in:ex

Converging and conflicting ethical values in the internal/external security continuum in Europe

European Commission, 7th Framework Programme

Milestone report 1.1: Catalogue of the Current Technologies

Milestone report submitted September 2009 (M19) in fulfilment of requirements of the FP7 Project, Converging and Conflicting Ethical Values in the Internal/External Security Continuum in Europe (INEX)

PRIO	International Peace Research Institute, Oslo	PO Box 9229 Grønland NO-0134 Oslo, Norway	T: +47 22 54 77 00 F: +47 22 54 77 01	www.inexproject.eu

Table of contents

SUMMARY

This milestone report highlights the academic findings of the work produced by *Work Package 1 (WP1)* on *Ethical Premises and consequences of security technologies* in the period M1-M4. It also sets out the path that the forthcoming deliverable/s within the work package will aim to pursue. The work by WP1 has so far produced two deliverables – those being the D.1.1 titled *State-of-Art Review of Scholarly Research on Security Technologies and Their Relation to the Societies which they Serve*, and D.1.2 titled *Catalogue of Security and Border Technologies at use in Europe Today*. This milestone report will draw particular attention to the analysis and findings of the latter deliverable – dealing with issues directly related to the use of technology in the management of borders in the European Union (EU). How to achieve efficient and accurate border control and surveillance are key concerns behind EU efforts to develop technologies in the fields of authentication and identification, data assemblage, and physical detection. D.1.2 is significantly more thorough than D.1.1 in the discussion of the relevant technologies and measures implemented, and it offers a catalogue of a wide range of scientific data found in several appendices. Further research by WP1 revolves around crucial aspects related to security technologies and touches upon the following predicaments: (a) the impact of security technologies on persons; (b) the political and ethical implications of pro-activity, prevention and profiling; (c) the human consequences of profiling; (d) the "monitoring the future" in security practices and; (e) the political and ethical dimensions of governmental practices relating to data protection and privacy. WP1 works closely with the other work packages on the project, but first and foremost shares a mutually constituted thematic approach with WP2.

I. INTRODUCTION

In order to examine the current catalogue of security and border technologies at use in Europe today, it is significant to reiterate the very overarching objective of the INEX project - namely its function “to contribute to existing understandings of European security through an innovative analysis of the value based premises and ethical consequences of the inter/external security continuum."[1] WP1 seeks to examine the ethical premises and consequences of security technologies and their work falls into phase 1 of the INEX project, which is chiefly focusing on the thematic particularities of the new security landscape. According to the INEX Annex, WP1’s primary objective – which further resolves itself into several subsidiary objectives – is to “clarify the ethically based social and cultural underpinnings of contemporary security technologies in general and their use in the internal and external policing in the European Union”[2] The contents of this milestone report named “Implications and Description of Security and Border Technologies at use in Europe Today” – are mainly based on WP1’s deliverable D.1.2 “*Catalogue of Security and Border Technologies at use in Europe Today*.”[3]

The milestone report is organized as follows. After the introduction, it will briefly introduce the key findings of deliverable D.1.2. Further, it draws attention to the four thematic approaches related to security and border technologies as elevated by WP1 – those being (a) identifying persons on the move; (b) data collection, assemblage and profiling; (c) technologies of border control and surveillance; and (d) the security technology industry and the European institutions. Finally, this milestone report seeks to establish WP1’s proposals to further study and examination in the INEX Project and beyond.

II. KEY FINDINGS

It has been argued that globalization has led to a smaller, more borderless world. In order to manage insecurities stemming from the high influx of impulses across borders, the EU and its Members are moving in the direction of adapting advanced border control and security technologies. Consequently, the research objectives and subsequent analysis by WP1 focuses

[1] Annex I: Description of Work, INEX Project: Converging and conflicting ethical values in the internal / external security continuum in Europe, prepared 31st January 2008, p.16
[2] Bigo *et al*, 2008
[3] Onwards referred to as deliverable D.1.2

on the management of insecurities through existing technology, as well as the development of new technologies. Border control and surveillance have been the major concern behind the EU efforts to develop technologies in the field of authentication and identification (biometrics in particular), data assemblage (setting-up of databases and software instruments for data treatment purposes), and physical detection ground, airborne and satellite surveillance systems. Thus, the catalogue seeks to "focus on the question of technology and how technology is put to use in the management of borders in the European Union."[4] The key finding of deliverable D.1.2 is that enhanced and advanced technology is increasingly becoming a policy priority for the EU and its Members and that this trend carries with it an important impasse – namely that there is a blurred line between responding to insecurities and maintaining the civil liberties of peoples. Moreover, D.1.2 understands that the tasks of managing and detecting coercive violence through the management[5] of borders is not longer reserved for public authorities, but to a larger extent shared in symbiosis with the private security industry. The next four sections of this milestone report will present WP1's findings in deliverable D.1.2 to more depth.

