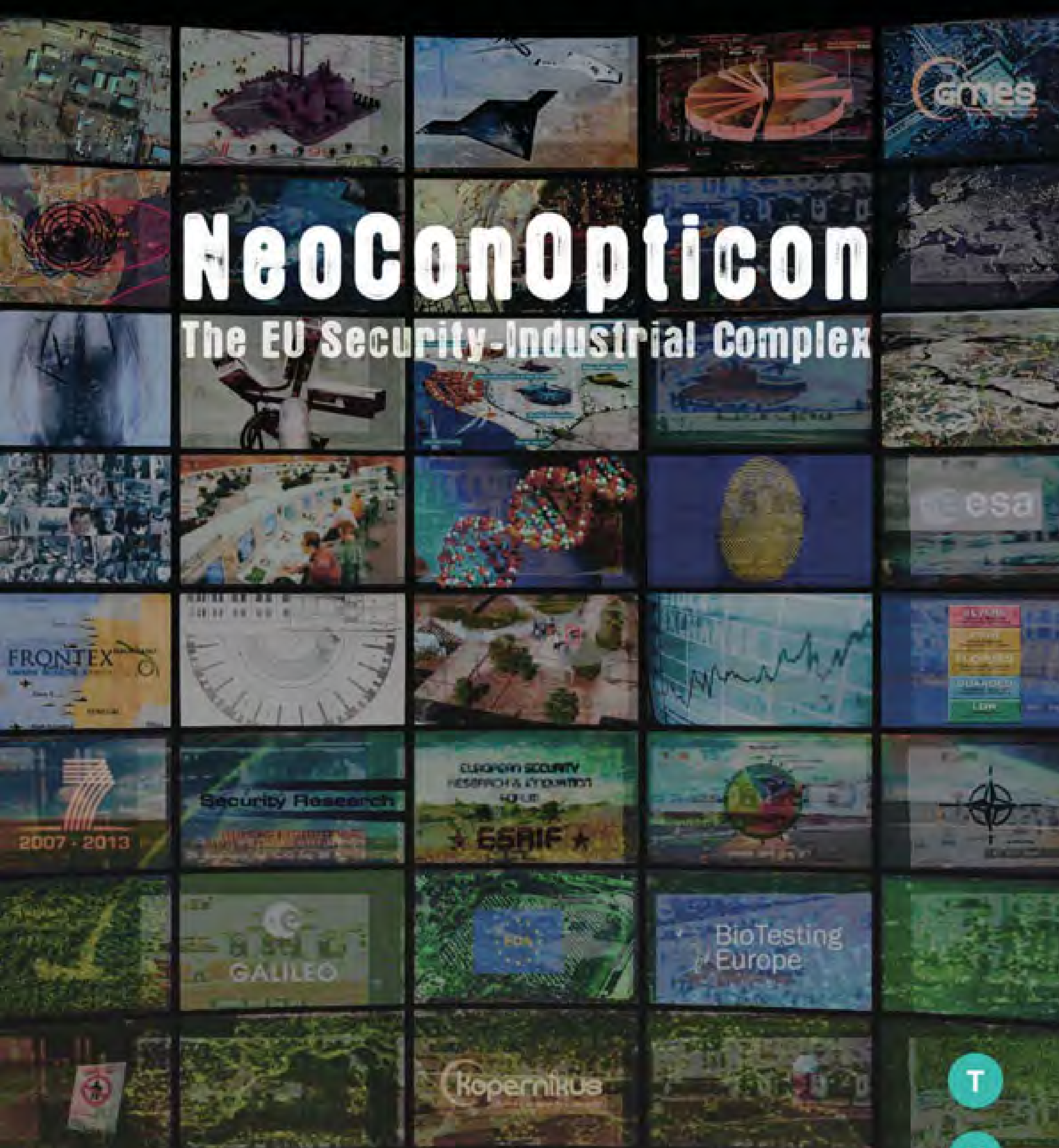
TRANSNATIONAL INSTITUTE

NeoConOpticon

The EU Security-Industrial Complex



In association with
statewatch

Copyright and publication details

Acknowledgments

This report was produced by Ben Hayes for Statewatch and the Transnational Institute. Additional research was conducted by Max Rowlands and Fiona O'Malley of Statewatch, while Tony Bunyan and Trevor Hemmings (also Statewatch) provided a constant stream of invaluable comments, information and guidance (several sections also draw heavily on Tony Bunyan's columns for the Guardian newspaper's 'Liberty Central' website). The information and analysis provided by Frank Slijper (Dutch Campaign Against the Arms Trade and TNI), Matthias (from Gipfelsoli), and Kamil Majchrzak (ECCHR) was also invaluable, as was Thomas Mathiesen's advice in respect to the variations on the 'Panopticon' discussed in this report.

The report was edited by Nick Buxton and Fiona Dove of the Transnational Institute (TNI) and benefited from helpful comments and suggestions from Wilbert van der Zeijden and David Sogge at TNI and Eric Toepfer of CILIP, Germany. The author also gained much insight from discussions at a number of conferences and seminars. In particular, the *International Workshop on Surveillance and Democracy* organised by Minas Samatas at the University of Crete in June 2008, and the seminars on the EU organised at the 'Militarism: Political Economy, Security, Theory' conference at the University of Sussex, organised by Iraklis Oikonomou and Anna Stavrianakis in May 2009. The comments of Kevin Haggerty (Department of Sociology, University of Alberta) on an earlier draft paper on the European Security Research Programme (ESRP), prepared for the 'Surveillance and Democracy' conference, were also very helpful in terms of shaping this report.

NeoConOpticon

The EU Security-Industrial Complex

Contents

PART I: INTRODUCTION

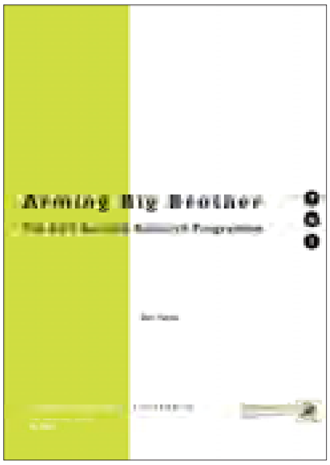
> *Governmental spending on products and services for homeland security should reach $141.6bn worldwide in 2009... The high priority given to homeland security has made that market one of the few recession-resistant sectors of the defence industry, some experts believe.*
>
> Visiongain Market Research, 2009 [1]

1 Summary of the report

In 2006, Statewatch and the Transnational Institute published *Arming Big Brother*, a briefing paper examining the development of the European Union's Security Research Programme (ESRP). The ESRP is a seven year, €1.4 billion programme predicated on the need to deliver new security enhancing technologies to the Union's member states in order to protect EU citizens from every conceivable threat to their security (understood here purely in terms of bodily safety).

The ESRP also has the explicit aim of fostering the growth of a lucrative and globally competitive 'homeland security' industry in Europe. To this end, a number of prominent European corporations from the defence and IT sectors have enjoyed unprecedented involvement in the development of the security 'research' agenda.

Arming Big Brother set out a number of concerns about the pending ESRP, including the implicit threat posed to civil liberties and fundamental rights by EU 'research' into surveillance and other security technologies. The report was also highly critical of the corporate influence on the EU security research programme and warned of various dangers in actively pursuing a 'security-industrial complex' in Europe.


Arming Big Brother
The EU's Security Research Programme

Arming Big Brother, published in 2006, was widely distributed and debated.[2] The online version has been downloaded over 500,000 times.

This follow-up report contains new research showing how the European Security Research Programme continues to be shaped by prominent transnational defence and security corporations and other vested interests. Though technically a Research and Development (R&D) programme, the ESRP is heavily focused on the application of security technologies (rather than objective research *per se*), and is increasingly aligned with EU policy in the fields of justice and home affairs (JHA, the 'third pillar'), security and external defence (CFSP, the 'second pillar').

[1] *Global Homeland Security 2009-2019*, ASD reports, see: http://www.asdreports.com/shopexd.asp?ID=1442.

[2] Hayes, B. (2006) *Arming Big Brother: The EU's Security Research Programme*. Amsterdam: TNI/Statewatch. Available at: http://www.statewatch.org/analyses/bigbrother.pdf.

Aligned to the EU's policy objectives, the corporate-led research under the ESRP favours the public procurement of new security technologies and EU security policies that mandate their implementation. This largely hidden influence is now exerting a tremendous influence on the EU policy agenda in an expanding cycle of largely unaccountable and highly technocratic decision-making.

The report is comprised of two substantial sections. The first revisits the development of the European Security Research Programme to date. It shows that the design of the ESRP has been outsourced to the very corporations that have the most to gain from its implementation. The second focuses on the implementation of the ESRP and the broader consolidation of the EU security-industrial complex. It examines the role played by specific actors, and the relationship between specific EU 'research' projects and EU policy measures. This report examined all 95 of the projects funded so far under the security research programme (to the end of 2008) and looked at several thousand related EU-funded R&D projects from other thematic programmes. What emerges from the bewildering array of contracts, acronyms and EU policies is the rapid development of a powerful new 'interoperable' European surveillance system that will be used for civilian, commercial, police, security and defence purposes alike.

Despite the often benign intent behind collaborative European 'research' into integrated land, air, maritime, space and cyber-surveillance systems, the EU's security and R&D policy is coalescing around a high-tech blueprint for a new kind of security. It envisages a future world of red zones and green zones; external borders controlled by military force and internally by a sprawling network of physical and virtual security checkpoints; public spaces, micro-states and 'mega events' policed by high-tech surveillance systems and rapid reaction forces; 'peacekeeping' and 'crisis management' missions that make no operational distinction between the suburbs of Basra or the Banlieue; and the increasing integration of defence and national security functions at home and abroad.

It is not just a case of "sleepwalking into" or "waking up to" a "surveillance society", as the UK's Information Commissioner famously warned,[3] it feels more like turning a blind eye to the start of a new kind of arms race, one in which all the weapons are pointing inwards. Welcome to the NeoConOpticon.

Ben Hayes, June 2009

[3] *Waking up to a surveillance society*, Information Commissioner's Office Press Release, 2 November 2006, see: http://www.ico.gov.uk/upload/documents/pressreleases/2006/waking_up_to_a_surveillance_society.pdf.

In just a few years, the homeland security industry, which barely existed before 9/11, has exploded to a size which is now significantly larger than either Hollywood or the music business. Yet what is most striking is how little the security boom is analysed and discussed as an economy, as an unprecedented convergence of unchecked police powers and unchecked capitalism, a merger of the shopping mall and the secret prison. When information about who is or is not a security threat is a product to be sold as readily as information about who buys Harry Potter books on Amazon or who has taken a Caribbean cruise and might enjoy one in Alaska, it changes the values of a culture. Not only does it create an incentive to spy, torture and generate false information but it creates a powerful impetus to perpetuate the sense of peril that created the industry in the first place.

Naomi Klein [4]

2 Neo-what? The ideas behind the title

The 'Panopticon' and beyond

The Panopticon was a model prison designed in 1785 by the English social theorist Jeremy Bentham. Also known as the 'Inspection House', the design allowed the prison guards to observe all the prisoners (from the Greek: *pan-opticon*) without the prisoners themselves being able to tell when they were being watched. As a prison design, the success of the Panopticon was short-lived,[5] but several centuries later, the term was adopted by the French philosopher Michel Foucault as a metaphor for techniques of surveillance and social control in modern society.[6] His central argument was that 'panopticism', the principle of omnipresent surveillance, had created a *"whole new type of society… transported from the penal institution to the entire social body"*.[7] From secure accommodation to hospitals, schools, work and domestic life, the act of being watched – what Foucault called the disciplinary power of the gaze – was shown to be every bit as important as the coercive power of the state in regulating individual behaviour.

Foucault's model of control and surveillance was welcomed by many intellectuals as a "long sought, eminently accurate model of the contemporary state and of the tendency innate in all modern power".[8] The arrival of what is now widely termed the 'surveillance society' appeared to confirm Foucault's hypothesis and, as international systems for mass surveillance appeared, some scholars went as far as to pronounce the arrival of a global, or super-panopticon.[9]

Surveillance, however, has also "spilled out of its old nation--state containers to become a feature of everyday life, at work, at home, at play, on the move",[10] leading many to conclude that the Panopticon may have run its course as a useful theoretical framework for understanding contemporary surveillance practices.[11] Used as readily by corporations, commercial enterprises, consumers and social networks as by the coercive institutions of state, surveillance systems are "rapidly becoming the dominant organising practice of our late modern world".[12] Underpinned by the revolution in information technology, this process has also been called "the end of forgetting": a new era in which information can be stored, retrieved and reproduced at will. The question that this new era poses is not just who is doing the surveillance, but who is doing the remembering?[13]

Some criticism has been directed at those who focus overwhelmingly on the negative properties of surveillance and the image conjured up by Orwell's 'Big Brother', while

[4] Klein, N. (2007) The Shock Doctrine. London: Penguin (page 306).

[5] There are only half a dozen prisons following the Panopticon design, most of them completed before 1820.

[6] Foucault, M. (1979) Discipline and Punish: The Birth of the Prison. Harmondsworth: Penguin.

[7] Foucault, M. (1979: pages 216 and 298)

[8] Bauman, Z. (1999) In Search of Politics. Cambridge: Polity Press (page 60).

[9] Gill, S. (1995) 'The Global panopticon? The Neoliberal State, Economic Life and Democratic Surveillance', Alternatives, 1995 (2).

[10] Lyon, D. (ed) (2003) Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination. London: Routledge, 2003 (page 11).

[11] Lyon, D. (ed) (2006) Theorizing Surveillance: The Panopticon and Beyond. Portland: Willan Publishing.

[12] 'Surveillance and Social Sorting', The New Transparency, see: http://www.surveillanceproject.org/projects/the-new-transparency/about.

[13] Bossewitch, J. & Sinnreich, A. (2009) 'Beyond the Panopticon: Strategic Agency in an Age of Limitless Information', Paper presented at Media in Transition 6: Stone and Papyrus, Storage and Transmission, April 24-26, 2009. Massachusetts Institute of Technology. Cambridge, MA USA, available at: http://www.radarresearch.com/aram/index.php?view=article&id=62%3Abeyond-the-panopticon-strategic-agency-in-an-age-of-limitless-information&option=com_content&Itemid=57.

ignoring the wider impact of the technological revolution and the way in which contemporary surveillance is both employed and *enjoyed*. These are valid criticisms: a whole generation in the rich world is becoming contentedly dependent upon GPS mobile phone devices, satellite navigation, webcams, Facebook and the other high-tech communications systems they avail themselves of. And in a world in which everyone from retailers to researchers to rescue missions benefit from the latest surveillance-based technologies, it is to be expected that states and governments seek to do the same.

This report does not start from the standpoint that security technology is bad. On the contrary, genuine, civilian-led efforts to enhance the capacity of states to prevent and respond to crime and catastrophic events through technology should, in principle, be welcomed. *It is the way in which they will work in practice that should determine their acceptability*. Yet, despite increasingly sophisticated critiques of 'old-fashioned' concerns about surveillance, it remains the case, as Thomas Mathiesen put it, that *"never in the history of mankind has there been a technology which so clearly has had a "double character" (to borrow an expression from Marx)"*; a 'dark side' comprising *"the use of sophisticated and rapidly advancing technology for surveillance purposes, a surveillance which quickly is coming to a point where it threatens the democratic fibres of our societies"*.[14]

On the 'dark side' of surveillance: the NeoConOpticon

Various alternatives to the 'Panopticon' have been put forward to supplement or challenge Foucault's ideas. Thomas Mathiesen introduced 'synopticism' to explain the (dialectical) process of 'the masses watching the few', and the way in which popular culture has helped condition society into accepting new techniques of surveillance and control;[15] Didier Bigo has used the concept of the 'banopticon' to describe the exclusionary practices of profiling and containment employed by Europe's police forces and at its borders;[16] while Michalis Lianos has put forward the idea of the 'periopticon' to describe a post-modern governmental model of control beyond freedom, democracy and coercion.[17]

The idea behind the 'NeoConOpticon' is to emphasise both the central role played by the private sector in 'delivering' surveillance-based security policies and the inherently neo--conservative appeal to the 'defence of the homeland' against threats to the 'Western way of life' used by the EU and other powerful actors.[18] Neocon ideology is centred upon the "right to limitless profit-making",[19] which is at the very heart of the EU's desire to create a lucrative Homeland Security industry. The EU's security policies are premised on the neocon philosophy of global policing and intervention in failed states to both pre-empt 'threats' to security and further the spread of the free market and western-style democracy around the world.[20]

The 'NeoConOpticon' also attempts to capture the evident link between 'Homeland Security' policies and a burgeoning Homeland Security industry, another trend synonymous with the Bush administration.[21] The crude appeal to Homeland Security in neoconservative discourse is epitomised by NATO's 'Grand Strategy for an Uncertain World' of 2008, with its assertion that: "*What the Western allies face is a long, sustained and proactive defence of their societies and way of life. To that end, they must keep risks at a distance, while at the same time protecting their homelands*".[22]

Many critics have described the 'European project' as neoliberal, a definition that largely befits its economic and social policies. While the EU's foreign policy is intimately linked to neoliberal globalisation (based as it is on access to new markets for capital, goods and services as part of the 'Global Europe' strategy),[23] there is little or nothing essentially liberal about the processes of militarisation and securitisation described in this report. The EU may have some liberal and even progressive policy objectives, but the majority of the EU's immigration, asylum, criminal justice and counter-terrorism policies are conservative and reactionary. Linked to the EU's Common Foreign and Security Policy,[24] which promises "more reliable partners, more secure investments, more stable regions", an inherently conservative world view is taking hold of EU consensus.[25]

[14] Mathiesen, T. (1999) *On Globalisation of Control: Towards an Integrated Surveillance System in Europe*. London: Statewatch.

[15] Mathiesen, T. (1997), 'The Viewer Society: Michel Foucault's 'Panopticon' Revisited', *Theoretical Crininology*, 1(2). Discussing 'Big Brother's new avatar', Zygmunt Bauman has similarly lamented the way in which the 'reality television' shows of the same name have rendered the term "nothing but an empty verbal shell… The present generation has all but forgotten the old meaning [and] the fears haunting Orwell's contemporaries", he suggests. Bauman, Z. (2002) *Society Under Siege*. Cambridge: Polity Press (pages 61-66).

[16] Bigo, D. (2006) 'Globalized (in)Security: the Field and the Ban-opticon', *Harvard Conference Paper*, available at: http://www.ces.fas.harvard.edu/conferences/muslims/Bigo.pdf.

[17] Lianos, M. (2008) '"Periopticon": Control Beyond Democracy', paper presented to *International Workshop on Surveillance and Democracy*, University of Crete, June 2008.

[18] 'Neocon' is an oft-used but rarely defined term that describes the political philosophy of neo-conservatism. It is claimed that the term was first used pejoratively to describe people who moved from left to right but in recent times the term has become synonymous with the Bush regime and its claims to spread free market liberalism, democracy and human rights to other countries through USA military force (a strategy embodied in the neo-con 'Project for the New American Century' of 2000, see Project for the New American Century (2000) *Rebuilding America's Defenses: Strategy, Forces and Resources For a New Century*, available at: http://www.newamericancentury.org/RebuildingAmericasDefenses.pdf). Neoconservative has also been used to describe political movements in countries as diverse as China, Iran and Japan and has for some become so "poor, abused, unrecognizable, meaningless" that it should be killed. For a discussion of Neoconservatism see Wikipedia: http://en.wikipedia.org/wiki/Neoconservatism. On 'worldwide neoconservatism see: http://en.wikipedia.org/wiki/Neoconservatism_(worldwide). See also Goldberg, J. (2007) 'Kill this word: poor, abused, unrecognizable, meaningless 'neocon", *National Review* 2 April 2007, available at: http://findarticles.com/p/articles/mi_m1282/is_5_59/ai_n18744605/.

[19] Klein, N. (2007) *The Shock Doctrine*. London: Penguin (page 322).

[20] *A secure Europe in a better world: European Security Strategy*, EU Council document 15895/03, 8 December 2003; available at: http://www.iss-eu.org/solana/solanae.pdf. See also: *Climate Change and International Security: Paper from the High Representative and the European Commission to the European Council*, EU Council document S113/08, 14 March 2008, available at: http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/reports/99387.pdf.

[21] See further chapters 15 and 16 in Klein, N. (2007) *The Shock Doctrine*. London: Penguin.

[22] NATO (2008) *Towards a Grand Strategy for an Uncertain World*, available at: http://www.csis.org/media/csis/events/080110_grand_strategy.pdf.

[23] See GLOBAL EUROPE: competing in the world, European Commission website: http://ec.europa.eu/trade/issues/sectoral/competitiveness/global_europe_en.htm.

Seeing parallels between the development of a global *lex mercatoria* (the international system of laws, rules and norms in which neo-liberal economic globalisation is embedded), Thomas Mathiesen has suggested the emergence of an international *lex vigilitoria* underpinning a rapidly-developing system for global surveillance and control (much of it anchored in EU law and policy).[26] The 'NeoConOpticon' is a crude attempt to encapsulate these ideas: a coherent state-corporate project, potentially global in scope, designed to impose a high-tech security apparatus for the express purpose of maintaining and extending the current neo-liberal order into the 21st century.

Building the NeoConOpticon

This report uses other potentially contentious terms to help explain developments at the EU level. The idea of an EU 'security-industrial complex' was used in our previous report in a purely descriptive sense to describe the integration of EU security policy making and the emerging homeland security industry. Today it describes a more literal truth, one in which, in the words of a former EU Commissioner, *"security is no longer a monopoly that belongs to public administrations, but a common good, for which responsibility and implementation should be shared by public and private bodies"*.[27]

In the absence of critical scrutiny, this state-corporate nexus is increasingly geared toward the production of a new kind of security. This is a security based not on the traditions of the 'free', liberal democratic society and the social structures that used to provide people with a sense of security (the welfare state, the pension system, the prospect of long-term employment and so on), but an increasing authoritarianism born out of the irrational politics of insecurity, paranoia and moral panic. In 1980, Stuart Hall identified as 'authoritarian populism' the appeal by the state to popular fears about immigration, crime and terrorism and left-wing subversion.[28] Thirty years on it has proved an enduring technique of government.

The model 'surveillance economy' identified by this report is neither the UK, which has been a driving force behind many surveillance policies in Europe, nor the USA, the spiritual homeland of homeland security, but Israel, where the military-industrial complex has helped produce a world-leading security industry.[29] Despite its "hyper-militaristic existence" and "massive expenditures on illegal settlements, illegal roads, the illegal wall and, of course, the illegal occupation itself",[30] Israel has, by retaining the trappings of modern liberal democracy, successfully positioned itself as the Homeland Security State *par excellence*, with revenues to match.[31]

Policing the NeoConOpticon

This report uses the model of 'Full Spectrum Dominance' to explore and conceptualise the inevitable outcome of authoritarian EU approaches to security, risk and public order. The term was first used at the turn of the century by the USA's Department of Defence as a euphemism for control over all elements of the 'battlespace' using land, air, maritime, IT and space-based assets.[32] The doctrine seeks to harness the full capacity of the so-called 'Revolution in Military Affairs' engendered by the revolution in IT.

In a domestic security context, Full Spectrum Dominance implies both an intensive model of international surveillance and a model of policing based primarily on military force. Steve Wright, an expert on military and security technology, explains that "The events of 9/11 and the so called revolution in military affairs (RMA) have merely accelerated an ongoing trend to build cybernetic military systems where weapons are simply the muscle deployed by a nervous system based upon an intelligent handling of data through communication, command and control". Wright also foresees the deployment of these systems in domestic security scenarios as "no hiding place military doctrines" begin "to inhabit future living spaces" and governments "move away from just mass supervision to more prophylactic systems of targeting".[33] These ideas are explored further in section 10 (page 29).

In the final analysis, Full Spectrum Dominance offers a new model of policing based not on 'consent', as the liberal democratic model holds, but on continual processes of public submission to authority. Perhaps more importantly, as a project, this model implies the end of resistance to this process (complete domination = complete submission). It follows that if freedom is to survive, then this project cannot be allowed to succeed.

[24] As Bernd Hamm has explained: 'The *conservative worldview* is basically authoritarian and, hierarchical. The state is like the traditional family: the president governs and expects discipline and obedience from his children. Disobedience is met with physical punishment. The world is evil; father protects and needs the means to protect. He is the moral authority; whatever he does is right… The [homeland] is seen as more moral than other nations and hence more deserving of power. It has the right to be hegemonic and must never yield its sovereignty or its overwhelming military and economic power'. Hamm, B. (2005) (ed) *Devastating Society: the neoconservative assault on democracy and justice*. London: Pluto (page 5).

[25] Solana, J. (2000) *The Development of a Common Foreign and Security Policy of the EU and the role of its High Representative*, available at: http://afa.at/globalview/052000/solana.html.

[26] Mathiesen, T. (2006) "*Lex Vigilitoria*' – towards a control system without a state?' in Bunyan, T. (ed) *The War on Freedom and Democracy: Essays on Civil Liberties in Europe*. London: Spokesman (pages 38-42).

[27] Frattini, F. (2007) 'Security by design', *Homeland Security Europe*, based on a speech by Commissioner Frattini to the EU Security Research Conference in Berlin, 26 March 2007, available at: http://www.homelandsecurityeu.com/currentissue/article.asp?art=271247&issue=219.

[28] Hall, S. (1980) 'Popular-Democratic vs. Authoritarian-Populism: Two Ways of 'Taking Democracy Seriously'', in A.Hunt (ed), *Marxism and Democracy*. London: Lawrence and Wishart.

[29] Gordon, N. (2009) 'The Political Economy of Israel's Homeland Security', *The New Transparency Project, Working Paper III, IRSP IV*, available at: http://www.surveillanceproject.org/files/The%20Political%20Economy%20of%20Israel%E2%80%99s%20Homeland%20Security.pdf

[30] Rose, H. & Rose, S. (2008) 'Israel, Europe and the academic boycott', *Race and Class*, vol. 50, no. 1, pp. 1-20.(page 16).

[31] Gordon, N. (2009) 'The Political Economy of Israel's Homeland Security', *The New Transparency Project, Working Paper III, IRSP IV*, available at: http://www.surveillanceproject.org/files/The%20Political%20Economy%20of%20Israel%E2%80%99s%20Homeland%20Security.pdf

[32] Department of Defense (2000). *Joint Vision: 2020*. Washington: USDOD.

[33] Wright, S. (2006) 'Report. Sub-lethal vision: varieties of military surveillance technology', *Surveillance & Society*, 4(1/2): 136-153, available at: http://www.surveillance-and-society.org/Articles4(1)/sublethal.pdf (page 137). The 'STOA Report' is "An appraisal of technologies for political control", European Parliament DG Research, Working document (Consultation version), 6 January 1998, available at: http://cryptome.org/stoa-atpc.htm.

PART II: BRINGING IN BIG BUSINESS: THE EUROPEAN SECURITY RESEARCH PROGRAMME

> *This spring a so-named Group of Personalities in the Field of Security Research is to submit a report to the European Commission that will outline a research program for Europe's future security. It will then lead to a call for proposals for six to eight projects financed to the tune of 65 million euros ($83 million) over a three year period. The sum is tiny compared to the 17.5 billion euro outlay for the EU's sixth research and development program. In the long run, however, it will lay the cornerstones of a "Homeland Security" system in Europe. Members of the group - legislators, businessmen and researchers - were chosen on the basis of their know-how and skills in the security sector.*
>
> The Experts Looking Out for Europe's Security', *Intelligence Online*, January 2004 [34]

3 Setting out the stall: the Group of Personalities

The history and development of the European Security Research Programme is documented in our previous report, *Arming Big Brother*.[35] As EU policy-making goes, it was an extraordinary process. The 'Group of Personalities' (GoP) on security research was convened in 2003. It met only twice but served to cement the structure, objectives and ideology of the future ESRP. The GoP included the European Commissioners for Research and Information Society, plus, as 'observers', the Commissioners for External Relations and Trade, the High Representative for the EU's Foreign and Security Policy, as well as representatives of NATO, the Western European Armaments Association and the EU Military Committee (see figure 1, over). Also represented were eight multinational corporations – Europe's four largest arms companies (EADS, BAE Systems, Thales and Finmeccanica), and some of Europe's largest IT companies (Ericsson, Indra, Siemens and Diehl) – along with seven research institutions, including the Rand Corporation.

Four members of the European Parliament (MEPs) were there too, adding a democratic sheen to the process, though one of them, Karl Von Wogau, is well known as a chairman of the European Parliament's Committee on Security and Defence. Mr. Von Wogau is also an advisory board member of Security and Defence Agenda (SDA), an arms industry 'think tank' and lobby group.[36] Six members of the GoP later contributed to Von Wogau's book, the '*Path to European Defence*',[37] including Burkhard Schmitt, the GoP's *rapporteur* [report writer] and assistant director of the EU Institute of Security Studies, another individual described as a 'proponent of free trade in the defence industry'.[38]

In February 2004 the European Commission announced that it had established the €65 million 'Preparatory Action for Security Research' (PASR, see following section),[39] claiming a tenuous mandate from the meeting of EU heads of state at the Thessaloniki European Council in June 2003.[40] There had been no 'Green Paper' on security research, setting out possible policy options, and no public debate. More controversial was the choice of a legal basis for the PASR: Article 157 of the EC Treaty on the 'competitiveness of the Community's industry', rather than Article 163 on 'R&D'. This political decision meant the ESRP would now develop under the auspices of the Commission's Directorate-General for Enterprise, instead of DG Research, the established Research & Development (R&D) arm of the Commission. This implied that the goals of the DG Enterprise (industrial competitiveness and long-term profits) were more important than those of its R&D counterpart (the creation of a 'knowledge society').

[34] *Intelligence Online* n° 468, available at: http://www.intelligenceonline.com/NETWORKS/FILES/468/468.asp?rub=networks.

[35] Hayes, B. (2006) *Arming Big Brother: The EU's Security Research Programme*. Amsterdam: TNI/Statewatch. Available at: http://www.statewatch.org/analyses/bigbrother.pdf.

[36] See SDA website: www.securitydefenceagenda.org.

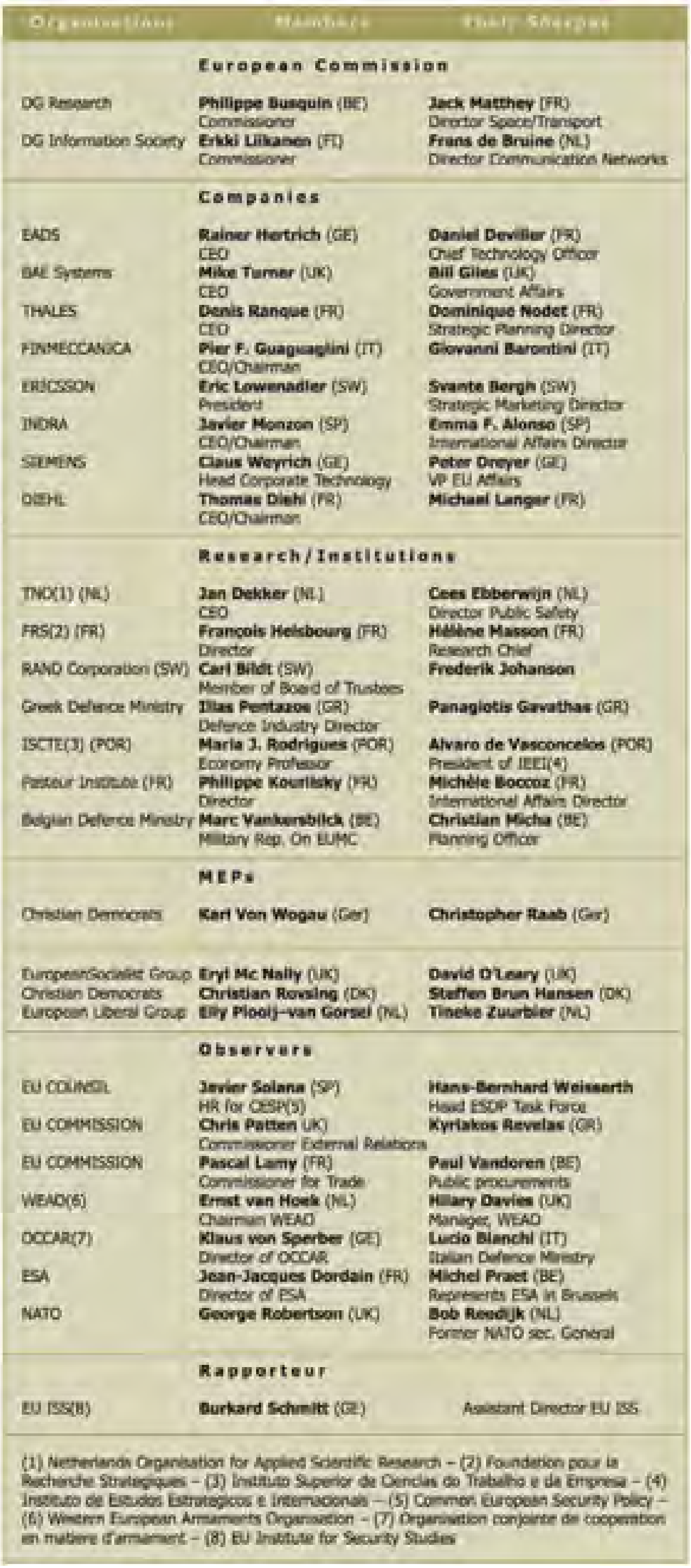
[37] Von Wogau, K. (ed) (2004) *The Path to European Defence*. Brussels: Maklu-Uitgevers.

[38] Source: *US Army War College's Strategic Studies Institute*, see http://www.strategicstudiesinstitute.army.mil.

[39] *European Commission Decision 2004/213/EC of 3 February 2004 on the implementation of the Preparatory Action on the Enhancement of the European industrial potential in the field of security research.*

[40] *Thessaloniki European Council 19 and 20 June 2003: presidency Conclusions, Council doc. 11638/03, 1 October 2003.*

The Group of Personalities on Security Research, 2003 [41]



Organisations	Members	Their Sherpas
	European Commission	
DG Research	**Philippe Busquin** (BE) Commissioner	**Jack Matthey** (FR) Director Space/Transport
DG Information Society	**Erkki Liikanen** (FI) Commissioner	**Frans de Bruine** (NL) Director Communication Networks
	Companies	
EADS	**Rainer Hertrich** (GE) CEO	**Daniel Deviller** (FR) Chief Technology Officer
BAE Systems	**Mike Turner** (UK) CEO	**Bill Giles** (UK) Government Affairs
THALES	**Denis Ranque** (FR) CEO	**Dominique Nodet** (FR) Strategic Planning Director
FINMECCANICA	**Pier F. Guaguaglini** (IT) CEO/Chairman	**Giovanni Barontini** (IT)
ERICSSON	**Eric Lowenadler** (SW) President	**Svante Bergh** (SW) Strategic Marketing Director
INDRA	**Javier Monzon** (SP) CEO/Chairman	**Emma F. Alonso** (SP) International Affairs Director
SIEMENS	**Claus Weyrich** (GE) Head Corporate Technology	**Peter Dreyer** (GE) VP EU Affairs
DIEHL	**Thomas Diehl** (FR) CEO/Chairman	**Michael Langer** (FR)
	Research/Institutions	
TNO(1) (NL)	**Jan Dekker** (NL) CEO	**Cees Ebberwijn** (NL) Director Public Safety
FRS(2) (FR)	**François Heisbourg** (FR) Director	**Hélène Masson** (FR) Research Chief
RAND Corporation (SW)	**Carl Bildt** (SW) Member of Board of Trustees	**Frederik Johanson**
Greek Defence Ministry	**Ilias Pentazos** (GR) Defence Industry Director	**Panagiotis Gavathas** (GR)
ISCTE(3) (POR)	**Maria J. Rodrigues** (POR) Economy Professor	**Alvaro de Vasconcelos** (POR) President of IEEI(4)
Pasteur Institute (FR)	**Philippe Kourilsky** (FR) Director	**Michèle Boccoz** (FR) International Affairs Director
Belgian Defence Ministry	**Marc Vankersbilck** (BE) Military Rep. On EUMC	**Christian Micha** (BE) Planning Officer
	MEPs	
Christian Democrats	**Karl Von Wogau** (Ger)	**Christopher Raab** (Ger)
EuropeanSocialist Group	**Eryl Mc Nally** (UK)	**David O'Leary** (UK)
Christian Democrats	**Christian Rovsing** (DK)	**Steffen Brun Hansen** (DK)
European Liberal Group	**Elly Plooij-van Gorsel** (NL)	**Tineke Zuurbier** (NL)
	Observers	
EU COUNSIL	**Javier Solana** (SP) HR for CESP(5)	**Hans-Bernhard Weisserth** Head ESDP Task Force
EU COMMISSION	**Chris Patten** UK) Commissioner External Relations	**Kyriakos Revelas** (GR)
EU COMMISSION	**Pascal Lamy** (FR) Commissioner for Trade	**Paul Vandoren** (BE) Public procurements
WEAO(6)	**Ernst van Hoek** (NL) Chairman WEAO	**Hilary Davies** (UK) Manager, WEAO
OCCAR(7)	**Klaus von Sperber** (GE) Director of OCCAR	**Lucio Bianchi** (IT) Italian Defence Ministry
ESA	**Jean-Jacques Dordain** (FR) Director of ESA	**Michel Praet** (BE) Represents ESA in Brussels
NATO	**George Robertson** (UK)	**Bob Reedijk** (NL) Former NATO sec. General
	Rapporteur	
EU ISS(8)	**Burkard Schmitt** (GE)	Assistant Director EU ISS

(1) Netherlands Organisation for Applied Scientific Research – (2) Foundation pour la Recherche Stratégiques – (3) Instituto Superior de Ciencias do Trabalho e da Empresa – (4) Instituto de Estudos Estratégicos e Internacionais – (5) Common European Security Policy – (6) Western European Armaments Organisation – (7) Organisation conjointe de coopération en matière d'armement – (8) EU Institute for Security Studies

[41] See also: 'The Experts Looking Out for Europe's Security', *Intelligence Online* n° 468, available at: http://www.intelligenceonline.com/NETWORKS/FILES/468/468.asp?rub=networks.

