



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

European Commission, 7th Framework Programme

Milestone report 1.2: Human / Ethical Consequences of Pro-activity

Milestone report submitted September 2009 (M19) in fulfillment 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	3
Introduction	4
Key findings	5
Pro-activity and technology.....	5
The consequences of pro-activity in Europe	8
Bringing back the human /ethical elements	10
Conclusion and future paths	11
References.....	12

Summary

This milestone report highlights the academic findings of in the work produced by the *Work Package 1 (WP) Ethical premises and consequences of security technologies on the Human / ethical consequences of pro-activity*. It also sets out the path on which the forthcoming work within the work package will aim to pursue. The report is foremost based on the work prepared in the first deliverable D.1.1. *State-of-Art Review of Scholarly Research on Security Technologies and Their Relation to the Societies Which they serve*. It also draw on important findings found in the *D.1.2 Catalogue of Security and Border Technologies at Use in Europe*, and work prepared by WP2 documented in the deliverable D.2.1 *The Law-Security Nexus in Europe: State-of-the art report*. The findings prove that an increasing attention is given on pro-active practices in combating terrorism. This has lead to a growing development of technologies in the name of security that aims to predict the future with the ultimate goal of preventing a future terrorist attack from taking place. In many respect the consequences of pro-activity also put many of the fundamental rights and freedoms of individuals in a democratic society at odds. In particular questions regarding privacy, reliability and social justice become a matter of increasing concern. How to assure that these rights are respected along with the development of new technologies in the name of security is a great challenge for the EU. WP1 have suggested that in the development of new security practices modalities for implementing these rights needs to be integrated. This can be done through implementing a so called data protection culture and including the privacy by design. At the same time as pro-active measures need to take these into account, it is also necessary to further look at how existing modalities can be developed in order to better correspond to the changing character of security practices. WP1 will in future work continue to look at alternative ideas and concrete models for how to better ensure the rights and freedoms of individuals in regards to the growing attention on new security technologies occupied with monitoring the future. It will also continue relevant synergies with other working packages within the project.

Introduction

The INEX project serves to contribute to the existing understandings of European security through an analysis of the value-based premises and ethical consequences of the ‘internal/external security continuum’ in Europe. The primary objective of work package 1 (WP1), titled: *Ethical premises and consequences of security technologies*, as stipulated in the INEX Annex: ‘description of work’, 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, in particular”.¹

This milestone report titled ‘Human / ethical consequences of pro-activity’ is based on the progress and workflow produced under the WP1 so far related to the analysis of the human / ethical consequences of pro-activity, thus the ability of technology to act in the future.² The report sets out the key findings and presents the relevant issues identified by WP1. The report is mainly based on the deliverable: D.1.1. *State-of-Art Review of Scholarly Research on Security Technologies and Their Relation to the Societies Which they serve*, but will also draw on findings from D.1.2 *Catalogue of Security and Border Technologies at Use in Europe*³. In addition, findings from WP2 particularly outlined in the deliverable D.2.1: *The Law-Security Nexus in Europe: State-of-the art report*⁴ constitutes an important element in this report.

The report will first provide an explanation of pro-activity and the new security technologies present in the European landscape. It will then present the main findings on the human / ethical consequences of pro-activity acknowledged along with certain recommendations. Next chapter will conclude the findings and give an indication on the path for the future work WP1 will pursue.

¹ Annex I: Description of Work, (2008). INEX Project: Converging and conflicting ethical values in the internal / external security continuum in Europe, prepared 31st January 2008, p. 26

² Ibidem, p. 26-27

³ Anthony Amicelle, Didier Bigo, 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.

⁴ Fuster, Gonzales, Gloria, Paul De Hert, and Serge Gutwirth (2008), *State-of-the-art-report on the current scholarship on the Law-Security Nexus in Europe*. INEX Deliverable: D.2.1. Vrije Universiteit Brussel.

