the research agenda. The market for civil security has globally grown by a factor larger than 10 since 2001, and, despite the Snowden revelations in 2013, the demand for surveillance ICT by public authorities and private facility operators is rapidly rising. ICT research policy is a core proactive form of public security and social policy, by creating a pool of solutions and measures to be drawn upon in the middle term. In this setting, ICT research success is premised upon a high-tech solutionist, economistic mantra of innovation after which research policy results are measured along econometric indicators. In this respect, reflection upon undesirable side effects of ICT and security-relevant technologies on society is currently methodologically neglected and side-stepped. What is more, the paper questions the capacity of the developed technologies to be "fit-for-purpose", that is, to factually deliver on the comprehensive societal tasks they have been deployed for. The analysis is directed toward ICT function creep, that is, application of the developed technologies other than the originally envisioned, to intended and unintended "dual use" of ICT, that is, the unsolicited transfer of civil technologies to military use. The lack of agreed-upon, rigorous criteria for evidence, which makes (ex-post) evaluations, but also (ex-ante) assessment an arbitrary endeavour, should give place to institutionalization of impact assessment methodologies and practices in the interest of broader segments of society.

Methods

In this paper a threefold methodological approach is pursued: First, a scoping of EU policy documents is done in order to trace legal and policy contexts for ICT (research) policy; Second, a mapping of stakeholders with their diverging agendas within the organizational regime along an influence (power/interest) matrix. The author draws, lastly, on his experience from expert agenda consultations at both German and at EU level, concerning the current and the future ICT/security research programmes.

Results and Discussion

The European Security Research Programme:

Responding to the European Security Strategy (2003) the European Commission launched the mission-oriented research *Programme to advance European security through Research and Technology* (2004). Budgeted with € 1.4 B under FP7, and with € 1.7 B under Horizon 2020, it is tailored to address four key areas: Fostering Resilience against Disasters and Crises, Fighting against Crime and Terrorism, Border and External Security, and Digital Security. The programme focus is on CBRNE detection, telecommunication data mining technologies, such as DPI, profiling and predictive analytics, biometric identification and pattern recognition, location tracking technologies, as well as surveillance in the form of drones and CCTV. Security research should be mission-driven and serving the five priority areas of the European Union's Internal Security Strategy (ISS): Disrupt international Crime Networks; Prevent terrorism and address radicalisation and recruitment; Raise levels of security for citizens/businesses in cyberspace; Strengthen security through border management; Increase Europe's resilience to crises and disasters. Two major issues have already raised criticism, e.g. by Statewatch, and the European Parliament:

1) The programme is supply-led, promoting industrial interests and not serving the needs of end-users or of the citizens at large.

2) The funded technological research raises serious ethics and fundamental rights questions and is fostering societal insecurity instead of security.

The Challenge:

Security policy and, by default, security research are value-laden, contentious public policy fields. They ought to be informed both by expert evidence and by citizens' values throughout the R&D&I process. Yet, problem definitions, goals, and innovation paths for security research are predominantly shaped by interest groups from the industry. This imbalance in stakeholder participation has, in turn led to a biased "high-tech" understanding of security.

Public concern is growing about how emerging as well as readily available ICT and security technologies, such as biometrics, pattern recognition and detection, risk profiling, and the use of remote sensing and surveillance 'drones', impact on society. What is at stake with such technologies goes beyond issues of data protection and privacy, and poses fundamental questions about the blurring military and civil applications ("Dual Use"), non-intended and non-anticipated consequences of their marketization, such as discrimination of minority social groups, and feasibility and desirability of maximum-security societies. If ethics and societal impacts are to be properly addressed in current and

future EU ICT/security research programmes then comprehensive appraisal by experts and citizens themselves is required.

Power asymmetries in the leverage certain actors, such as high-tech Research and Technology Organisations (RTOs), or lobbyists from industry associations have, help them exercise disproportional influence upon the formulation of objectives and the programme of the EU ICT/security policy. c the issue of increasing and streamlining the engagement of civil society actors, being the ultimate beneficiaries of research on security technologies, during the policy cycle of security research in order to enhance both its legitimacy and its effectiveness. The three governance mechanisms recommended below contribute at different stages of the security research policy cycle to make both the process more accountable and responsive to the citizens' needs, and the results more socially and ethically acceptable.