The Group of Personalities' report

The Group of Personalities proposed that European security research should be funded at a level similar to that of the USA. A US annual per capita expenditure of "more than four dollars on security-related R&D for each citizen" would *"mean that an overall EU security R&D budget of 1.8 billion for 450 million Europeans would be desirable"*, suggested the GoP. In its final analysis, the report called for a minimum of €1 billion per year in EU funds for the ESRP to *"bridge the gap between civil and traditional defence research, foster the transformation of technologies across the civil, security and defence fields and improve the EU's industrial competitiveness"*.[43]

The Group of Personalities' 2004 report centred upon a demand for the EU to foster the development of a European security–industrial complex through a programme of security research. The report put forward four main arguments in support of these recommendations. First, it argued that security, terrorism, proliferation of weapons of mass destruction, failed states, regional conflicts, organised crime and illegal immigration are the main sources of anxiety for both citizens and policy-makers. Second, it proposed that technology is vital for security: 'Technology itself cannot guarantee security, but security without the support of technology is impossible. It provides us with information about threats, helps us to build effective protection against them and, if necessary, enables us to neutralize them'. Third, it claimed that there are 'synergies' between the (military) defence and (civil) security sectors: *"technology is very often multi-purpose. Civil and defence applications increasingly draw from the same technological base and there is a growing cross-fertilisation between the two areas… As a result, the technology base for defence, security and civil applications increasingly forms a continuum… applications in one area can often be transformed"*.[44] Fourth, it stated that there is a strong economic case for subsidising the development of the security–industrial complex in Europe.

The GoP noted that the US Department of Homeland Security (DHS) budget 'includes a significant percentage devoted to equipment, and around $1 billion dedicated to research'. The scale of US investment in Homeland Security research, said the GoP, meant that the US was "taking a lead" in the development of "technologies and equipment which… could meet a number of Europe's needs". This was seen to be problematic because the US technology would 'progressively impose normative and operational standards worldwide' and 'US industry will enjoy a very strong competitive position'.[45] This argument has since been put to the author repeatedly by those involved with the ESRP. If European governments are to spend billions procuring security technology and equipment anyway, then surely it is better that they buy European, they suggest. And better still if European corporations can cash-in on the lucrative global market for security technologies at the same time.

After lengthy negotiations, the ESRP would ultimately have to make do with just under €200 million per year allocated to the security research component of the seven-year, Seventh Framework Programme (FP7), with the same amount again allotted to 'space research'. When additional EU security research and technology budgets and national security research programmes are taken into account, however, the total figure available may be much closer to the original GoP demand for the EU to match the billion dollars spent annually on security R&D in the USA.

'Research for a Secure Europe', the final report of the Group of Personalities, was published in March 2004, setting out the ideology and objectives of the future European Security Research Programme.[42]

[42] Group of Personalities (2004) *Research for a Secure Europe*, available at: http://ec.europa.eu/research/security/pdf/gop_en.pdf.

[43] GoP report, page 27.

[44] GoP report, page 13.

[45] GoP report, page 21.

What were the initial expectations? … [Y]ou have to understand that the home of security research at the Commission is DG Enterprise and Industry – and there you have the answer immediately. We needed to create a security research programme that would make real, meaningful contributions to the various areas of security policy and thus help to increase the security of the European citizens - from demonstrating the value of such contributions a European Security Equipment Market (ESEM) would grow. And we needed to make this sustainable, we needed to strengthen the European Security Technological and Industrial Base and its supply chains. If this sounds familiar to you from the defence side – yes it is.

European Commission spokesperson to
EU security research event, 2008 [46]

4 Preparatory actions: EU security research 2004-2006

The EU's Preparatory Action for Security Research (PASR) ran from 2004 to 2006, providing a total of €65 million to 39 projects over the three years.[47] The 'priority areas' for security research, decided by the European Commission on the basis of the GoP's recommendations, were:

(i) improving situation awareness
(ii) optimising security and protection of networked systems
(iii) protecting against terrorism
(iv) enhancing crisis management
(v) achieving interoperability and integrated systems for information and communication.

In 2004 alone, the ratio of applications received to projects funded was 13 to one. There would be no shortage of takers when the 'pocket change' on offer, as one British defence industry official put it, was replaced by the substantial coffers of FP7.[48]

The most striking feature of the Preparatory Action for Security Research was the extent of the involvement of the defence industry. Of 39 security research projects, 23 (60%) were led by companies that primarily service the defence sector. One third of the PASR projects (13) were led by Thales (France), EADS (Netherlands), Finmeccanica companies (Italy), SAGEM Défense Sécurité (part of the SAFRAN Group, France) and the AeroSpace and Defence Industries Association of Europe (ASD, Europe's largest defence industry lobby group). Together with BAE Systems (UK), these companies participated in 26 (67% or two-thirds) of the 39 projects.

The European Security Research Programme is predicated on the need to support the technological base of European industry but in 2006 alone the defence revenues of Thales, EADS, Finmeccanica, SAGEM and BAE Systems – corporations most heavily involved in the PASR – totalled more than $60 billion. Nor apparently are these transnational corporations losing out in the lucrative global homeland security market. All offer 'global solutions' to global security problems from locations around the world. EADS is one of the top ten suppliers to the USA's Department of Homeland Security (DHS), and BAE Systems is among the top ten suppliers to the Pentagon.[49]

In addition to the 39 projects funded under the PASR, the EU was also funding security-related research projects from its mainstream framework research' programme of 2002-6 (the €16.3 billion, 'FP6' programme). In a report for the European Parliament, Didier Bigo and Julien Jeandesboz estimate that by the end of 2006, 170 projects – relating di-

[46] Blasch, B (2008) 'Welcome on behalf of the European Commission and the European Programme', STACCATO [*Stakeholders platform for supply Chain mapping, market Conditions Analysis and Technologies Opportunities*"] *Final Forum 24 April 2008*, ASD Europe, available at: http://www.asd-europe.org/Objects/2/Files/blasch.pdf.

[47] Lists of projects funded under the PASR from 2004-6 are available on the European Commission's security research website: http://ec.europa.eu/enterprise/security/index_en.htm.

[48] Source: *Defensenews.com*, 26 February 2006.

[49] Sources: 'FACTBOX – Top 10 pentagon contractors', *Reuters*: http://www.reuters.com/article/companyNewsAndPR/idUSN0739108620070507; EADS website: http://www.eads-nadefense.com/news/press_re/ngc_tankerpr.htm.

rectly or indirectly to the themes and priorities identified by the GoP and the European Commission – had been funded under FP6.[50] The relevant FP6 research priorities included IT security, aeronautics, space and satellite-based monitoring and surveillance.

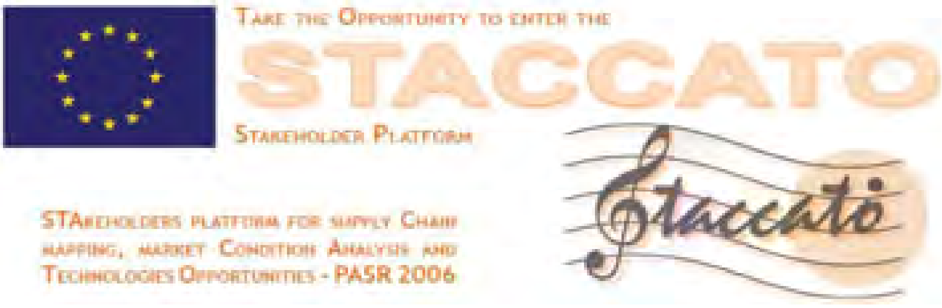
Taking the PASR and FP6 programmes together, by the end of 2006 the EU had already funded at least 50 research projects concerned with surveillance issues: biometric identification systems, surveillance and detection technologies, databases and information management, and risk profiling systems. In the majority of cases, these projects concerned the application of existing security technologies for policing and law enforcement purposes, rather than actual research into security technologies *per se* (specific projects are examined in more detail in Part III of this report).

Another important observation about the PASR is that eight of the 39 projects were not concerned with R&D but the longer-term development of the EU Security Research Programme and the infrastructure necessary for its implementation. As we shall see in the following section, in enhancing the EU's 'institutional capacity' for security research (the official justification for such projects) corporations again took centre stage. There is, of course, nothing new about governments consulting industry about policy, particularly at the EU level, but while corporations have been embraced by the ESRP, parliaments and civil society – with a few chosen exceptions – have been largely excluded. The process, as we shall see, has been wholly undemocratic.

EU Security Research Network & Stakeholder Platform

The 2004 SeNTRE project (Security Network for Technological Research in Europe, PASR) was led by the lobby group ASD (AeroSpace and Defence Industries Association of Europe), with the support of 21 partner organisations, two-thirds of which came from the defence sector.[51] Its main objective was "to support the European Commission to define the strategic research agenda for Security in support of and to link with the [planned] European Security Research Advisory Board". The SeNTRE consortium's findings included a 'methodology for security research' based on 'threats and mission classification', a government and law enforcement 'user needs survey', a technological survey within the SeNTRE consortium and the 'identification of technology driven innovations and priorities'. The SeNTRE consortium also delivered an 'organised platform of users and technology experts for future consultation' which almost certainly provided the basis for the European Security Research and Innovation Forum (see section 7, page 22).[52]

The 2005 Stakeholders platform for supply Chain mapping, market Condition Analysis and Technologies Opportunities (STACCATO) was a follow-up to the SeNTRE project. It was also funded under the PASR and led by the lobby group ASD. STACCATO produced an (unpublished) report entitled "How to foster the European Security Market", mapped existing security research competencies in the 27 Member States and proposed "methods and solutions for the creation of a security market and a structured supply chain in Europe".[53]


Take the Opportunity to enter the
STACCATO
Stakeholder Platform
STAkeholders platform for supply Chain mapping, market Condition Analysis and Technologies Opportunities - PASR 2006
Staccato

Flyer recruiting participants to the ESRP produced by the STACCATO project.

High-level study on 'threats' and responses

The ESSTRT consortium (on 'European Security, Threats, Responses and Relevant Technologies') was commissioned under the PASR to produce a 'high-level study on European security' led by Thales UK, with the support of the Institute for Strategic Studies and the Crisis Management Initiative. ESSTRT's final report, 'New Approaches to Counter-Terrorism', focused not just on counter-terrorism but the whole gamut of internal security, with the justification that 'many of the responses discussed are relevant to dealing with crime, major accidents and natural disasters'.[54] Like the GoP, ESSTRT argued that European states should pursue a technological approach to counter these threats and enhance security through intelligence gathering inside and outside of the EU, by strengthening EU border controls, subjecting the population to widespread surveillance and protecting potential terrorist targets (this is what the 'high-level' study calls the 'four fence model').

[50] Bigo, D. & Jeandesboz, J. (2008) *Review of security measures in the 6th Research Framework Programme and the Preparatory Action for Security Research*. Brussels: European Parliament, available at: http://www.pedz.uni-mannheim.de/daten/edz-ma/ep/08/EST21149.pdf.

[51] The SENTRE consortium included *IABG*, *QinetiQ*, *IPSC*, *ARC* (Austrian Research Centers), *FhG* (Fraunhofer-Gesellschaft), *EADS Astrium*, *Finmeccanica*, *Dassault Aviation*, *Sagem*, *Rheinmetall*, *EADS*, *Thales Avionique*, *Herstal Group*, *Saab Ericsson Space*, *BAE Systems*, TNO, the EU Joint Research Centre (Institute for Protection and Security of the Citizen), Istituto Affari Internatiozionale, Délégation Générale de l'Armement (Centre d'Etude du Bouchet), VTT (Technical Research Centre of Finland).

[52] See also Blasch, B (2008), note 46, above.

[53] STACCATO was comprised of four work packages: Stakeholder Platform (led by EADS), Market Condition Analysis (Finmeccanica), Integration of Priorities and Recommendations (Thales) and Analysis of Competencies of the Supply Chain (EU Joint Research Centre). See further 'STACCATO RESULTS and DELIVERABLES', *ASD* website: http://www.asd-europe.org/content/default.asp?PageID=34.

[54] ESSRT (2006) *Final report: New European Approaches to Counter Terrorism*. London: Thales Research and Technology, International Institute for Strategic Studies, Crisis Management Initiative (CMI) & Thales e-Security (TeS), available at: http://www.iiss.org/programmes/defence-analysis-programme/analysis-archive/european-security-high-level-study/.

Contrary to repeated European Commission claims that the ESRP is concerned only with security technology (and not security policy), the ESSTRT study contained over 70 detailed recommendations – including 32 specific EU 'policy actions'. In addition to the final report, ESSTRT delivered a set of 24 reports and annexes to the European Commission, including 'Threats to European Security', 'Technology Survey', 'Political Legal and Ethical Aspects of Security', 'Technology Gaps', and 'Responses to Terrorist Threats'. The ESSTRT recommendations conclude with an extraordinary 'unified Strategic Aim governing future activities at all levels', drafted in the style of an EU Treaty provision or Declaration, calling on member states to 'avoid policies likely to create new obstacles for counter-terrorism policies and measures' (see box below).

ESSTRT also recommended that the European Commission 'develop a communications strategy that fosters public awareness of threats and of the extent and limits of governments' ability to counter them'. Such a strategy should stress 'that it is a *long-term challenge*; that while it may be driven by external factors, considerable attention needs to be devoted to the capacity for *internal generation* of terrorist cells within EU member states (emphasis in original). The advice continued with a call on the EU member states to adopt 'minimum standards of law enforcement' that 'allow necessary powers to security organisations including – depending on legislation – access to bank records, ability to intercept communications, and the capacity to use surveillance measures'.[55]

Setting the agenda?

FINAL REPORT

New European Approaches to Counter Terrorism

21 MARCH 2006

THALES

"The Member States and their institutions will:

- consistent with the European Treaties and in the spirit of solidarity between them, ensure they meet the fundamental goals of the European Union in the face of the challenge from Terrorism, whether externally driven or internally generated, including:

- The continued free movement of peoples, goods, services and capital; and the free flow of information

- The protection of civil society and individual rights, by maintaining social justice, harmony and stability

- The maintenance of growth in economic activity

- The enhancement of political relations with external partners

- as the basic condition for achieving this Aim, establish an overall set of criteria by which further EU actions, either by Member States or by their institutions, can be judged, criteria which will include ***the avoidance of policies likely to create new obstacles for counter-terrorism policies and measures****".*

(ESSTRT recommendation to EU, emphasis added).

The PASR-funded 'High Level Study on European Security, Threats, Responses and Relevant Technologies' was led by Thales UK, with the support of the EU Institute for Security Studies and the Crisis Management Initiative.

In addition to the ESSTRT, SENTRE and STACCATO projects, there were five further PASR projects geared toward the strategic development of the ESRP: the IMPACT project on an EU CBRN [chemical, biological, radiological and nuclear weapons] counter-terrorism research and acquisition programme; PETRANET, establishing a 'user network for the take-up of security research'; SECURESME, on increased participation of small and medium-sized enterprises in the ESRP; and the USE-IT and SUPHICE projects on secure communications networks for security research.

Only one of the 39 PASR projects, the PRISE project led by the Austrian Academy of Sciences, focused specifically on issues of privacy and civil liberty in the context of European security research. The PRISE consortium set out to develop "acceptable and accepted principles for European Security Industries and Policies" based on 'privacy enhancing security technologies'. In its final report, PRISE produced detailed and well-reasoned criteria and recommendations, including the entrenchment of EU privacy and data protection standards in all security technologies.[56] Unfortunately, these appear to have had little influence on the development of the ESRP or the broader EU political agenda. Instead, EU policy makers are now talking about limiting the availability of privacy enhancing technologies to the people of Europe on the grounds that they could be 'exploited' by terrorists and criminals (see further section 25, page 75).

[55] ESSTRT, 2006: 6-7, see note above.

[56] Full details of the project and all reports are available on the PRISE website: http://www.prise.oeaw.ac.at/.

It is rare on a national level, but even more so at European level, that end-users of security research results jointly define the required medium-term research development alongside the suppliers and performers of security research. This is exactly what the European Commission has successfully managed to achieve with the creation and implementation of the European Security Research Advisory Board (ESRAB)…

Its preparation underlines the importance attached to security research and technology. Without it there can be no progress towards either the social aspirations for a more free, secure and open Europe or the benefits of a more competitive technology supply chain. All of these hopes for the future depend upon new solutions being developed and implemented and these all depend upon Europe having the technological capability.

Preface, Report of the European Security Research Advisory Board, 2006 [57]

5 Setting the agenda: the European Security Research Advisory Board

The European Security Research Advisory Board (ESRAB) was established by European Commission Decision on 22 April 2005 'to advise on the content of the ESRP and its implementation, paying due attention to the proposals of the Group of Personalities'.[58] Like the GoP, ESRAB included 'experts from various stakeholder groups: users, industry, and research organisations'. There was no consultation of the European or national parliaments on who to appoint to ESRAB; nominations for the 50 positions on the board came instead from the EU ambassadors (the permanent representations of the member states), the newly established European Defence Agency and other unspecified 'stakeholder groups'.

ESRAB had a mandate to advise the Commission on any questions relating to the development of the ESRP and to make recommendations on:

- the strategic missions and priority areas for security research;
- implementation issues such as the exchange of classified information and intellectual property rights;
- the use of publicly owned research/evaluation infrastructures;
- a security research communications strategy.

ESRAB was left to adopt its own rules of procedure. There were two ESRAB working groups with 25 representatives on each. Group 1, the 'Technology group', dealt with 'security research demand requirements' while Group 2, the 'Enablers Group', addressed the 'technology supply chain requirements'. This structure appears to have had less to do with research than the needs of commerce and the objective of better integrating the supply chain (corporations) with the demand chain (governments).[59]

The defence and security industries were well represented, occupying 14 of 50 seats. Seven of the eight corporations on the GoP – EADS, BAE Systems, Thales and Finmeccanica, Ericsson, Siemens and Diehl – were given seats on ESRAB. The board was chaired by Markus Hellenthal of EADS and Tim Robinson of Thales, who had one 'presidential term' each. The remainder of the ESRAB seats went to the member states (18 seats), academics and research institutes (14), the EU, which was represented by the European Defence Agency and EUROPOL, and two 'civil liberty groups and think tanks'.[60]

The European Commission made much of the inclusion of two "civil society organisations and thinktanks", but while it apparently considers the Crisis Management Initiative (set-

[57] ESRAB (2006) *Meeting the challenge: the European Security Research Agenda – A report from the European Security Research Advisory Board*. Brussels: European Commission, available at: http://ec.europa.eu/enterprise/security/doc/esrab_report_en.pdf.

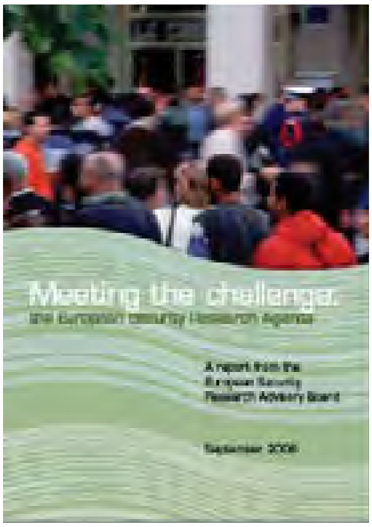
[58] *European Commission Decision 2005/516/EC of 22 April 2005 establishing the European Security Research Advisory Board.*

[59] A full list of the 50 members of the European Security Research Advisory Board is provided in the Group's final report, available at: http://ec.europa.eu/enterprise/security/doc/esrab_report_en.pdf.

[60] ESRAB was 'supported' by 14 different Commission services and five members of the European Parliament. No explanation is given as to why these actors did not participate as full ESRAB members. See Gasparini, G. and Leone, C., *'Meeting the challenge: the European Security Research Agenda', the final report of the European Security Research Advisory Board*, IAI/Finmeccanica [unreferenced paper on ESRAB], available at: http://www.iai.it/pdf/ESRAB/ESRAB-GaspariniLeone.pdf.

up by the ex-Finnish prime minister, Martti Ahtisaari) to be a 'civil liberties' organisation.[61] As to the 'thinktank' to which the Commission referred, it was either the EU-funded Institute for Security Studies (rapporteur for the GoP) or the Italian Istituto Affari Internazionali (Institute of International Affairs), both of which have conservative agendas.

The ESRAB report



The final report of the European Security Research Advisory Board, 'Meeting the challenge: the European Security Research Agenda', was published in September 2006, setting the research priorities for the FP7 programme 2007-13.[62] The report adopted the same technological-economy driven approach to security as the GoP before it, while incorporating much of the thinking behind the 'high--level' studies commissioned under the preparatory Action for Security Research (notably the ESSTRT and SENTRE projects, above).

The report proposed an extremely broad definition of 'security research', encompassing all 'research activities that aim at identifying, preventing, deterring, preparing and protecting against unlawful or intentional malicious acts harming European societies; human beings, organisations or structures, material and immaterial goods and infrastructures, including mitigation and operational continuity after such an attack (also applicable after natural/industrial disasters)'. ESRAB then developed the five core ESRP 'mission areas': 'border security', 'protection against terrorism *and organised crime*' (note the mission creep), 'critical infrastructure protection', 'restoring security in case of crisis' and 'integration, connectivity and interoperability'.

For each of these apparently distinct 'mission areas' ESRAB proposed the same response: impose total surveillance (so--called 'situation awareness and assessment') using every viable surveillance technology on the market; introduce identity checks and authentication protocols based on biometric ID systems; deploy a range of detection technologies and techniques at all ID control points; use high-tech communications systems to ensure that law enforcement agents have total information awareness; use profiling, data mining and behavioural analysis to identify suspicious people; use risk assessment and modelling to predict (and mitigate) human behaviour; ensure rapid 'incident response'; then intervene to neutralise the threat, automatically where possible. Finally, ensure all systems are fully interoperable so that technological applications being used for one mission can easily be used for all the others. This extreme model of security is discussed further in part III of this report.

'Ethical concerns'

Scientists for Global Responsibility (SGR, a UK based group of critical academics) report that the 'War on Terror' has "fuelled the relentless increase in the global military burden" and "contributed to a variety of changes in the ways in which security is framed by policy makers – many of them very controversial'. Among the most significant, suggest SGR, "has been the growing emphasis on high-technology, weapons-based approaches to tackling security problems".[63]

The European Security Research and Advisory Board's report devoted just one of its 84 pages to 'ethics and justice', observing that "security technologies, and the government policies accompanying them, raise many different ethical and legal concerns amongst the European citizens".[64] Here, ESRAB recognised the "lively public debate on civil liberties" and "potential loss of privacy" associated with security and counter-terrorism measures and recommended that "respect of privacy and civil liberties should be the [ESRP's] guiding principle". This was one of the report's ten 'key findings', but apart from the recommendation that security research should "take into account the mutual dependency triangle of technology, organisational dynamics and human impact", there was no further mention, whatsoever, of how civil liberties and human rights might actually be protected, never mind protected within the kind of high-tech scenarios outlined below.

Although the EU treaties place a clear legal obligation on policy-makers to protect fundamental rights, ESRAB adopted a more fluid perspective on rights and liberties, viewing them as a "political challenge", an experiment to find a "socially acceptable" balance. In this trade-off scenario, civil liberties have effectively been reduced to 'ethical concerns' that must be 'balanced' with the needs of security, and, by implication, can be restricted when the case for security has been made. To the extent that many people hold this 'baggage' to represent fundamental freedom developed over centuries and enshrined in the constitutional make-up of European democracy, this too is a paradigm shift.

Moreover, whereas the ESRAB report went to great lengths to persuade the reader of the ways in which technology

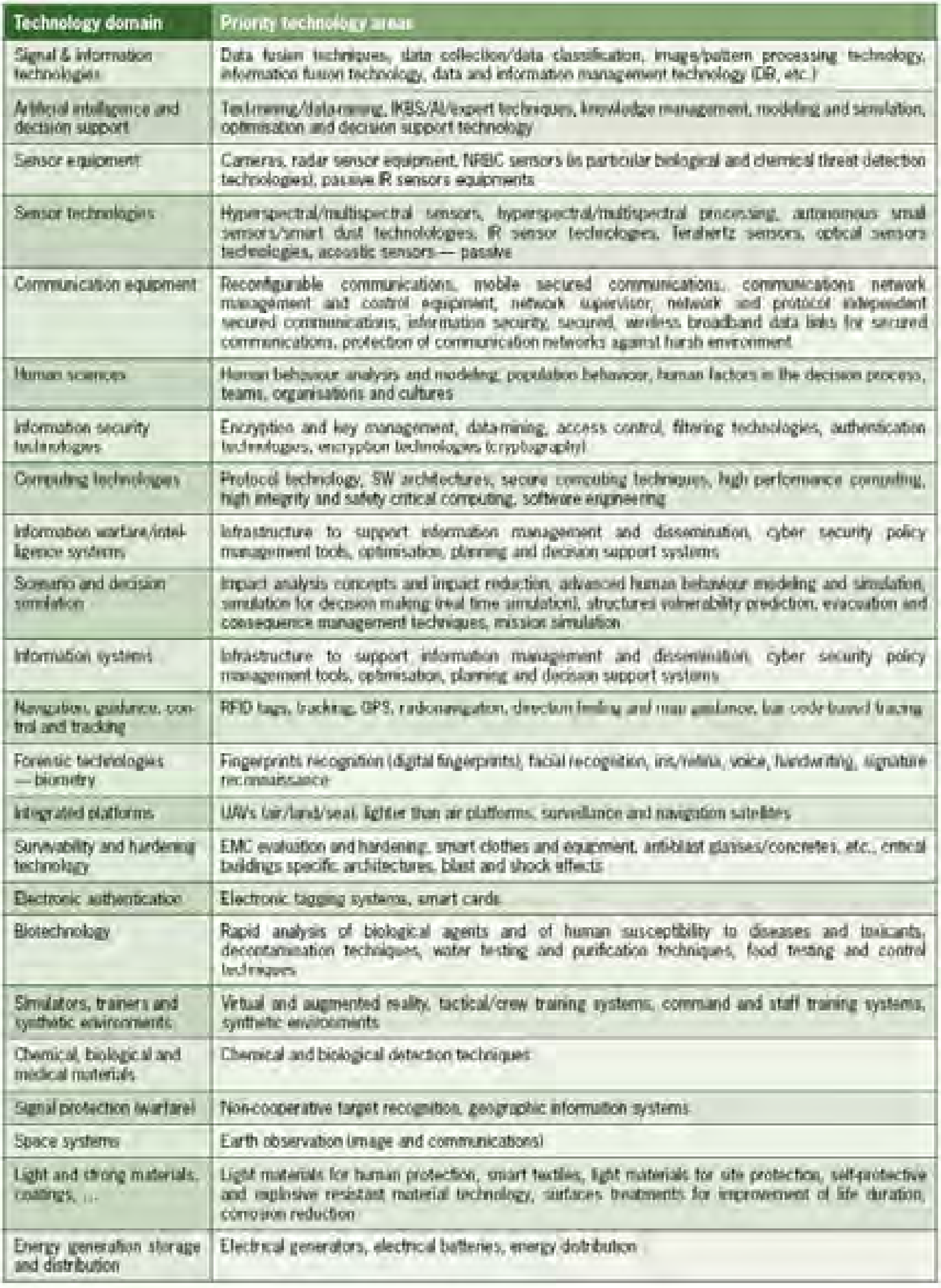
[61] The Crisis Management Initiative (CMI) is "an independent, non-profit organisation that innovatively promotes and works for sustainable security. CMI works to strengthen the capacity of the international community in comprehensive crisis management and conflict resolution. CMI's work builds on wide stakeholder networks. It combines analysis, action and advocacy", see CMI website: http://www.cmi.fi/.

[62] ESRAB (2006) *Meeting the challenge: the European Security Research Agenda – A report from the European Security Research Advisory Board*. Brussels: European Commission, available at: http://ec.europa.eu/enterprise/security/doc/esrab_report_en.pdf.

[63] Langley, C., Parkinson, S. & Webber, P. (2008) *Military influence, commercial pressures and the compromised university*, Scientists for Global Responsibility, available at: http://www.sgr.org.uk/ArmsControl/BehindClosedDoors_jun08.pdf.

[64] ESRAB report (page 60), available at: http://ec.europa.eu/enterprise/security/doc/esrab_report_en.pdf.

ESRAB: 'Cross mission-area technologies' [65]



Technology domain	Priority technology areas
Signal & information technologies	Data fusion techniques, data collection/data classification, image/pattern processing technology, information fusion technology, data and information management technology (DB, etc.)
Artificial intelligence and decision support	Text-mining/data-mining, IKBS/AI/expert techniques, knowledge management, modeling and simulation, optimisation and decision support technology
Sensor equipment	Cameras, radar sensor equipment, NRBC sensors (in particular biological and chemical threat detection technologies), passive IR sensors equipments
Sensor technologies	Hyperspectral/multispectral sensors, hyperspectral/multispectral processing, autonomous small sensors/smart dust technolologies, IR sensor techologies, Terahertz sensors, optical sensors technologies, acoustic sensors — passive
Communication equipment	Reconfigurable communications, mobile secured communications, communications network management and control equipment, network supervisor, network and protocol independent secured communications, information security, secured, wireless broadband data links for secured communications, protection of communication networks against harsh environment
Human sciences	Human behaviour analysis and modeling, population behavior, human factors in the decision process, teams, organisations and cultures
Information security technologies	Encryption and key management, data-mining, access control, filtering technologies, authentication technologies, encryption technologies (cryptography)
Computing technologies	Protocol technology, SW architectures, secure computing techniques, high performance computing, high integrity and safety critical computing, software engineering
Information warfare/intelligence systems	Infrastructure to support information management and dissemination, cyber security policy management tools, optimisation, planning and decision support systems
Scenario and decision simulation	Impact analysis concepts and impact reduction, advanced human behaviour modeling and simulation, simulation for decision making (real time simulation), structures vulnerability prediction, evacuation and consequence management techniques, mission simulation
Information systems	Infrastructure to support information management and dissemination, cyber security policy management tools, optimisation, planning and decision support systems
Navigation, guidance, control and tracking	RFID tags, tracking, GPS, radionavigation, direction finding and map guidance, bar code based tracing
Forensic technologies — biometry	Fingerprints recognition (digital fingerprints), facial recognition, iris/retina, voice, handwriting, signature reconnaissance
Integrated platforms	UAVs (air/land/sea), lighter than air platforms, surveillance and navigation satellites
Survivability and hardening technology	EMC evaluation and hardening, smart clothes and equipment, anti-blast glasses/concretes, etc., critical buildings specific architectures, blast and shock effects
Electronic authentication	Electronic tagging systems, smart cards
Biotechnology	Rapid analysis of biological agents and of human susceptibility to diseases and toxicants, decontamination techniques, water testing and purification techniques, food testing and control techniques
Simulators, trainers and synthetic environments	Virtual and augmented reality, tactical/crew training systems, command and staff training systems, synthetic environments
Chemical, biological and medical materials	Chemical and biological detection techniques
Signal protection (warfare)	Non-cooperative target recognition, geographic information systems
Space systems	Earth observation (image and communications)
Light and strong materials, coatings, …	Light materials for human protection, smart textiles, light materials for site protection, self-protective and explosive resistant material technology, surfaces treatments for improvement of life duration, corrosion reduction
Energy generation storage and distribution	Electrical generators, electrical batteries, energy distribution

can help protect against threats like crime and terrorism, it showed no interest whatsoever in the root causes of these phenomena or social policies that might address them, save for a single reference to the EU's 'social sciences and humanities' research programme (which is to receive a fraction of the funding available for security and space, see over). Instead, ESRAB has promoted a new academic discipline of 'security economics', which includes risk analysis, public finance analysis, drawing out the 'economic costs' of insecurity and research to combat terrorist financing.

[65] It is notable that 'crowd control' technologies, 'crowd-stopping devices' and 'less-lethal weapons' were among the security technologies included in the draft ESRAB report, obtained by the author, but omitted from the final version (unpublished 'final draft' of above ESRAB report, v.2.7, dated September 2006 (page 52)). On 'less lethal weapons', see further page 69 of this report.

[The FP7 programme] does not really invite political debate. Indeed we are not dealing with choices that could be discussed but with what presents itself as the simple enactment of the "Lisbon agenda", fully endorsing its slogans, such as "knowledge society", "economy of knowledge", "knowledge and its exploitation" as "the key for economic growth" and "the competitiveness of enterprises… what we are dealing with is an assemblage of what, in French, we call "mots d'ordre". Mots d'ordre are not made to induce thinking and debate but to produce agreement on consensual perception, putting on the defensive those who feel constrained to a "yes, but…". Yes to employment, yes to the European model, yes to all those improvements, and certainly yes to the progress of knowledge. But… the "but" is coming too late, after so many agreements, and it will be easy to fall into the trap, instead of addressing the means while ratifying the perceived consensual goals. It is the very functioning and aim of mots d'ordre to capture and inhibit the capacity to think.

Professor Isabelle Stengers, philosopher of science [66]

6 The FP7 programme and beyond: security research 2007-2013

FP7 is the EU's seventh Framework Programme for research.[67] It runs from 2007 to 2013 and has a total budget of €51 billion divided across 10 collaborative research topics (see diagram over) and three themes: 'ideas', 'people' and 'capacities'.[68] 'Security and space' has a combined budget of €2.8 billion, which will be divided equally between the two topics.

The security research component of FP7 provides a master class in how to prevent debate by substituting specific proposals for generalities, and disguising the aims with the means.[69] The rationale and priority areas for security research in FP7 are *identical* to those laid out by ESRAB but are condensed into a few pages, with none of the substance. To read the FP7 programme on its own, with its stated commitment to civil liberties, privacy, fundamental rights and democracy, unseasoned observers will find little cause for concern.

The call for proposals in the first year of the European Security Research programme proper (2007) elicited 325 eligible applications, with total requested funding of more than a billion euros. The European Commission apportioned €156.5 million Euros to 46 successful projects (making the programme seven times over-subscribed).[70] These projects are examined in more detail in parts IV to VI of this report.

Of the 46 FP7 security research projects funded under the 2007 call, 17 (or 37%) are led by organisations that primarily service the defence sector, with a further five led by corporations from the security industry. While the defence sector appears less dominant than it was in the Preparatory Action for Security Research (PASR 2004-2006, above), the overwhelming majority of projects feature one or more well known 'personalities' from the defence sector.

Of the European defence giants, Thales (leading three of the projects and participating in a further five) and Finmeccanica companies (leading two ESRP projects and participating in a further six) are particularly well represented. EADS also features strongly, as do Saab, Sagem and BAE Systems. Of the organisations represented on the GoP and ESRAB, the Swedish (FOI) and Dutch (TNO) defence research agencies are leading four projects and each participating in a further seven.

[66] Stengers, I. (2005) *Speech to the "What Science, What Europe?" conference in the European Parliament*, 2 -3 May 2005, available at: http://www.peoplesearthdecade.org/articles/article.php?id=381.

[67] See *Seventh Framework Programme*, European Commission website: http://cordis.europa.eu/fp7/.

[68] The EU Council (the member states) had originally agreed a total budget of €72 billion. Although substantially less was ultimately agreed, FP7 still represents a 60% increase on the previous FP6 budget.

[69] *Decision No. 1982/2006/EC of the European Parliament and of the Council of 18 December 2006 concerning the Seventh Framework Programme of the European Community for research, technological development and demonstration activities (2007-2013)*, OJ 2006 L 412/1.

[70] Due to delays in the launch of FP7 and the time taken by the European Commission to evaluate the proposals, complete the contractual negotiations and publish the relevant information, at the time of writing (June 2009) only the results of the 2007 call for proposals are available (these were finally published by the Commission in May 2009). At this time, the Commission is still evaluating the proposals to be funded under the 2008 call. The 2009 call for proposals under the ESRP/FP7 is planned for September 2009. A list of projects funded under the 2007 call is available on the European Commission's security research website: http://ec.europa.eu/enterprise/security/index_en.htm. All projects funded under the EU's framework research programmes can be found by searching the CORDIS website: http://cordis.europa.eu/search/index.cfm?fuseaction=proj.advSearch.

While there may be something instinctively uncomfortable about arms manufacturers moving into the Homeland Security sector, their dominance of this emerging market also reflects substantial effort upon their part to re-focus their core business strategies in the aftermath of 9/11. Whereas before 2001 the concept of Homeland Security had not even entered the popular lexicon, after 9/11 corporations were quick to establish divisions mirroring the restructured federal state apparatus in the USA and the newly established DHS. European defence companies were quick to follow the lead of their US counterparts, leaving them well placed to exploit the EU's own embrace of homeland security.

The same is true of Israeli organisations and corporations, whose Homeland Security expertise predates 9/11 and is born out of the politcs of the occupation and the attempt to surveille and control Palestinian populations. Israeli actors are participating in ten of the first 46 ESRP projects, leading four of them. It is also notable that the FP7 security research programme now includes demonstration projects (where prototype security systems are manufactured and tested) and infrastructure projects (for example, communications systems, critical infrastructure and crisis management capacity). Such projects are clearly geared toward the public procurement (at either EU or national level) of security technologies, rather than objective research in the traditional sense.

SECURITY RESEARCH
Towards a more secure society and increased industrial competitiveness
SECURITY RESEARCH PROJECTS
May 2009

Research for EU industrial competitiveness [71]

Research for global capital investors [72]

Broadening the EU security research programme

Substantial funds for 'security research' are also available under a range of other EU budget lines, suggesting that the overall EU 'security research' will be significantly larger than the annual €200 million allocated to the ESRP. A separate 'Critical Infrastructure Protection programme' (CIP) has been initiated by the EU's Joint Research Centre, and a joint call for proposals was issued under the security research and information and communication technologies (ICT) components of FP7. The CIP programme has its own budget to develop the "technology building blocks for creating secure, resilient, responsive and always available information infrastructures" and "transport and energy infrastructures that survive malicious attacks or accidental failures and guarantee continuous provision of services" (see further section 20, page 58).

Funds for security technology are also available under the €4 billion EU fund for 'Solidarity and Management of Migration Flows', of which €1.8 billion is earmarked for external borders and some €676 million is committed to the EU Return Fund for the expulsion and repatriation of 'illegal aliens'.[73] There will be further funding for security research at the national level. At least seven member states have already established national security research programmes in accordance with

[71] Overview of first 45 projects funded under 2007 ESRP, available at: http://ec.europa.eu/enterprise/security/doc/fp7_project_flyers/securityresearch-lowdef.pdf.