Identifying person on the move

It can be argued that there are three sets of distinguishable modalities and technological stakes related to border control and surveillance such as identifying persons on the move, surveillance of individuals in their journey towards and within the EU, as well as the detection and interception of undesirable persons on the move. In later years, the EU has been very active in developing new techniques of identification and verification of persons on the move – particularly in the field of biometrics.[6] According to Woodward, the different biometric-based systems provide automatic and quick identification of a person by converting a biometric measure into digital form, and further storing and comparing this measure against a digital database.[7] Biometrics as a form of identification has been employed for centuries, although there has been a current effort to make identification of such measures from human checks to automated checks. In this regards, biometrics to indentify persons on the move is meant to act as a part of the European Commission efficient and interoperable immigration

[4] Bigo *et al*, 2009, p.5

[5] Krahmann, 2008

[6] Examples of biometric measures are facial recognition, finger prints, keystroke dynamics, signature and voice. Experimental technologies and technologies currently being developed are iris recognition, emotional recognition, and gait.

[7] Woodward, 2001, p.3

policy – and thus to act as a “smart border” in the distinction between *bona fide* and *mala fide* travellers.[8] Subsequently, the logic and stakes that lie behind setting up of the biometric border have changed over the years, fuelled by the belief that migration, terrorism and organized crime will be better fought through the production of digitalized information bases, consisting of the largest possible number of individuals.

Although the advantages of biometric technologies are obvious such as combating illegal immigration,[9] combating terrorist networks, as well as hinder other cross border criminality, the disadvantages have been given little somewhat attention. The progressive trend towards the generalization of biometrics in multiple layers of society as a whole, l*et al*one in border control, has become a contentious debate in the general public. An expanded adoption of biometric technologies will limit people’s civil liberties and in some cases, generalize certain peoples or groups of peoples. One example where biometric technology has progressively made its way to the general EU public is through travel documents.[10] For travellers, such a digitalized system brings about the possibility of more control with less awareness of it. This could mean a smoother journey in general for people on the move, but could also have severe, negative implications for certain people or groups of people. This is related to unreliability of the very technology of the automated biometric systems.

Data collection, assemblage and profiling

Data collection, exchange and assemblage are three crucial facets of the technological management and surveillance of individuals passing through and within the European borders. As mentioned above, such management and surveillance is achieved through the use of systems of both human and automated checks that specifically aim to trace movement of persons across frontiers. In practice, these supporting databases or systems interlink a whole range of policy questions, and draw attention to our belief that people crossing borders is an issue of security. Consequently, it is worth noting that “these technology-based instruments

[8] Bigo *et al*, 2009, p.6
[9] Brouwer, 2007, p.47
[10] For example, as a part of the anti-terror legislation, the US has required nationals from the EU to have an electronic passport as of 26 October 2006. See Brouwer, 2007, p.50

lead to a blurring of the boundaries between asylum, immigration, visa issues and anti-terrorism."[11]

At present, there are three major databases in use that deal with movements across borders - namely Customs Information System (CIS), EURODAC and Schengen Information System (SIS).[12] Out of these three databases, EURODAC is the only database in use that contains biometric data,[13] and access to this database is supposed to be limited to national authorities dealing with asylum requests only. However, this notion is currently challenged, and issues of new functionalities and widened access are strongly debated. An example of this is SIS, which was set up to address several public policy and public security issues based on a wide range of categories including persons wanted for arrests for extradition, *mala fide* third-country nationals crossing borders, missing persons, witnesses, prosecuted persons, and persons or objects under surveillance.[14] As noted above, who is granted access to information gathered and contained in these databases has been widely debated, and there are recurrent proposals to grant national intelligence and security agencies the right to use SIS – particularly in the aftermath of 9/11.