Key Findings

New technologies in the name of security have evolved substantially in recent times in Europe. Albeit, a strong focus on their development and deployment the ethical and political implications they give rise to have attracted less attention.⁵ This may be regarded as problematic in the sense that the current evolution of security technologies has participated in the transformation of security practices, with an emphasis on pro-activity, profiling, and preventions, which threatens to “render obsolete the existing provisions for the safety of the individual as regards the practices of security agencies and services”.⁶

Before looking at the human / ethical consequences of pro-activity acknowledged in the work produced by WP1, it is necessary to further examine the means of pro-activity, and its relationship with emerging technologies in the field of security.

Pro-activity and Technology

The European Union made substantial steps towards establishing a common counterterrorism strategy in 2003. The member states concluded that in dealing with terrorism “...*Concerted European actions are indispensable*”,⁷ It was also highlighted that “*none of the new threats is purely military; nor can any be tackled by purely military means ... Dealing with terrorism may require a mixture of intelligence, police, judicial, military and other means.*”⁸ In the formulation of the 2005 counterterrorism strategy four dimensions were highlighted that would constitute the foundation of the concerted European approach, these were: ‘prevent’, ‘protect’, and ‘respond’.⁹ The aim with this approach, in particular with respect to the dimension of prevention, is to target the source of terrorism and the way it spread throughout society, in order to avoid a future terrorist attack. In this context many European and international counterterrorism initiatives have started to move towards the usage of forward-looking strategies¹⁰, often described in different terms constituting different realities. One of the terms that has been under much scrutiny and debate is the term of pro-activity.^{11 12} Pro-

⁵ 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, p.22.

⁶ Ibidem

⁷ Keohane, Daniel (2005). The EU and Counterterrorism, *Working Papers*, Center for European Reform, May, London, p.6.

⁸ Ibidem, p.6.

⁹ Fuster, Gonzales, Gloria, Paul De Hert, and Serge Gutwirth (2008), *State-of-the-art-report on the current scholarship on the Law-Security Nexus in Europe*. INEX Deliverable: D.2.1. Vrije Universiteit Brussel, p.28.

¹⁰ Levi, Michael and David S. Wall (2004), “Technologies, Security and Privacy in the Post-9/11 European Information Society”, *Journal of Law and Society*, Volume 31, Number 2, June, pp. 194-220.

¹¹ Other terms used are: anticipation, radical prevention or pre-emption.

activity refers to activities that seek to follow traces, particularly in electronic form, that are left by individuals or groups targeted by surveillance.¹³ In this sense Pro-activity is about crime detection, rather than crime solving as seen with traditional reactive policing. The idea is basically “to learn more about what the targets are up to” in order to obstruct them to carry out criminal activities, most notably terrorist actions. Therefore different information is collected in the purpose of intelligence rather than as evidence to be used in a criminal investigation.¹⁴ Proactive measures seek to predict what is yet to happen in the future in order to prevent terrorist attacks from actually taking place.¹⁵ A measure in line with pro-activity that has received great attention is profiling strategies. Profiling is a technique “*through which the data gathered through surveillance is integrated in a predetermined analytical framework*”.¹⁶

The pro-activity (and profiling) framework is very much dependent on technology.¹⁷ This holds true not only in concrete operations, but also as “a part of its symbolic economy”.¹⁸ In order for security professionals to claim they can predict the future, thus preventing future terrorist attacks from taking place, they must justify their access to knowledge that ordinary people do not possess, such as “secured databases, personal data including details about one’s private life or biometric information”. In addition, security professionals claim a specific “know-how” through profiling techniques (and certain risk analysis) not yet available, but which is also dependent on technological devices like data-mining, data-integration, or the analysis of different software. In this context further access to sophisticated technology becomes crucial since it is considered as a means to know more. In turn, this leads to a substantial growth and spread of actors involved in development and implementation of security practices.¹⁹

A great benefit with technology is that information and intelligence on people gathered by police, immigration / border agencies, and intelligence services can be transferred and circulated with high speed in disregard of seas, oceans and borders. This lay the ground for a “re-articulation” of surveillance and control with the technologies of speed hence “allowing for new complementarities between surveillance (permanent in time) and control (localized in

¹² Fuster, Gonzales, Gloria, Paul De Hert, and Serge Gutwirth (2008), *State-of-the-art-report on the current scholarship on the Law-Security Nexus in Europe*. INEX Deliverable: D.2.1. Vrije Universiteit Brussel, p.26

¹³ 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, pp.24-25.