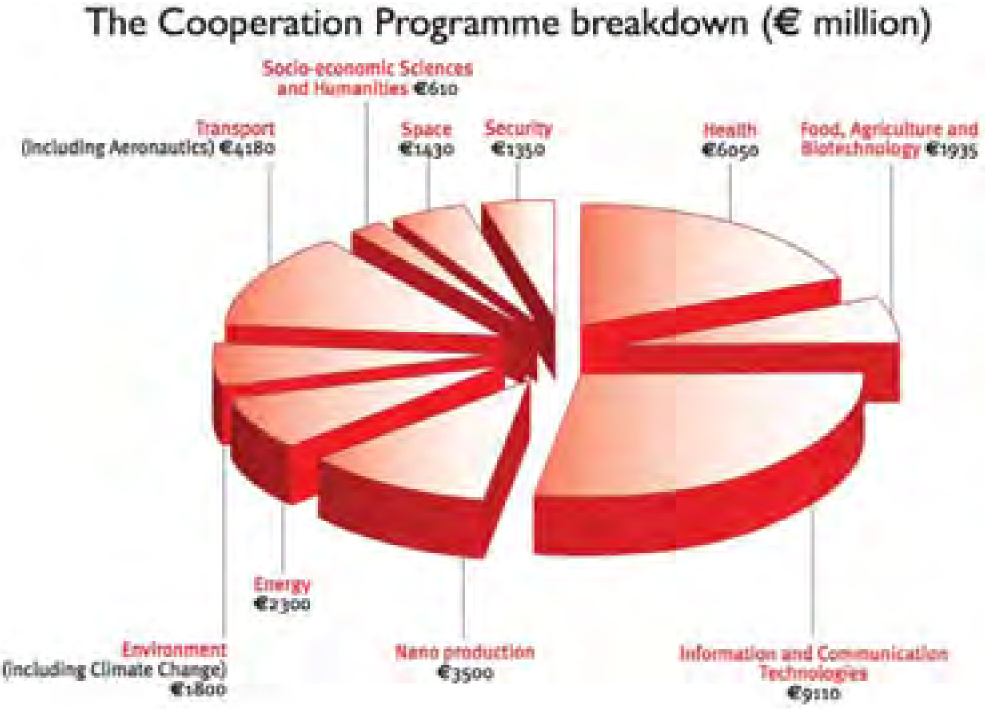
[72] Visiongain Market Research (2009) *Global Homeland Security 2009-2019* ($2,481.00), see ASD reports: http://www.asdreports.com/shopexd.asp?ID=1442.

[73] See *Solidarity and Management of Migration Flows*, European Commission website: http://ec.europa.eu/justice_home/funding/intro/funding_solidarity_en.htm. Further funds for border control equipment and technology were also available to the new member states under the 'Schengen Facility' (worth around €1 billion) and are available to Bulgaria and Romania under the 'Transition Facility' (worth around €100 million per year), source: Frattini, F. (2007), 'Security by design', *Homeland Security Europe*, available at: http://www.homelandsecurityeu.com/currentissue/article.asp?art=271247&issue=219.

earlier recommendations from the GoP and ESRAB – UK, France, Germany, Austria, The Netherlands, Sweden and Finland – and the EU has already begun setting-up a 'network of national ESRP coordination points' through the FP7-funded SEREN project.[74] 'Phase one' of the SEREN project will develop the network of national contact points for security research among EU and non-EU participating states.

Just as security-related research permeated the wider FP6 programme,[75] a good deal of convergence between the ESRP and the other elements of FP7 (listed below) is likely. The EU Space programme now includes a significant security and defence component (see section 18, below), while EU funded research into food, energy, transport, information and communications technology and environment inevitably include food security, energy security, transport security and so on. If the hype around 'nano-technology' – which is to receive a staggering €3.5 billion under FP7 – is translated into applied science, it too has the potential to impact fundamentally on military and security research by revolutionising surveillance capabilities, biological and chemical warfare, munitions and armaments.[76] According to Steve Wright, nanotechnologies will change the way that weapons are constructed "to achieve more effective target acquisition and destruction". "Super miniaturization will enable individual soldiers to become part of a more efficient battlefield where commanders use surveillance to actually see through the helmets of their men."[77]

The FP7 cooperation budget [78]



Research in the service of the ESRP?

Under the ESRP, the FORESEC project on 'Europe's evolving security: drivers, trends and scenarios' will provide "cogent guidance, orientation and structure to all future [EU] security related research activities" and "enhance the shared vision and facilitate the emergence of a coherent and holistic approach to current and future threats and challenges for European security amongst the community of official and non-official constituencies involved".

The FORESEC project is led by the Crisis Management Initiative, with the support of FOI (the Swedish state defence research institute), the International Institute for Strategic Studies (IISS), Austrian Research Centres GMBH, the Centre for Liberal Strategies (Bulgaria) and the Joint Research Centre of the European Commission. The preliminary conclusions' of the FORESEC asks whether, as "the scope of societal risk grows over time", "an ever-increasing share of our wealth [will] have to be expended on security?"[79] Those familiar with the EU constitution will recall a similar clause regarding military expenditure.

[74] See SEREN project website: http://www.seren-project.eu/.

[75] Bigo, D. & Jeandesboz, J. (2008) *Review of security measures in the 6th Research Framework Programme and the Preparatory Action for Security Research*. Brussels: European Parliament, available at: http://www.pedz.uni-mannheim.de/daten/edz-ma/ep/08/EST21149.pdf.

[76] Langley, C. (2005) *Soldiers in the laboratory: Military involvement in science and technology - and some alternatives*, Folkstone: Scientists for Global Responsibility (pages 54-55), available at: http://www.sgr.org.uk/ArmsControl/MilitaryInfluence.html. See also 'Industry, NGOs at odds over nanotech regulation', *Euractiv* 4.3.2009, available at: http://www.euractiv.com/en/science/industry-ngos-odds-nanotech-regulation/article-179936.

[77] Wright, S. (2006) 'Report. Sub-lethal vision: varieties of military surveillance technology', *Surveillance & Society*, 4(1/2): 136-153, available at: http://www.surveillance-and-society.org/Articles4(1)/sublethal.pdf (page 136).

[78] Source: European Commission FP7 brochure.

[79] Eriksson, A. (2008) 'First ESRIF results – Long term threats and challenges and needed capabilities', *FORESEC 2008 Workshop on "Europe's evolving security: drivers and trends", 2-3 July 2008*, availabe at: www.foresec.eu/wp3_docs/anders.ppt. See also Rintakoski, K. (2008) 'European Security Research Challenges for Foresight and risk assessment', FORS-seminar on security and risk assessment, 13 November 2008, available at: www.operaatiotutkimus.fi/seminaarit/108/Kalvot/Rintakoski.pdf.

Two further FP7 security research projects deal with the nature of the 'threats' to European security. The CPSI project, on 'changing perceptions on security and intervention' is led by TNO (the Research Laboratory for applied science of The Netherlands, which has a division on defence and security) and will examine "which interventions are effective for increasing security" and provide "practical and ready-to-use tools" for "policy makers and other end-users, to formulate policy regarding security".

The FESTOS project on the 'foresight of evolving security threats posed by emerging technologies' is led by Tel Aviv University with the support of Turku School Of Economics, the Technical University of Berlin, the European Foundation For Scientific Cooperation (a Polish NGO) and Efp Consulting Ltd (a specialist consultancy based in the UK and Israel offering services for EU framework research programme applications and project management). The goal of FESTOS is to "identify and assess evolving security threats posed by abuse or inadequate use of emerging technologies" and "to propose means to reduce their likelihood". "Looking ahead to 2030', the foresight study will identify "security threats that could stem from future technologies [including] Robotics, Cognition, New Materials, Nano and Biotechnologies" and "construct threat scenarios by analysing the impact of the identified threats on the background of envisioned security climates". The irony of security research into the threat from security research is presumably lost on the architects of the security research programme.

Meanwhile the EUSECON consortium comprises 14 of "the leading European research players" in the "newly emerging field of European security economics", including the RAND Corporation, the University of Jerusalem and Oxford University in order to develop "new analytical and conceptual insights" on security. EUSECON will establish a network of researchers to provide "research-based policy advice on economic aspects of security".[80] The "unifying theme of the proposed research are the human drivers of the new insecurity, that is terrorism and organized crime".

'Roadmaps' for research: the future direction of FP7

At least nine further projects promise to deliver 'roadmaps' setting out future research agendas for the EU and the security research component of the FP7 programme. This includes the CRESCENDO project on 'Coordination action on Risks, Evolution of Threats and Context assessment by an Enlarged Network for an R&D Roadmap', which is essentially a follow-up to and continuation of the work of the SENTRE and STACCATO projects (see section 4, above).[81] Similarly, the STRAW project will produce "a reviewed taxonomy on Security (based mostly on STACCATO) linked with a Data Base with information of providers, users and technologies", maintaining the stakeholder platform developed under the PASR. The STRAW consortium is led by IT giant Atos Origin, and features the defence and security lobby groups ASD and EOS (the European Organisation for Security) alongside Thales and Elsag Datamat (a Finmeccanica company). In addition there will be EU security research 'roadmaps' for the environment (SECURENV), the transport system (DEMASST), IT and other cyber-systems (ESCORTS), border control (GLOBE), the maritime frontier (OPERMAR), the policing of large scale public events and protests (EUSEC II), chemical, biological, radiological and nuclear material (CREATIF) and emergency response systems (NMFRDISASTER).

Ethical research?

The FP7 programme has at least demonstrated an increased commitment to research into the ethics of security research. The widely respected Oslo Peace Research Institute is coordinating the INEX project on "converging and conflicting ethical values in the internal/external security continuum in Europe". Its research will address "the ethical consequences of the proliferation of security technologies", the "legal dilemmas that arise from transnational security arrangements", "ethical and value questions that stem from the shifting role of security professionals" and "the consequences of the changing role of foreign security policy in an era when the distinction between the external and internal borders grows less distinct". Similarly, the DETECTER project, led by the Department of philosophy at the University of Birmingham (UK) on 'Detection technologies, terrorism, ethics and human rights' will examine "the compliance of counter-terrorism with human rights and ethical standards in the rapidly changing field of detection technologies".

As valuable as these projects may be, the crucial question posed by this report is whether they can have any meaningful impact on the broader trajectory of the ESRP and the development and implementation of the specific technologies examined below. In separating out the 'ethical dimension' of security research – rather than putting it at the heart of the ESRP (as promised by ESRAB and the European Commission) and thus at the centre of *every* security research project – the concern must be that 'ethics and justice' will be at best 'pigeon-holed', at worst ignored altogether.

[80] See EUSECON project website: http://www.economics-of-security.eu/eusecon/index.html.

[81] The CRESCENDO project features many of the same participants as SeNTRE and STACCATO. Its objective is to "strengthen, enlarge and render sustainable the networks created by SeNTRE and STACCATO", to "elaborate recommendations for some key themes for the Security Research Programme" and "analyse the evolution of threats (aggressions) and risks (accidents) assessment taking into account the balance between security and civil liberties".

ESRAB recommends the creation of a European Security Board (ESB), to foster greater dialogue and a shared view of European security needs. The board should bring together, in a non-bureaucratic manner, authoritative senior representatives from a cross stakeholder community of public and private stakeholders to jointly develop a strategic security agenda and act as a possible reference body for the implementation of existing programmes and initiatives… Consensus at the ESB level should help in the sharing of tasks and shaping relations between national and EU programmes/policies as well as influencing the deployment of funds.

European Security Research Advisory Board: key findings

7 2030 vision: the European Security Research and Innovation Forum

The creation of the 'European Security Research and Innovation Forum' (ESRIF) was announced at the '2nd European Conference on Security Research' in Berlin on 26 March 2007. ESRIF was not unveiled to the public until six months later (somewhat cynically on 9/11) in a Commission press release entitled 'public-private dialogue on security research'.[82] In all but name, however, ESRIF continues the GoP-ESRAB corporate governance of the ESRP, but with a wider remit.

According to the ESRIF website, "ESRIF will go beyond FP7 security research; it will go towards meeting long term security research and technological development needs throughout the EU to be covered by national, EU and private investments".[83]

ESRIF is comprised of a 65-member plenary and some 660 security research consultants divided into 11 working groups. An 'integration team' is responsible for co-ordinating the work of the plenary and the working groups. ESRIF's mandate includes:

- the identification of long term threats and challenges mainly building on foresight and scenario techniques;
- linking predictions and expectations about future developments
- related research requirements
- making the best possible use of the various funding instruments
- development of the 'supporting framework' for security research ('society, market and governance related')

ESRIF is taking a "mid and long term perspective (up to 20 years)… not only addressing the European but also the national and sometimes regional level". The ESRIF 'roadmap' on security research will be presented at the annual EU Security Research Conference in Stockholm on 29 September 2009.[84] Like ESRAB before it, it can be expected to draw upon the findings of high-level studies commissioned by the ESRP as well as the contributions of its members.

[82] *The European Security Research and Innovation Forum (ESRIF) - Public-Private Dialogue in Security Research*, European Commission press release dated 11 September 2007.

[83] See ESRIF website: http://www.esrif.eu/.

[84] See SCR09 conference website http://www.src09.se.

The 65 members of the ESRIF plenary were selected and appointed in the same way as for ESRAB (above): appointed by EU and member state officials without consultation with the European or national parliaments. The plenary was initially chaired by Gijs de Vries (the former EU Counter-terrorism coordinator), who has now been replaced by Dragutin Mate, former Slovenian Interior Minister, with Giancarlo Grasso of Finmeccanica and Jürgen Stock (Deutsches Bundeskriminalamt) appointed deputy chairs. Of the 65 plenary members, 30 represent the 'supply side' of security research and 33 the 'demand side', with five from 'civil society'.[85] Seventeen of the ESRIF members were also represented on ESRAB, including Thales, EADS, Finmeccanica and Sagem.[86]

The five 'think-tanks, civil liberty organisations and other relevant experts' represented on ESRIF are the German Federal Government Office for Population Protection and Disaster Relief (BBK), the European Institute for Risk, Security and Communication Management (EURISC), the European Corporate Security Association, the Centre of Biomedical Engineering at the Bulgarian Academy of Sciences and the ever-present Crisis Management Initiative. Again, there are no civil liberties or privacy organisations. Nor are there any members of the European Parliament on the ESRIF plenary. Several non-EU member state representatives are represented, however, including the Counter Terrorism Bureau of the National Security Council of the State of Israel ('demand side').

The ESRIF stakeholders

ESRIF is subdivided into 11 working groups comprised of the 65 ESRIF plenary members and a further 595 selected security research 'stakeholders'. Each working group has been assigned a 'leader' and a *'rapporteur'* (arguably the more influential position within ESRIF's *ad hoc* structure). Half of the 22 key actors are from the defence sector, with by now familiar organisations occupying key positions.

ESRIF working groups

Working Group		Leader	Rapporteur
WG1	Security of the citizens	Van Duyvendijk, Cees TNO [NL]	Suchier, Jean-Marc SAGEM Securité [FR]
WG2	Security of critical infrastructures	Travers, Eleanor Dublin Airport Authority [IE]	Holger Mey EADS [DE]
WG3	Border security	Berglund, Erik FRONTEX [EU]	Barontini, Giovanni Finmeccanica [IT]
WG4	Crisis management	Unger, Christoph BBK Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, DE	Prinz, Johannes FREQUENTIS [AT]
WG5	Foresight and scenarios	Rintakoski, Kristiina Crisis Management Initiative [FI]	Eriksson, Anders FOI [SE]
WG6	CBRNE	Stig Hansen, John-Erik National Centre for Biological Defence [DK]	Busker, Ruud TNO [NL]
WG7	Situation awareness & role of space	Madaleno, Utimia EMPORDEF [PT]	Comparini, Massimo Thales Alenia Space, IT
WG8	Identification of people and assets	Delville, Thierry Direction de l'administration de la police nationale, FR	Walsh, Martin European Biometrics Forum, IE
WG9	Innovation issues	Sieber, Alois Joint Research Centre, Ispra, EU	Desimpelaere, Luc Barco, BE
WG10	Governance and coordination	Accardo, Lucio Ministry of Defence, IT	Bell, Sandra RUSI, UK
WG11	Human and societal dynamics of security	Muresan, Liviu EURISC Institute [RO]	Sundelius, Bengt SEMA [SE]

[85] Note that several of the ESRIF plenary members represent more than one of three categories.

[86] A full list of members of the European Security Research and Innovation Forum is available on the ESRIF website: http://www.esrif.eu/documents/members_22012009.xls.

Euractiv [EU news website], 30 September 2008 [87]

2 December 2008

Breaking News: Coroner rules out unlawful killing of de Menezes

POLICY SECTIONS

cience & Research

ERA - European Research Area

Lead markets - gateway to growth?

Knowledge and technology transfer

European Institute of

HOME ▸ SCIENCE & RESEARCH

News

EU security research seeks respect of civil liberties

Published: Tuesday 30 September 2008

Europe needs to strike the right balance between enhancing security and preserving civil liberties, stressed politicians on the occasion of the third European conference to showcase concrete applications of security research for citizens.

> *"We need to listen to the technical experts to tell us what is technically feasible. Then we need to listen to experts on fundamental rights to see whether there are consequences of using these technologies that would put these rights in danger. It is only when we have considered all sides of the equation that we can find a balanced response".*
>
> Franco Frattini, former EU Commissioner for Justice and Home Affairs [88]

According to figures provided by the European Commission in response to a freedom of information request by the author, out of 660 security research 'stakeholders' participating in the ESRIF working groups, 433 (66%) are from the 'supply side' (defence and security contractors). This percentage rises to 69 per cent if the 'double hatters' (representing multiple interests) are taken into account.[89] Some companies are particularly well represented in the stakeholder database, including EADS (43 registrations), Finmeccanica (29), Thales (19) and AeroSpace and Defence Industries Association of Europe (ASD, 11).

The 'Demand side' stakeholders account for another 200 (or 30%) of the places on ESRIF. This includes 62 representatives of EU institutions and agencies: 28 from the European Commission's DG Enterprise, which is overseeing the ESRP, nine each from DG Justice, Liberty and Security (EU home affairs) and the European Defence Agency, three from EUROPOL, two from FRONTEX, eight from other Commission Directorates and three members of the European Parliament. Just nine out of the 660 ESRIF stakeholders' (1.4%) come from the 'civil society' category. These are the organisations represented on the ESRIF plenary noted above, together with the Institute of European Affairs, the George C. Marshal Association and an Irish consultant. Again, there is a not an established civil liberties or privacy organisation in sight.

ESRIF accountability

Given its composition, it is very difficult to see how ESRIF will find the 'balanced response' the EU has repeatedly claimed to be seeking. On the contrary, in establishing three successive security research 'advisory groups' (the GoP, ESRAB and ESRIF), the European Commission has plainly failed to ensure the balanced representation of stakeholders it has promised. Whereas corporations have played a central role

[87] 'EU security research seeks respect of civil liberties', *Euractiv* 30.9.2008: http://www.euractiv.com/en/science/eu-security-research-seeks-respect-civil-liberties/article-175851.

[88] Frattini, F. (2007), 'Security by design', *Homeland Security Europe*, available at: http://www.homelandsecurityeu.com/currentissue/article.asp?art=271247&issue=219.

[89] Some of the 660 stakeholders are represented in more than one of the 11 ESRIF working groups. When the total of 889 registrations are analysed, 'supply-side' (industry) representation on ESRIF increases to 72%.

in the development of the ESRP, with very few (specifically chosen) exceptions, Europe's parliaments and civil liberties and human rights organisations have been marginalised and excluded. This is not just a question of failing to 'balance' rights and liberties with security. For Corporate Europe Observatory and others in civil society, the appointment of industry-dominated stakeholder groups to develop EU policy represents an unlawful act of maladministration.[90]

According to the European Commission, the European Security Research and Innovation Forum is an "informal group, set up jointly and co-owned by its stakeholders from the demand and supply side of security technologies/solutions"; it is *"neither a Commission body nor a Commission driven exercise"*.[91] This is an astonishing statement insofar as it suggests that the Commission has effectively outsourced the strategic development of a €1.4 billion EU research programme to a wholly unaccountable, informal group. If the claim is false, and it is clear that ESRIF is, if not 'driven' then at least 'steered' by the European Commission, then the Commission has failed spectacularly to ensure adequate accountability mechanisms and reported the discharge of its responsibilities quite dishonestly. Both propositions are wholly unacceptable.

The real reason that ESRIF has been established as an informal grouping is the absence of a suitable legal basis in the EU Treaties for the European Commission to establish an advisory body dealing with both security policy and technology issues. This also speaks volumes. Instead of seeking to legitimise the Commission's activities in this area, the EU and its member states have chosen instead to give a dubious mandate to an informal body.

Running ESRIF and its predecessors on an *ad hoc* basis without formalising the role of the chosen 'stakeholders' also makes it very difficult for outside observers to understand the formation and implementation of EU security research policy. Crucially, the absence of legitimate funding for ESRIF'S activities also favours those organisations large enough to provide their expertise, advice and assistance for free, hence the massive over-representation of the defence industry. According to the new European Commission register of lobbyists interests, the likes of EADS, Thales and the lobby group ASD spend hundreds of thousands of Euros every year on EU lobbying activities alone.

Their invitation to help shape the EU security research agenda gives these organisations a competitive advantage when bidding for the funds on offer under subsequent EU tenders. Moreover, since the FP7 application process is lengthy, time consuming and thus expensive, those organisations that can afford to develop their ideas into multiple applications are inevitably better placed than small organisations which are forced into collaborative roles with 'big business' (and 'big academia'). It is no coincidence that a whole industry has sprung up around EU research framework programme applications (services available to the highest bidder).

The confusion that surrounds the failure to clearly separate the design of the programme (and setting of its priorities), on the one hand, from the would-be applicants (and their clamour for funding), on the other, has engendered a structural conflict of interests and may even have contaminated the evaluation process. Standard practice for the evaluation of research proposals is for the European Commission to use independent, external evaluators with some expertise in the field in question. In security research, this inevitably means security technology experts. When the PASR proposals were being evaluated, however, the Commission was apparently so short of relevant experts that its own officials were involved in the evaluation process – a clear breach of the rules governing EU funded research. The Commission duly recruited enough independent security research experts for the FP7 programme, but many of these were inevitably drawn from the same pool of stakeholders involved in the development of the ESRP itself.[92]

[90] Complaint by Corporate Europe Observatory to the European Ombudsman against the European Commission re Biofuels Research Advisory Council (BIOFRAC) and European Biofuels Technology Platform (EBFTP), April 2008.

[91] See ESRIF website: http://www.esrif.eu/.

[92] By the time FP7 had gotten underway, the Commission had recruited enough evaluators with the requisite security research expertise. The list of 143 evaluators used in 2007, obtained by the author, contains 21 'non-research public bodies' (including 14 interior and defence ministries and national police agencies), 28 'non-research private bodies' (mostly management, government and IT consultants with a few security research specialists), 41 'research organisations' (the majority of which are private companies, and 17 of whom are concerned specifically with security, military, aerospace and nuclear research), an impressive array of professors and PhDs from 35 universities (departments largely unspecified) and 18 'others' (including nine defence procurement and law enforcement agencies). At least 20 of the evaluators come directly from organisations represented on ESRAB or its successor organisation, the European Security Research and Innovation Forum (ESRIF). There must be significant doubts as to whether this cross section of security research evaluators provides the necessary degree of independence expected of the European Commission.

Formed under recommendation of the European Security Advisory Board (ESRAB) which advocated close private/public interaction when implementing the European Commission's Security Research under the 7th Research Framework Programme, EOS during its start-up phase will enjoy organisational and structural support from the AeroSpace and Defence Industries Association of Europe (ASD).

Though working closely with the European Commission and the European Security Research and Innovation Forum (ESRIF), the European Security Organisation shall also act as a link between the European Commission, European and National Institutions and EOS members, as well as between members themselves.

Luigi Rebuffi, CEO, European Organisation for Security [93]

8 A lobbyist's dream

The European Organisation for Security

The European Organisation for Security (EOS), a new umbrella lobby group representing the interests of the security and defence industry, was launched in May 2008.[94] EOS' CEO is Luigi Rebuffi, a former Director of Thales; the chairman is Markus Hellenthal of EADS, who also chaired the EU's Security Research and Advisory Board (ESRAB, above). EOS describes itself as "an organisation that can easily get and manage all kind of contracts, faster to set up than traditional Associations and easily providing resources for effective management of projects and studies for its members".[95] EOS is modelled on 'ERTICO', the "multi-sector, public/private partnership pursuing the development and deployment of Intelligent Transport Systems and Services in Europe", which was established to lobby EU officials responsible for transport policy.[96] EOS is a 'non-profit organisation' in which all members own an equal share and is funded by membership fees of €4,000-7,000 (the higher figure is for members of the Board of Directors).

At the time of writing EOS has 26 members, including ASD, BAE, Dassault, Diehl, EADS, Fincantieri (a Finmeccanica company), Indra, Sagem, Smiths, Saab, Thales, and TNO. One third of the EOS membership is also represented on the ESRIF plenary (above). While it is an exaggeration to suggest that ESRAB *recommended* the creation of EOS (see quote above), the new organisation shares the same core objectives as the ESRP, namely to "promote a coherent EU security market" and "contribute to the definition of an all encompassing European civil security policy". EOS claims to be supporting the creation, development and operations of the European Security Research and Innovation Forum, the ESRIF Secretariat of the European Commission, the work and management of the ESRIF and the European Commission's ESRP Integration Team, as well representing the "interest and positions of a wide part of private security stakeholders" on ESRIF. EOS also provides "support functions on key issues (e.g. co-ordination of work and projects/activities in specific sectors, facilitate dialogue with users/operators, link with SMEs)" and will support "the implementation of ESRIF recommendations in the long term".

EOS also aims to "advise on security policy definition and implementation in other relevant EU Forums", participate in EC Task Forces and projects and liaise directly with a number of Commission DGs. To this end, EOS has established seven working groups dealing with broadly the same subjects as ESRIF (above): Green & Blue Borders, Surveillance, Security & Safety; Civil Protection (including crisis management); Energy Infrastructures Security and Resilience; Supply Chain Security; Air Passenger transport Security; ICT networks, data protection, Information Society Security; Surface Transport Security.

[93] See unreferenced 'background paper' on EOS, available at : http://www.isi-initiative.eu.org/getdocument.php?id=210.

[94] See EOS website: http://www.eos-eu.com/.

[95] See unreferenced 'background paper' on EOS (page 12), available at : http://www.isi-initiative.eu.org/getdocument.php?id=210.

[96] ERTICO and EOS are registered as 'SCRLs' under Belgian Law and managed as a independent, non-profit entities. See ERTICO website : http://www.ertico.com/.

Where supply meets demand

There is nothing new about business interests attempting to define themselves as NGOs: the term BONGOs (Business Oriented NGOs) was conceived to describe them,[97] but it is not every day that Europe's largest defence industry-lobby group creates a new organisation on the back of a specific EU policy measure, as the ASD membership has effectively done with the European Organisation for Security. EOS joins a host of security and defence industry-funded thinktanks, publications, PR groups and events management companies, perhaps the best known of which is the 'Security and Defence Agenda'. SDA is another Brussels-based 'thinktank' whose members include Europe's largest defence contractors, NATO and the EU Defence Agency, with patrons such as Karl von Wogau MEP, George Robertson and Javier Solana, who welcomed the re-launch of SDA as "the sort of platform for new thinking and ideas that we need in Brussels to help forge consensus on common policies".[98] Despite the vast majority of its funding coming from industry membership and corporate sponsors, SDA describes itself as "an independent organisation without institutional or corporate ties".

In addition to a host of new and established security 'BONGOs' are the national and international security 'GONGOs': Government Oriented NGOs masquerading as independent 'thinktanks' or research organisations. Examples here include the EU Institute for Security Studies, a body created under the 'Second Pillar' of the European Union that describes itself as "an autonomous agency with full intellectual freedom [that] researches security issues of relevance for the EU and provides a forum for debate".[99] The European Homeland Security Association (another Belgian non-profit organisation),[100] the European Corporate Security Association and the European Biometrics Forum are among other 'non profits', GONGOs and BONGOs to emerge in this area. In turn, these associations and think-tanks produce and contribute to a host of academic, quasi-academic and business-oriented journals. 'Homeland Security Europe', for example, is an online and hard-copy publication produced by GDS Publishing, a division of GDS International specialising in "industrial and business management journals for the world's most exciting markets".[101] Contributors to HSE magazine include Franco Frattini, former Vice President of the European Commission ("Security by design"), Max-Peter Ratzel, Director of Europol ("United we stand") and Christian Sommade, Executive Director of the European Homeland Security Association ("We must be ready for the worst at anytime"), ensuring that the views of policy-makers and practitioners are presented to a wide audience alongside 'vendor perspectives'.[102] The same 'supply-side-meets-demand-side' collusion that permeates the European Security Research Programme is evident in countless international security conferences at which senior security policy-makers and practitioners discuss the future trajectory of European Security with representatives of big business. This conference circuit includes the regular EU security research 'brokerage events' (at which Commission officials, national Research Councils and would-be grant recipients discuss potential funding for the development of their projects), 'thinktank' events, 'roundtables', QUANGO (quasi-autonomous non-governmental organisations) forums, and overtly commercial hardware and software exhibitions.

[97] For a discussion of BONGOS, GONGOS, QUANGOS etc. in an EU context see Cutrin, D. (2003), 'Private Interest Representation or Civil Society Deliberation? A Contemporary Dilemma for European Union Governance', *Social & Legal Studies*, Vol. 12, No. 1, 55-75 (2003).

[98] SDA was formerly known as the 'New Defence Agenda'. Mr. Solana was speaking at the 'launch' of SDA, see: http://www.securitydefenceagenda.org/.

[99] See EUISS website http://www.iss.europa.eu/index.php?id=103

[100] See EHSA website: http://www.e-hsa.org/home_english.php.

[101] See HSE website: http://www.homelandsecurityeu.com/aboutus.asp. HSE is part of the GDS, a media group whose portfolio also include *Food Safety Europe*, *Next Generation Pharma Europe*, *HR Management EU*, *Financial Services Technology EU* and similar titles produced for the US market, see: http://www.gdsinternational.com/.

[102] See HSE website: http://www.homelandsecurityeu.com/index.asp.

PART III: FROM SECURITY RESEARCH TO SECURITY POLICY

Counter-terrorism is more than a response to acts of terrorism; it is an autonomous arena of supply that requires a demand to survive and succeed. But the demand for counter-terrorism and the protection it ostensibly supplies are not automatic; they must be created and sustained. The division of labour within the counter-terrorist arena means that like toothpaste, cereal and SUVs, different products require different sales strategies.

Lipschultz & Turcotte, 'The political economy of Threats and the Production of Fear' [103]

9 Towards a political economy of the ESRP

This report has explored the political development of the European Security Research Programme, from its conception in 2003 to its full implementation under the FP7 programme. What is striking are the lengths that the EU is going to establish a competitive Homeland Security industry in Europe, how closely it is working with industry to do this, and how little regard it has shown for the wider consequences of this project.

It would be over-simplistic, however, to suggest that the EU is simply an empty shell for the furthering of corporate interests. The development of the ESRP is the result of specific political, economic, social and cultural factors. In taking the political decision to foster a globally competitive homeland security industry, the EU member states have unleashed a complex set of competing actors and organisations. Transnational corporations are vying with one another in order to set the EU agenda for security research by 'selling' ideas to European Commission officials so as to maximise potential funding for their R&D activities, while the member states are effectively competing with one another to claw back funds from their contributions to the FP7 budget. The more competitive (they would say astute) states have established dedicated governmental and non-governmental agencies to help national actors compete for EU funds (this also helps explain the relative success of the larger EU member states as well as countries likes Ireland and Israel in securing EU security research contracts).

Within the framework of the ESRP, the member states have also used their political influence to ensure that their national corporate interests are represented in key positions on unaccountable bodies like ESRIF and ESRAB. As one anonymous ESRP official put it: "If the Italian government thinks Finmeccanica's interests and Italy's national interest equate to the same thing, there is not much that the European Commission can do about it".[104] This proposition also helps explain the prominent role in the ESRP played by Thales (France) and EADS (the European Aeronautic Defence and Space Company, a French-German-Spanish interest) and the Dutch and Swedish defence research agencies.

The contemporary EU is, then, very much one created in the image of the EU's most powerful members, where the national interest and the commercial interest, at least where 'investment' is concerned, are usually one and the same thing. As Iraklis Oikonomou has explained, organised labour at the European level has been equally supportive of EU policies favouring the militarisation of the EU, the defence industry being a large employer that has long used the prospect of job losses to justify its continued support from the state.[105]

Fuelled by a new politics of fear and insecurity, the corporate interest in selling security technology and the national security interest in buying security technology has converged at the EU level. The trappings of democratic government, however, remain firmly rooted in the nation-state. The remainder of this report examines the vision of the new EU security-industrial complex, its possible impact on state policy and practice, and the implications for civil liberties and social justice.

[103] Lipschultz, R. D. & Turcotte, H. (2005) 'Duct Tape or Plastic? The political economy of Threats and the Production of Fear' in Hartman, B., Subramaniam, B. & Zerner, C. (2005) (eds) *Making Threats: biofears and environmental anxieties*. New York: Rowman & Littlefield (page 26).

[104] Source: off-the-record conversation with the author.

[105] Oikonomou, I. (2009), 'Kopernikus/GMES and the militarisation of EU space policy', paper presented at *Militarism: Political Economy, Security, Theory* conference University of Sussex, on the 14th and 15th of May 2009.

We now have a larger budget for research, policy and applications at European level. Research should not be done 'per se' but should be linked to needs and effectively deployed to the benefit of citizens and of the economy.

Security is no longer a monopoly that belongs to public administrations, but a common good, for which responsibility and implementation should be shared by public and private bodies.

Franco Frattini, former EU Commissioner for Justice and Home Affairs [106]

10 Full spectrum dominance: the mission explained

The significance of the European Security Research programme can only be appreciated in the wider context of EU security policy. The following sections explore the influence of the ESRP on the security policy of the EU, and vice versa. It looks at what is being 'researched' (and sometimes procured), by whom, and to what end. The research also suggests a paradigm shift in the security strategy of the European Union (EU), a shift characterized by the pursuit of the US military doctrine of 'Full Spectrum Dominance', a euphemism for control over all elements of the 'battlespace' using land, air, maritime, and space-based assets.

The EU has not formally adopted a strategy of Full Spectrum Dominance. Rather, EU policies on a whole host of formerly distinct 'security' issues—including policing; counter-terrorism; critical infrastructure protection; border control; crisis management; external security; defence, maritime, and space policy—are converging around two interrelated objectives. The first is the widespread implementation of surveillance technologies and techniques to enhance security, law enforcement and defence capabilities in these core 'mission areas.' The second is the drive for 'interoperability,' or the integration of surveillance tools with other government information and communications systems so that they may be used for multiple tasks across the spectrum of law enforcement and security. 'Joined-up surveillance' for 'joined-up government' is another way of describing this trend.

The pursuit of a domestic policy of full spectrum dominance has particularly profound implications for civil liberties, the rule of law and other democratic traditions. Magnus Hörnqvist, a Swedish academic, has described the way in which the rule of law is being eclipsed by the 'logic of security'.[107] His hypothesis is that it is *security and not the law that is now the primary principle from which the use of physical force and other coercive measures can proceed.* Within this process "the law has been ruptured in two directions simultaneously: upwards, through the erasure of the line between crimes and acts of war, and downwards, through the erasure of the line between criminal offences and minor public order disturbances". In turn, "the law is made superfluous… other methods are required that correspond more closely to military logic: neutralising, knocking out and destroying the enemy".[108]

Border security is based not just upon the checking of persons crossing national and international borders by immigration officers, but sophisticated surveillance of the internal population (to identify and prevent the entry of so-called 'illegals') and the world beyond (for example in the Mediterranean or off the coasts of north and west Africa). The 'fights' against crime and terrorism are no longer centred solely on

[106] Frattini, F. (2007), 'Security by design', *Homeland Security Europe*, available at: http://www.homelandsecurityeu.com/currentissue/article.asp?art=271247&issue=219.

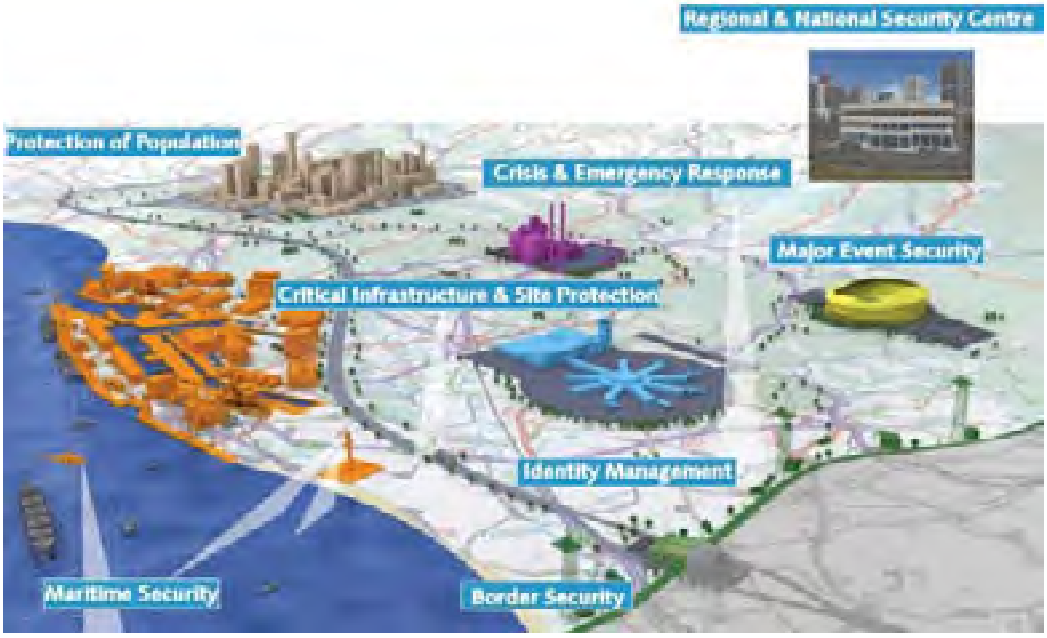
[107] Hörnqvist, M (2004) The Birth of Public Order Policy, *Race & Class*, Vol. 46, No. 1, pages 30-52.

[108] Hörnqvist, M (2004: page 35).

Flights of fancy? Military Full Spectrum Dominance (NATO style)

NATO UNCLASSIFIED

'Interopable security': Domestic Full Spectrum Dominance


Regional & National Security Centre
Protection of Population
Crisis & Emergency Response
Major Event Security
Critical Infrastructure & Site Protection
Identity Management
Maritime Security
Border Security

police investigations into criminal acts, but rather seek to identify, disrupt and destroy criminal/terrorist networks and their supporters. Myriad law enforcement agencies are now engaged in surveillance of entire populations in an attempt to identify suspicious persons before they commit criminal or terrorist acts (or even manage to enter the territory of the 'free world'). The protection of critical infrastructure and the policing of so-called 'major/mega-events' (sporting contests, summit gatherings, protests etc.) is increasingly oriented around military technology, high-tech surveillance and security checkpoints.