Interestingly, the development of advanced biometric databases that have the aim to protect the "the common good," have been considered chiefly on their technical feasibility as opposed to their legal, political and practical implications.[15] This can be seen in a declaration of the Council "on combating terrorism" (2004), as well as the "*Hague Programme.*"[16] Similarly, Visa Information Schengen (VIS) is another biometric database currently in the process of becoming available to the EU and its Members. VIS' purpose is to assist in the process of visa applications, including the prevention of frauds, assisting in the process of identifying and returning undocumented migrants, as well as being an anti-terrorist measure. So far, society's reactions to the new methods of data collection, assemblage and profiling have been mainly focused on the weaknesses and risks following the "mass-consumerist" implementation of biometric technologies. Moreover, criticism has touched upon elements such as a concern for the efficiency of biometrics, reliability of technology, as well as the

[11] Bigo *et al*, 2009, p16
[12] Additionally SIS-II and VIS are in the process of being established
[13] Contains fingerprints and control images from the age of 14
[14] Bigo, 2009, p.17
[15] See Brouwer, 2008
[16] See European Commission, 2005

divisions between “untrusted” and “trusted” travellers It is also indicated that technology-based in security and border control processes are not value-neutral.

Accordingly, there has been an intensification of financial surveillance fuelled by the high levels of capital mobility. In the case of collecting, assembling and profiling illegitimate financial circulation, there has been an even higher governmental readiness to take advantage of communication technologies.[17] Here, information sharing has occurred between a wide range of national authorities and commercial actors such as banks. A significant problem has been that terrorist financing has been hard to detect, as the transfers are of relatively low value and appear legitimate. Even though there are clear differences between the border control and surveillance of people on the move and capital circulations, similar questions can be asked related to mobility and digital borders. Deliverable D.1.2 states that: “from tracking terrorist funds to biometric checks, the requirement to have access to a maximum of personal data plays a central role concerning the aim of proactively managing risks which would be linked to free circulation.”[18] This increases the chances of personal data being used for functions that stretch further than what was initially planned, which again leads to an ethical debate connecting civil liberties, suspicion and combating illegitimate circulations across borders. Overall, systems and technical devises containing personal data that are used to detect, intercept and interdict *mala fide* transaction of any kind, has proved to be complex.

Technologies of border control and surveillance

The detection, interception and interdiction of so-called undesirable circulations across the EU border, has become a foremost policy issue within Europe – particularly in maritime border surveillance. Contentious here is the notion that surveillance also involves all movements *in the direction* of the Exclusive Economic Zone (EEZ).[19] To tackle both national and maritime border surveillance, it has been proposed to establish EUROSUR,[20] a “system of systems,” that embraces elements of common monitoring and information sharing.[21] Heavy research funding by the EU through the FP7s Security Theme indicates that the problems of

[17] For example, EU-supported security research funded through several projects such as the PASR Funded Project GATE

[18] Bigo *et al*, 2009, p.23

[19] Ibid, 2009, p.25 (emphasis in original text)

[20] The only system close to resemble the proposed EUROSUR is the French SPATIONAV System. However, other systems of maritime surveillance can be found such as SIVE and MarSur

[21] European Commission, 2008, p.19

illegal immigration by sea are a highly prioritized topic within the EU. Overall, the actual basis for the "deployment, research and development of (...) technical devises and systems is not the enforcement, surveillance and defence of a borderline. It reflects, rather, the transformation of the classical sovereign narrative of territorial defence and border enforcement and its re-articulation around the notions of prevention, pro-activity and profiling."[22]

The security technology industry and the European institutions

The European Commission, in accordance with other European institutions, has developed a symbiotic relationship with different actors of the security sector ranging from governmental security and defence institutions, the security industry, and research institutions.[23] It can be argued that there has been a commoditization, privatization and promotion of security – the field of border management being no exception. This is due to the increasing focus on responding to transborder insecurities such as terrorism, illegal immigration, organized crime, critical infrastructure protection, as well as crisis management. Another reason is the overlapping functions and capabilities needed for both military and non-military security purposes, which often employ the same technology in their work. This trend has resulted in a need for more efficient and advanced technology, and thus has driven the private security technology industry closer to the respective governmental institutions in terms of research. In fact, INEX is one such research project, which specifically deals with ethical, legal, social and political considerations linked to contemporary security practices in Europe.[24] Significant private actors are BAE Systems, Diehl, EADS, Thales, Siemens, Sagem and Ericsson.