Conclusions

In conclusion, three recommendations of institutional/organizational nature are at hand: These are meant to make the ICT/security research governance regime more transparent and legitimate, but also more accountable and responsive to the needs and concerns of society, and not merely serve particularistic economic interests. Moreoever, strengthening checks and broadening participation would decisively contribute to minimizing negative non-intended effects of those technologies once applied.

1) Upstream & Streamline CSO Participation

There is a documented need to integrate civil society and its diverse organisations (CSOs) in the early stages of public policy decision making, particularly when the stakes are as high as in the civil security realm. The requirement to engage relevant societal stakeholders beyond organised interests is inscribed both in European Commission's *"White Paper on Good Governance"* (2002), but also in the *"Regulation of the European Parliament and of the Council establishing Horizon 2020"* (2012). The implication for security research is that CSOs should not be any longer a "fig-leaf" add-on, promoting "acceptance" for new security technologies, but instead co-define the agenda of security research and make sure that **1) it meets the needs of society, 2) it benefits society, and 3) does not have negative impacts on society.**

2) Conduct impact assessments and evaluations

Initiated after 2005 and under update pending for 2014, the European Commission's "*Guidelines for Regulatory Impact Assessment"* prescribe continuous legitimacy/effectiveness crash tests for policies, such as security research, in order to guarantee that they are 1) fit for purpose (effective), 2) proportional (positive cost-benefit trade-off), 3) informed by scientific evidence, and 4) serving overarching EU values and principles. Specifically, this entails that security research delivers on its primary task, that is, it enhances European citizens' security without infringing civil liberties along the "*The Stockholm Programme - An open and secure Europe serving and protecting citizens*" (2010), and complies with the *EU Charter of Fundamental Rights* (2010).

3) Rethink the meaning of Innovation

The current master narrative for innovation in the EU is preoccupied with market-driven, growth-oriented R&D. Yet, civil security is a public good and not merely a field of industrial competitiveness. Moreover, the dominant high-tech "solutionism" is ill-designed to address comprehensive societal

security challenges, such as economic disparities, inequality, and discrimination, and it may even backfire, in terms of generating new problems. Already in 2010 the European Commission report *"Empowering people, driving change; Social Innovation in the European Union"* pointed towards the huge untapped potential of organisational and institutional innovation for making societies more inclusive, sustainable, and resilient in the spirit of the Lisbon Treaty, by funding non-technological research initiatives**.**

Acknowledgments

Part of this research has been enabled by the EU FP7 security research project SecurePART (2014-2016), Grant Agreement No. 608039.

References and Notes

Georgios Kolliarakis works since 2009 with the University of Frankfurt (Cluster of Excellence 'Formation of Normative Orders'), where he conducts research on civil security and on strategic negotiations in conflict. Parallel to that, he manages an EU FP7 international collaboration in security research. Previously, he has been part of a research project on the 'Transformation of Security Culture' (BMBF/German Ministry of Research). At the Ludwig-Maximilians University of Munich (Geschwister-Scholl-Institut for Political Science) he has been since 2006 part of a European network about 'Human Security in the Western Balkans' and the role of criminal and terrorist organizations (EU FP6). Georgios regularly participates in expert consultations at national and EU level on the future agenda, impact, and evaluation of security research. He has experience in engaging practitioners, scholars, and other societal stakeholders in various forums to promote exchange and transfer of knowledge and create wider societal value out of research. He has presented over 30 papers in international conferences, and has chaired over 20 workshops and congress panels. In his graduate seminars he focuses on the analysis of non-intended effects of policies using table-top simulations. His practical training in multilateral negotiations and crisis mediation took place, among others, at the Clingendael Institute of International Relations in Den Haag. After studying Engineering at the National Technical University of Athens, Georgios earned a Master's degree in Political Geography from the Friedrich-Wilhelms University of Bonn, and a PhD in International Politics and Conflict Resolution from the Ludwig-Maximilians University of Munich.

© 2015 by the authors; licensee MDPI and ISIS. This abstract is distributed under the terms and conditions of the Creative Commons Attribution license.