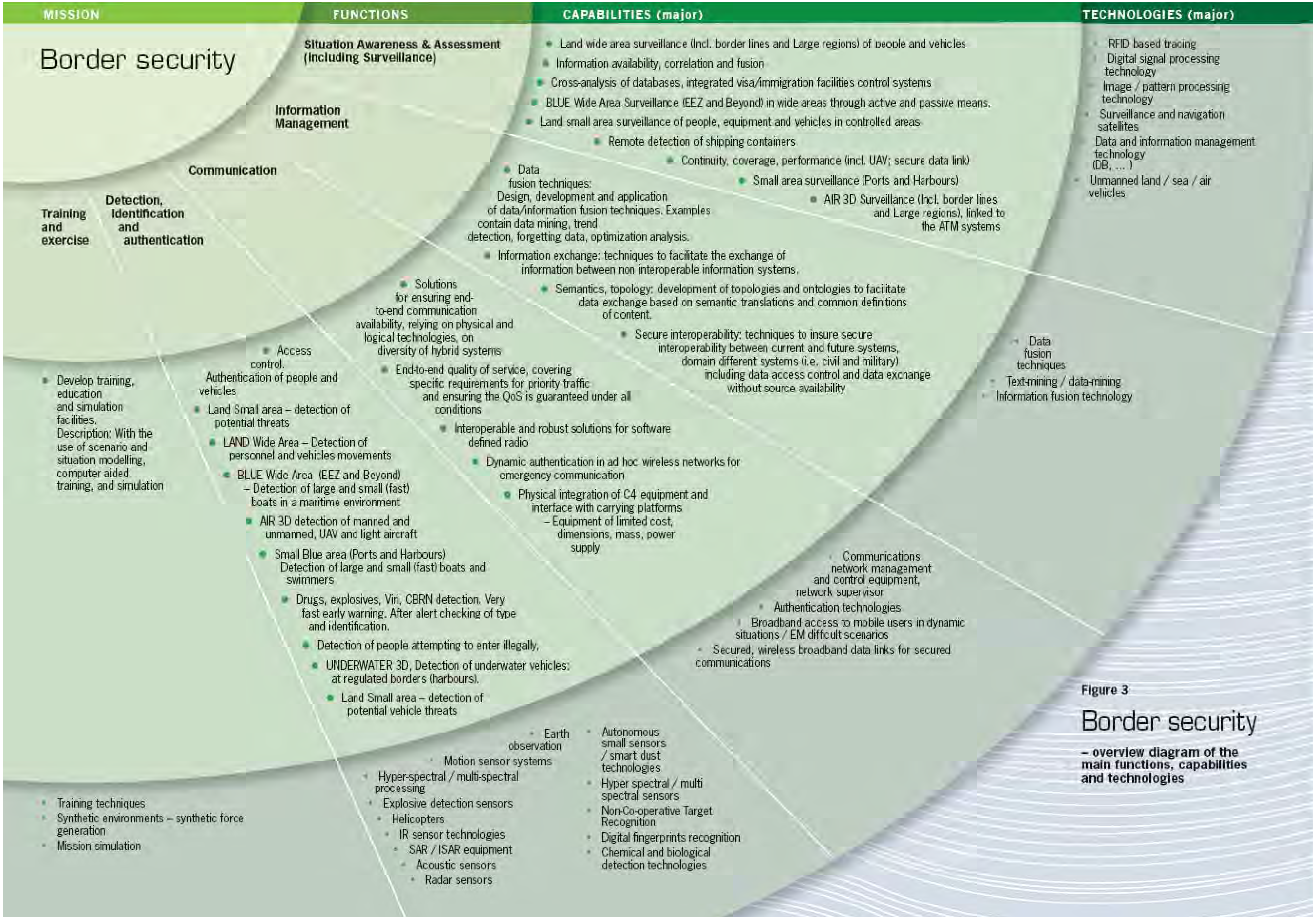
As noted earlier, the European Security Research Programme is comprised of five key 'mission areas': 'border security', 'protection against terrorism *and organised crime*', 'critical infrastructure protection', 'restoring security in case of crisis' and 'integration, connectivity and interoperability'. For each of these apparently distinct 'mission areas', it is observed that the same response was proposed: maximise the use of security technology; use risk assessment and modelling to predict (and mitigate) human behaviour; ensure rapid 'incident response'; then intervene to neutralise the threat, automatically where possible. ESRAB also recommended the development of fully interoperable security systems so that technological applications being used for one 'mission' can easily be used for all the others. The diagrams taken from the ESRAB report and reproduced on pages 32, 42, 57 and 62 help explain exactly what is proposed.

Promoted by the private sector, the Full Spectrum Dominance model is also grounded in a number of distinct trends in the defence and security policies of the most powerful western states. The first is the so-called Revolution in Military Affairs and the pursuit of high-tech weapons systems geared toward military superiority. The 'shock-and-awe' tactics of Gulf War II and 'SeaPower21', the US naval strategy of 2005 are also manifestations of the Full Spectrum Dominance paradigm. The same is true of the claim that "Dominating the information spectrum is as critical to conflict now as occupying the land or controlling the air has been in the past".[109]

The second key trend is the integration of security and defence functions and the erasure of the 'traditional' boundaries between internal policing (traditionally a civilian enterprise) and external security and defence (traditionally the preserve of the military and the intelligence services). In the EU this is a longer-term process that is the result of both European integration in this field (insofar as it has created common internal and external security zones) and the overlapping mandates, powers and equipment given to state agencies in the 21st century. For example, criminal justice systems uses GPS satellite-tracking to monitor 'offenders'; the military now assists in the control of borders and the protection of airports; police are using unmanned aerial vehicles for domestic surveillance; the wars on drugs, terror and failed states are converging, and a new international armada to combat piracy has been hastily assembled off the coast of Africa. Meanwhile, G8 summits take place in Baghdad-style 'green zones', while protesters outside are tightly controlled by paramilitary style 'peacekeeping'; international 'e-borders' now monitor journeys across continents, from start to finish; and the surveillance of telecommunications is becoming an international privilege rather than a judicially controlled police power. Far from the 'open society' briefly promised by the end of the Cold War, movement within and between states, as well as within the cyber-world, is increasingly policed and controlled.

The third key trend is the development of international frameworks for 'global policing' based on western foreign policy objectives and an expansive definition of 'national security', which is now seen to encompass everything from health pandemics to piracy on the high seas to the effects of climate change (changing definitions of national security are discussed in section 24, page 72). A fourth trend is the development and consolidation of the security-industrial complex (described above) and the novel idea that security is now "a common good, for which responsibility and implementation should be shared by public and private bodies".

[109] Citation from Wright, S. (2006) 'Report. Sub-lethal vision: varieties of military surveillance technology', *Surveillance & Society*, 4(1/2) , available at: http://www.surveillance-and-society.org/Articles4(1)/sublethal.pdf.



MISSION

FUNCTIONS

CAPABILITIES (major)

TECHNOLOGIES (major)

Border security

Situation Awareness & Assessment (including Surveillance)

- Land wide area surveillance (Incl. border lines and Large regions) of people and vehicles
- Information availability, correlation and fusion
- Cross-analysis of databases, integrated visa/immigration facilities control systems
- BLUE Wide Area Surveillance (EEZ and Beyond) in wide areas through active and passive means.
- Land small area surveillance of people, equipment and vehicles in controlled areas
- Remote detection of shipping containers
- Continuity, coverage, performance (incl. UAV; secure data link)
- Small area surveillance (Ports and Harbours)
- AIR 3D Surveillance (Incl. border lines and Large regions), linked to the ATM systems

- RFID based tracing
- Digital signal processing technology
- Image / pattern processing technology
- Surveillance and navigation satellites
- Data and information management technology (DB, ...)
- Unmanned land / sea / air vehicles

Information Management

- Data fusion techniques: Design, development and application of data/information fusion techniques. Examples contain data mining, trend detection, forgetting data, optimization analysis.
- Information exchange: techniques to facilitate the exchange of information between non interoperable information systems.
- Semantics, topology: development of topologies and ontologies to facilitate data exchange based on semantic translations and common definitions of content.
- Secure interoperability: techniques to insure secure interoperability between current and future systems, domain different systems (i.e. civil and military) including data access control and data exchange without source availability

- Data fusion techniques
- Text-mining / data-mining
- Information fusion technology

Communication

- Solutions for ensuring end-to-end communication availability, relying on physical and logical technologies, on diversity of hybrid systems
- End-to-end quality of service, covering specific requirements for priority traffic and ensuring the QoS is guaranteed under all conditions
- Interoperable and robust solutions for software defined radio
- Dynamic authentication in ad hoc wireless networks for emergency communication
- Physical integration of C4 equipment and interface with carrying platforms – Equipment of limited cost, dimensions, mass, power supply

- Communications network management and control equipment, network supervisor
- Authentication technologies
- Broadband access to mobile users in dynamic situations / EM difficult scenarios
- Secured, wireless broadband data links for secured communications

Detection, Identification and authentication

- Access control. Authentication of people and vehicles
- Land Small area – detection of potential threats
- LAND Wide Area – Detection of personnel and vehicles movements
- BLUE Wide Area (EEZ and Beyond) – Detection of large and small (fast) boats in a maritime environment
- AIR 3D detection of manned and unmanned, UAV and light aircraft
- Small Blue area (Ports and Harbours) Detection of large and small (fast) boats and swimmers
- Drugs, explosives, Viri, CBRN detection. Very fast early warning. After alert checking of type and identification.
- Detection of people attempting to enter illegally,
- UNDERWATER 3D, Detection of underwater vehicles: at regulated borders (harbours).
- Land Small area – detection of potential vehicle threats

- Earth observation
- Motion sensor systems
- Hyper-spectral / multi-spectral processing
- Explosive detection sensors
- Helicopters
- IR sensor technologies
- SAR / ISAR equipment
- Acoustic sensors
- Radar sensors

- Autonomous small sensors / smart dust technologies
- Hyper spectral / multi spectral sensors
- Non-Co-operative Target Recognition
- Digital fingerprints recognition
- Chemical and biological detection technologies

Training and exercise

- Develop training, education and simulation facilities. Description: With the use of scenario and situation modelling, computer aided training, and simulation

- Training techniques
- Synthetic environments – synthetic force generation
- Mission simulation

Figure 3

Border security

– overview diagram of the main functions, capabilities and technologies

PART IV: FULL SPECTRUM DOMINANCE IN THE BORDERLANDS

> *In addition to its traditional geophysical characteristics, the border has taken on virtual, de-territorialized attributes as well. Castles, walled cities, and extensive border battlements have been replaced by gated communities, expansive border zones, and management by "remote control." The contemporary border is constituted as much by data-flows, artificial zones and spaces of enclosure that seep into the city and the neighbourhood, as by older state and geographic boundaries.*
>
> Editorial on 'Smart Borders', *Surveillance & Society* [110]

11 Points of departure: from migration controls to social controls

The EU's policy on border control dates back a quarter of a century to early attempts by the then EEC member states to control migration, and in particular to prevent 'illegal' or unauthorised migration, through *ad hoc* intergovernmental cooperation. These aspirations were subsequently embodied in the 1990 Schengen Convention and a raft of subsequent measures. Ever-stricter attempts to control migration and the securitisation of migration policy itself have fundamentally transformed the nature of border controls. From checkpoints between countries and at ports of origin, these controls now represent mere nodes in a sprawling law enforcement apparatus that has spread simultaneously *inwards* and *outwards*.

The EU's border controls have spread outwards as the EU has refined its attempt to prevent the arrival and entry of 'illegal migrants'. Since the member states often make no meaningful distinction in practice, this inevitably includes refugees fleeing war and poverty. This has allowed European states to claim to continue to uphold the Geneva Conventions on the protection of refugees and the right to asylum, while simultaneously denying increasing numbers of would--be refugees access to EU territory.[111]

This process began in the 1990s with the creation of an immigration 'buffer zone' Central and Eastern European countries that wished to join the EU. Their accession shifted the buffer zone to an EU 'neighbourhood' that stretches from West Africa to Central Asia.[112] This is part of the EU's 'global approach' to migration, which centres on countries of origin and transit of migrants bound for Europe. The policy framework includes funding for immigration controls (so-called 'migration management') in cooperating states, a preference for 'regional protection' (i.e. outside Europe) of refugees headed for Europe, and the deployment of EU 'border management' agencies to third countries.

Having fortified many of the traditional entry points to Europe, the focus of the 'war on migration' has shifted to the islands of the Mediterranean and the coastlines of Africa and the Middle East. For FRONTEX, the newly created EU border management agency, this 'southern maritime frontier' is the 'first line of defence' of 'Europe's borders'.[113] Since 2003 FRONTEX has coordinated a host of joint police and naval missions to combat 'illegal' immigration by sea and is now in the process of setting--up a permanent European Patrols Network for the Mediterranean and a corps of Rapid Border Intervention Teams (RABITs) for deployment to 'illegal immigration hotspots'.[114]

[110] Amoore, L, Marmura S. & Salter, M.B. (2008) 'Smart Borders and Mobilities: Spaces, Zones, Enclosures', *Surveillance & Society*, vol 5 no 2, available at: http://www.surveillance-and-society.org/journalv5i2.html.

[111] For example, in July 2009, the UNHCR stated that it would not participate in the new Greek asylum procedure unless "structural changes" were made. See UNHCR press release, 17 July 2009: http://www.statewatch.org/news/2009/jul/greece-unhcr.prel.pdf.

[112] See *European Neighbourhood Policy*, European Commission website: http://ec.europa.eu/world/enp/index_en.htm.

[113] FRONTEX is an independent body tasked with coordinating the 'management' of the EU's external borders. It also has a mandate to address illegal immigration within the territory of the EU, and plays an increasing role in the implementation of the EU's expulsion strategy. FRONTEX is supervised by a management board comprised of the member states' 'border chiefs'. The agency currently has a staff of 200 with operational HQ in Warsaw, Poland. See FRONTEX website: http://www.frontex.europa.eu/.

[114] See *Joint Operations*, FRONTEX website: http://www.frontex.europa.eu/examples_of_accomplished_operati/. Note that while FRONTEX 'officially' became operational in 2006, joint operations have taken place under the auspices of the agency since 2003.

This militarised approach to immigration control is part of a broader EU maritime security and defence strategy. In 2005, following the lead of the USA's 'SeaPower21' strategy, the Chiefs of European Navies (CHENS) launched a 20-year 'Vision for the Future Role of European Maritime Forces' to meet the demands of the European Security Strategy (2003) and enhanced NATO Maritime Joint Operations.[115]

The rationale behind the CHENS strategy is that the sea: "has already been used for terror attacks by boats armed with rockets and small arms" and "for logistic support to terrorism". The sea is also a potential conduit for CBRN material and "criminal activity including narcotics, human trafficking and piracy", all of which is "increasing in sophistication and volume".

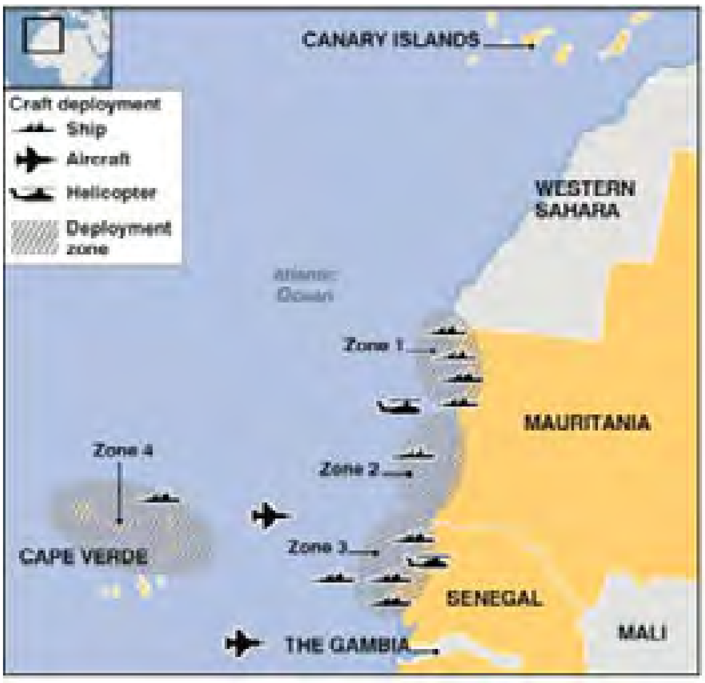
In November 2008, the EU agreed to launch its first naval mission under the auspices of the CFSP, led by the UK, to combat piracy and armed robbery off the Somali coast. It joins NATO, US, Japanese, Chinese, Saudi Arabian and numerous other forces in the Indian Ocean, contributing to a confusing array of national and international missions in the open waters.[116]

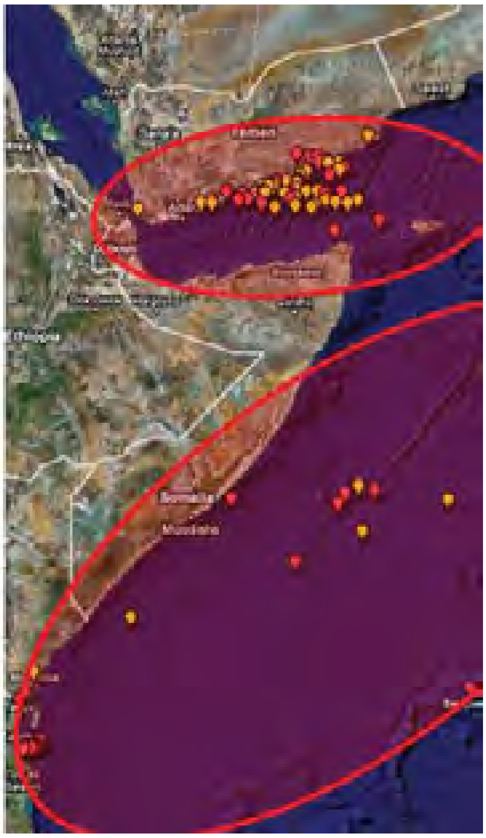
Homeland Security Europe

"Maritime terrorism has emerged as a formidable threat in the world, targeting both naval and civilian vessels. In Europe the threat is compounded by the use of maritime vessels and shipping lanes by criminals, who are often in league with terrorists. With the possibility that weapons of mass destruction could be used as a terrorist weapon, efforts to pre-empt such attacks which could cause mass civilian casualties has become a top European Priority, making it necessary for the alliance to expand its maritime frontier. Also with arrest of several Morrocans [sic] suspected of involvement with the Madrid blasts, people are asking how safe Europe's frontiers are". [119]

The EU's border controls are also spreading *inwards*, as large scale IT systems are developed to detect 'illegal' immigrants, to exchange information on persons to be refused entry and facilitate security checks on travellers. This includes the introduction of biometric ID systems, the recording of entry, exit and transit through European countries, and the development of automated targeting and risk-profiling systems.

FRONTEX operations in East Africa [117]





Reported instances of piracy off the Somali and Yemeni coastlines [118]

[115] CHENS (2005) *A Vision for the Future of EU Maritime Forces by the Chiefs' of European Navies*, available at: http://www.chens.eu/products/ENV%20 2025.pdf. See also 'European Interagency Strategy for Maritime Security Operations – A paper Supported by the Chief's of European Navies', unreferenced document available at: http://www.chens.eu/products/MSO%20Strategy.pdf.

[116] See: *Operation Atalanta*, EU Council website: http://www.consilium.europa.eu/uedocs/cmsUpload/081113%20Factsheet%20EU%20NAVFOR%20-%20 version%201_EN.pdf.

[117] Source: FRONTEX graphics, BBC website: http://news.bbc.co.uk/1/hi/world/europe/5331896.stm.

[118] Source: EU Council website: http://consilium.europa.eu/cms3_fo/showPage.asp?id=1518&lang=en.

[119] 'Maritime & Port Security', *Homeland Security Europe* magazine: http://www.homelandsecurityeu.com/coverage_ms.asp. The same text appears in 'Maritime terrorism: a new challenge for NATO', *Institute for the Analysis of Global Security*, see: http://www.iags.org/n0124051.htm.

Nanne Onland, Director of *Dartagnan BV*, vendor of immigration, border control systems and registered traveller programs, suggests that "ultimately the border authorities of the destination country will be able to tell the traveller before boarding the plane whether they are welcome or not. *The Border Police officer at the port of arrival will become the last line of defence rather than the first […] dealing with exceptions rather than checking travellers and granting them admission to the country on the spot*" (emphasis added). "In fact", argues Onland, "we could theoretically foresee that the vast majority of the travellers arriving at certain borders will be (pre) registered travellers and hence a 'friendly flow'". [120]

Crucially, the widespread and increasingly mandatory collection, analysis and exchange of highly personal datasets does not stop at the border. This new generation of 'e-borders' is being linked into existing law enforcement databases and government IT systems, providing a high-tech security blanket that will ultimately stretch from Europe's airports and land borders to illegal immigration 'snatch squads' and police on the streets equipped with hand-held fingerprint scanners.

While many lament the onset of the 'surveillance society', it is important to recognise that many of its most controversial systems – fingerprinting, ID cards, populations databases, 'terrorist' profiling, travel surveillance and so on – have been (and are still being) 'tested' on migrants and refugees or otherwise legitimised at the border.[121] Acquiescence to these controls and indifference to the suffering of migrants and refugees at the hands of 'Fortress Europe' has paved the way for their use in domestic security scenarios.

[120] Onland, N (2007) 'Registered traveller programs - a public and private partnership', *Homeland Security Europe*, available at: http://www.homelandsecurityeu.com/currentissue/printarticle.asp?art=271309).

[121] See further Fekete, L. (2009) *A Suitable Enemy: Racism, Migration and Islamophobia in Europe*. London: Pluto Press.

To carry out the necessary checks, the Cyprus National police Force is using an AFIS [Automatic Fingerprint Identification System] supplied by Motorola and mobile live-scan fingerprint readers at asylum centres and police stations throughout the country. The system provides the police and immigration authorities with an electronic link between the AFIS system and the EURODAC database [allowing] Cyprus to capture the fingerprints and facial images of individuals that have been stopped and found to be without valid visas or identification documents, or those that are claiming asylum. This information is transmitted to a central server at the national law enforcement headquarters in Nicosia and searched against its database... Today, around 150 crimes are solved each year using the Printak Biometric Identification Solution (BIS).

Police Information Technology Review, 2009 [122]

12 EUROSUR: the European Border Surveillance System

In February 2008, the European Commission produced a Communication (position paper) on the creation of a 'European Border Surveillance System' (EUROSUR) to 'support the Member States in reaching full *situational awareness* on the situation at their external borders and increase the *reaction capability* of their law enforcement authorities' (emphasis in original).[123]

EUROSUR aims primarily "to reduce the number of illegal immigrants who manage to enter the EU undetected and to increase internal security of the EU as a whole by contributing to the prevention of cross-border crime and to enhance search and rescue capacity". With surveillance technology at the heart of other areas of EU maritime policy, from the enforcement of fisheries regulations and the prevention of pollution at sea, to vessel and cargo tracking, ship safety and collision avoidance systems, the EU also cites a need for 'interoperability' across EU maritime, security and defence systems. According to the European Commission, the EUROSUR system will be developed in three phases: (i) interlinking and streamlining existing national surveillance systems, (ii) common tools and applications for border surveillance at EU level, and (iii) creating 'a common monitoring and information sharing environment for the EU maritime domain'.

The internal dimension of EUROSUR was set out in a separate Communication that includes plans for the facilitation of border crossing for what the Commission calls *bona fide* [i.e. non-suspicious] travellers, the creation of an EU entry-exit system, an Electronic System of Travel Authorisation (ESTA) to facilitate the entry of suspicious travellers, and "an efficient tool for identifying overstayers".[124] This 'tool' is very much like the one described on the previous page, and is to be created by fusing the second generation Schengen Information System (SIS II)[125] [the SIS links border checkpoints and police officers throughout the Schengen area to persons and items of interest to the authorities] with the EU Visa Information System (VIS), which will contain the fingerprints and personal data of all visa entrants, to a new entry-exit system which will record all movement into and out of the EU. [126] An 'alert' on the SIS – a *de facto* arrest warrant – will then be automatically issued for visa holders whose visas have expired and whose exit cannot be verified. The Biometric Matching System is being built by Sagem Défénsé Sécurité and Accenture. This will enable the fingerprints of travellers to be checked against SIS, VIS and EURODAC (the EU asylum applicants fingerprint database).

[122] 'Fingers on the pulse', Gary Mason, *Police Information Technology Review*, June/July 2009

[123] *Commission Communication on the creation of a European border surveillance system (EUROSUR)*, COM (2008) 68, 13 February 2008, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0069:FIN:EN:PDF.

[124] *Commission Communication on the next steps in border management in the European Union*, COM (2008) 68, 13 February 2008, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0069:FIN:EN:PDF.

[125] The development of SIS II has been beset by problems, including allegations of the mismanagement of the initial tender process against the Commission and, more recently, a lack of progress in the development of SIS II compatible systems within in the member states.

[126] For a week between 31 August and 6 September 2009, the EU member states were encouraged to record *everyone* crossing the external borders of the EU; the data is to be used to support a "legislative proposal on the creation of a system of electronic recording of entry and exit data" in 2010. This exercise applied to EU citizens and third-country nationals, suggesting that the planned EU entry-exit system will be much broader in scope than US VISIT, its Transatlantic counterpart, which does not record the movement of US citizens. Between the EU member states there are some 1,626 designated points of entry by air, sea and land, although they were permitted to limit this exercise "to the most important/busy border crossing points". See *Outcome of proceedings: Strategic Committee for Immigration, Frontiers and Asylum/Mixed Committee (EU-Iceland/Liechtenstein/Norway/ Switzerland)', on : 19-20 May 2009. Subject: Data collection exercise on entries and exits at the external borders for a short period of time*. EU Council document 10410/09, 8 June 2009.

Despite the obvious link between the EU's high-tech vision of an interoperable border surveillance system and the European Security Research Programme, the Commission's EUROSUR Communication makes no mention at all of the activities it is funding in this area. Nor is there any mention of the European Security Research and Innovation Forum (ESRIF), whose Working Group 3 deals specifically with 'integrated border management and maritime surveillance'.

Working Group 3 is led by FRONTEX; the rapporteur is the Italian defence giant Finmeccanica which, in 2007 announced a 'joint initiative' with Thales on 'maritime management' to promote multi-user systems and "standards to foster the development of synergies between various civil and military maritime sectors". WG3 is divided into four subgroups on 'regulated borders' and 'unregulated air, land and sea borders'. It has 80 members, 20 from the 'demand side' (governments and state agencies) and 60 from the 'supply side' (industry).[127]

EUROSUR and the European Security Research Programme

EUROSUR is backed by a plethora of security research projects. STABORSEC (Standards for Border Security Enhancement, PASR) consortium, led by Sagem Défénsé Sécurité, recommended no less than 20 detection, surveillance and biometric technologies for standardisation at the EU level.[128] The OPERAMAR project (FP7), on the interoperability of European and national maritime surveillance assets, will 'provide the foundations for pan-European Maritime Security Awareness'. OPERAMAR is led by Thales Underwater Systems in conjunction with Selex (a Finmeccanica company) and has a mandate to develop technical requirements, a strategic research roadmap, priority areas for additional security research, and "common requirements and operational procedures, as well as new interoperability standards, at the EU level, that should be adopted at national and local level". OPREMAR, a follow-up to the SOCBAH project,[129] is being tested for three scenarios: 'Mediterranean, Black Sea and Atlantic Ocean (Canary Islands)'. The WIMA2 project on Wide Maritime Area Airborne Surveillance (FP7), led by Thales Airborne Systems, argues that "You cannot control what you do not patrol", while EFFISEC is a €16 million project on Efficient Integrated Security Checkpoints for land border and port security that promises the "integration of a set of existing and complementary technologies (biometrics, e-documents, signal recognition and image analysis, trace and bulk detection of substances, etc.)".[130] It envisages "*massive deployment* in mid-term (2014-2020) at land/maritime border check points" (emphasis added).

Satellite surveillance for border control

The MARitime Security Service project (MARISS, PASR) expanded border surveillance into space by developing "satellite based surveillance and monitoring for enhanced operational maritime border control and maritime domain awareness". Supported by the European Space Agency, MARISS provided monitoring capabilities "for the detection of non-cooperative vessels and suspicious activity in open waters" to national and European government agencies including "police, border guards, coast guards, intelligence services and national navies as well as appropriate European and international agencies".[131] The MARISS consortium was led by Telespazio (a Finmeccanica-Thales joint venture) and included Thales Alenia Space, EADS Astrium, Qinetiq, SELEX-SI and Starlab.

Meanwhile, the LIMES project on 'Land and Sea Integrated Monitoring for European Security' (funded under the FP6 programme), also led by Telespazio, extended MARISS' scope to include land border and critical infrastructure surveillance using "Very High Resolution satellites… to enable critical 4D spatial analysis of updated reference data with the aim to assess risks, improve security and enhance preparedness".[132]

Autonomous border control systems

The obsession with high-tech border control systems can be seen most clearly in the €20 million TALOS project (FP7), which will develop and field test "a mobile, modular, scalable, autonomous and adaptive system for protecting European borders" using both aerial and ground unmanned vehicles, supervised by a command and control centre (the SECTRONIC, AMASS and UNCOSS projects (all FP7) are also based on the development of autonomous border control systems).[133] According to the TALOS project contract "the ground platforms will be both the watching stations

[127] Only 'around 15-20' of the 80 members of WG3 are said to be 'active' participants. These actors came together at a 2009 workshop organised by the European Commission in order to "prepare the R&D Demonstration Programme" for the "European-wide integrated border control system". Speakers included DG Enterprise, DG Justice Liberty and Security, the European Defence Agency, Finmeccanica, Thales, Telespazio, Telvent, Indra, Sagem and the European Organisation for Security (EOS). See 'Workshop to prepare the R&D Demonstration Programme: European-wide integrated border control system', 12 March 2009, European Commission website: http://ec.europa.eu/enterprise/security/events/border_control_workshop.htm.

[128] See STABORSEC project website: http://staborsec.jrc.it/.

[129] The SOCBAH project was led by Galileo Avionica (a Finmeccanica company) in conjunction with Thales Underwater Systems and Thales Research & Technology. Finmeccanica (Alenia Aeronautica) and Thales also participated in the BSUAV project on the use of unmanned aerial vehicles/drones for border surveillance in a consortium led by Dassault Aviation (PASR; on UAVs see section 19, page 55).

[130] EEFISEC is led by Sagem and features Thales, two Finmeccanica companies, Smiths and TNO. It will allow "systematic" security checks of "pedestrians, cars and buses with a high level of confidence", while "maintaining flow" at the border by "lowering the number of travellers, luggage and vehicles that have to go through in depth supplementary checks".

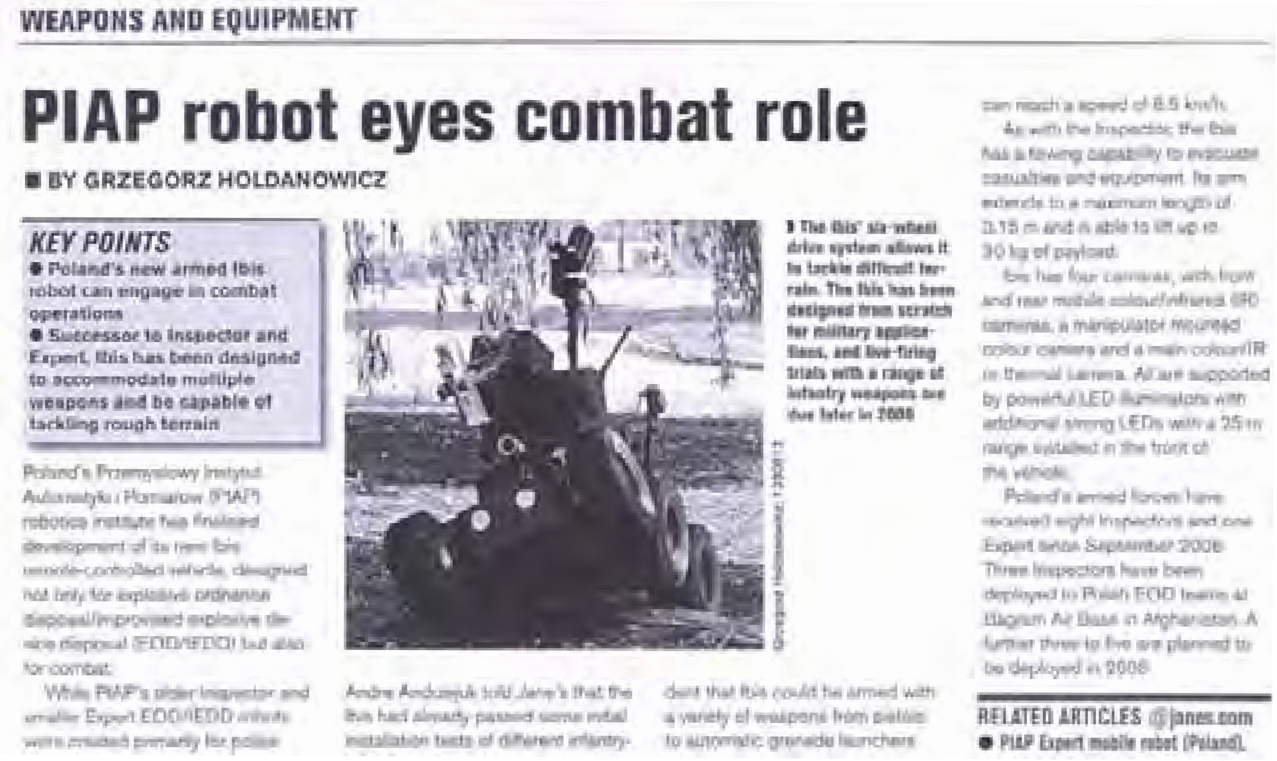
[131] MARISS services were tested "on a pre-operational basis in the following areas: South Spanish Coast; North Atlantic Channel; Western Atlantic; Southern Baltic Sea; Sicily Channel; Aegean Sea; North African Coastal area, Canary Islands, Portugal continental coast (and Gorringe fishing area), Azores area and Libyan coastline".

[132] LIMES test areas were "Eastern EU land borders, Spain and UK for Infrastructure Surveillance, a big event for Event Planning and a [Non-Proliferation Treaty] Monitoring Area". See LIMES project brochure, available at: http://www.fp6-limes.eu/uploads/docs/Brochure_Limes.pdf.

[133] The SECTRONIC project is working on the 'observation and protection of critical maritime infrastructures; passenger and goods transport, energy supply, and port infrastructures'. It will establish 'control centres' equipped with "all accessible means of observation (offshore, onshore, air, space)… *able to protect the infrastructure by non-lethal means in the scenario of a security concerned situation*" (emphasis added). Participants in the SECTRONIC project include the NATO Undersea Research Centre. See SECTRONIC project website: http://www.sectronic.eu/. The AMASS project is to develop "autonomous, unmanned surveillance buoys with active and passive sensors" and "un-cooled thermal imagers" in coastal waters to detect and identify local threats to security. Another defence robotics specialist, ECA (France), is leading the UNCOSS project on an 'underwater coastal sea surveyor' system.

Backroom border control

The border guards of the future? PIAP's combat robot [134]



WEAPONS AND EQUIPMENT

PIAP robot eyes combat role

■ BY GRZEGORZ HOLDANOWICZ

KEY POINTS

- Poland's new armed Ibis robot can engage in combat operations
- Successor to Inspector and Expert, Ibis has been designed to accommodate multiple weapons and be capable of tackling rough terrain

Poland's Przemyslowy Instytut Automatyki i Pomiarow (PIAP) robotics institute has finalised development of its new Ibis remote-controlled vehicle, designed not only for explosive ordnance disposal/improvised explosive device disposal (EOD/IEDD) but also for combat.

While PIAP's older Inspector and smaller Expert EOD/IEDD robots were created primarily for police

André Andrzejuk told Jane's that the Ibis had already passed some initial installation tests of different infantry-

dent that Ibis could be armed with a variety of weapons from pistols to automatic grenade launchers

▶ The Ibis' six-wheel drive system allows it to tackle difficult terrain. The Ibis has been designed from scratch for military applications, and live-firing trials with a range of infantry weapons are due later in 2008

Grzegorz Holdanowicz / 2008 / 1

can reach a speed of 6.5 km/h.

As with the Inspector, the Ibis has a towing capability to evacuate casualties and equipment. Its arm extends to a maximum length of 3.15 m and is able to lift up to 30 kg of payload.

Ibis has four cameras, with front and rear mobile colour/infrared (IR) cameras, a manipulator mounted colour camera and a main colour/IR or thermal camera. All are supported by powerful LED illuminators with additional strong LEDs with a 25 m range installed in the front of the vehicle.

Poland's armed forces have received eight Inspectors and one Expert since September 2006. Three Inspectors have been deployed to Polish EOD teams at Bagram Air Base in Afghanistan. A further three to five are planned to be deployed in 2008.

RELATED ARTICLES @janes.com
- PIAP Expert mobile robot (Poland).

and the first reaction patrols, which will inform the Control and Command Centre and an intruder about her/his situation, *and will undertake the proper measures to stop the illegal action almost autonomously* with supervision of border guard officers (emphasis added). Participants in the TALOS consortium (FP7) include PIAP Security Engineering (the project coordinator, Poland), whose combat robot has just been awarded a silver medal at the 'EUREKA 2008'

[134] Source: Jane's International Defence Review, July 2009. Full article available on: http://www.antiterrorism.com.pl/aboutus_articles_01.php.

show in Brussels,[135] and the defence giant Israel Aircraft Industries, whose 'operational solutions ensure that you detect, locate and target terrorists, smugglers, illegal immigrants and other threats to public welfare, swiftly and accurately, 24 hours a day, even in bad weather and low visibility conditions'.[136] It is understood that the original bid to the European Commission promised to equip the border control robots with less lethal 'directed energy' weapons (see further page 69), but that this was removed because of ethical concerns.