¹⁴ Crelinsten, Ronald (2009). *Counterterrorism*, Cambridge: Polity Press p.91

¹⁵ 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 ,pp.24-25

¹⁶ Ibidem, p.24.

¹⁷ Ham, Shane and Robert D. Atkinson (2002), *Using Technology to Detect and Prevent Terrorism*, Progressive Policy Institute, January.p.2

¹⁸ 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, p.25.

¹⁹ Ibidem, p.25.

space or border) techniques”.²⁰ The use of technology in form of for example electronic surveillance, mail openings, track conversations and secret searches has greatly enhanced the abilities and capabilities of intelligence agencies to collect and disaggregate data on their targets.²¹ Technology is regarded as an essential and necessary tool to locate terrorists / and terrorist organizations before they launch an attack.²² ²³ One area that has seen a great expansion in the use and development of technologies is the area of border security²⁴ ²⁵. Here the forward-looking notion of security clearly becomes instrumental with a growing focus on reliance on ‘intelligence-led’ surveillance, risk management, and profiling.²⁶

The WP1 have found that the justification for investing in security technologies in Europe most often is framed as twofold. The first one highlights the nature of the so called “new threats” that are less visible and more difficult to predict. In this context, as mentioned above, new technologies in the name of pro-activity are regarded as able to close this gap by allowing for anticipation and reaction to insecurities before they occur. The second justification has to do with the investment in new technologies as an economic necessity, thus as a financial contribution of “an industrial basis in the EU”.²⁷ The new measures of technological management of insecurities in the name of pro-activity certainly give rise to debate around the consequences for fundamental rights and freedom of individuals. This notion is necessary to take a closer look into this.

²⁰ 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, p.8.

²¹ Crelinsten, Ronald (2009). *Counterterrorism*, Cambridge: Polity Press pp. 98-99

²² Fuster, Gonzales, Gloria, Paul De Hert, and Serge Gutwirth (2008), *State-of-the-art-report on the current scholarship on the Law-Security Nexus in Europe*. INEX Deliverable: D.2.1. Vrije Universiteit Brussel, p.28.

²³ Ham, Shane and Robert D. Atkinson (2002), *Using Technology to Detect and Prevent Terrorism*, Progressive Policy Institute, January.p.12

²⁴ Zimmermann, Doron (2006). The European Union and Post-9/11 Counterterrorism: A Reappraisal, *Studies in Conflict and Terrorism*, Vol 29, pp. 127

²⁵ See in; Anthony Amicelle, Didier Bigo, 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.

²⁶ 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, p.21.

²⁷ Ibidem, pp.21-23

The consequences of pro-activity in Europe

According to some the contemporary security practices fall outside the scope of scrutiny and investigation entitled by a democratic society. The underlying assumption here is that intrusiveness is a requirement for efficiency. In this sense privacy undermines efficiency with the consequence of increasing the potential for insecurity. Hence, the ethical and political effects of pro-active security technologies are widely neglected.²⁸

In the debate surrounding the current conception of security and security technologies in Europe the notion of right to security is often brought to the surface. It is here acknowledged that in the context of an increasing attention for pro-activity and technology security professionals and politicians emphasize the right of citizens to be secured by the state. However, while doing this they often forget the other aspect of the notion of rights to security that stipulates the individual's right to be protected from the abuses of the state. In this respect, the notion of a right to security has often neglected existing modalities for safeguarding freedoms and rights of individuals. It is therefore necessary to promote updates and development of new modalities that can stand up to the new requirements demanded.²⁹