An issue raised for discussion is that scientific considerations have been relatively minor compared to commercial interests. Additionally, the contemporary practice of security does not have a homogenous approach for all peoples in any given population. According to deliverable D.1.2, there is a three-fold hypothesis related to the commoditization, privatisation and promotion of security – namely that (a) involvement of private agents in the context of the EU's security policies is driven by commercial and promotional concerns; (b) engagement

[22] Bigo *et al*, 2009, p.31
[23] See research by Bigo *et al*, 2008 (Deliverable D.1.1)
[24] Bigo *et al*, 2009, p.41; Also see Annex I Annex I: Description of Work, INEX Project: Converging and conflicting ethical values in the internal / external security continuum in Europe, prepared 31st January 2008

with the European governmental arenas also offers possibility for anticipating on industrial requirements, establishing industrial partnerships, as well as new and more targeted products; and (c) contribution to the production of a certain socially constructed image on the contemporary existing and 'new threats', as well as the efficient management of these threats.[25]

III. THE WAY FOWARD

WP1 has identified several areas that need further study and attention. First, it will be essential to examine the impact that different security technologies have on persons, and groups of persons. This particular aspect is currently sidelined in contemporary EU-funded security research. Subsequently, questions involving the political and ethical implications of an efficient maintenance of the 'smart border' need to be addressed. Second, the human consequences of profiling, pro-activity and prevention is an issue that WP1 aims to examine in upcoming deliverables. Third, the question related to the 'monitoring of the future' in security practices also needs to be explored in future research. Finally, dilemmas related to the political and ethical dimensions of governmental practices, particularly in terms of data protection and privacy are essential elements of future research. Accordingly, the outcomes and conclusion reached by the workshop organized by WP1 and WP2, as well as the CHALLENGE Programme on 7-8 April 2009, titled "*Prevention, Pre-emption and Precaution: Monitoring the Future in Security and Life Sciences, Governmentality of Unease, Freedom and Biopolitics*" will play a pivotal role. In conclusion, all of the above areas are foreseen to be approached in the workshop scheduled to be held in April 2010 (Deliverable D.1.4), on *The imbedded value assumptions and ethical consequences of security technologies* as well as in the two deliverables D.1.5.Working Paper on *The Lifting of the Internal Borders in an Enlarged EU: The Relationship between the Schengen Information System and the EC Rule of Law*, and D.1.6. Working paper analyzing *The transformation of gendered security values as a result of the evolution of security technologies.*

[25] Bigo *et al*, 2009, p.48

IV References

Annex I: Description of Work, INEX Project: Converging and conflicting ethical values in the internal / external security continuum in Europe, prepared 31st January 2008.

Amicelle, Anthony, Bigo, Didier, Philippe Bonditti, Julien Jeandesboz and Francesco Ragazzi (2009) *Catalogue of Security and Border Technologies at use in Europe Today*, INEX Deliverable D.1.2., Centre d'Etudes sur les Conflits, Paris, June.

Bigo, Didier, Philippe Bonditti, Julien Jeandesboz and Francesco Ragazzi (2008), *State-of-Art Review of Scholarly Research on Security Technologies and Their Relation to the Societies Which They Serve*, INEX Deliverable D.1.1., Centre d'Etudes sur les Conflits, Paris, November.

Brouwer, E. (2007), *The use of biometrics in EU databases and identity documents* In J. Lodge ed., Are you who you say you are? the EU and Biometrics Borders, Nijmegen: Wolf LegalPublishers, 45-66.

Brouwer, E. (2008), *Digital borders and real rights: effective remedies for third-country nationals in the Schengen Information System*, Leiden: Martinus Nijhoff Publishers.

European Commission (2005b), *Communication from the Commission to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs*, Brussels, COM(2005) 597 final.

European Commission (2005a), *The Hague Programme: Ten priorities for the Next Five Years*, Brussels, COM(2005) 184 final.

European Commission (2008a), *Report on the evaluation and future development of Frontex*, Brussels, COM(2008) 67 final.

Krahmann, E. (2008), *Security: Collective Good or Commodity*? European Journal of International Relations, 14(3), 379-404.

Woodward, J.D. (2001), *Biometrics: Facing Up to Terrorism*, Testimony Series RAND