As Steve Wright has pointed out in respect to the use of combat robots, "it's one thing to say they save the President from sending another letter of regret to the parents of human soldiers killed in action: but who is going to take a robot to tribunal for violating human rights?" [137]

Designers of the integrated EU border surveillance system aspire to the standards set by the 'SIVE' surveillance system (*Sistema Integrado de Vigilancia Exterior*/ Integrated External Surveillance System) which covers the Strait of Gibraltar, the closest point between Europe and Africa, and stretches along 115 kilometres of Spanish coastline.[138] SIVE is capable of detecting and tracking any vessel crossing the Strait, including the tiny 'zodiacs' into which people once crammed in the hope of reaching mainland Europe, down to 'targets' of just one metre squared. On the African side, the Spanish enclave of Ceuta is sealed off by 9.7 kilometres of three-metre high, barbed-wire topped metal fencing.[139]

In representations to the EU, the Director of Indra's Security Systems Division describes SIVE as "A pioneer maritime border surveillance system" and presents the system as something of a victim of its own success.[140] The 'threat', as Indra puts it, has evolved; the departure points have spread east along the coast of Morocco to Algeria, and to the south and west as far as Mauritania and Senegal; while the relatively unguarded Canary and Balearic Isles are among the new destinations. The Spanish authorities have already introduced satellite surveillance, using images provided from the Ikonosos satellite in combination with UAVs and mobile sensor equipment, all of which has been tested for 'full integration' into the SIVE system. The EU has also funded an 'interoperable' communications system (the 'Seahorse' programme), linking the Spanish and Portuguese authorities initially with their counterparts in Mauritania, Senegal and Cape Verde with the aim of extending this to more EU and African states.[141]

Indra and Skysoft are part of the GLOBE consortium funded under the ESRP/FP7 and led by Telvent, which claims rather grandly to lead the European Union's Border Management Project. It certainly has ambitious plans to "fight against illegal immigration from all sources" through "preventive, control and integration initiatives involving immigrants and entails the new concept of the extended border, which includes country of origin, transit area, regulated and unregulated border crossings, and the country of the destination itself".[142]

A plethora of further maritime surveillance initiatives, including actions of the EU Maritime Policy Task Force,[143] the EU Joint Research Centre,[144] the European Defence Agency,[145] and FRONTEX,[146] are taking place outside of the framework of the ESRP.[147]

[135] See PIAP website: http://www.antiterrorism.eu/news026.php.

[136] See Israel Aircraft Industries website: http://www.iai.co.il/Default.aspx?FolderID=16130&lang=EN.

[137] Wright, S. (2006) 'Report. Sub-lethal vision: varieties of military surveillance technology', *Surveillance & Society*, 4(1/2) (page 146), available at: http://www.surveillance-and-society.org/Articles4(1)/sublethal.pdf.

[138] See *Sistema Integrado de Vigilancia Exterior*, Guardia Civil website: http://www.guardiacivil.org/prensa/actividades/sive03/index.jsp.

[139] After a series of desperate attempts by people to storm the fence in September 2005, Spain and Morocco sent troops to Cueta (and Melilla, a second Spanish enclave) and at least four people were shot dead. One year later Amnesty International reported 'a climate of impunity' over the continuing 'killings of migrants and asylum-seekers trying to cross the border, the use of excessive force by law enforcement officials, collective expulsions, and violations of the principle of non-refoulement'. See 'Spain and Morocco: Failure to protect the rights of migrants - one year on', *Amnesty International Spain*, AI Index: EUR 41/009/2006, October 2006.

[140] 'SIVE: a pioneer System for Border Surveillance. What is beyond?', presentation by Perez Pujazón (Indra) to European Commission workshop, available at: http://ec.europa.eu/enterprise/security/doc/border_control_workshop/n_jm_perez_pujazon.pdf.

[141] Seahorse was established as a cooperation program between Spain, Portugal and several African countries and funded under the EU's AENEAS 'migration management' programme.

[142] See TELVENT press release, 22 April 2008: http://www.reuters.com/article/pressRelease/idUS121430+22-Apr-2008+PNW20080422. The aim of the GLOBE project is to develop "the full scope of an integrated border management system, moving throughout the four main layers of border control (Country of origin, transit areas, regulated and unregulated border lines and internal territory)". Telvent is also leading the INTEGRA 'migration management' project, funded by Spain's Ministry of Science and Innovation, on the development of an "integrated system for managing migratory movements from country of origin to country of destination, closing borders to illegal people and irregular traffic without disrupting regular activity occurring within the realm of legality and regulation", see TELVENT press release, 12 September 2008, http://biz.yahoo.com/pz/080912/150240.html.

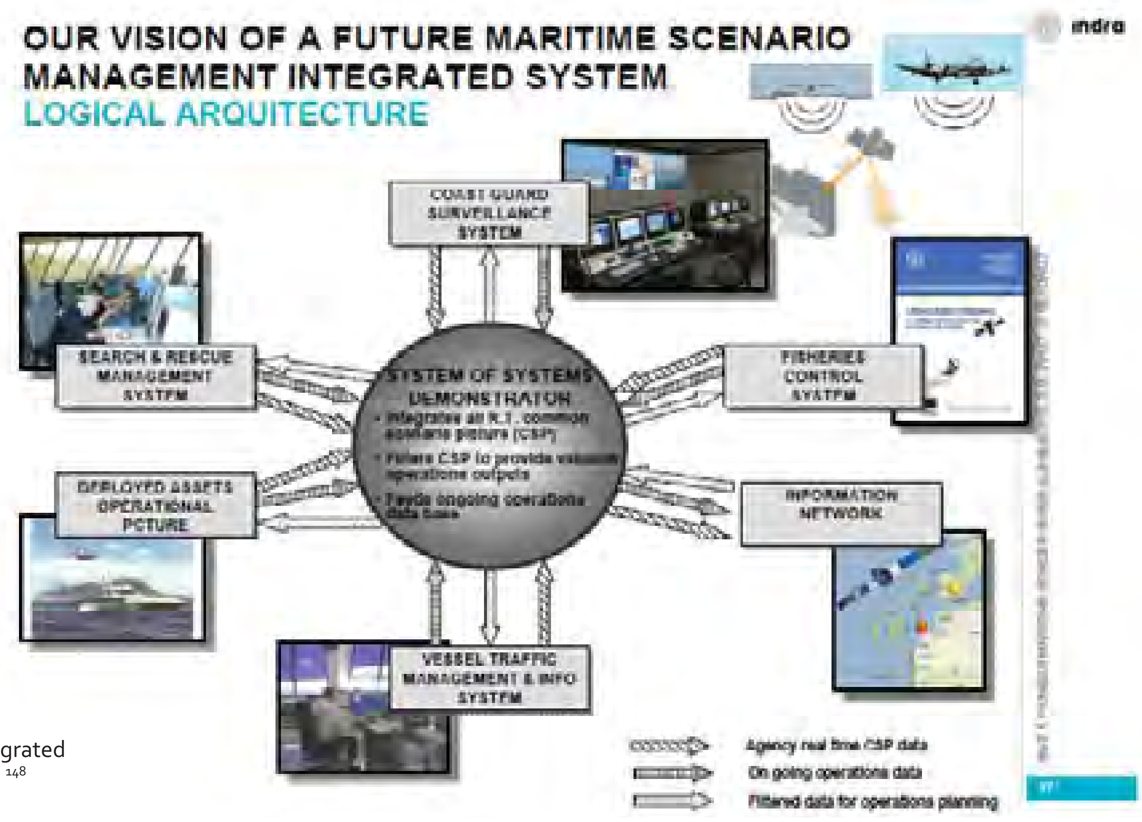
[143] The Maritime Policy Task Force was established to ensure a 'cross-pillar', harmonised approach to maritime surveillance and the actions of policy-makers across the EU's spheres of competence.

[144] The JRC's MASURE Action will provide additional R&D support for ship detection and the use of imaging satellites for maritime surveillance; data sharing policies and practices; new tools for maritime surveillance; and the monitoring of maritime pollution (in conjunction with the European Group of Experts on satellite Monitoring of sea-based Pollution (EGEMP)), see 'Maritime surveillance at JRC: MASURE action'. Presentation by Guido Ferraro, Harm Greidanus, June 2007, available at: https://maritimeaffairs.jrc.ec.europa.eu/c/document_library/get_file?p_l_id=9003&folderId=9015&name=DLFE-419.ppt.

[145] The EDA has contracted Saab Systems in a consortium with FOI (the Swedish Defence Research Agency) to produce an 'architecture study' for a Maritime Surveillance Network. The consortium will also examine the political and legal obstacles to the implementation of such a system. Working groups on Maritime Surveillance Networking, Future Unmanned Arial Systems, Surveillance of Small and Difficult Maritime Objects and Maritime Mine CounterMeasures have also been established within the EDA.

[146] A communications network between the national coordination centres for maritime surveillance and FRONTEX, the EU Border Management Agency, is being established as part of the EUROSUR infrastructure.

[147] See also the CONTRAFFIC project, on technology developed by the JRC and the European Anti-Fraud Office (OLAF) to automatically gather and analyze data on global maritime container movements to enable the identification of potentially suspicious consignments; the ROTIS II project (FP6) on Remotely Operated Tanker Inspection System II (ROTIS II); and the FREESUBNET project, a Marie Curie Research Training Network that aims "to provide a European-wide excellence in quality training to young and experienced researchers in the emerging field of Cooperative Autonomous Intervention Underwater Vehicles (AUVs) which are steadily becoming the tool of choice to carry out missions at sea without tight human supervision"'.



OUR VISION OF A FUTURE MARITIME SCENARIO MANAGEMENT INTEGRATED SYSTEM

LOGICAL ARQUITECTURE

COAST GUARD SURVEILLANCE SYSTEM

SEARCH & RESCUE MANAGEMENT SYSTEM

FISHERIES CONTROL SYSTEM

DEPLOYED ASSETS OPERATIONAL PICTURE

INFORMATION NETWORK

VESSEL TRAFFIC MANAGEMENT & INFO SYSTEM

SYSTEM OF SYSTEMS DEMONSTRATOR

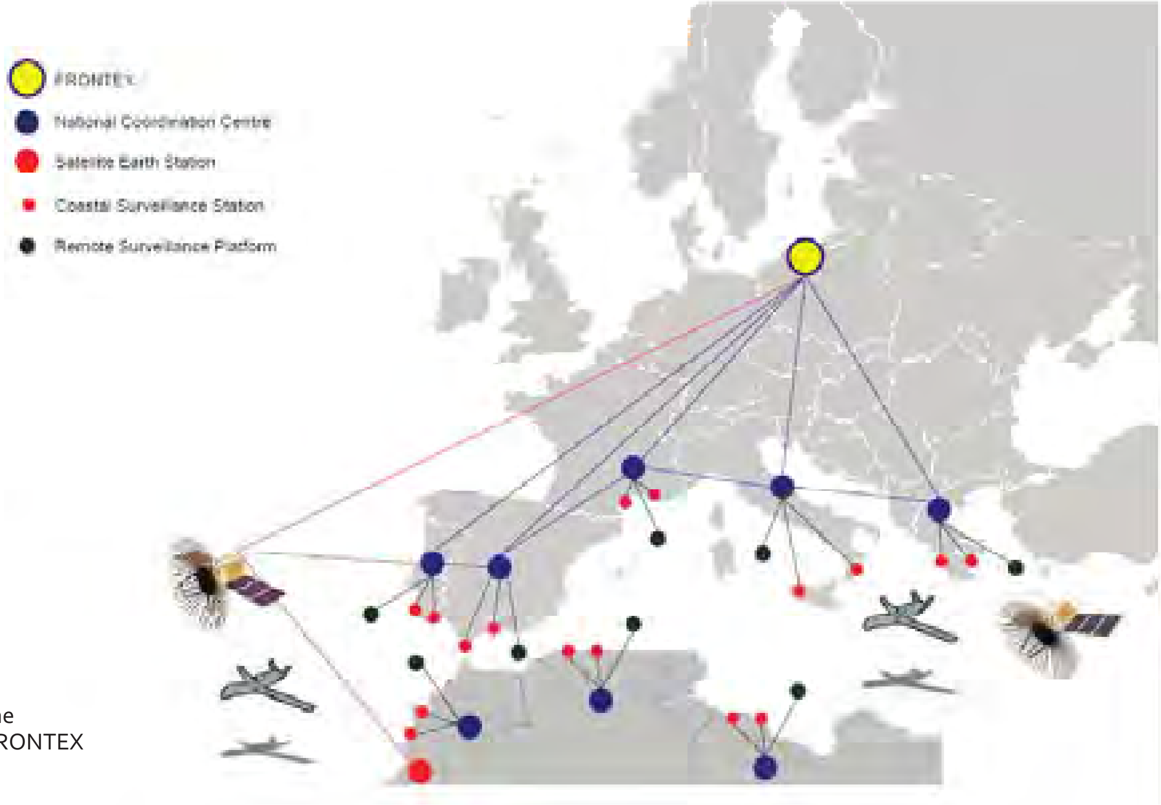
- Integrates all R.T. common situational picture (CSP)
- Filters CSP to provide valuable operations outputs
- Feeds ongoing operations data base

Agency real time CSP data

On going operations data

Filtered data for operations planning

Indra's vision for integrated border management [148]


FRONTEX
National Coordination Centre
Satellite Earth Station
Coastal Surveillance Station
Remote Surveillance Platform

From Warsaw to the Western Sahara: FRONTEX & EUROSUR [149]

[148] Source: 'SIVE: a pioneer System for Border Surveillance. What is beyond?', presentation by Perez Pujazón (Indra) to European Commission workshop, available at: http://ec.europa.eu/enterprise/security/doc/border_control_workshop/n_jm_perez_pujazon.pdf.

[149] Source: 'GLOBE: Phase 1 of the Demonstration Project for the Integrated Border Management System', presentation by Víctor Luaces (Telvent) to European Commission workshop, available at: http://ec.europa.eu/enterprise/security/doc/border_control_workshop/i_victor_luaces.pdf.

Saudi Arabia has awarded a contract to EADS Defense & Security as prime contractor for a full national border surveillance program after an international competition lasting many years, the European company said July 1 in a statement.

Under the contract, EADS will install during the next five years surveillance equipment over some 9,000 kilometers of borders, including mountains, deserts and coastline, to provide operational awareness, the company said. The deal is the largest contract ever put up to international competition as a full solution, the company said.

Industry estimates put the deal at about 1.5 billion to 1.6 billion euros ($2.1 billion to $2.3 billion).

"The solution will ensure border coverage is visible and managed at the sector level, whilst simultaneously providing situational awareness at the regional and national level," the company said.

Defence News, 1 July 2009 [150]

Boeing has won a US government contract to develop security equipment for monitoring the 7,500 miles of borders the US has with Mexico and Canada. [...]

Industry experts estimate the three-year Department of Homeland Security contract is worth $2.1bn (£1.1bn) to Boeing. [...]

The Boeing project involves partnerships with companies including Unisys.

It will include tracking sensors and communications equipment allowing border patrol staff to keep a closer watch on the borders.

The system will work together with cameras, developed by an Israeli company, which can spot people from 14 kilometres away.

BBC, 21 September 2006 [151]

13 R&D for global apartheid?

According to the worst scenarios, one in seven people on earth today could be forced to leave their home over the next 50 years as the effects of climate change worsen an already serious migration crisis.[152] As things stand, climate refugees will require a visa they have no chance of obtaining. As Zygmunt Bauman has noted, it is an extremely troubling paradox in this age of globalisation and mass migration that while travelling for profit is encouraged, travelling for survival is condemned.[153] Regardless of whether or not the world is able to reduce the emission of greenhouse gasses, and regardless of the extent to which the climate actually changes in the 21st century, 'enhanced border controls' now represent the lowest common denominator of European integration and global insecurity; the one thing that all states and governments deem necessary is to combat not just unauthorised immigration, but threats of every kind. Given that border controls are already undergoing rapid militarisation, what will the world's borderlands look like ten, twenty, or fifty years from now?

The fall of the Berlin Wall in 1990 briefly threatened to confine separation barriers and physical border to the past, but in the 21st century Brunei, China, Israel, Kazakhstan, Iraq, India, Iran, Israel, Russia, Saudi Arabia, Turkmenistan, the UAE and Uzbekistan have all built, or started building, new and highly militarised borders and barriers of one kind or another.[154] So too have the EU and the USA. Joseph Nevins and other vociferous critics of contemporary border controls have adopted the term 'global apartheid' to capture the distinctive role of immigration controls in maintaining race and class disparities across the world.[155] If the world's richest and most powerful countries all erect these kinds of barriers to keep out or otherwise control the planet's poorest and least powerful inhabitants, how else can such a system be described? The EU may have free movement for its citizens – subject to the kinds of checks described in this report – but at what cost?

Frances Webber has observed that "The number of deaths at sea ought to have reduced dramatically as a result of such intensive surveillance of sea traffic by the EU border patrols, the armed forces of Europe and of the southern Mediterranean. But the numbers drowned, or listed as 'missing', continue to rise, despite – or in some cases because of – surveillance and interception".[156] With companies like Boeing and EADS winning highly lucrative contracts in countries like the USA and Saudi Arabia, the idea that the EU needs to subsidise growth in this area seems exaggerated to say the least. The R&D spend seems designed instead to meet the EU's own policy objectives. Since 1993, the anti-racist organisation UNITED has maintained a list of *documented* deaths at the hands of 'Fortress Europe'.[157] It currently stands at 13,250 (the actual number of deaths is inevitably much higher). If there is a role for the subsidy of R&D in this field, it should surely start with the principle of increasing safety at sea. Though as UNITED says, if 13,250 deaths doesn't prick Europe's conscience, what will?

[150] 'EADS Wins Saudi Border Surveillance Project', *Defence News*, 1 July 2009: http://www.defensenews.com/story.php?i=4166445&c=EUR.

[151] 'Boeing secures US border contract', *BBC*, 21 September 2006: http://news.bbc.co.uk/1/hi/business/5368266.stm. See also US Government Accountability Office (2008) *Secure Border Initiative: DHS Needs to Address Significant Risks in Delivering Key Technology Investment*, available at: http://www.gao.gov/products/GAO-08-1148T.

[152] 'Climate change to force mass migration', *Guardian*, 14 May 2007: http://www.guardian.co.uk/environment/2007/may/14/climatechange.climatechangeenvironment.

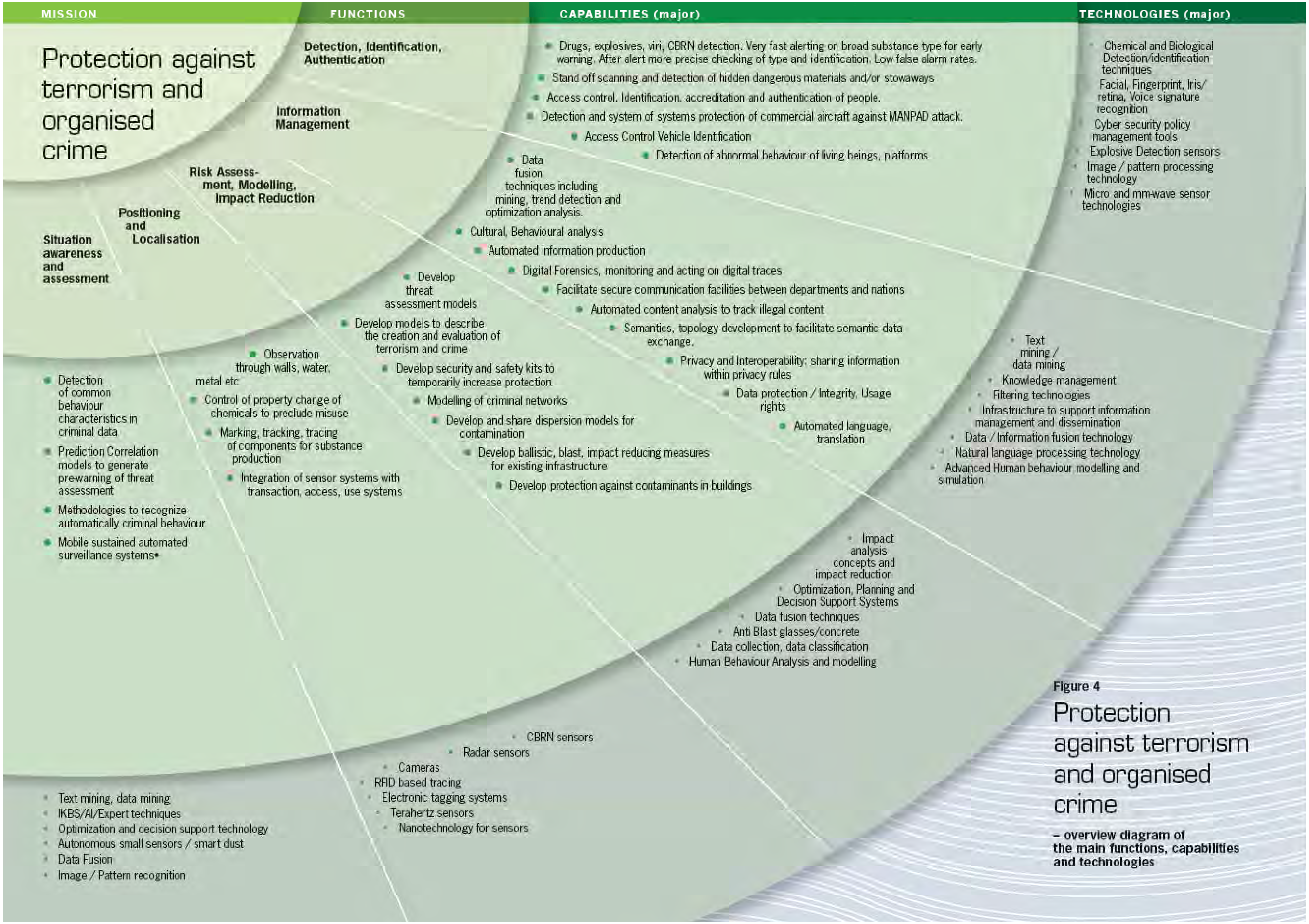
[153] Bauman, Z. (2002) Society Under Siege. Cambridge: Polity Press (page 84).

[154] See list of separation barriers maintained on Wikipedia: http://en.wikipedia.org/wiki/Separation_barrier.

[155] Nevins, J (2006) *Boundary Enforcement and National Security in an Age of Global Apartheid*, Speech given at a fundraiser for La Coalición de Derechos Humanos, Tucson, Arizona, 7 July 2006, available at: http://deletetheborder.org/files/Global%20Apartheid_set%20up.pdf.

[156] Webber, F (2006) *Border Wars and Asylum Crimes*. London: Statewatch (page 6), available at: http://www.statewatch.org/analyses/border-wars-and-asylum-crimes.pdf.

[157] See *Death by Policy: The Fatal Realities of "Fortress Europe"*: http://www.unitedagainstracism.org/pages/campfatalrealities.htm.



MISSION

FUNCTIONS

CAPABILITIES (major)

TECHNOLOGIES (major)

Protection against terrorism and organised crime

Detection, Identification, Authentication

Information Management

Risk Assessment, Modelling, Impact Reduction

Positioning and Localisation

Situation awareness and assessment

- Drugs, explosives, viri, CBRN detection. Very fast alerting on broad substance type for early warning. After alert more precise checking of type and identification. Low false alarm rates.
- Stand off scanning and detection of hidden dangerous materials and/or stowaways
- Access control. Identification, accreditation and authentication of people.
- Detection and system of systems protection of commercial aircraft against MANPAD attack.
- Access Control Vehicle Identification
- Detection of abnormal behaviour of living beings, platforms
- Data fusion techniques including mining, trend detection and optimization analysis.
- Cultural, Behavioural analysis
- Automated information production
- Digital Forensics, monitoring and acting on digital traces
- Facilitate secure communication facilities between departments and nations
- Automated content analysis to track illegal content
- Semantics, topology development to facilitate semantic data exchange.
- Privacy and Interoperability; sharing information within privacy rules
- Data protection / Integrity, Usage rights
- Automated language, translation
- Develop threat assessment models
- Develop models to describe the creation and evaluation of terrorism and crime
- Develop security and safety kits to temporarily increase protection
- Modelling of criminal networks
- Develop and share dispersion models for contamination
- Develop ballistic, blast, impact reducing measures for existing infrastructure
- Develop protection against contaminants in buildings
- Observation through walls, water, metal etc
- Control of property change of chemicals to preclude misuse
- Marking, tracking, tracing of components for substance production
- Integration of sensor systems with transaction, access, use systems
- Detection of common behaviour characteristics in criminal data
- Prediction Correlation models to generate pre-warning of threat assessment
- Methodologies to recognize automatically criminal behaviour
- Mobile sustained automated surveillance systems•

- Chemical and Biological Detection/identification techniques
- Facial, Fingerprint, Iris/retina, Voice signature recognition
- Cyber security policy management tools
- Explosive Detection sensors
- Image / pattern processing technology
- Micro and mm-wave sensor technologies
- Text mining / data mining
- Knowledge management
- Filtering technologies
- Infrastructure to support information management and dissemination
- Data / Information fusion technology
- Natural language processing technology
- Advanced Human behaviour modelling and simulation
- Impact analysis concepts and impact reduction
- Optimization, Planning and Decision Support Systems
- Data fusion techniques
- Anti Blast glasses/concrete
- Data collection, data classification
- Human Behaviour Analysis and modelling
- CBRN sensors
- Radar sensors
- Cameras
- RFID based tracing
- Electronic tagging systems
- Terahertz sensors
- Nanotechnology for sensors
- Text mining, data mining
- IKBS/AI/Expert techniques
- Optimization and decision support technology
- Autonomous small sensors / smart dust
- Data Fusion
- Image / Pattern recognition

Figure 4

Protection against terrorism and organised crime

– overview diagram of the main functions, capabilities and technologies

PART V: COMBATTING CRIME AND TERRORISM: FULL SPECTRUM SURVEILLANCE

The key to victory in modern conflict is informational superiority. The side that enjoys the highest degree of information superiority can manoeuvre its forces quickly and decisively to achieve tactical and operational advantage over its enemy. It can also precisely and effectively engage every vital element of the enemy's forces to reduce their fighting capabilities to nil...

Michal Fiszer (a Polish Air Force and military intelligence veteran) [158]

14 The EU's PATRIOT Acts

In the years since 9/11 the EU has gone much further than the USA in terms of the legislation it has adopted to facilitate the surveillance of its citizens. While the PATRIOT Act has achieved notoriety, the EU has, quietly, adopted legislation on the mandatory fingerprinting of all EU passport, visa and residence permit-holders, and the mandatory retention - *for general law enforcement purposes* - of all telecommunications data (our telephone, e-mail and internet 'traffic' records), all air traveller data (on passengers into, out of and across Europe) and all financial transactions.

Under national laws implementing EU legislation, state agents are beginning to access a previously unimaginably detailed picture of the lives of their citizens, often in the absence of any judicial or democratic controls. In the UK, for example, the data retention regime has removed the obligation on the police to seek judicial authorisation for access to telecommunications records (now all that is required is the consent of a senior officer). According to the latest figures, the British police (together with a host of other UK public bodies) used these new powers a staggering 519,620 times during 2007.[159] As mandatory data retention is gradually extended from fixed and mobile telephony to internet service providers, state surveillance of telecommunications will increase further still. Cross--border powers over multinational service providers mean that states can increasingly conduct 'foreign' communications surveillance as easily as domestic surveillance.

There appears to be little prosprect of any trend toward more and more unregulated surveillance powers in Europe. According to the officials currently elaborating a new five year plan for EU Justice and Home Affairs policy, this is instead just the beginning of a 'digital tsunami' that will 'revolutionalise law enforcement', providing a wealth of new information for 'public security authorities' (see section 25, page 75).

The security services have also developed virtually undetectable 'bugs', tracing technologies and 'spyware' that can be surreptitiously installed on a suspect's personal computer. In November 2008, the German Parliament approved legislation giving the police the power to conduct 'remote searches' of personal computers. In the same month, the EU adopted a new strategy on 'cybercrime' proposing 'a series of operational measures, such as cyber patrols, joint investigation teams and remote searches'.[160]

[158] 'AGS: NATO's Battlefield Eye In The Sky', *Defence Industry Daily*, 20 October 2006: http://www.defenseindustrydaily.com/ags-natos-battlefield-eye-in-the-sky-02727/.

[159] See 'Telephone tapping (and mail-opening figures) 1937-2007', *Statewatch*: http://www.statewatch.org/uk-tel-tap-reports.htm.

[160] *Fight against Cyber Crime: Cyber Patrols and Internet Investigation Teams to Reinforce the EU Strategy*, European Commission press release dated 11 September 2007, available at: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/08/1827&format=HTML&aged=0&language=EN&guiLanguage=en. See also 'Watching the computers', Tony Bunyan, Guardian, 9 June 2009: http://www.guardian.co.uk/commentisfree/libertycentral/2009/jun/09/remote-access-surveillance-rootkit.

The EU is also continuing to develop a host of law enforcement databases and information systems, including the Schengen Information System, the Europol Information System (the criminal intelligence database of the European Police Office), Eurodac (a database containing the fingerprints of all asylum applicants and irregular migrants in the EU), the Visa Information System and automated data comparison systems that will link the DNA and fingerprint databases of the member states.

The EU's celebrated data protection laws have already been left behind, with domestic police surveillance often exempted from the norms and standards that apply to other public sector data controllers. Individual rights to privacy and undue interference from the state enshrined in the Universal Declaration, currently celebrating its 60th anniversary, are being wholly undermined.[161]

In November 2008, the EU adopted a long awaited Framework Decision on data protection in police and judicial matters.[162] The new law, however, only covers the international transfer of personal data (i.e. between agencies in the member states and outside the EU). It does not, much to the dismay of privacy advocates, regulate data protection in the police sector at the national level, where rules are inconsistent, frequently weak and insufficiently enforced. The Framework Decision, which is supposed to protect well established fundamental rights, has been roundly condemned by privacy organisations, the European and some national parliaments, and the European Data Protection Supervisor (EDPS) for failing to uphold even the basic guarantees of the first ever international Data Protection Convention of 1981.[163]

[161] See 'Europe's Big Brothers', Ben Hayes & See T. Hammarberg, *Guardian*, 6 December 2008, available at: http://www.guardian.co.uk/commentisfree/2008/dec/06/humanrights-surveillance/print.

[162] *EU Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters* (OJ 2008 L 350/60).

[163] See 'Comments from EU Data Protection authorities to the Portuguese Council Presidency on draft Framework Decision on personal data in police and judicial issues' (7 November 2007), *Statewatch observatory on data protection in the EU*: http://www.statewatch.org/eu-dp.htm.

Europe is confronted with extremely diverse threats backed by unseen command structures and business-like financing mechanisms. Various security agencies concur that information is the key to defeating the enemy. This new environment has not only created a greater need for information but also a greater need to share and effectively control access to that information. This is the single greatest challenge European Security is facing today.

The STRAW consortium (an EU funded security research project) [164]

15 Situation awareness

Surveillance systems no longer just watch. High-definition CCTV is being combined with face (and gait) recognition software; motorway cameras can read car licence plates and track selected cars; a new generation of satellite based surveillance tools are being developed; computer programmes can monitor, screen and analyse billions of calls and emails simultaneously, in real time; new software can supposedly identify 'suspicious behaviour' or 'hostile intent'.[165] EU law has placed obligations on the telecommunications, financial and air travel sectors to retain customer records for long periods for police purposes. Combining these and other datasets – such as consumer lifestyle databases built by specialised data mining companies, or credit reference agencies – creates an incredibly detailed picture of peoples' lives and interests; their cultural, religious and political affiliations; and their financial and medical health.

Widespread concerns about surveillance among European citizens has seen the term 'situation awareness' find favour with policy-makers and practitioners. Working Group 7 of the European Security Research and Innovation Forum (ESRIF, above) on 'Situation awareness including the role of space' has a mandate to assess surveillance technology "relevant to urban security, homeland surveillance and peace enforcement scenarios". 'Situational awareness' was described in ESRAB's report as "the capture, fusion, correlation and interpretation of disparate forms of real-time and historical data and their presentation in a clear manner, facilitating effective decision-making and performance in a complex environment". 'Interoperable databases' were described as "essential to allow surveillance information to be cross-referenced against multiple heterogeneous sources in order to address illicit access of people and goods".[166]

ESRIF WG7 will examine "Present and needed sensors, based on ground, air and space"; identify "*new rules* and new technologies to foster information sharing" and propose "an international cooperation framework regarding fusion of data sources". So, with EU legislators abdicating their responsibility for regulating the international exchange and collection of data in the context for formal data protection rules, the private sector is instead being encouraged to develop a new framework and rules through ESRIF. WG7 is led by EMPORDEF, the Portuguese defence group responsible for state holdings in the defence industry, with Thales Alenia Space appointed as *rapporteur*.

Surveillance projects funded under the PASR included the ISCAPS project on the surveillance of public places, the PROBANT and HAMLET projects on the tracking of persons, the TRIPS project on the surveillance of railway stations and the EUROCOP project on geo-spatial information for pedestrian police officers. The mania for surveillance systems has continued under the FP7 programme with the SUBITO programme on "real time detection of abandoned luggage [and] the fast identification of the individual who left them", the LOTUS project on the detection of illicit bomb and drugs factories, the IDTECT4ALL project on novel intruder detection technology, and the ODYSSEY project on the development of a "Strategic pan-European ballistics intelligence platform". The European Defence Agency has also awarded several surveillance related R&D contracts.[167]

[164] See STRAW project website: http://www.straw-project.eu/.

[165] *Protecting the right to privacy in the fight against terrorism*. Issue Paper by Thomas Hammarberg, Council of Europe Commissioner for Human Rights (CommDH/IssuePaper(2008)3/04). Strasbourg: Council of Europe, available at: https://wcd.coe.int/ViewDoc.jsp?id=1380905&Site=CommDH&BackColorInternet=FEC65B&BackColorIntranet=FEC65B&BackColorLogged=FFC679.

[166] ESRAB (2006) *Meeting the challenge: the European Security Research Agenda – A report from the European Security Research Advisory Board*. Brussels: European Commission (page 25), available at: http://ec.europa.eu/enterprise/security/doc/esrab_report_en.pdf.

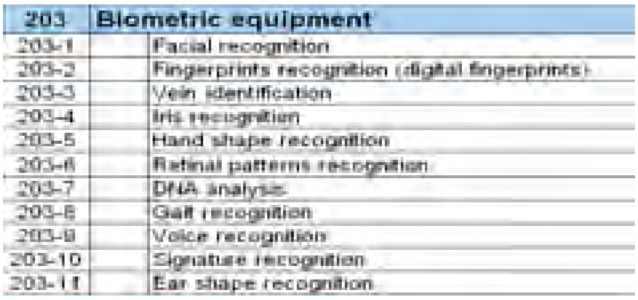
[167] See Contracts 4 and 13, 'Annual List of Contractors – 2007' (2008/S 62-083197), *European Defence Agency* website: http://www.eda.europa.eu/procurement.aspx.

16 The dawning of the biometric age

Say goodbye to PINs and photo IDs. Say hello to digital fingerprints and iris scans—and to new opportunities for security businesses.

Business Week, May 2009 [168]

Identity shopping



203	Biometric equipment
203-1	Facial recognition
203-2	Fingerprints recognition (digital fingerprints)
203-3	Vein identification
203-4	Iris recognition
203-5	Hand shape recognition
203-6	Retinal patterns recognition
203-7	DNA analysis
203-8	Gait recognition
203-9	Voice recognition
203-10	Signature recognition
203-11	Ear shape recognition

Having agreed on the mass fingerprinting of the European population, 'biometrics' is one area of security technology where Europe can already claim to lead the world. When the EU adopted legislation on the mandatory fingerprinting of EU passport holders in 2005, the EU Joint Research Centre suggested that "once the public becomes accustomed to using biometrics at the borders, their use in commercial applications will follow". The "large-scale introduction of biometric passports in Europe", it continued, provides a "unique opportunity": "Firstly, the creation of a demand market based on user acceptance"; "Second, the fostering of a competitive supply market".[169] As one US commentator has observed: "Pre-9/11, the expectation was that [advances in biometrics] would percolate up from the commercial sector. But with the emphasis on security after 9/11, there are now major government initiatives".[170]

Every nation in the European Union must institute fingerprint-enabled e-passports by the summer of 2010. They are required to use interoperable technology and, under the 'Prum Convention', obliged to provide future access to their national biometric databases for checks by other member states.[171] An EU Automated Fingerprint Identification System (AFIS) is being established to provide this facility. According to news reports, the USA, UK, Australia, Canada and New Zealand have established a working Group, the International Information Consortium, to develop their own automated system for exchanging fingerprinting data.[172]

The European Biometrics Forum (EBF), a group "whose overall vision is to establish the European Union as the World Leader in Biometrics Excellence by addressing barriers to adoption and fragmentation in the marketplace",[173] has been appointed *rapporteur* for ESRIF Working

[168] 'The Dawning of the Biometric Age', *Business Week*, 29 May 2009: http://www.businessweek.com/innovate/content/may2009/id20090520_625039_page_2.htm.

[169] See 'EU Report on biometrics dodges the real issues', *Statewatch news online*, March 2005: http://www.statewatch.org/news/2005/mar/17eu-biometric-report.htm.

[170] Lawrence Hornak, co-director of the USA National Science Foundation Center for Identification Technology Research, cited in 'The Dawning of the Biometric Age', *Business Week*, 29 May 2009: http://www.businessweek.com/innovate/content/may2009/id20090520_625039_page_2.htm.

[171] The 'Prum Treaty' was signed on 27 May 2005 by Germany, Spain, France, Luxembourg, Netherlands, Austria and Belgium, full text available at: http://www.statewatch.org/news/2005/aug/Prum-Convention.pdf. EU legislation implementing the Prum treaty and extending its scope across the EU was adopted in June 2008 (see Decisions 2008/615/JHA and 2008/616/JHA).

[172] See 'FBI wants instant access to British identity data', Guardian, 15 January 2008: http://www.guardian.co.uk/uk/2008/jan/15/world.ukcrime. The USA, UK, Australia, Canada and New Zealand have long worked together on surveillance through the ECHELON 'global eavesdropping' system.

[173] See European Biometrics Forum website: http://www.eubiometricforum.com/.

Group 8 on the 'identification of people and assets'. The EBF is also participating in at least five EU-funded research projects and leads the BIOTESTING EUROPE consortium (PASR) in support of EU legislation on the fingerprinting of passport, visa and residence permit holders.[174]

The development of EU legislation in this area was also supported by several FP6 research projects, including the MTIT and DIGITAL PASSPORT projects.[175] The EU also funded 3DFACE, a €10 million project led by Sagem, which is looking at fusing "3D face recognition technology, including fusion with 2D face recognition technologies, and its application in highly secure environments".[176]

The EU's research into biometrics is by no means limited to ID systems mandated by EU legislation; funding has supported long term research into applied biometrics for more than a decade, including numerous R&D projects geared toward the commercial application and development of biometric technology.