When individuals are subjects to certain categorization inherent in predetermined models these might not only fail, but also stand in sharp contrast to the legal understanding of presumption of innocence.³⁰ The legal dilemmas in particular in regard with the terms of prosecution whereas the question of intent, known in legal language as *mens rea* becomes somewhat difficult to prove in the use of pro-active approaches, and other forward-looking strategies.³¹ Furthermore, the inherent assumption in the foundation of pro-activity and related forward-looking strategies is that by increasing the level of knowledge it will eventually lead to a situation in which anticipation will be possible and one is able to monitor the future. Such a departure has the ability to “trigger and endless expansion of the scope information that is gathered”.³² In this context issues regarding the right to privacy, and the capacity of individuals to be aware of what type of data that is being collected, and who is responsible for gathering the information, and when this was taking place, become rather hard to distinguish and apprehend.³³ In sum, this whole procedure may possess a serious risk of mistreatment and

²⁸ 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, p.23.

²⁹ Ibidem, p.26.

³⁰ Ibidem, p.25

³¹ Crelinsten, Ronald (2009). *Counterterrorism*, Cambridge: Polity Press p.92

³² 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, p.25

³³ Ibidem, p.25

abuse of databases and information. Such misuse would not only highlight a violation of the principle of proportionality, but also affect a great number of innocent civilians.³⁴

The investigating techniques of predictive data mining that filter data through pre-established criteria relate constitute an element that clearly interferes with different rights.³⁵ Because of the particular models with pre-established criteria certain groups will more likely get exposed to surveillance and other activities related to security which gives rise to deep discrimination.³⁶ As a consequence social justice becomes questionable along with the fact that certain groups already vulnerable in the society become even further exposed³⁷ which might lead to social exclusion.³⁸

In sum one may conclude that with the growing usage and evolvement of new security practices in the name of pro-activity questions regarding privacy, reliability and social justice becomes a matter of increasing concern. How to safeguards these rights along with the development of new technologies in the name of security possess a great challenge for European policy makers. In its work WP1 have highlighted a couple of recommendations necessary to take into account.

³⁴ Fuster, Gonzales, Gloria, Paul De Hert, and Serge Gutwirth (2008), *State-of-the-art-report on the current scholarship on the Law-Security Nexus in Europe*. INEX Deliverable: D.2.1. Vrije Universiteit Brussel, p.31.

³⁵ Ibidem, p.31.

³⁶ Ibidem, p.30.

³⁷ 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, p.25

³⁸ Ibidem, p.23.

Bringing back the human / ethical elements

Findings by WP1 indicate that there is an agreement among scholars that new security initiatives (as mentioned above) needs to be developed together with legal and technical safeguards. It is essential that new measures become a subject to oversight and that overview together with strict provisions and judicial review is integrated in the further development of the various security practices.³⁹ In the development and update of modalities taken these considerations into account one idea would be to promote a “data-protection culture that would underpin the security culture advocated by many in European capitals.⁴⁰ It is necessary to adopt a fair information practice and informational self-determination. However, implementing this in a time where technology is constantly changing and adapting has been acknowledged as rather difficult.

There is a need for developing and investing in alternative models that is able to guarantee privacy. This can be labeled as privacy by design, where considerations of privacy is integrated and included in the development of technological devices. Hence, Privacy by design shall guarantee that individuals become aware of what data and for which purpose the data is being collected. In addition, it shall allow for enhancing the scrutiny of the surveillants themselves, what one may refer to as “watch the watchers”.⁴¹ A concrete example of an alternative model is instead of establishing principles; one may use a chart of questions. This charter would cover the means through which the data is collected and also contain the social context in where the actual collection is taking place, and what the data is used for. Proposing questions instead of using available principles could have the benefit of an easier adoption to the rapid evolution of security practices.⁴² WP1 will in future work continue to look at alternative ideas and concrete models for how to better ensure the rights and freedoms of individuals in regards to the growing attention on new security technologies occupied with monitoring the future.