Selected 'biometrics' projects funded by the European Commission

- **BIOTESTING EUROPE** (PASR): roadmap for standardisation of biometric ID systems in the EU
- **MTIT (FP6)**: Minutiae Template Interoperability Testing for interoperability of fingerprint biometrics
- **DIGITAL PASSPORT** (FP6): next generation European digital passport
- **BIOSEC** (FP6): iris, fingerprint and voice identification
- **3DFACE** (FP6): facial recognition
- **TURBINE** (FP7): Trusted revocable biometric identities
- **BIO-RESIDENCE** (FP6): the use of biometrics in entry and access systems
- **BIOSECURE** (FP6): sensitive applications like online commerce and banking
- **HUMABIO** (FP6): the technology required to read and analyse biometric data
- **FIDIS** (FP6): implications of biometrics for the 'European information society'
- **BITE** (FP6): Biometric Identification Technology Ethics
- **VEIN BIOMETRIC (FP7)**: Security Applications Using Infra-Red Vein Imaging
- **FINGER_CARD**: Biometric Matching and Authentication System on Card
- **MOBIO** (FP7): bi-modal authentication systems in the framework of mobile devices
- **ACTIBIO** (FP7): unobtrusive authentication using activity related and soft biometrics
- **BEE** (FP7): Business Environment of Biometrics involved in electronic commerce
- **WABY** (FP7): A Walk-By Biometric Identification System Based On Face Recognition
- **VIPBOB**: VIrtual Pin Based on Biometrics
- **BANCA** (FP7): Biometric Access Control for Networked and e-Commerce Application
- **SABRINA** (FP7): Secure Authentication by Biometric Rationale Integration into Network Applications
- **HIDE** (FP7): Homeland Security, Biometric Identification & Personal Detection Ethics
- **RISE** (FP7): Rising pan European and International Awareness of Biometrics and Security Ethics
- **BIOTEST** (1996): biometric testing services

[174] BIOTESTING EUROPE will produce a 'roadmap' on 'what needs to be tested', 'which components should be certified (sensors/algorithms/ subsystems etc.)', 'who is going to perform the tests', 'what are the costs and who will pay/invest' See BIOTESTING EUROPE project website: www.biotestingeurope.eu. EBF also participated in the STACCATO (PASR) and CRESCENDO (ESRP, FP7) projects.

[175] The MTIT project on 'Minutiae template interoperability testing' featured Sagem, Motorola and Fraunhofer and promised to "improve the interoperability of minutiae-based fingerprint systems within a timescale to meet the needs of EU policy legislation". DIGITAL PASSPORT, on the 'Next generation European digital passport with biometric data for secure and convenient boarder [sic] passage', was designed to meet Schengen Information System and ICAO specifications.

[176] EU legislation mandates digital photographs as well as fingerprints in all future European passports, the International Civil Aviation Organization (ICAO, a UN body) has also mandated digital photographs using harmonised technical specifications. The 3DFACE project included a "large scale field trial on some important European airport sites, in order to test end-to-end performance of the system and to analyse resulting social and operational issues".

Ethical concerns, democracy and human rights

EU research funded to date assumes public consent to biometrics, with potential and tangible opposition reduced to 'ethical concerns'. It also assumes that the ethical concerns about the collection and use of biometric data relate simply to privacy and data protection, and can somehow be solved by privacy-friendly technology. This leaves little or no room for dissenting voices that view frequent or compulsory fingerprinting as a major civil liberties or human rights issue, and which might render the technology unwarranted, unacceptable or even illegal. The BITE project on 'Biometric Identification Technology Ethics', for example, promoted "research and public debate on bioethical implications of emerging biometric identification technologies",[177] while the TURBINE project is a "multi-disciplinary privacy enhancing technology, combining innovative developments in cryptography and fingerprint biometrics". It aims to provide an effective integrated biometrics system, while solving major issues related to "privacy concerns associated to the use of biometrics for ID management".[178] The HIDE[179] project, on Homeland Security, Biometric Identification & Personal Detection Ethics, is the latest "platform devoted to ethical and privacy issues of biometrics and personal detection technologies which addresses transnational (European) and international problems". HIDE's ambition is "to become the preeminent catalyst for innovative policy solutions to emerging ethical problems in the area of surveillance technologies… especially where collaboration among national and international agencies, communities, businesses, and NGOs is crucial".[180]

Whereas the architects of the ESRP view the introduction of biometric ID systems and other commercial applications as an economic imperative that *may* raise ethical issues, the European Court of Human Rights has adopted a more critical interpretation. In December 2008, in the case of *S. & Marper v. UK*, the Court ruled that the UK police policy of taking DNA samples and fingerprints from *everyone* arrested by the police, and then keeping them indefinitely on the police national databases – even if the person arrested is released without charge or subsequently acquitted – violates the European Convention on Human Rights.

The case was brought by an 11-year-old boy charged with burglary but later acquitted, and an adult male against whom initial charges of harassment were dropped. The Court found that: "*The blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences […] fails to strike a fair balance between the competing public and private interests and that the respondent State has overstepped any acceptable margin of appreciation in this regard*". Accordingly, the Court ruled that "*the retention at issue constitutes a disproportionate interference with the applicants' right to respect for private life and cannot be regarded as necessary in a democratic society*".[181]

The judgement has obvious implications for the large scale ID systems currently being developed by the EU. For example, the plan to allow access to law enforcement agencies to the EU Visa Information System (VIS), which is to contain the fingerprints of *every* applicant for a visa for an EU member state (some 20 million people a year). VIS will include records and biometrics from children as young as six and tens of millions of people who have not committed any criminal offences. This hardly seems proportionate in the context of the *S & Marper* judgement.

Many of the EU member states, however, have long since shown a different inclination to what is "proportionate in a democratic society". In its response to the European Court ruling, the UK proposes to end the indefinite retention of fingerprints and DNA samples from arrested persons who are later not charged or acquitted and to keep them for six years instead (12 years where terrorist and serious sexual offences are concerned). In the eyes of many readers of the Court judgement, this still exceeds by some distance "any acceptable margin of appreciation" in the state's interference with the individual right to privacy in a democratic society.[182]

[177] See BITE project website: http://www.biteproject.org/.

[178] See TURBINE project website: http://www.turbine-project.eu. See also the FIDIS 'Network of Excellence' (2004-7) on the "future of identity in the information society", which sought "technologies which address trust and security", FIDIS project website: http://www.hideproject.org/.

[179] See HIDE project website: http://www.hideproject.org/.

[180] The HIDE project is coordinated by the Centre for Science, Society and Citizenship (Italy), participants include the International Biometric Group (a US corporation that describes itself as the "biometric industry's leading consulting and technology services firm"), Sagem and Fraunhofer, along with several European universities and private consultants. The Centre for Science, Society and Citizenship is also coordinating the RISE project (Rising pan European and International Awareness of Biometrics and Security Ethics), which aims to "promote pan-European and International Awareness on Ethical Aspects of Biometrics and Security Technologies". Participants in the RISE project include the European Biometric Forum and Global Security Intelligence (USA), see RISE project website: http://www.riseproject.eu/ (not yet online at time of writing).

[181] See Judgment in case of S. & Marper v. UK (Application nos 30562/04 and 30566/04), available at: http://www.statewatch.org/news/2008/dec/echr-marper-judgment.pdf.

[182] See 'Keeping the Right People on the DNA Database: Science and Public protection, Home Office Conultation, May 2009, available at: http://www.guardian.co.uk/politics/2009/may/07/dna-database-reforms-human-rights/print.

Both homeland security and surveillance are being extensively deployed not only to monitor – an array of activities ranging from terrorist suspects to critical infrastructure sites, gated communities, hospital and schools, and consumer behaviour – but as a prime instrument of social sorting that discriminates between one person and another on the basis of a computer profile or data image.

Neve Gordon, Working Paper III of the New Transparency project [183]

17 Suspect communities: profiling and targeting systems

A principle component of the emerging 'surveillance society' is the increasingly widespread process of 'social sorting', a continual process based on "codes, usually processed by computers, [that] sort out transactions, interactions, visits, calls, and other activities". These codes are "the invisible doors that permit access to or exclude from participation in a multitude of events".[184]

In a security context, this means identifying and making distinctions between those persons who pose a threat, 'risks' who could pose a threat, and those 'trusted citizens' who are free to go about their business. However, these codes (also known as 'profiles' in a law enforcement context) can often be based on discriminatory assumptions about race, class, faith etc., institutionalising discrimination against ethnic minorities and other 'suspect communities'.

Projects funded by the EU in this area include the aforementioned HUMABIO project, which will use 'biodynamic indicators and behavioural analysis' for human monitoring and authentication; the SAMURAI project on the detection of "suspicious and abnormal behaviour monitoring using a network of cameras and sensors for situation awareness enhancement"; the INDECT project, which promises "automatic detection of threats and recognition of abnormal behaviour or violence"; and the ADABTS project on the 'Automatic Detection of Abnormal Behaviour and Threats in crowded Spaces'. ADABTS, led by FOI (the Swedish military research agency) and featuring BAE systems, the UK Home Office and TNO (the Dutch military research agency), will demonstrate the "prediction of the evolution of behaviour, so that potentially threatening behaviour can be detected as it unfolds, thus enabling pro-active surveillance".

Looking out for you?
Behavioural analysis
and smart CCTV

[183] Gordon, N. (2009) 'The Political Economy of Israel's Homeland Security', *The New Transparency Project, Working Paper III, IRSP IV*, available at: http://www.surveillanceproject.org/files/The%20Political%20Economy%20of%20Israel%E2%80%99s%20Homeland%20Security.pdf.

[184] Lyon, D. (ed., 2003) *Surveillance as social sorting*, Routledge: London & New York (page 13).

The EU has also funded a host of projects on data-mining software, data-mining in financial markets and biomedical research, and data-mining in environmental research. It has keenly promoted the technology across the private and public sector. The ADMIRE project on Advanced Data Mining and Integration Research for Europe ('making data-mining easier'), for example, aims to deliver "a consistent and easy-to--use technology for extracting information and knowledge… from multiple heterogeneous and distributed resources".

How to make threats and alienate people

In November 2002 the EU adopted a secret Recommendation on 'the development of terrorist profiles'.[185] The text, which was not published, notes that "most but not all EU countries were working on profiles in the area of terrorism" and calls upon the member states to "pass on information to Europol which will develop the terrorist profiles and make them available to the relevant authorities in the Member States".

Nationality, means of travel, age, sex, physical distinguishing features '(e.g. battle scars)', education, "use of techniques to prevent discovery or counter questioning", places of stay, place of birth, psycho-sociological features, family situation, expertise in advanced technologies and "attendance at training courses in paramilitary, flying and other specialist techniques" were all put forward as characteristics which might indicate propensity to commit acts of terrorism. The EU's programme on 'radicalisation and recruitment', which implicitly encourages the use of profiling in counter--terrorism operations and the targeting of 'moderate' as well as 'extremist' Mosques, schools, community centres and websites, and those who visit them, also includes a dedicated research budget.[186]

No information has been produced on the implementation of the EU's recommendations in this area but the EU has funded the HITS-ISAC project, coordinated by Saab, to develop a technical framework for the "cross-border exchange of differentiated sources of data" in order to "prevent, predict, and protect against potential terrorist activities and organised crime".[187] Alessandro Zanasi, a retired Carabinieri [Italian police] telephone interception specialist, ESRAB and ESRIF member, and co-founder of Temis, a company specialising in 'text intelligence', is participating in three European Commission and "some other confidential ones".[188]

Risk profiling and 'pro-active' surveillance systems turn the right to be presumed innocent on its head: everyone is a 'suspect' who may be asked to account for themselves or interrogated on the basis of assumptions or information unknown to them. Of course, some people are more suspect than others; profiling begins with this very principle. In response to the EU Recommendation on 'terrorist profiling', the now disbanded EU Network of Experts on Fundamental Rights argued that profiling could only be justified "in the presence of a fair, statistically significant demonstration of the relations between these characteristics and the risk of terrorism, a demonstration that has not been made at this time".[189] The European Parliament "*has raised repeated concerns related to profiling, in particular regarding race, ethnicity and religion, in the context of data protection, law enforcement cooperation, exchange of data and intelligence, aviation and transport security, immigration and border management and treatment of minorities. However there has been no adequate examination of the legal and other issues which might lead to some agreement on what is acceptable and what is not*".[190]

The Council of Europe Commissioner for Human Rights has suggested that while technologies that enable 'profiling' and 'data mining' may appear attractive security solutions, they are just as likely to lead to actions against large numbers of innocent people on a scale that is unacceptable in a democratic society.[191] It is important to stress the inevitability in this; that this is something that cannot be fixed by better design. As Douwe Korff (a professor specialising in surveillance technologies) has explained, "Attempts to identify very rare incidents or targets from a very large data set are mathematically certain to result in either an unacceptably high number of "false positives" (identifying innocent people as suspects) or an unacceptably low number of "false negatives" (not identifying real criminals or terrorists). This is referred to scientifically as the 'base-rate fallacy'; colloquially, as 'If you are looking for a needle in a haystack, it doesn't help to throw more hay on the stack'".[192]

Moreover, as privacy expert Bruce Schneier observes: "the effectiveness of any profiling system is directly related to how likely it will be subverted". "Profiling is something we all do, and we do it because – for the most part – it works", suggests Schneier, "But when you're dealing with an intelligent adversary… you invite that adversary to deliberately try to subvert your profiling system". [193]

[185] *Draft Council Recommendation on the development of terrorist profiles*, EU Council document 11858/3/02, 18 November 2002, available at: http://www.eclan.eu/Utils/ViewFile.aspx?MediaID=168&FD=4E.

[186] *Commission programme for the prevention of and response to violent radicalisation*, European Commission website: http://ec.europa.eu/justice_home/funding/2004_2007/radicalisation/funding_radicalisation_en.htm.

[187] Project website http://www.hits-isac.eu/

[188] Temis offers "automated information analysis [of] reports, e-mails, news, etc.)", see 'New Tools for New Intelligence: Text Mining and European Commission Funding', presentation by Alessandro Zanasi to *La Inteligencia Competitiva* Conference, Madrid, 29 November 2007, available at: http://www.madrimasd.org/Inteligencia-Competitiva/documentos/Alessandro_Zanasi-TEMIS_Italia.pdf.

[189] *The Balance Between Freedom and Security in the Response by the European Union and its Member States to the Terrorist Threats*, report of the EU Network of Experts on Fundamental Rights, 2003, Brussels: European Commission, available at: http://ec.europa.eu/justice_home/cfr_cdf/doc/obs_thematique_en.pdf.

[190] *Working Document on problem of profiling, notably on the basis of ethnicity and race, in counterterrorism, law enforcement, immigration, customs and border control*, European parliament Committee on Civil Liberties, Justice and Home Affairs (*Rapporteur*: Sarah Ludford), 30 September 2009 (PE413.954v02-00), available at: http://www.statewatch.org/news/2008/oct/ep-draft-report-on-profiling-ludford-oct-08.pdf.

[191] *Protecting the right to privacy in the fight against terrorism*. Issue Paper by Thomas Hammarberg, Council of Europe Commissioner for Human Rights (CommDH/IssuePaper(2008)3/04). Strasbourg: Council of Europe (page 4), available at: https://wcd.coe.int/ViewDoc.jsp?id=1380905&Site=CommDH&BackColorInternet=FEC65B&BackColorIntranet=FEC65B&BackColorLogged=FFC679.

[192] Cited in 'Surveillance Society', Ben Hayes, *Red Pepper*, January 2008: http://www.redpepper.org.uk/Surveillance-Society.

[193] 'Behavioral Profiling', *Schneier on Security*, August 2006: http://www.schneier.com/blog/archives/2006/08/behavioral_prof.html.

There is also much evidence to suggest, and not least from Northern Ireland, that the targeting of a 'suspect community' and what Professor Paddy Hillyard has called the 'sociology of street encounters', can be wholly counter-productive by undermining counter-terrorism efforts and fuelling 'radicalisation'.[194] Or, as the Northern Ireland Committee for the Administration of Justice has put it: "People are not going to report incidents or crucial information to the police when either their last contact [with the police/security services] has been at best unpleasant and at worst humiliating and abusive, or that they have heard how a neighbour or relative has been treated".[195]

Amnesty International - End racial Profiling Campaign

'Racial profiling occurs when race is used by law enforcement or private security officials, to any degree, as a basis for criminal suspicion in non--suspect specific investigations. Discrimination based on race, ethnicity, religion, nationality or on any other particular identity undermines the basic human rights and freedoms to which every person is entitled'.[196]

Ethnic injustice under the war on terror

'Since the 9/11 attacks in New York, 32 percent of British Muslims report being subjected to discrimination at airports, and stops and searches of British Asians increased five-fold after the June 2007 attempted bombings in London and Glasgow. Identity checks have been conducted on 11 year olds at German mosques by police carrying machine guns. A data mining exercise in Germany trawled through the sensitive personal data of 8.3 million people—without finding a single terrorist. Muslims, Roma, and migrant groups across Europe have reported feeling that they are all considered suspicious and have to constantly prove their innocence or legal right to stay. From street stops to airport searches to data mining, ethnic profiling affects many thousands of people and stigmatizes entire communities. Widely practiced but little scrutinized, ethnic profiling is a form of discrimination that is illegal in most circumstances' (Rebekah Delsol, *Open Society Justice Initiative*, 2008).[197]

[194] Hillyard, P. (1993) *Suspect Community: People's Experience of the Prevention of Terrorism Acts in Britain*. London: Pluto.

[195] *War on Terror: Lessons from Northern Ireland – Executive summary*, Committee for the Administration of Justice, January 2008, available at: http://www.caj.org.uk/Front%20page%20pdfs/Terror%20summary_12pp%20pages.pdf.

[196] *Racial profiling,* Amnesty International website: http://www.amnestyusa.org/us-human-rights/racial-profiling/page.do?id=1106650.

[197] Delsol, R. (2008) *Ethnic Profiling, ID Cards and European Experience*, Open Society Justice Initiative Presentation to *Identity Cards and Suspect Communities Roundtable Seminar*, oganised by Northern Ireland Human Rights Commission, available at: http://www.statewatch.org/news/2008/oct/n-ireland-nihrc-id-cards-profiling.pdf

> *Can we still talk of the peaceful use of space when bombs and grenades are guided by navigation satellites?*
>
> Frank Slijper, 'From Venus to Mars: The European Union's steps towards the militarisation of space' [198]

18 The EU's space race: Galileo and Kopernikus

The EU is developing two satellite-based surveillance systems. The first and better known is the Galileo system, conceived in the mid-1990s and lauded as the world's first *civilian* GPS system – one that would give the EU strategic independence from the USA. By 2004, Galileo had become the EU's first 'Public Private Partnership' (PPP), with defence giants Thales, EADS and Finmeccanica among those selected to co-finance the deployment phase. A director of EADS explained the corporate rationale: "GPS started as a military system but a massive market has developed around it and US industry has reaped the benefits many times over. All kinds of industries are dependent on GPS now – everything from oil and gas, to electricity distribution, to telecommunications".[199]

By 2007, the Galileo PPP consortium had collapsed, with corporate sources publicly blaming the EU's 'rigid governance'. Even the Director General of the European Space Agency called for a "European vision... that doesn't start with governance".[200] Costs are now being born by the EU alone, with €3.4 billion earmarked for Galileo's deployment phase put out to tender.

As explained in the 2008 TNI briefing on EU space policy, the industrial sector in Europe today is largely concentrated within three major companies: EADS' Astrium, Thales Alenia Space, a joint venture between Thales (67%) and Finmeccanica (33%), incorporating Telespazio, and the Bremen-based OHB Technology, which has experienced enormous growth over the past decade. Other important companies, with space divisions that have less than a thousand employees, include Dassault (France), Oerlikon Space (Austria), Saab Space (Sweden), Sonaca (Belgium), Terma (Denmark) and VEGA Aerospace (UK).[201]

The EU finally commenced the €3.4 billion deployment phase in 2009, with EADS Astrium and OHB providing spacecraft components and rocket company Arianespace selected to launch the Galileo system's first operational platforms.[202] While the EU argues that Galileo is another economic imperative for Europe, not everyone is convinced. An unnamed diplomat from an EU member state, cited on *Euractiv.com*, suggests instead that: "everybody knows

[198] *Slijper* F (2009) *From Venus to Mars*: *The European Union's steps towards the militarisation of space*. Amsterdam: Transnational Institute, available at: http://www.tni.org/detail_pub.phtml?&know_id=276.

[199] 'Bidding starts to put EU's Galileo navigation system into space', *Independent*, 2 July 2008: http://www.independent.co.uk/news/business/news/bidding-starts-to-put-eus-galileo-navigation-system-into-space-858415.html.

[200] 'Bidding starts to put EU's Galileo navigation system into space' (above).

[201] *Slijper* F (2009) *From Venus to Mars*: *The European Union's steps towards the militarisation of space*. Amsterdam: Transnational Institute, available at: http://www.tni.org/detail_pub.phtml?&know_id=276.

[202] Contracts give impetus to Galileo, BBC, 16 June 2009: http://news.bbc.co.uk/1/hi/sci/tech/8102047.stm

that there is no business case for Galileo. We only need a European system of our own, because at a militarily very critical moment we can't trust [foreign-owned] GPS to be available".[203] This 'strategic imperative' would also go some way to giving the EU the military independence from the USA/NATO that a number of member states covet.

With its gradual but firm steps toward militarisation, the EU is no longer committed solely to the peaceful use of space. In 2008 the European Parliament (EP) dropped its long-standing opposition to the use of Galileo for defence and crisis management operations under the auspices of the Common Foreign and Security Policy. The EP's report, drafted by Karl von Wogau MEP of the GoP (see section 3, above), also contains provisions favouring the development of satellite-based missile defence systems through NATO.[204] The European Defence Agency also has a stake in so-called 'MilSatCom', and has contracted the London Satellite Exchange Ltd. to produce a study that will "support the definition of [its] future MilSatCom R&T goals".[205]

In the law enforcement sector, satellite-tracking applications could have a range of uses. In Germany, satellites used in conjunction with other technologies already charge lorries by the kilometre for using the roads, according to their size and emissions. Citing congestion rather than pollution, the UK government floated the idea of tracking *all* car journeys by satellite in 2005 as part of its planned road-pricing scheme. This proposal met with ridicule in the media and a public petition that reached 1.8 million signatures.[206] There has been no such public outcry, however, over the satellite tagging of some 400,000 criminal offenders in the UK since 1999.[207] In December 2008, the European Commission published an Action Plan on the Deployment of Intelligent Transport Systems (ITS) in Europe and a proposed Directive establishing an EU framework for ITS.[208]

Kopernikus/GMES

The second EU satellite surveillance system is known as GMES. This initially stood for Global Monitoring for *Environmental Security* before being changed to Global Monitoring for Environment *and Security*. The whole system was re-launched and renamed 'Kopernikus' in 2008. GMES/Kopernikus is a 'system-of-systems' for 'earth observation', based on the common use of national satellite observation systems. It is currently in 'pre-operational' mode and developing five core services:

- Marine Environmental Services
- Atmospheric Environmental Services
- Land Environmental Services
- Support to Emergencies and Humanitarian Aid
- Support to security-related activities

According to the European Commission, Kopernikus will "significantly improve the living conditions of our generation and the generation of our children". It will do this by providing "vital information to decision-makers and business operators that rely on strategic information with regard to environmental, e.g. climate change and adaptation, or security issues". As with Galileo, the Commission argues that Kopernikus is an economic imperative, suggesting that anything that prevented its development "would undoubtedly cause a substantial opportunity cost for Europe, both in terms of money waste and loss of worldwide influence in such a strategic area".[209]

Kopernikus will use satellite surveillance systems in conjunction with ground and water sensors, and unmanned aerial vehicles (UAVs, examined below). The range of Kopernikus' potential surveillance capabilities varies in resolution from kilometres to centimetres (depending on how frequently the data needs to be updated) and Kopernikus will be capable of monitoring people as well as the environment, offering "clear potential for commercial applications in many different sectors by providing earth observation data for free to anybody who might have a use for them", including air and water quality managers, city planners and transport managers, agricultural surveyors and law enforcement and security agencies. In 2007, the EU adopted the INSPIRE Directive establishing an Infrastructure for Spatial Information in the European Community.[210]

[203] Galileo dossier, *Euractiv.com*, update 23 April 2008: http://www.euractiv.com/en/science/galileo/article-117496.

[204] European Parliament (2008) *Report on Space and security*, Committee on Foreign Affairs, EP doc. A6-0250/2008, 10 June 2008.

[205] See Contract 16, 'Annual List of Contractors – 2007' (2008/S 62-083197), *European Defence Agency* website: http://www.eda.europa.eu/procurement.aspx.

[206] PM denies road toll 'stealth tax', *BBC*, 21 February 2007: http://news.bbc.co.uk/1/hi/uk_politics/6381153.stm. See also: 'Big Brother is watching: surveillance box to track drivers is backed', *Guardian*, 31 March 2009: http://www.guardian.co.uk/uk/2009/mar/31/surveillance-transport-communication-box/print.

[207] 'Number of criminals ripping off electronic tags has soared', Daily Mail, 07 April 2008: http://www.dailymail.co.uk/news/article-557781/Number-criminals-ripping-electronic-tags-soared.html.

[208] Communication from the Commission - Action plan for the deployment of Intelligent Transport Systems in Europe, COM (2008) 886 final, 16 December 2008; Proposal for a Directive of the European Parliament and of the Council laying down the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other transport modes, COM (2008) 887 final, 16 December 2008: http://europa.eu/legislation_summaries/transport/intelligent_transport_navigation_by_satellite/tr0010_en.htm.

[209] Source: Kopernikus website, European Commission: http://ec.europa.eu/gmes/overview.htm.

[210] *Directive 2007/2/EC of the European Parliament and of the Council of 14 March 2007 establishing an Infrastructure for Spatial Information in the European Community (INSPIRE).*

Satellite surveillance and EU R&D

According to Iraklis Oikonomou of the University of Sussex, "the immediate beneficiaries of Kopernikus are the two largest European space-industrial actors: EADS and Thales Alenia Space", which have been awarded contracts worth hundreds of millions of euros for the development of the Sentinel 1, 2 and 3 satellites.[211] While the European Space Agency is taking the lead role, the R&D programme is being overseen by the European Commission DG for Enterprise and Industry (which is also running the ESRP).

The EU has awarded at least 116 research contracts within the framework of GMES/Kopernikus.[212] The vast majority of GMES projects funded to date focused on environmental security, using earth observation systems to monitor everything from climate change, to land degradation, deforestation and water resources,[213] but Kopernikus introduces a much stronger security and defence component.

Two projects, ASTRO+ and GEOCREW, demonstrated the use of European satellite systems to support internal and external EU security, defence and crisis management operations. The European Defence Agency has launched its own programme on 'Multinational Space-based Imaging System for Surveillance, Reconnaissance and Observation' (MUSIS) in order to define "an EU requirement for space imagery, working together with the Council General Secretariat (including the EUMS)".[214]

Data protection: pie in the sky

In its quest for ubiquitous surveillance of the planet, it is starting to appear that the EU will leave no stone unturned. But what of the security and privacy of the data generated by GMES/Kopernikus and Galileo? According to one journalist who attended the launch of Kopernikus at the GMES forum in Lille on the 16-17 September 2008, "no answers were forthcoming. It seems that this is yet another example of technology outstripping the legal and civil codes required to regulate how it is used".[215] While there has been some serious debate about the privacy implications of future satellite surveillance capabilities in the USA,[216] there has been precious little – if any – in the European Union. In the course of extensive research into EU-funded activities in this area, not one single project dealing with privacy or data protection in the context of the EU's sprawling satellite surveillance programme can be identified. Neither is there any concern for 'data protection' or privacy in the EU's INSPIRE Directive (on an EU Infrastructure for Spatial information) or the INSPIRE implementing regulations.[217]

[211] Oikonomou, I. (2009), 'Kopernikus/GMES and the militarisation of EU space policy', paper presented at *Militarism: Political Economy, Security, Theory* conference University of Sussex, on the 14th and 15th of May 2009.

[212] This includes BOSS4GMES which will "provide the technical, financial and contractual foundations [to] enable the transition of GMES (Global Monitoring for Environment and Security) from a concept to an effective, operational programme"; the GIGAS forum, which aims to integrate the EU's GMES/INSPIRE architecture with that of GEOSS, the 'Global Earth Observation System of Systems' developed by the 76 country 'Group on Earth Observations'; the HUMBOLDT project on the 'Harmonisation of Spatial Information in Europe'; the OASIS project on an 'Open Advanced System for Crisis management'; the ORCHESTRA project on 'Open Architecture and Spatial Data Infrastructure for Risk Management'; the OSIRIS project on 'Open architecture for Smart and Interoperable networks in Risk management based on In-situ Sensors'; and the WIN project on an interoperable information structure for the environment and risk management. A useful summary of Kopernikus/GMES projects is available at: http://kokos.vsb.cz/wiki/images/6/60/Horakova.pdf.

[213] The majority of the GMES projects to date have an environmental or humanitarian purpose, such as monitoring the impact of climate change or assisting humanitarian operations. The projects include the LIMES, RESPOND and PREVIEW projects on the use of satellites to provide information services for civil protection, 'disaster reduction' and reconstruction efforts; the RISK-EOS project on 'geo-information services to support the management of flood, fire and other risk'; the GEOLAND project on environmental monitoring; the FOREST project on area and land use mapping; the GSE LAND Information Service; the TERRAFIRMA Pan European Ground Motion Information Service; the GMFS project on global Monitoring for Food Security; the POLAR VIEW project on satellite and remote sensing in the Arctic and Antarctic; the PROMOTE project on 'GMES services relevant to the ozone layer, UV-exposure on the ground, air pollution and climate change'; the MERSEA project on the development of the ocean-based component of GMES; the MARCOAST marine and Coastal Information Service; the MARISS project surveillance of maritime traffic for law enforcement and security purposes; the TANGO project on 'Telecommunications Advanced Networks for GMES Operations'; the GEMS project on 'Global and Regional Earth-System Monitoring using Satellite and In-Situ Data'; and the ASTRO+ and GEOCREW projects on the support of internal and external EU security and crisis management operations and crisis monitoring from space.

[214] *EDA and Commission to work closely together on research*, European Defence Agency Press Release, 18 May 2009: http://www.eda.europa.eu/newsitem.aspx?id=471.

[215] Kopernikus – what's in it for Joe public?, Hunt P., *Statewatch news online*, 8 October 2008: http://www.statewatch.org/news/2008/oct/06Kopernikus-phil-hunt.htm.

[216] Gorman, S. 'Satellite-Surveillance Program to Begin Despite Privacy Concerns', *Wall Street Journal,* 1 October 2008, available at: http://online.wsj.com/article/SB122282336428992785.html?mod=googlenews_wsj.

[217] *Commission Regulation 1205/2008/EC of 3 December 2008 implementing Directive 2007/2/EC of the European Parliament and of the Council as regards metadata*.

19 Eyes in the skies: unmanned aerial vehicles

UAV [Unmanned Aerial Vehicle] use in Europe has been slower to emerge than in the US and in Israel. However, experience of using mature UAV systems on operations in Iraq and in Afghanistan has dramatically improved the European perspective on their utility, and the military market is growing at a significant rate…

Once restrictions on its emergence are finally swept away, the potential scale of the commercial market is likely to be much larger than the military market. […] In the wide range of areas where it would be feasible to replace manned aircraft with UAVs, the market for non-military applications is much larger than the defence sector and includes: Police/Paramilitary/Security applications; Agriculture spraying/planning; Low Earth Orbiting Satellites; Logistics/parcel delivery; Commercial passenger transport; Aerial photography.

Frost & Sullivan, study on UAVs for European Commission [218]

Unmanned Aerial Vehicles (UAVs) – or pilotless 'drone' planes – have achieved infamy across the Middle East, Pakistan and Afghanistan, where they are widely used by occupying forces for surveillance and targeted assassinations [there are two kinds of UAV: armed and unarmed 'drone' planes' and miniature spy planes, both of which are piloted remotely from the ground]. While the military has pioneered the development and deployment of UAVs, manufacturers are keen to develop Homeland Security and civilian markets. The trade in UAVs is dominated by US and Israeli firms, with a number of Europe's largest defence contractors ready to exploit an emerging European market.[219]

The EU has long supported 'research' into the commercial development of UAVs. To date at least a dozen projects have been funded under the EU's various framework research programmes. These include the aforementioned projects on the use of UAVs for border surveillance (BSUAV and WIMA2S); the €5 million CAPECON study on the 'utilisation of safe and low cost Unmanned Air Vehicles (UAVs) in the civilian commercial sphere', led by the state-owned Israel Aircraft Industries Ltd.; the €5.5 million IFATS project on 'innovative future air transport systems' (featuring Israel Aircraft Industries Ltd.. EADS and Thales); the €4.3 million INOUI 'roadmap' for 'innovative operational UAV integration', featuring Boeing Europe; and the µDRONES project on the development of UAVs for the surveillance of urban environments, featuring Thales.

A major obstacle to the introduction of UAVs is that they are currently prohibited from flying in European airspace because of well-founded concerns about potential collisions with traditional aircraft. The air traffic control community is particularly suspicious, and demands that UAVs adhere to equivalent safety standards as their manned counterparts, which some argue render UAV systems too expensive to implement.[220] The European Commission is evidently unperturbed, and simply sees a commercial opportunity that will inevitably lead to a change in the law (what might be called 'technocratic determinism').

In June 2009, the European Defence Agency signed contracts for a Mid-air Collision Avoidance System (MIDCAS) for 'sense and avoid' type drones, which it believes is the key to allowing their use in civilian airspace. The EDA's MIDCAS consortium, supported by Sweden, France, Germany, Spain and Italy, includes Thales and Sagem, who are responsible for the 'sense' function. Sagem is also in charge of standardization aspects, liaising with regulatory authorities (Eurocontrol, EASA, FAA, DGAC, etc) as well as the aviation community (aircraft manufacturers, pilot

[218] Frost & Sullivan (2007) *Study analysing the current activities in the field of UAVs*, European Commission, available at: http://ec.europa.eu/enterprise/security/doc/uav_study_element_1.pdf.

[219] Frost & Sullivan (2007) *Study analysing the current activities in the field of UAVs*, European Commission, available at: http://ec.europa.eu/enterprise/security/doc/uav_study_element_1.pdf.

[220] 'UAVs in Europe: When Will They File and Fly?' A*vionics Magazine*, 1 July 2006: http://www.aviationtoday.com/av/categories/military/UAVs-in-Europe-When-Will-They-File-and-Fly_1009.html.

Coming to an airspace near you?

associations, etc.), “to develop a European standard for the Sense and Avoid function”.[221] The EDA and the European Commission are already synergising their R&D into Software Defined Radio and for UAVs.[222]

In the UK, the Home Office and the Ministry of Defence (MoD) have both developed extensive UAV deployment plans. The Home Office plans to develop a national unmanned air vehicle fleet to support police and emergency response operations, “most likely via the contracting of services rather than outright acquisition”,[223] and at least four UK police and emergency services (Merseyside, West Midlands, Kent and Essex) forces have piloted, or are planning to use, UAVs to support their operations. The MoD reportedly has an R&D programme for spy planes equipped with “highly sophisticated monitoring equipment that allows them to secretly track and photograph suspects without their knowledge”, deployable within three years,[224] while BAE systems is leading a £32 million public-private consortium (the ASTRAEA project) “to promote and enable safe, routine and unrestricted use of [UAVs]”.[225]

According to a report by Frost & Sullivan for the European Commission, European military forces have “progressively expanded their inventory of UAV systems”.[226] The UK, France, Germany, Sweden, Ireland, Italy, Spain, The Netherlands, Denmark, Poland and Norway all use mini-UAVs. The UK, France and Italy are considering purchasing long-endurance, mid-altitude UAV’s and “have also been examining the potential for weaponising current UAV models”. NATO is also developing its ability to undertake advanced ground surveillance using fleets of UAVs to support a variety of new mission requirements, “including nation building, homeland security and humanitarian relief” (Germany, Italy, Poland, Greece, Spain, Slovenia, Romania and Turkey have all offered European bases for the NATO AGS system).[227] In the light of these and other developments, the Frost & Sullivan report predicts that the number of military UAVs in service will increase rapidly in the short-term before levelling out. Growth of the market beyond this point is dependent upon the take up of UAVs in the civilian sector.

[221] ‘Thales and Sagem Take Major Role in EDA’s MIDCAS Contract’, *ASD-Network*: http://www.asd-network.com/press_detail_B.asp?ID=21012&NID=283303.

[222] *EDA and Commission to work closely together on research*, European Defence Agency Press Release, 18 May 2009: http://www.eda.europa.eu/newsitem.aspx?id=471.

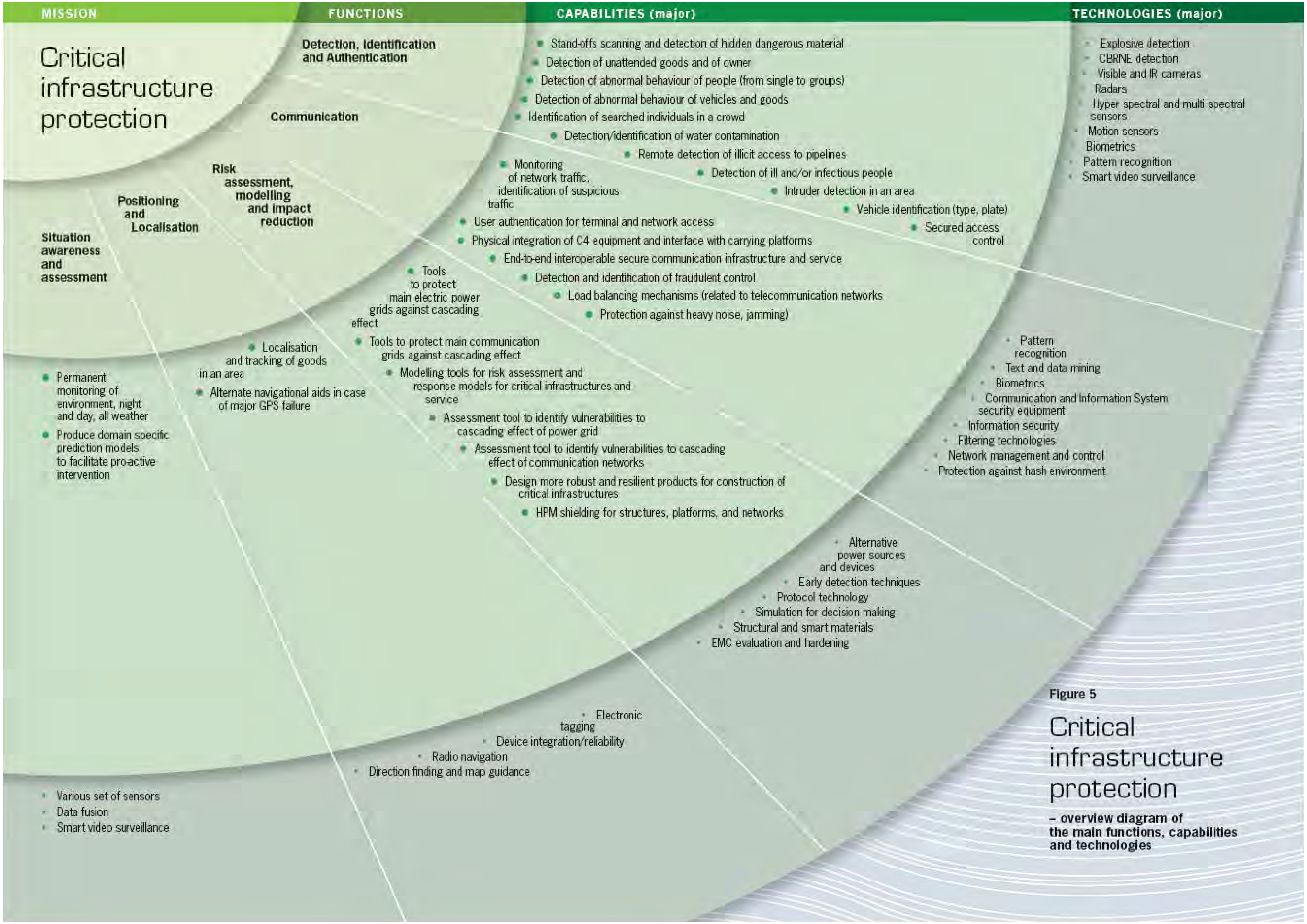
[223] ‘UK Home Office plans national police UAV fleet’, *Flight International*, 17 July 2007: http://www.flightglobal.com/articles/2007/07/17/215507/uk-home-office-plans-national-police-uav-fleet.html.

[224] ‘Unmanned spy planes to police Britain’, *Independent, 6 August 2008, available at:* http://www.independent.co.uk/news/uk/home-news/unmanned-spy-planes-to-police-britain-886083.html.

[225] See ASTRAEA website: http://www.projectastraea.co.uk/.

[226] Frost & Sullivan (2007) *Study analysing the current activities in the field of UAVs*, European Commission, available at: http://ec.europa.eu/enterprise/security/doc/uav_study_element_1.pdf.

[227] AGS: NATO’s Battlefield Eye In The Sky’, *Defence Industry Daily*, 20 October 2006: http://www.defenseindustrydaily.com/ags-natos-battlefield-eye-in-the-sky-02727/.



MISSION

Critical infrastructure protection

FUNCTIONS

Detection, Identification and Authentication

Communication

Risk assessment, modelling and impact reduction

Positioning and Localisation

Situation awareness and assessment

CAPABILITIES (major)

- Stand-offs scanning and detection of hidden dangerous material
- Detection of unattended goods and of owner
- Detection of abnormal behaviour of people (from single to groups)
- Detection of abnormal behaviour of vehicles and goods
- Identification of searched individuals in a crowd
- Detection/identification of water contamination
- Remote detection of illicit access to pipelines
- Detection of ill and/or infectious people
- Intruder detection in an area
- Vehicle identification (type, plate)
- Secured access control

- Monitoring of network traffic, identification of suspicious traffic
- User authentication for terminal and network access
- Physical integration of C4 equipment and interface with carrying platforms
- End-to-end interoperable secure communication infrastructure and service
- Detection and identification of fraudulent control
- Load balancing mechanisms (related to telecommunication networks
- Protection against heavy noise, jamming)

- Tools to protect main electric power grids against cascading effect
- Tools to protect main communication grids against cascading effect
- Modelling tools for risk assessment and response models for critical infrastructures and service
- Assessment tool to identify vulnerabilities to cascading effect of power grid
- Assessment tool to identify vulnerabilities to cascading effect of communication networks
- Design more robust and resilient products for construction of critical infrastructures
- HPM shielding for structures, platforms, and networks

- Localisation and tracking of goods in an area
- Alternate navigational aids in case of major GPS failure

- Permanent monitoring of environment, night and day, all weather
- Produce domain specific prediction models to facilitate pro-active intervention

TECHNOLOGIES (major)

- Explosive detection
- CBRNE detection
- Visible and IR cameras
- Radars
- Hyper spectral and multi spectral sensors
- Motion sensors
- Biometrics
- Pattern recognition
- Smart video surveillance

- Pattern recognition
- Text and data mining
- Biometrics
- Communication and Information System security equipment
- Information security
- Filtering technologies
- Network management and control
- Protection against hash environment

- Alternative power sources and devices
- Early detection techniques
- Protocol technology
- Simulation for decision making
- Structural and smart materials
- EMC evaluation and hardening

- Electronic tagging
- Device integration/reliability
- Radio navigation
- Direction finding and map guidance

- Various set of sensors
- Data fusion
- Smart video surveillance

Figure 5

Critical infrastructure protection

– overview diagram of the main functions, capabilities and technologies

PART VI: A WORLD OF RED ZONES AND GREEN ZONES

Europe has been turned into a killing field by those exploiting holes in the protective blanket intended to keep its citizens safe. Much has been made of the need to improve intelligence gathering and sharing in the fight against home grown and transnational terrorism, but the events of the past almost four years [sic] show clearly that intelligence alone is not the answer when the threats faced are largely covertly planned and executed. While intelligence must inevitably form part of the battle against terrorism, it must be supported by protective technologies...

Article issued by Niche Events, organisers of Transec World Expo 2007 [228]

20 Critical infrastructure protection

The terrorist attacks of 9/11, and those on the Madrid and London transport systems, have inevitably focused attention on the protection of publicly and privately owned 'critical infrastructure' and the way in which governments respond to terrorist attacks and other emergencies. The €75 million spent on improving security after the Madrid bombings, for example, has in turn focused the Homeland Security industry on the potential market for critical infrastructure protection (CIP) and crisis management.

The EU does not have the clearest of mandates to act in this area – domestic policing and security policy is very much a member state competence – but argues that "due to interdependencies and the general nature of today's economy, there exists in the EU a certain number of critical infrastructures which if disrupted or destroyed would have a serious impact on the entire Community or on a number of Member States".[229] Or as Tom Hardie-Forsyth, Chairman of the NATO Ad Hoc Group on CIP puts it: "If you pretend that a single nation can protect its assets single-handedly, then you are really dreaming".[230]

NATO's CIP programme is based on its experience in protecting critical infrastructure in the Balkans and Afghanistan. The military alliance has also contributed to CIP operations within the EU, including the massive security effort that accompanied the Olympics in Greece, the European football championships in Portugal and the World Cup in Germany. Without formal agreement, NATO's CIP programme appears to have acquired a mandate for 'domestic peacekeeping'. The emerging doctrine for critical infrastructure protection is very much in keeping with the model outlined above: establish command and control centres equipped with the latest localisation and situational awareness technologies; employ a wide range of detection, identification and authentication technologies; use risk assessment and impact reduction techniques; intervene rapidly to neutralise any threat to security.

The EU Critical Infrastructure Protection (CIP) programme was launched in 2004, followed by a dedicated EU funding programme on 'Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks', which runs alongside the ESRP/FP7 (2007-2013). An EU Directive identification and designation of European critical infrastructures was adopted in December 2008.[231] According to Commission Vice-President Barrot, the Directive will "raise the level of security for all EU citizens, provide legal clarity to operators and increase competitiveness".[232] Under

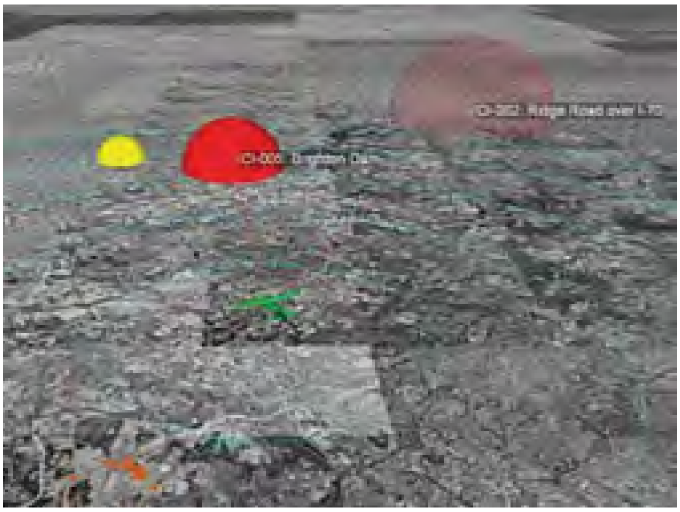
[228] 'EUROPE: Europe fights a rearguard action combating terrorism', available on *Cargo Security International* website: http://www.cargosecurityinternational.com/channeldetail.asp?cid=19&caid=8625.

[229] See *The European Programme for Critical Infrastructure Protection (EPCIP)*, European Commission Press Release, 12 december 2006 (Reference: MEMO/06/477), available at: http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/06/477&format=HTML&aged=0&language=EN.

[230] Cited in Conference documentation of *Partnership for Peace Seminar: Critical Infrastructure Protection and Civil Emergency Planning*, 17–18 November 2003, Stockholm, available at: http://www.krisberedskapsmyndigheten.se/upload/6332/critical-infrastructure-protection_november-2003.pdf.

[231] Directive 2008/114/EC *on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection*

[232] See Empowerment of EU complicates security, European Voice, 29 January 2009: http://www.europeanvoice.com/folder/energyquarterlypipelinesandsecurityofsupply/100.aspx?artid=63804.



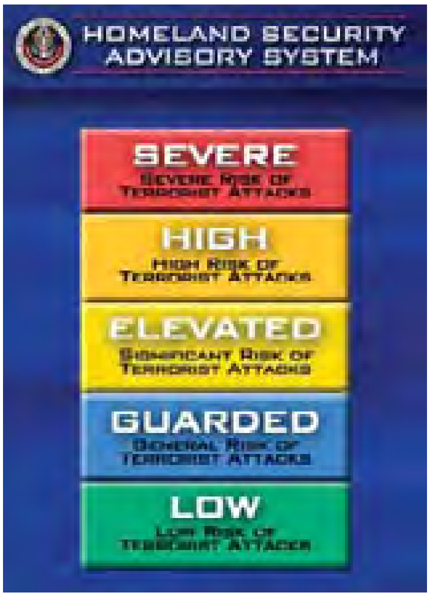
Painting the world red

> *"The system will use all kinds of remote and local sensors to warn you of an incursion. There will be a sensor field and you will be sitting miles away at your laptop and say 'Oops, we have an intruder'. It's very closely tied in with advanced sensor systems".*
>
> Art Schatz, senior VP of Metal Storm [233]

the Directive, the EU will identify and designate 'European Critical Infrastructure' (ECI) within the energy and transport sectors, and then develop a 'common approach' to the protection of these infrastructures. The Directive is to be reviewed after three years with the possibility of widening the focus to the Information and Communication Technology (ICT) sector. Operator Security Plans (OSPs) are to be developed for each designated ECI, covering "identification of important assets, a risk analysis based on major threat scenarios and the vulnerability of each asset, and the identification, selection and prioritisation of counter-measures and procedures". Whilst the total number of ECI is as yet unknown, the ESRAB report predicted that "the number of systems employed by those infrastructures will be in the order of thousands".[234]

While the CIP Directive is not yet in force, the EU is already actively pursuing CIP policies in the following areas: energy, ICT, water, food, health, the financial system, public order, civil administration, transport, the chemical and nuclear industries and space. An EU Network and Information Security Agency (ENISA) was established in 2004,[236] and in 2005 the Commission created a Critical Infrastructure Warning Information Network (CIWIN), bringing together member-state CIP specialists to assist the Commission in drawing up programmes to facilitate exchange of information on shared threats and vulnerabilities and appropriate counter-measures and strategies.[237] The EU has also discussed the possibility of setting-up a terrorist threat warning network across the EU (as already exists in the USA and UK).

A separate and long awaited package of EU measures on Chemical, Biological, Radiological and Nuclear security designed to restrict access to potentially lethal materials was agreed by the EU in 2009. The package includes €100m of EU funding to enhance the protection of CBRN facilities. Rebecca Harms, co-leader of the new Green group in the parliament, was among those who welcomed the measures. "Nuclear technology poses a clear terrorist threat. Nuclear power stations are like pre-installed bombs because they are not safe from attack, for example by aircraft", she said.[235]


HOMELAND SECURITY ADVISORY SYSTEM
SEVERE
Severe Risk of Terrorist Attacks
HIGH
High Risk of Terrorist Attacks
ELEVATED
Significant Risk of Terrorist Attacks
GUARDED
General Risk of Terrorist Attacks
LOW
Low Risk of Terrorist Attacks

[233] Wright, S. (2006) 'Report. Sub-lethal vision: varieties of military surveillance technology', *Surveillance & Society*, 4(1/2): 136-153, available at: http://www.surveillance-and-society.org/Articles4(1)/sublethal.pdf (page 144).

[234] ESRAB (2006) *Meeting the challenge: the European Security Research Agenda – A report from the European Security Research Advisory Board.* Brussels: European Commission, available at: http://ec.europa.eu/enterprise/security/doc/esrab_report_en.pdf.

[235] 'EU commits €100m to nuclear and radiological security', *euobserver.com*, 24 June 2009: http://euobserver.com/885/28368.

[236] http://www.enisa.europa.eu/.

[237] *Communication on a European Programme for Critical Infrastructure Protection,* European Commission, COM (2006) 786 final, 12 December 2006, available at: http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0786en01.pdf.

The EU's intervention in the area of critical infrastructure protection has not been without its controversies. In the weeks following the foiled terrorist plot to bring down transatlantic airliners using liquid explosives, the European Commission adopted a Regulation on the screening of passenger hand luggage and the carrying of liquids, a measure that led to the '100ml rule' and the confiscation of hundreds of tons of bottled water and 'illegal' toiletries across Europe. Unfortunately the Commission did not see fit to either consult the EU member states on the content of the Regulation (which was apparently supplied by MI5 in response to the transatlantic police investigation), or to publish the actual annex of the Regulation containing the new rules. Following legal challenges by MEPs and civil society organisations, the Commission relinquished and published the annex (it had already been leaked by Statewatch and other organisations).[238] This kind of secret rule-making has now been legitimised, *inter-alia*, for future 'crisis management' situations (see further 'crisis management', below).

Critical infrastructure protection and security research

Working Group 2 of the European Security Research and Innovation Forum on the 'security of critical infrastructure' has a mandate to improve the protection of critical infrastructure and utilities such as 'energy infrastructures and supplies (including gas and water supply)', 'food safety and security', health, 'financial infrastructure' transport, the chemical industry and space. The leader of WG2 is Transport Security Solutions Ltd. (Ireland); the *rapporteur* is the defence giant EADS.

While the EU has funded civil research in this area – on the protection of the water supply (WATERSAFE, PASR; SECUREAU, FP7), government information systems (VITA) and the security implications of environment accidents (SECURENV, FP7), amongst others[239] – much of the thinking behind the CIP techniques being explored by the ESRP is derived from military technology and practice.

EADS, for example, led the PALMA consortium on man-portable air-defence systems (MANPADs, PASR), for the protection of commercial aircraft from rocket attack. The consortium, which included Thales, is now awaiting a decision on its application to the ESRP for a much larger investment. In 2008, BAE Systems was awarded a $29 million contract from the Department of Homeland Security to test its infra-red aircraft missile defence system on commercial aircraft under its C-MANPADs program. Despite these vast sums, there is little if any evidence to suggest that the commercial airlines themselves actually want MANPADs technology, or that terrorists equipped with hand-held rocket launchers actually pose a significant threat to European air travellers.

Transport security

The EU CIP programme is focussed on both energy and transport security, but it is the latter that has moved to the centre of the EU's R&D programme to date. Under the PASR, the EU funded research projects on the protection of the security of the air transport system (PATIN) and the transport infrastructure (TRIPS, led by Ansaldo STS, a Finmeccanica company, and featuring Thales, BAE Systems, Diehl, Sagem and PIAP). Under the FP6 programme, the EU funded the COUNTERACT programme, which included a series of 'targeted studies' to equip public transport operators with new 'tools' to combat terrorist activities. The consortium notes that "By virtue of the similarity of problems across big cities in Europe, such security solutions have a potentially very important EU-wide market". The focus of phase II of the project will be the "definition and rationale for Mass transport" (i.e. recommendations for an EU transport security programme).

Integrated security solutions for critical infrastructure

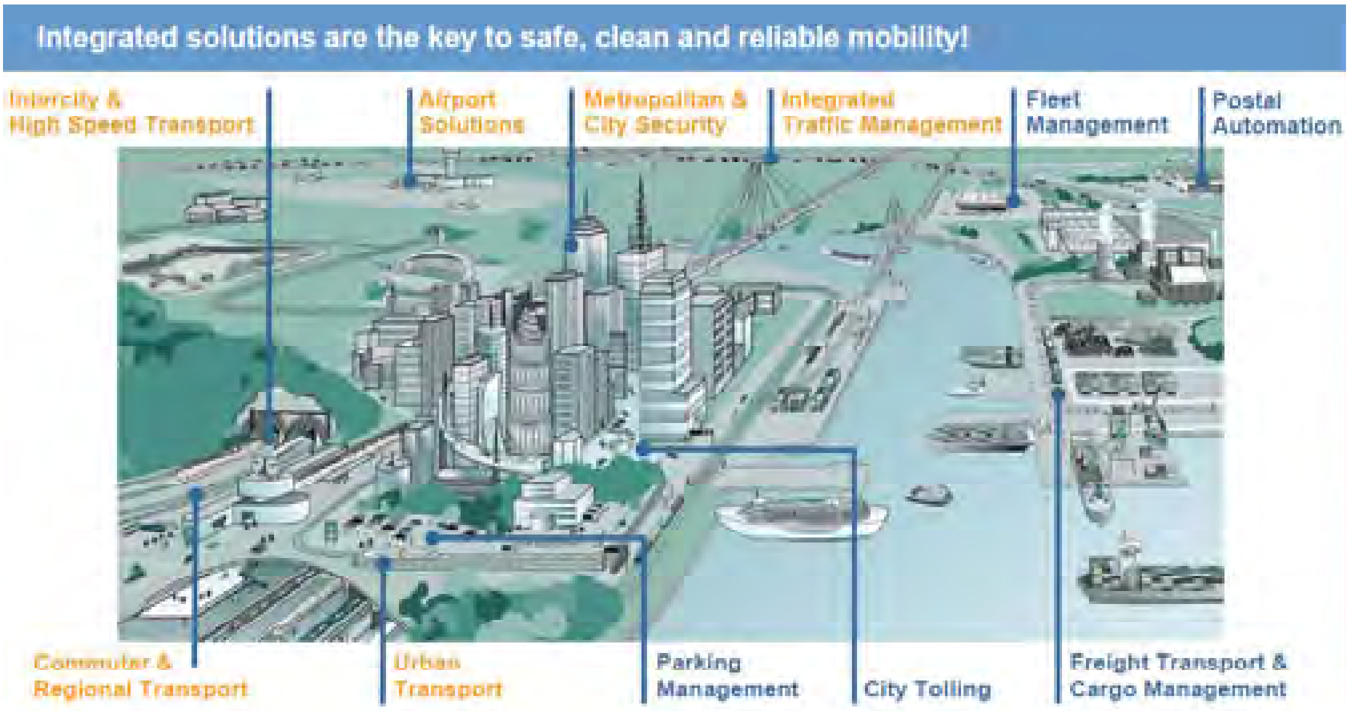
IMSK is a €23 million ESRP project led by Saab in a consortium that features TNO, Telespazio, Fraunhofer, Selex, Thales and Diehl that has received funding from the ESRP to produce an 'integrated mobile security kit' that will combine technologies for area surveillance; checkpoint control; CBRNE detection and support for VIP protection into a mobile system for rapid deployment at venues and sites (hotels, sport/festival arenas, etc) which temporarily need enhanced security.

The goal of IMSK is to "Increase the security of citizens in the scope of events gathering a large number of people, such as medium to large scale sports events (from football games to the Olympic Games), political summits (G8 summit) etc".

The majority of Europeans will doubtless welcome efforts to protect critical infrastructure in the light of terrorist attacks on public transport systems. But few people appear to have made the link between high-tech CIP and actual policing 'on the ground'. Critical infrastructure may be publicly or

[238] Action brought on 25 October 2007, *European Parliament v Commission of the European Communities* (Case C-474/07).

[239] See also the VIKING project (FP7) on 'the analysis, design and operation of resilient and secure industrial control systems for critical infrastructures'; GST (FP6) on the use of 'telematics' for automobile traffic safety; the UAN project on an 'Underwater acoustic network to protect critical infrastructures such as off-shore platforms and energy plants' (FP7).


Integrated solutions are the key to safe, clean and reliable mobility!
Intercity & High Speed Transport
Airport Solutions
Metropolitan & City Security
Integrated Traffic Management
Fleet Management
Postal Automation
Commuter & Regional Transport
Urban Transport
Parking Management
City Tolling
Freight Transport & Cargo Management

Integrated security in the city (by Siemens) [240]

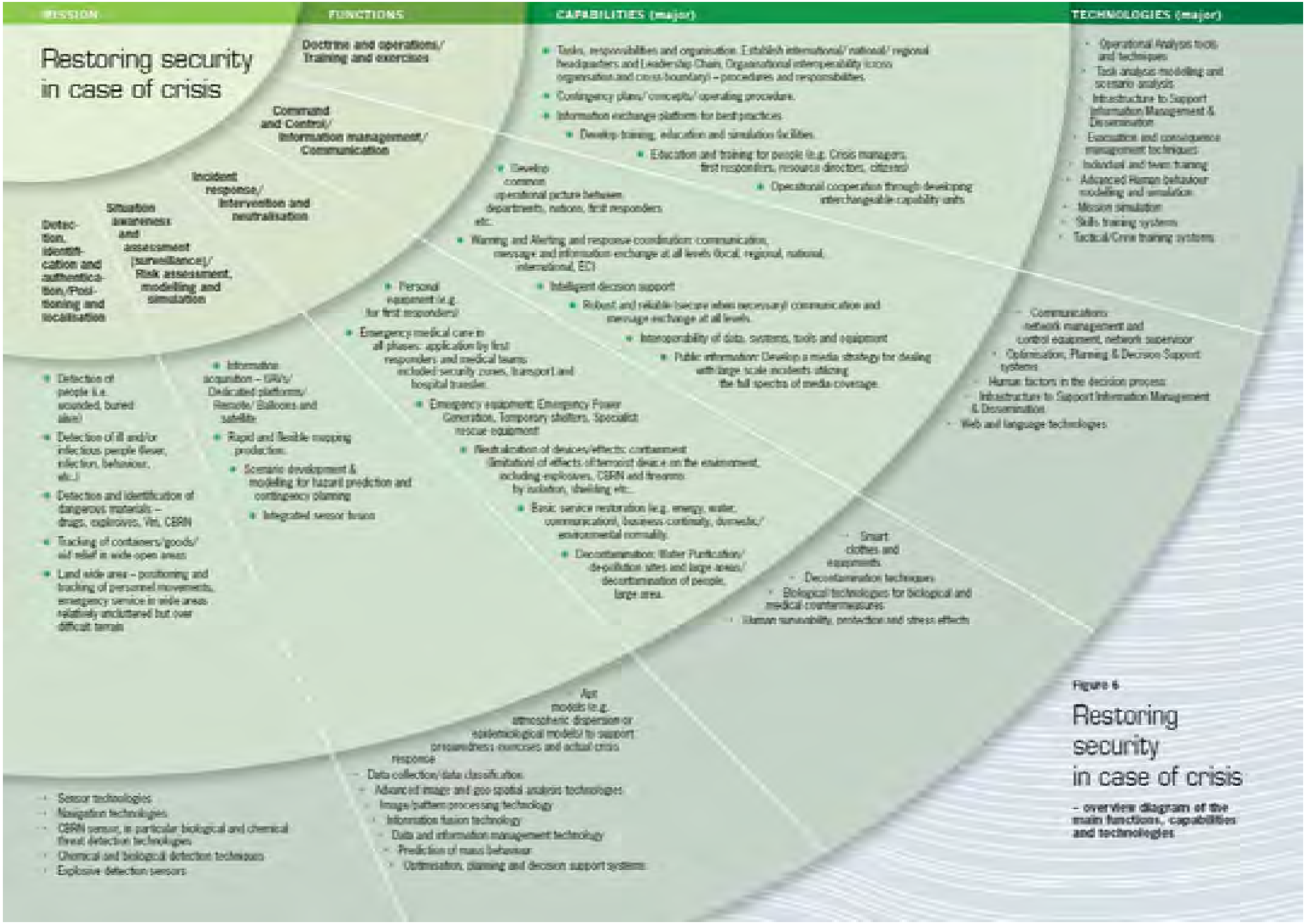
privately owned (often in accordance with the EU's internal market rules) and protected by private security, but it inevitably impacts on *public* space. From surveillance cameras to security checkpoints, the protection of critical infrastructure is having an increasing impact on the way in which the surrounding public spaces are accessed and controlled.

Residents of Hackney, London, the primary site for the 2012 Olympic Games, are rightly concerned that the legacy of the games will not just be the regeneration of so-called 'brownfield' sites, but a high-tech security blanket that is used for general policing of the local area.[241] The security budget for the Games has already risen from £600 million to £838 million (approaching one billion euros), and the security procedures for workers and residents at the new Olympics sites have already been heavily criticised.[242] Despite these concerns, too few people in Europe appear to be critically evaluating Critical Infrastructure Protection in the EU.

[240] Source: Presentation on 'Priority subjects for future research Reflections about a common understanding of security' by Alex Birsul (Siemens) to Workshop on "Security of Mass Transportation", available at: http://www.bmbf.de/pub/WS_MT_Birsul.pdf.

[241] See 'Security' posts on games.monitor.org.uk: http://www.gamesmonitor.org.uk/topic/security.

[242] Ministers plan 'Big Brother' police powers, Telegraph, 4 February 2007: http://www.telegraph.co.uk/news/uknews/1541513/Ministers-plan-Big-Brother-police-powers.html.



MISSION

FUNCTIONS

CAPABILITIES (major)

TECHNOLOGIES (major)

Restoring security in case of crisis

Doctrine and operations/ Training and exercises

Command and Control/ Information management/ Communication

Incident response/ Intervention and neutralisation

Situation awareness and assessment (surveillance)/ Risk assessment, modelling and simulation

Detection, identification and authentication/Positioning and localisation

- Tasks, responsibilities and organisation. Establish international/ national/ regional headquarters and Leadership Chain. Organisational interoperability (cross organisation and cross boundary) – procedures and responsibilities.
- Contingency plans/ concepts/ operating procedure.
- Information exchange platform for best practices.
- Develop training, education and simulation facilities.
- Education and training for people (e.g. Crisis managers, first responders, resource directors, citizens)
- Operational cooperation through developing interchangeable capability units
- Develop common operational picture between departments, nations, first responders etc.
- Warning and Alerting and response coordination: communication, message and information exchange at all levels (local, regional, national, international, EC)
- Intelligent decision support
- Robust and reliable (secure when necessary) communication and message exchange at all levels.
- Interoperability of data, systems, tools and equipment
- Public information: Develop a media strategy for dealing with large scale incidents utilizing the full spectra of media coverage.
- Personal equipment (e.g. for first responders)
- Emergency medical care in all phases: application by first responders and medical teams included security zones, transport and hospital transfer.
- Emergency equipment: Emergency Power Generation, Temporary shelters, Specialist rescue equipment
- Neutralization of devices/effects: containment (limitation) of effects of terrorist device on the environment, including explosives, CBRN and firearms by isolation, shielding etc.
- Basic service restoration (e.g. energy, water, communication), business continuity, domestic/ environmental normality.
- Decontamination: Water Purification/ de-pollution sites and large areas/ decontamination of people, large area.
- Information acquisition – UAVs/ Dedicated platforms/ Remote/ Balloons and satellite
- Rapid and flexible mapping production.
- Scenario development & modeling for hazard prediction and contingency planning
- Integrated sensor fusion
- Detection of people (i.e. wounded, buried alive)
- Detection of ill and/or infectious people (fever, infection, behaviour, etc.)
- Detection and identification of dangerous materials – drugs, explosives, Wit, CBRN
- Tracking of containers/goods/ aid relief in wide open areas
- Land wide area – positioning and tracking of personnel movements, emergency service in wide areas relatively uncluttered but over difficult terrain

- Operational Analysis tools and techniques
- Task analysis modelling and scenario analysis
- Infrastructure to Support Information Management & Dissemination
- Evacuation and consequence management techniques
- Individual and team training
- Advanced Human behaviour modelling and simulation
- Mission simulation
- Skills training systems
- Tactical/Crisis training systems

- Communications network management and control equipment, network supervisor
- Optimisation, Planning & Decision Support systems
- Human factors in the decision process
- Infrastructure to Support Information Management & Dissemination
- Web and language technologies

- Smart clothes and equipments
- Decontamination techniques
- Biological technologies for biological and medical countermeasures
- Human survivability, protection and stress effects

- Apt models (e.g. atmospheric dispersion or epidemiological models) to support preparedness exercises and actual crisis response
- Data collection/data classification
- Advanced image and geo spatial analysis technologies
- Image/pattern processing technology
- Information fusion technology
- Data and information management technology
- Prediction of mass behaviour
- Optimisation, planning and decision support systems

- Sensor technologies
- Navigation technologies
- CBRN sensor, in particular biological and chemical threat detection technologies
- Chemical and biological detection techniques
- Explosive detection sensors

Figure 6

Restoring security in case of crisis

– overview diagram of the main functions, capabilities and technologies

At first I thought the Green Zone phenomenon was unique to the war in Iraq. Now, after years spent in other disaster zones, I realize that the Green Zone emerges everywhere that the disaster capitalism complex descends, with the same stark partitions between the included and the excluded, the protected and the damned.

Naomi Klein [243]

Could an event within a single MS [Member State] require an EU response? What would be the threshold for this?

EU Council Presidency, October 2005 [244]

21 Policing the red zone: crisis management policy

Where EU Critical Infrastructure Protection policy concerns the policing of 'green zones', sites of high security that must be protected from external threats, EU crisis management policy is about the policing of the 'red zone', a metaphorical place defined not by its spatial limitations but the state of emergency that prevails within. In the climate change and international security scenario (described above) for example, Europe is the green zone, Africa the red zone. Again there is a strong link between military approaches to security crises, which have evolved as part of the EU's *external* crisis management capability, and the development of new approaches to address 'crisis' situations within Europe.

The EU's military capability has been under development for a decade. It is based, according to the European Security Strategy of 2003, on a "new strategic culture that fosters early, rapid and, when necessary, robust intervention" in 'failed states'. With the support of Turkish forces, the EU nominally reached its 'Headline Target' of 60,000 soldiers available for rapid reaction operations on 1 January 2007, though just six months later Turkey withdrew from the EU defence framework.[245]

This has scuppered the EU's ambition to maintain 15 rotating "Battlegroups" of at least 1,500 combat soldiers, of which two are ready for deployment at all times. The Battlegroups have not yet been deployed, save for an EU training exercise that saw one Battlegroup dispatched to the fictional country of Vontinalys to oversee "the first ever free elections" and counter the threat from "local mafia and offshore pirates".[246]

While the Battlegroups have remained on standby, since 2003 the EU has deployed peacekeepers and non-military (police and civilian) crisis management personnel in more than 20 operations in Africa, the Balkans, the Middle East and South-East Asia.[247] The EU also has also launched two ongoing border control missions in Moldova-Ukraine and Georgia-Southern Caucasus. The largest ongoing EU troop deployments are in support of the UN-sanctioned missions in Chad (3,700 troops), Bosnia-Herzegovina (2,900, down from 7,000) and DR Congo (2,300). The largest 'crisis management' operation is the mission in Kosovo which has seen 1,900 European police officers, judges, prosecutors and customs officials sent to support the 'rule of law' in the newly independent territory. The Kosovo deployment (initially a

[243] Klein, N. (2007) *The Shock Doctrine*. London: Penguin (page 414).

[244] *EU Critical Infrastructure Protection (CIP)*, EU Council document 13882/05, 28 October 2005: http://register.consilium.eu.int/pdf/en/05/st13/st13882.en05.pdf.

[245] Turkey, which is not an EU member state, actively *participated* in *EU military* operations between 2003 and June 2007. The refusal to institutionalise Ankara's role in EDSP decision-making and allow it to participate in the European Defence Agency, coupled with long-standing disputes with Greece over Cyprus, precipitated Turkey's withdrawal, see 'Turkey Turns Cold to European Defense: Implications for Western Security', Washington Institute, 2 June 2008: http://www.washingtoninstitute.org/print.php?template=C05&CID=2894.

[246] 'In defence of Europe', Mark Mardell's Euroblog, *BBC*, 5 June 2008: http://www.bbc.co.uk/blogs/thereporters/markmardell/2008/06/in_defence_of_europe.html.

[247] See list of EU operations, European Security and Defence Policy, Council of the EU website: http://www.consilium.europa.eu/showPage.aspx?id=268&lang=EN.

NATO mission) demonstrated that the EU is prepared to act without a Security Council mandate, despite its repeated promises to only act under the auspices of the UN.

The European Defence Agency is also apparently preparing to launch a crisis management procurement programme.[248] Yet despite the apparently rapid development of the EU military capability, the Union remains far short of its desired operational capacity of 60,000 combat ready troops, not least because of ongoing member state commitments in Afghanistan.

The external-internal security continuum

In 2000 the EU called for states to 'cooperate voluntarily to provide up to 5,000 police officers for international missions across the range of conflict prevention and crisis management operations'. In October 2003, an informal meeting of EU defence ministers proposed the creation of a 'European Gendarmerie Force' (EGF).[249] A 'Declaration of Intent' was signed by France, Italy, the Netherlands, Portugal and Spain 'in the margins' (i.e.: outside of the formal proceedings) of another informal meeting of EU Defence Ministers in September 2004. The European Gendarmerie Force was launched by the five states on 19 January 2005. The EGFs headquarters are in Vicenza, Italy, the seat of Camp Ederle, the third largest US base in Italy. The EGF is comprised of 800 officers drawn from the *Gendarmerie National* in France, *the Arma dei Carabinieri* in Italy, the *Koninklijke Marechaussée* in Holland, the *Guarda Nacional Republicana* in Portugal and the *Guardia Civil* in Spain. The EGF is ready to deploy in thirty days, with 2,300 'reserves'.[250]

According to a report by the Spanish *Institute for International and Strategic Studies*, the EGF can "execute a broad spectrum of activities related to its police duties, including but not limited to security and public order; supervision and advice to local police; public surveillance, traffic regulations, border control and general intelligence; criminal investigation, including the detection of offences, monitoring of offenders and their presentation before the appropriate court authorities; protection of assets and persons and maintenance of public order in the event of disturbances; training of police officers in line with international standards; training of instructors, mainly through cooperation programmes".[251] Romania joined the EGF in December 2008 and Turkey joined as an 'observer' in 2009.

In July 2005, a week after the '7/7' bombings in London, the EU Council called for the development of: "arrangements to share information, ensure coordination and enable collective decision-making in an emergency, particularly for terrorist attacks on more than one Member State". The EU's 'Hague programme' (on Justice and Home Affairs cooperation 2004-9) also called for the establishment of "an integrated EU arrangement for crisis management".

Under the 'Emergency and Crisis Coordination Arrangements' subsequently drawn-up by the Counter-terrorism Coordinator's office and adopted without debate by the member states, an ad hoc 'Crisis Steering Group' composed of the Presidency (as Chair), the Secretary General/High Representative (Javier Solana), the Commission and the member state(s) affected will be established to coordinate the EU's response to emergencies.[252] It will have at its disposal the 'Civil-Military Cell' of the EU Military Staff (EDSP), a dedicated 'crisis co-ordination structure' (ARGUS) currently being developed within the Commission, and a host of EU agencies including the Monitoring and Information Centre (Commission), SITCEN (the EU intelligence agency), the EU Counter-Terrorism Coordinator (CFSP), EUROPOL and other EU agencies, presumably including the EGF. In order to facilitate rapid and cohesive decision-making in times of crisis, the ad hoc Crisis Steering Group "will prepare emergency decisions for COREPER", the EU's standing decision-making body in Brussels.

These 'Emergency and Crisis Coordination Arrangements', which were adopted by COREPER without consultation of the European or national parliaments, provide for executive decision-making by member state and EU officials in Brussels in the event of a crisis. Expediency is, of course, the whole point of 'emergency powers', but in the absence of any meaningful scrutiny of such provisions, confusion reigns. What are the EU's powers and remit? Where do member state responsibilities end and EU responsibilities begin? And what role will EU military staff and agencies play in an emergency or crisis? These are questions that should be answered before these new arrangements are implemented, not after the event.

Lessons from Katrina?

In the wake of Hurricane Katrina, the concern was how US military, law enforcement and emergency response agencies had acted, and the way in which race and class had shaped their actions.[253] The well-televised government response to Hurricane Katrina appalled viewers around the world. The military were sent in to 'secure' poor areas as people died in their homes and starved and froze in a sports arena; the federal government and the newly created Federal Emergency Management Agency (FEMA) took days to respond.

[248] See EDA website: http://www.eda.europa.eu/ccm.aspx.

[249] 'Five countries establish a European paramilitary police force'. *Statewatch news online*, September 2004: http://www.statewatch.org/news/2004/sep/06paramilitary.htm.

[250] See European Gendarmerie Force website: http://www.eurogendfor.org/.

[251] 'The New European gendarmerie Force', Analysis by Enrique Esquivel Lalinde, 9 May 2005, *Real Instituto Elcano*: http://www.realinstitutoelcano.org/analisis/735.asp.