³⁹ Fuster, Gonzales, Gloria, Paul De Hert, and Serge Gutwirth (2008), *State-of-the-art-report on the current scholarship on the Law-Security Nexus in Europe*. INEX Deliverable: D.2.1. Vrije Universiteit Brussel, p.30..

⁴⁰ 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, p.26.

⁴¹ Ibidem, p.27.

⁴² 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, p.26.

Conclusion and future paths

The combination of different forward looking security strategies and the evolving technology in which they are developed indeed triggers certain risks. The current techniques of prediction in the name pro-activity can be said to create a mixture of reality and fiction, “merging the boundaries of the virtual and actual”, hence “introducing fiction into reality”.⁴³ The coexistence of a loose definition of terrorism offences, and an increasing mistrust, together with extended attention and faith on practices such as investigation, surveillance, likely have the effect that certain rights of the individual are neglected. The very nature of these practices may lead to abuse and disrespect of restriction on fundamental rights of individuals, as the right to privacy, the right to fair trial, and the right to liberty and security. It is therefore crucial that measures safeguarding these rights are integrated in future development of forward looking strategies. The future work by the WP1 will continue to look at this by especially seek to develop ways of promoting data protection culture among stakeholder on security technologies in Europe. The future work will in particular focus on how privacy requirements can be included within the practice and the different products of technology, as mentioned above as privacy by design. In this context it is important to continue to investigate the existing modalities of the protection of personal data to assess if they are still sufficient.

Questions that will be further elaborated are: Is it possible to place privacy, rather than extensive surveillance, as the basic script of existing and developing technological systems? What are the requirements for an evolving, rather than a fixed, privacy enhancing system? (An area that might be further explored here is the questionnaire, mentioned above).⁴⁴

Also worth mentioning is that the work so far produced by the WP1, in particular the D.1.1, has produced relevant synergy effects with WP2. These effects have been acknowledge in this milestone report as findings from the deliverable D.2.1 relevant to the topic of discussion were highlighted several times. WP1 will in its forthcoming work continue this valuable synergy with WP2, but also strive to integrate findings from other Working Packages.

⁴³ Fuster, Gonzales, Gloria, Paul De Hert, and Serge Gutwirth (2008), *State-of-the-art-report on the current scholarship on the Law-Security Nexus in Europe*. INEX Deliverable: D.2.1. Vrije Universiteit Brussel, p.31..

⁴⁴ 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, p.27.

References

Annex I: Description of Work, (2008). INEX Project: Converging and conflicting ethical values in the internal / external security continuum in Europe, prepared 31st January 2008, p. 26

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.

Fuster, Gonzales, Gloria, Paul De Hert, and Serge Gutwirth (2008), *State-of-the-art-report on the current scholarship on the Law-Security Nexus in Europe*. INEX Deliverable: D.2.1. Vrije Universiteit Brussel.

Anthony Amicelle, Didier Bigo, 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.

Crelinsten, Ronald (2009). *Counterterrorism*, Cambridge: Polity Press.

Ham, Shane and Robert D. Atkinson (2002), *Using Technology to Detect and Prevent Terrorism*, Progressive Policy Institute, January.

Zimmermann, Doron (2006). The European Union and Post-9/11 Counterterrorism: A Reappraisal, *Studies in Conflict and Terrorism*, Vol 29, pp. 123-145

Keohane, Daniel (2005). The EU and Counterterrorism, *Working Papers*, Center for European Reform, May, London.

Levi, Michael and David S. Wall (2004), "Technologies, Security and Privacy in the Post-9/11 European Information Society", *Journal of Law and Society*, Volume 31, Number 2, June, pp. 194-220.