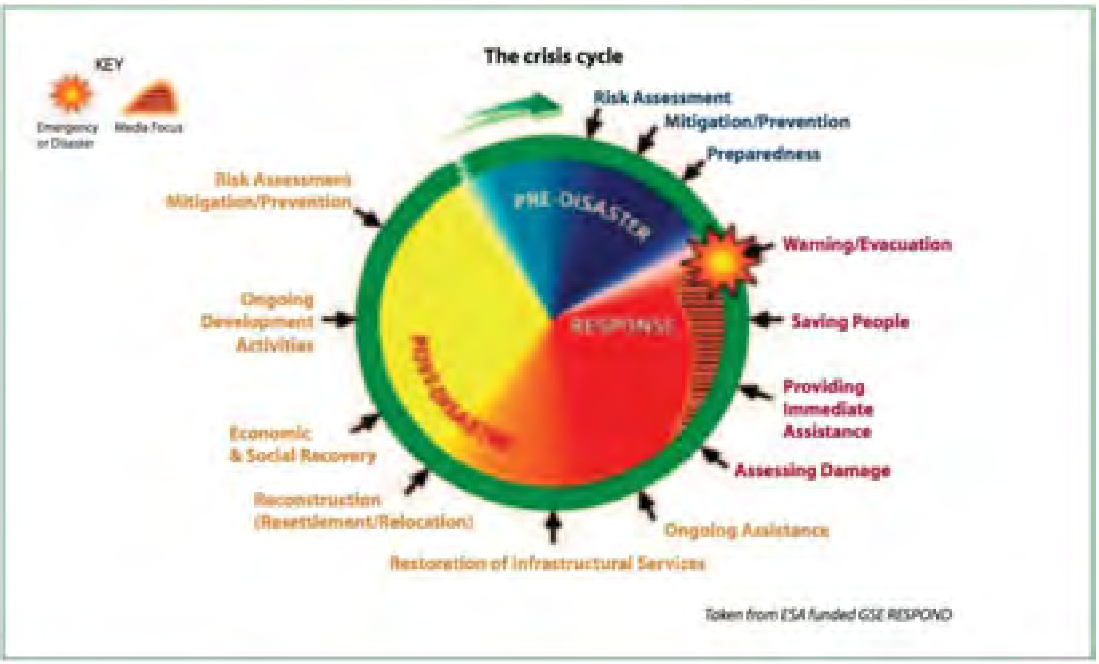
[252] 'EU emergency and crisis co-ordination arrangements', unreferenced/undated document available at: http://consilium.europa.eu/uedocs/cmsUpload/WEB15106.pdf.

[253] See Reifer, T., "Blown Away: U.S. Militarism & Hurricane Katrina' in Hillary Potter, ed., *Racing the Storm: Racial Implications and Lessons Learned from Hurricane Katrina* Lexington Books, forthcoming.

As Naomi Klein observed: “an already divided city was turned into a battleground between gated green zones and raging red zones”. Was this just bad government by an incompetent or overstretched administration (mainstream news organisations openly commented that they had seen better disaster relief in the Third World) or did it represent a deeper transformation, a new kind of policing for a spatially and racially segregated era of militarist population management? [254]

Within the ESRP, crisis management and critical infrastructure protection has already taken a distinctively militarist turn. This is not to say that this will inevitably lead to heavy-handed militarist deployments in domestic European crisis scenarios, though it certainly enhances this prospect, but rather it raises a set of important questions about the way in which states respond to emergencies and disasters. Chief among these concerns is the question of accountability. As the USA’s Federal Government Accountability Office found in May 2006: “Despite a massive deployment of resources and support from both military and civilian agencies, many have regarded the federal response as inadequate. As local, state, and federal governments responded in the days following Katrina, confusion surfaced as to what responsibilities the military has and what capabilities it would provide in planning and responding to a catastrophic event”.[255]

It would be interesting at least to compare the development of the EU’s fledgling crisis management capability programme with the changes in the federal structure of US government that many blame for the failings after Katrina, but again, no-one seems to be critically evaluating EU crisis management policy.



Taken from ESA funded GSE RESPOND

Cashing in on crisis: the ‘disaster capitalism’ cycle

[254] This question is beyond the scope of this report, but those who have read the *‘Shock Doctrine’* will have little trouble relating the failed state response to the emergence of a powerful disaster capitalism complex. See Klein, N. (2007) *The Shock Doctrine*. London: Penguin.

[255] *Hurricane Katrina: Better Plans and Exercises Needed to Guide the Military’s Response to Catastrophic Natural Disasters*, GAO Report to the Congressional Committees, United States Government Accountability Office, May 2006 (GAO-06-643), available at: http://www.gao.gov/new.items/d06643.pdf.

Crisis management and security research

Working Group 4 of the European Security Research and Innovation Forum is led by the German Federal Government Office for Population Protection and Disaster Relief (BBK), with *Frequentis*, Europe's self-proclaimed "number one provider" of control centre solutions, appointed as *rapporteur*. WG4 will report on Europe's preparedness to respond to man-made and natural catastrophes through internal and external 'risk and crisis management'. WG4's mandate includes "Computer assisted exercises for crisis and emergency management", integrated Early Warning Systems, emergency communication systems, civil military cooperation, civil-military emergency planning and intervention training.

As with other thematic areas of the ESRP, some of the projects funded to date are entirely civil in their scope, others draw overtly on militarist technologies, and many are a combination of the two. Under the PASR the EU funded the MARIUS project on the development of 'mobile autonomous reactive information systems' for 'urgency situations', led by EADS (apparently involving the deployment of military command helicopters); the TIARA project on the creation of a European network for reaction to radiological incidents; the BIO3R project, featuring *Sagem*, TNO and FOI, on threats from and responses to the use of biological weapons; the AEROBACTICS project on microbial dispersion models in cases of biological attacks; and the CRIMSON project on virtual simulations of crisis situations for training purposes.[256]

The latest security technology projects funded under the ESRP concern two main areas. The first is crisis management communication. R&D here includes the CHORIST project (FP6) on 'environmental catastrophes', and the BESECU project (ESRP/FP7), which asks whether 'people from different countries behave differently in a crisis' and if "culture and ethnicity play a role in determining how people respond in disasters". The findings will give the EU "confidence to predict how people will behave in emergencies, knowing that [its] computer models are based on how real people behave".[257] The second main focus area for the ESRP is the civil emergency services, what the Homeland Security industry calls 'first responders'.[258]

While the EU security research programme is as yet limited to communications systems, EADS has developed a new type of disinfection system that offers "significantly improved possibilities for countering epidemics and biological weapons". EADS' TransMADDS (Transportable Modular Aerosol-based Decontamination and Disinfection System) has demonstrated "a hitherto unequalled effectiveness against pathogenic germs during two major test campaigns" carried out by the UK Ministry of Defence. It is claimed that "the system can also be deployed to neutralise nuclear, biological and chemical weapons… as well as in civil emergencies, e.g. for disinfecting hospitals in the event of a 'superbug'". "Epidemics present a considerable danger to everybody," explained Bernd Wenzler, CEO of Defence Electronics (part EADS Defence & Security). "This disinfection system can make a substantial contribution to preventing the spread of infectious diseases… our new product is an ideal example of how modern technologies can be used for increasing the safety of all of us in everyday life".[259] It seems that the defence and security industry is determined to cash-in on every potential area of well-being.

[256] Crisis management projects funded under the EU's framework research programmes include OASIS (FP6) on generic research into crisis management, SPADE (FP6) on responses to air transport emergencies, and SICMA (FP7/ESRP) on the simulation of crisis management activities.

[257] These include the €15 million EULER project, led by Thales (and featuring EADS, Astrium, Selex, Elsag Datamat and Telespazio), which will equip future EU security and crisis management missions with 'European software defined radio for wireless joint security operations'; the CITRINE project, on 'Common Intelligence and Traceability for Rescues and IdentificatioN opErations', also led by Thales (and also featuring EADS and Finmeccanica) which will provide 'real-time information systems for rescue missions'; SERICOM, led by Qinetiq (the now privately owned UK defence research agency), which promises 'seamless communication for crisis management'; the COPE project which aims to improve civil crisis management through new technologies geared toward 'Common Operational Picture Exploitation'; INFRA, led by Israel's Athena GS3 Security Implementations Ltd., which is developing broadband communications networks for critical infrastructure such as "autonomous wireless broadband in underground tunnels and concrete buildings" and novel applications for 'first responder teams' (including thermal imaging, fibre optic sensors and indoor navigation).

[258] ESRP projects looking at the needs of the emergency services include: the CAST project, which will provide a 'comparative assessment of *security-centred* training curricula for first responders on disaster management in the EU' (emphasis added); the FRESP project, led by the Royal Military Academy of Belgium, which is developing a 'gas mask canister and protective hood' using 'nanoporous' absorbent materials to provide respiratory protection to 'first responders' to CBRN attacks, and the NMFRDISASTER project, which will establish a network of civilian researchers, including the Al Quds University of Palestine, to examine the 'Needs of Medical First Responders in Disasters'.

[259] 'EADS Successfully Tests New Disinfection System for Countering Epidemics', ASD-Network, July 2009: http://www.asd-network.com/press_detail_B.asp?ID=21699&NID=283303.

The protesters paid a high price for disturbing the sleep of Jacques Chirac and Tony Blair. The Dutch police arrested 143 of them outside the hotel, following a further 300 arrested the day before at a squat near police headquarters and another 150 at sundry locations in Amsterdam. All were entirely peaceful (albeit noisy), but all were charged under legislation criminalizing 'membership of an organization that aims to commit crimes' – apparently the model for the overbroad EU Joint Action agreed the following year. Over a hundred were immediately deported before they could challenge their detention in court (a spectacular breach of EC free movement law); some were deported without their belongings; the Danish consul was barred from visiting the detained Danes; some were sent back to Denmark in a military aircraft with a Dutch fighter-bomber escort; and information on those charged was handed over to at least some police intelligence agencies – despite the gross abuse of prosecutorial discretion in laying charges. It is not known how many were entered onto the EU's various databases or circulated within the ad hoc meetings of EU public order specialists. Those not expelled were held for three days and then released, some alleging mistreatment by the police and denial of their right to make a phone call; none was ever convicted. But by then the event they were demonstrating against was over. Well-rested Heads of State and Government had reached political agreement on the text of the Amsterdam Treaty. And so was born the 'Area of Freedom, Security and Justice'.

Steve Peers, EU Justice and Home Affairs Law (2000)[260]

22 The policing of protest: a full spectrum dominance case study

During the spring of 2009, a wealth of surveillance footage produced by mobile phone cameras brought public order policing in Europe into sharp relief. In London, G20 protesters were charged by baton-wielding policemen. Ian Tomlinson, a newspaper seller in the City, died of internal bleeding after being pushed to the ground by police officers as he was returning home from work. In Moscow, police and skinheads attacked a gay rights demonstration, and in Barcelona, the *Mossos d´Esquadra* meted out the same kind of punishment to striking students in the University of Barcelona and rowdy football fans celebrating in *Las Ramblas*. Allegations of serious police brutality against protesters may be rare or frequent, depending on the European country in question, but is there a link between the policing on the ground and the measures that have been adopted by the EU?

The policing of the 1997 'Eurotop' demonstrations in Amsterdam (described on the left by Professor Peers) set the tone for the EU police cooperation that followed. Under EU public order legislation adopted that year member states are obliged to share information on all large groups entering another member state to attend any event with a public order dimension, such as "sporting events, rock concerts, demonstrations and road-blocking protest campaigns". This includes the "fullest possible" details regarding: (a) the group in question: overall composition, nature of the group (whether aggressive and whether there is any chance of disturbances); (b) routes to be taken and stopping-off points; (c) means of transport; (d) any other relevant information.[261] It may seem astonishing, but attending a football match or a protest like 'Make Poverty History' now entails the possibility of a European police record.

Following the large protests against the EU in Gothenburg and the G8 in Genoa in 2001, where protesters were shot by police (and subject to repeated police attack in the case of Genoa),[262] the EU drew up its own operational rules for dealing with international protests and security at international summits. The 2001 EU 'manual on public order at international events' included information on the gathering of intelligence, how to stop and turn back 'suspected' protesters at EU borders and details on how to expel protesters in an 'efficient' manner if they are detained.[263]

As Tony Bunyan, Director of Statewatch, has suggested: since then a pattern has emerged within which EU citizens wishing to exercise their democratic right to protest – and to attend cross-border protests – are confronted by increasingly para--military style policing, denial of entry, preventive detention, the control and dispersal of protests and even expulsion from the country, sometimes with a lengthy re-entry ban.[264]

[260] Peers, S. (2000) *EU Justice and Home Affairs Law*. London: Longman (page 225).

[261] *Joint Action 97/339/JHA on cooperation in law and order* (OJ 1997 L 147/1).

[262] 'An Italian view of "public order policing" Italian style', Statewatch bulletin vol 11, no ¾: http://www.statewatch.org/news/2002/jul/08genoa.htm.

[263] *Council resolution of 6 December 2001, concerning a handbook with recommendations for international police cooperation and measures to prevent and control violence and disturbances in connection with football matches with an international dimension, in which at least one Member State is involved*, available at: http://europa.eu/cgi-bin/eur-lex/udl.pl?REQUEST=Seek-Deliver&COLLECTION=lif&SERVICE=all&LANGUAGE=en&DOCID=302G0124(01).

[264] 'We're not the only ones to stifle dissent', *Guardian*, 8 May 2009: http://www.guardian.co.uk/commentisfree/libertycentral/2009/may/08/civil-liberties-protest. The principle of 'free movement' is supposedly fundamental to the EU, with the Schengen Agreement supposed to ensure free movement for the people of the Schengen member states across national borders. But the Schengen rules allow the member states to re-introduce national border controls "where public policy or national security so require", a proviso that was first invoked by Belgium when it sealed its borders in January 2000 for an immigrant regularisation programme. France and Spain then reintroduced border controls to prevent protesters attending a planned demonstration against the EU at the December 2000 Biarritz summit. This exceptional restriction of free movement and the right to freedom of association then became the rule as states re-imposed border controls to prevent protesters attending demonstrations on at least 15 occasions in the next two years.

There has also been a concerted attempt within EU policy-making circles to equate protest with terrorism, whether by painting protesters as terrorists, or using terrorism laws and powers against activists and protest groups.[265]

In 2004 the EU produced a second manual on the prevention of terrorist attacks at the Olympic Games and comparable sporting events. The model of security it adopted was much like the approach to protests – operational planning, threat assessment, risk analysis, border control, preventive measures, criminal investigations and prosecutions. In 2006, the two EU security manuals were merged into a single 'handbook' on 'the security (both from a public order point of view as well as counter-terrorism) of all major international events', be they 'political, sporting, social, cultural or other', conflating the threat from protest, terrorism and so-called mass events, and proposing a singular, integrated response.[266]

Public order policing on the ground: the G8 in Germany

It is instructive to examine the recent 'operational planning' for the policing of large-scale international protests in Europe. This begins well in advance of the actual demonstration or protest, with the surveillance of the protest organisers, police raids on their homes and offices and the seizure of computers and mobile phones. Independent media organisations and protest website publishers are also routinely targeted before and during protests. Protesters are filmed, photographed and routinely stopped-and-searched, with police and paramilitary units ready to step-in at the first sign of 'trouble'. After the protest, this data is analysed, retained and exchanged among police agencies.

At the G8 summit in Heiligendam (Germany), in June 2007, the police used military surveillance equipment including satellites and widespread interception of telecommunications. One month before the summit, 1,000 police raided the homes of 40 activists. They took personal computers, address books and even cigarette butts for so-called 'scent samples' (this was a technique developed by the East German Stasi secret police to track down dissidents with dogs). The raids were authorised under Article 129a of the German Criminal Code (the 'formation of a terrorist organisation') but were later declared unlawful by the Federal Courts. Just before the actual summit, an independent media bus was confiscated by German police, part of a corps of 17,800 police and 2,000 military personnel drafted in for the event (a deployment that also appeared to violate Germany's constitution). Some 1,474 preliminary investigations were initiated against protesters by German public prosecutors; the overwhelming majority of charges were dropped.

The German Airforce contributed to a climate of intimidation by flying Tornado fighter planes over activist camps located near the official summit under the German 'safe' legal limit of 150 metres. Ultimately, the protesters, many of whom had travelled hundreds or thousands of miles to show their dissent, could not actually get anywhere near the event against which they were protesting, a summit which was held in what the German authorities called the 'red zone'. Around this zone they erected a 12 km fence topped by razor-wire, surrounded by a second zone of 10km in which all assemblies were prohibited.

Public order and EU security research

The EU has funded consecutive projects to 'Coordinate National Research Programmes and Policies on Major Events Security' (EU-SEC and EU-SECII) over the past five years. Like EU policies on the policing of protests, these projects are geared to 'harmonisation' and 'best practice'. The EU-SEC project, funded under the FP6 programme, was coordinated by the United Nations Interregional Crime and Justice Research Institute (UNICRI, which describes itself as a "security governance/ counter-terrorism laboratory") and included ten EU Member States police and interior ministries and EUROPOL. Its stated aim was to define 'harmonised' EU research needs and produce "a strategic research roadmap to orientate the European research agenda and the related allocation of funds".[267]

EU-SEC was also very much an operational 'research project'. It contributed to the establishment of an 'International Permanent Observatory on Security during Major Events' (IPO) at UNICRI, and a 'Security Planning Model', a security toolkit for national authorities planning major events.[268] EU-SEC also produced a case study on 'Private Public Partnerships in the Research on Security at Major Events'.[269] A handbook for G8-countries dealing with protests was also produced by UNICRI, together with "innovative research into intelligence sharing and cooperation in the European Union to combat terrorism". At the end of the three-year project the EU-SEC Consortium launched its own call for proposals to the "electronic tools" for information sharing amongst security planners across the EU and a European Major Events Register (EMER).[270] These initiatives "will also entail benefits for the European security technology market", confirmed the call.

EU-SEC II is funded under the ESRP/FP7, and is again led by the United Nations Interregional Crime And Justice Research Institute, with the project widened in geographical scope to include 20 EU member state police forces and interior ministries, along with EUROPOL. The projects will continue the "harmonization of national research policies" and set out the "needs and priorities among its partners, which constitute the demand side of the EU technology market".[271]

[265] In 2002, the Spanish Presidency of the EU produced a draft recommendation on the exchange of information about protesters which claimed that: *"The [EU Terrorism] working party has noticed a gradual increase, at various EU summits and other events, in violence and criminal damage orchestrated by radical extremist groups, clearly terrorising society. These acts are the work of a loose network, hiding behind various social fronts, by which we mean organisations taking advantage of their lawful status to aid and abet the achievement of terrorist groups aims"* (EU Council document 5712/02, 29 January 2001). See further: 'Exchanging information on terrorists or protesters?', *Statewatch news online*, April 2003: http://www.statewatch.org/news/2003/apr/16spainterr.htm.

[266] *Security handbook for the use of police authorities and services at international events*, EU Council document 15226/1/06 REV 1, 22 December 2006, available at: http://www.statewatch.org/news/2007/jan/eu-sec-handbook-int-events.pdf.

[267] See 'EU-SEC manual' (2007), available at: http://www.unicri.it/news/0807-1_EU-SEC_II/eusec_080707_manual.pdf.

[268] *IPO Programme*, UNICRI website: http://www.unicri-ipo.org/.

[269] 'Private Public Partnerships in the Research on Security at Major Events. A Case Study', available at: http://www.unicri.it/news/0807-1_EU-SEC_II/eusec_080707_ppp_cs.pdf.

[270] 'European Major Events Register (EMER) & Specialist Technical Equipment Pool (STEP). Database Scheme Proposal', available at: http://www.unicri.it/news/0807-1_EU-SEC_II/eusec_080707_emer_step.pdf.

[271] *EU SEC II*, UNICRI website: http://lab.unicri.it/eusecII.html.

Meanwhile, across the Atlantic…

The Pentagon's Joint Non-Lethal Weapons Directorate has come up with its own solution for "non-lethal methods of crowd and mob dispersal, checkpoint security, perimeter security, area denial, port protection, infrastructure protection and clarification of intent (identifying combatants from non-combatants)".[272] The 'Joint Silent Guardian' system is a non-lethal, directed energy weapon developed by *Raytheon*.[273] With a range of more than 250 metres, the Silent Guardian has now been mounted on military vehicles for the purposes of crowd control. According to *Global Research*, the high power microwave (HPM) device heats water in a person's outer layers of skin to the point of pain. Tests are said to have shown that the microwaves can reach through cracks in and around concrete walls and even through car windscreens.[274]

Raytheon describes the Silent Guardian system as "a revolutionary less-than-lethal directed energy application that employs millimeter wave technology to repel individuals or crowds without causing injury" and promotes the weapon as a 'protection system' that can "de-escalate aggression during law enforcement, checkpoint security and peacekeeping missions". Silent Guardian is controlled by an "easy-to-use joystick control with auto-tracking capabilities" that allows the 'precise targeting of specific individuals'. The U.S. National Institute of Justice is also promoting the use of so-called 'Active Denial System' technology for use in correctional facilities (prisons etc.).[275]

Others are less enthusiastic about the new technology. According to a 2008 report by Deutsche Stiftung Friedensforschung (DSF, the German Foundation for Peace Research), the weapon could cause serious or even lethal injuries.[276] The technology has already been tested on hundreds of volunteers. In order to produce pain while preventing burn injuries, the power and duration of microwave emitted by the 'trigger event' is controlled by a software program. DSF calculates that with the highest power setting, second- and third-degree burns with complete dermal necrosis (skin cell death) will occur after less than 2 seconds. Moreover, even at low power and duration settings there is the possibility for the operator to re-trigger immediately. According to an official accident report published by *Wired*, at least one volunteer has required treatment in a hospital burns unit.[277] Steve Wright has suggested: "if this system is ever allowed to be deployed in an algorithmic format as a self targeting pain beam, we are entering a new era of mass human rights violations."[278]

'Less lethal weapons' appeared in the draft report of the European Security Research Advisory Board, obtained by the author, but were omitted from the final report.[279] However, many of the 'key players' from the 'supply-side' of the European Security Research Programme are also part of the European Working Group on Non-Lethal Weapons, which "supports the development and use of technologies, devices and tactics which are intended to preserve life whilst enabling lawful and appropriate use of force in response to threats, be they individual or crowd based".

In 2006, the United States European [Military] Command showcased its non-lethal weapons program during a summit and capabilities exercise at a German base.[280] The EU Defence Agency has since installed a Non-Lethal Capabilities Project Team and awarded a contract to Thales Electron Devises to conduct a 'mapping' exercise on "directed energy capabilities development and their growth potential with focus on EDA".[281]

There are currently no international agreements restricting the development and proliferation of microwave-based weapons technology, save for an additional protocol to the Convention on Certain Conventional Weapons (CCW) that prohibits laser weapons intentionally designed to blind. According to a report by the University of Bradford, military establishments are keen to resist additional constraints on the development and use of 'non-lethal weapons' (NLWs). NATO itself has stated that "In order to ensure that NATO forces retain the ability to accomplish missions, it will be important that nations participating in NATO operations remain vigilant against the development of specific legal regimes which unnecessarily limit the ability to use NLWs".[282]

[272] *Frequently Asked Questions Regarding the Active Denial System*, Pentagon Joint Non-Lethal Weapons Directorate website: https://www.jnlwp.com/misc/faq/ADS%20FAQs%20September%202008.pdf.

[273] *Silent Guardian™ Protection System: Less-than-Lethal Directed Energy Protection*, Raytheon website: http://www.raytheon.com/capabilities/rtnwcm/groups/rms/documents/content/rtn_rms_ps_silent_guardian_ds.pdf.

[274] Curbing Social Protest in America: Microwave "Non-lethal" Weapons to be used for "Crowd Control" Just in Time for the Capitalist Meltdown: Army, Justice Department to Field 'Pain Ray', *Global Research*, October 14, 2008 http://www.globalresearch.ca/index.php?context=va&aid=10564.

[275] *Active Denial System Deters Subject Without Harm*, National Institute of Justice, US Department of justice website: http://www.ojp.usdoj.gov/nij/topics/technology/less-lethal/denial-system.htm

[276] Altmann, J. (2008) Millimetre Waves, Lasers, Acoustics for Non-Lethal Weapons? Physics Analyses and Inferences, Deutsche Stiftung Friedensforschung, available at: http://www.bundesstiftung-friedensforschung.de/pdf-docs/berichtaltmann2.pdf.

[277] Pain Ray Test Subjects Exposed to 'Unconscionable Risks', *Wired.com*, 14 October 2008: http://blog.wired.com/defense/2008/10/pain-ray-accide.html.

[278] Wright, S. (2006) 'Report. Sub-lethal vision: varieties of military surveillance technology', *Surveillance & Society*, 4(1/2): 136-153, available at: http://www.surveillance-and-society.org/Articles4(1)/sublethal.pdf (page 147).

[279] Unpublished 'final draft' report of the European Security Research Advisory Board, v.2.7, dated September 2006 (page 52)).

[280] *U.S. European Command Highlights Non-Lethal Alternatives*, US Depart of Defense website: See http://www.defenselink.mil/transformation/articles/2006-06/ta062206b.html. "We have conducted small scale demonstrations before, but this is the first time we conducted a comprehensive non-lethal weapons event for the European Command staff, component staff members and our European and African allies and partner nations", said a spokesperson, "It is an important demonstration of our interoperability and cooperation".

[281] See Contract 18, 'Annual List of Contractors – 2007' (2008/S 62-083197), *European Defence Agency* website: http://www.eda.europa.eu/procurement.aspx.

[282] Davison, N (2007) *The Contemporary Development of 'Non-Lethal' Weapons*, Bradford University Non-Lethal Weapons Research Project (page 37), available at: http://www.bradford.ac.uk/acad/nlw/research_reports/docs/BNLWRPResearchReportNo8_Mar06.pdf.

PART VII: FULL SPECTRUM GOVERNANCE

When people started to worry about asymmetric attacks and chemical warfare, what happened was that military technology was put in the hands of the police.

Bill Mawer, Head of strategy and technology, Smiths Detection [283]

23 Interoperability

'Interoperability' could be placed among a growing collection of 'weasel words' that Deirdre Curtin and others have identified in the discourse on the EU.[284] Words like 'governance' and 'legitimacy', which mean many things to European studies students, and EU officials, but very little to the world beyond. The Oxford English Dictionary describes interoperability as "(of computer systems or software) able to exchange and make use of information". Wikipedia offers a richer interpretation, defining interoperability as "a property referring to the ability of diverse systems and organizations to work together (inter-operate)", adding that the "the term is often used in a technical systems engineering sense, or alternatively in a broad sense, taking into account social, political, and organizational factors that impact system to system performance". In a European governmental context, interoperability is said to refer "to the collaboration ability of cross-border services for citizens, businesses and public administrations".[285]

The 'principle of interoperability' was first applied by the EU to the 'trans-European high-speed rail system' in the 1990s to harmonise infrastructure and facilitate cross-border train services.[286] It has since become a widely used principle and driving force in European integration. It may also come to be seen as an important process of globalisation in its own right. In the 'First Pillar' (internal market and social policy), the EU now has a dedicated programme on the 'Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens' (IDABC). IDABC issues recommendations, develops solutions and provides services that enable national and European administrations to communicate electronically and provides financing to projects addressing European policy requirements.

The drive for interoperability in EU Justice and Home Affairs (JHA) policy began in 2002, with the formation of an 'Ad Hoc Group on Third Pillar Information Systems' to explore the potential 'synergies' between the EU's SIS II, EUROPOL, CIS and EURODAC systems (described above). The group suggested two possible options: either (a) merge the existing systems in a single "Union Information System"'– which appeared both unlawful and technically impossible, or (b) harmonise 'data formats and their respective access rules… while allowing current systems to evolve to provide interoperability'.[287]

The EU counter-terrorism plan adopted after the Madrid bombings in March 2004 called on the European Commission to "submit proposals for enhanced interoperability" and "explore the creation of synergies between existing and future information systems". The subsequent Commission Communication defined interoperability as the "ability of

[283] Cited in 'Critical Infrastructure' dossier, *euractiv.com*: http://www.euractiv.com/en/security/critical-infrastructure/article-140597.

[284] Cutrin D. (2006) 'European Legal Integration: Paradise Lost?' in Curtin et al (eds) *European Integration and Law* (pages 1-54). Amsterdam: Intersentia.

[285] 'Interoperability', *Wikipedia*: http://en.wikipedia.org/wiki/Interoperability.

[286] *Council Directive 96/48/EC of 23 July 1996 on the interoperability of the trans-European high-speed rail system* (OJ 1996 L 235/6).

[287] *Report of the ad hoc group for the study of the 3rd pillar information systems*, EU Council 8857/03, 6 May 2003, available at: http://www.statewatch.org/news/2008/aug/eu-databases-8857-03.pdf.

IT systems and of the business processes they support to exchange data and to enable the sharing of information and knowledge".[288] It also described interoperability as a "technical rather than a legal or political concept"; a principle that is "disconnected from the question of whether the data exchange is legally or politically possible or required".

In the same breath, however, the Commission introduced the 'principle of availability', under which data held by law enforcement agencies in one member state should, in principle, be made available to all the others (a kind of 'free market' for police data), setting out the desired EU legal and political framework. The aforementioned Prum Treaty of 2005 (which was signed by seven member states and then extended across the EU) sought to implement the principle of availability by creating new automated data comparison systems that will link the DNA and fingerprint databases of the member states.

This kind of interoperability is very much about the harmonisation of access to data, which is seen as preferable to the creation of vast new databases. In practice, of course, the centralisation of access amounts to the same thing: a breaking down of the firewalls between government datasets, the creation of multipurpose surveillance systems, and an erosion of the laws and principles of data protection that currently act as barriers to police access or exchange of data (for example, the principles of 'purpose limitation', confidentiality and the bar on the onward exchange of data). The principle of 'probable cause', the idea that people should only be subject to law enforcement attention on the basis that they are suspected of committing an actual crime, is also undermined by the principles of interoperability and availability.

In June 2009, the European Commission proposed the creation of an EU Agency for the operational management of large-scale IT systems, arguing that the current situation "does not allow the full exploitation of the synergies between these systems and results in higher costs, less efficiency and overlaps".[289] The "dedicated, specialised Agency will be able to achieve important synergies and economies of scale". The new Agency will be assisted by advisory groups composed of national experts and should take over the operational management of SIS II, VIS and EURODAC in 2012. As *The Register* suggested, "Whatever the system does to make EU citizens more secure, it seems bound to benefit a number of different constituencies. Some governments will love the ability to track people within the community. IT vendors will love the prospect of massive pan-European systems and their associated budgets. And hackers will love the prospect of a one-stop shop for Euro ID information".[290]

From interoperable data to integrated security services

In a security context, 'interoperability' also implies enhanced cooperation between police, immigration, intelligence, military and government agencies, as well as with private sector security organisations. To this end, the EU has come up with yet another new principle, 'convergence', described as "the pooling of sovereignty" underpinned by legal harmonisation and the provision of standard training, equipment and information technology across all EU law enforcement agencies (see the 'Stockholm Programme', below). Instead of the classic 'separation of powers' and agencies, interoperability and convergence implies a new networked system of law enforcement in which executive organs will play a leading role, and where traditional systems of checks and balances will no longer apply.

Working Group 1 has the broadest of the ESRIF mandates: 'Security of the citizens' [sic]. This includes improved technologies in the following areas: "terrorism and organised crime, protection of soft targets (e.g. large scale events, crowds), urban security, civil protection, public health security (pandemics), cyber crime, on-line investigations, public-private trusted information exchange models, financial threats (e.g. currency manipulations, stock value manipulations) [and] non-proliferation of WMD and SALW [small arms and light weapons]".

The *rapporteur*, responsible for producing the findings of WG1, is *Sagem Défense Sécurité*, a company whose Global mission is to provide "a cross-fertilization between solutions that belong to apparently different worlds: multibiometrics (fingerprint technologies) for making transportation more secure, optronics (usually military oriented) applied to homeland security, inertial navigation applied to unmanned air vehicles etc".[291]

WG 10 of ESRIF, meanwhile, is tasked with the 'governance and coordination' of 'security research strategy and implementation between the European Union and Member States and relevant institutions or organisations, such as ESA [the European Space Agency], EDA [the European Defence Agency] and NATO', with the UK Royal United Services Institute appointed *rapporteur*.

[288] *Commission Communication on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs*, COM (2005) 597 final, 24 November 2005: http://www.eurowarrant.net/documents/cms_eaw_id1623_1_52005DC0597.pdf.

[289] *Legislative package establishing an Agency for the operational management of large scale IT systems in the area of freedom, security and justice*, European Commission, COM(2009) 292 final, 24 June 2009: http://www.statewatch.org/news/2009/jun/eu-com-it-agency-proposal-292-09.pdf; Proposal for a Regulation establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, European Commission, COM(2009) 293 final, 24 June 2009: http://www.statewatch.org/news/2009/jun/eu-com-it-agency-prop-regulation-293-09.pdf; Proposal for a Council Decision conferring upon the Agency established by Regulation XX tasks regarding the operational management of SIS II and VIS in application of Title VI of the EU Treaty, European Commission, COM(2009) 294 final, 24 June 2009: http://www.statewatch.org/news/2009/jun/eu-com-it-agency-prop-op-decision-294-09.pdfhttp://www.statewatch.org/news/2009/jun/eu-com-it-agency-prop-regulation-293-09.pdf.

[290] 'EU plans giant IT network for "freedom, security and justice', *The Register*, 25 June 2009: http://www.theregister.co.uk/2009/06/25/eu_it_system/.

[291] See SAGEM website: http://www.sagem-ds.com/eng/site.php?spage=02000000.

I see a shift in emphasis and an increasing balance between what we see as defence and homeland security.

'Security' is a more politically acceptable way of describing what was traditionally defence.

Tim Robinson, senior Vice-President of Thales' Security Division and former chairman of ESRAB [292]

24 Expanding the concept of national security

The trajectory of the European Security Research Programme and the principles of 'interoperability' and 'convergence' are increasingly embedded in new ways of thinking about security at the nation-state level, particularly among the EU's powerful member states. Despite the divisions over the war in Iraq and tensions over the future relationship between the EU and NATO, it is the similarities in the national security and defence strategies of the UK, France and Germany that provide the basis for the kind of European integration described in this report. Through the EU, their vision for global security in the 21st century is steadily being uniformly imposed across Europe.

Following the terrorist attacks of 9/11, the UK Ministry of Defence reviewed its ability to respond to the particular challenges raised by international terrorism by producing a 'New Chapter' to the Strategic Defence Review of 1998. 'Delivering Security in a Changing World', the UK Defence White Paper of 2003 argued for a radical restructuring of traditional defence to "meet the new threats and challenges of international terrorism, the proliferation of weapons of mass destruction, and weak and failing states".[293] The EU Security Strategy of 2003 called for the development of EU military and non-military capabilities to achieve the same ends.[294] The UK White Paper also recognised "the valuable contribution Defence could make to Home defence and security".

In 2006, Germany produced a White Paper on Security Policy to meet the twin objectives of homeland security ("the sovereignty and integrity of German territory") and a proactive foreign policy that "confront[s] global challenges, above all the threat posed by international terrorism and the proliferation of weapons of mass destruction".[295] These objectives are integral to a policy of further economic globalisation ("free and open world trade as the basis for our prosperity"). "Security cannot be guaranteed by the efforts of any one nation or by armed forces alone", concludes the German White Paper, "Instead, it requires an all-encompassing approach that can only be developed in networked security structures and within the context of a comprehensive national and global security philosophy".

The first National Security Strategy of the United Kingdom published in March 2008, subtitled "security in an interdependent world", took the same approach.[296] In addition to the "threats and risks" of terrorism, nuclear proliferation and WMD, global instability, conflict, failed and 'fragile' states, the UK strategy addresses "transnational crime, pandemics and flooding – not part of the traditional idea of national security, but clearly challenges that can affect large numbers of our citizens, and which demand some of the same responses as more traditional security threats, including terrorism".

[292] Source: *Euractiv* website: http://www.euractiv.com/en/security/critical-infrastructure/article-140597.

[293] *Delivering Security in a Changing World: Defence White Paper 2003*, Secretary of State for Defence, December 2003 (Cm 6041-I), available at: http://www.mod.uk/NR/rdonlyres/051AF365-0A97-4550-99C0-4D87D7C95DED/0/cm6041I_whitepaper2003.pdf.

[294] *A secure Europe in a better world: European Security Strategy*, EU Council document 15895/03, 8 December 2003; available at: http://www.iss-eu.org/solana/solanae.pdf.

[295] *White Paper 2006 on German Security Policy and the Future of the Bundeswehr*, Federal ministry of Defence, available at: http://www.realinstitutoelcano.org/materiales/docs/LibroBlanco2006_english.pdf.

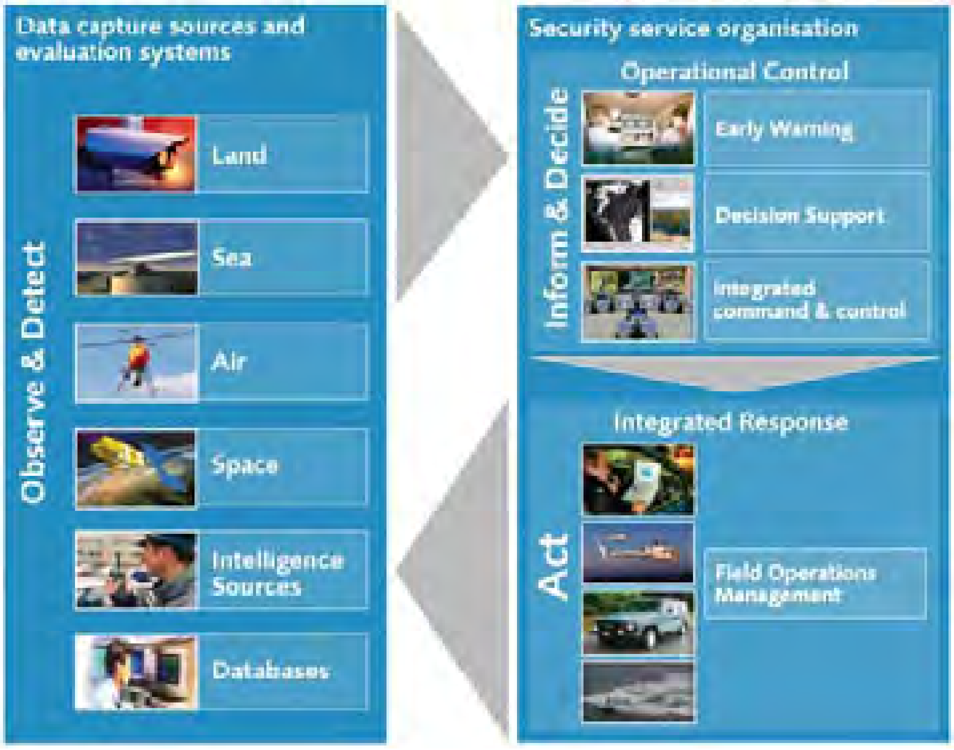
[296] *The National Security Strategy of the United Kingdom Security in an interdependent world*, Cabinet Office, 2008, available at: http://interactive.cabinetoffice.gov.uk/documents/security/national_security_strategy.pdf.

"Inside government", the UK strategy promises "a more integrated approach. The distinction between 'domestic' and 'foreign' policy is unhelpful in a world where globalisation can exacerbate domestic security challenges, but also bring new opportunities to tackle them". The UK also promises to tackle 'threat multipliers' such as climate change, competition for energy and poverty, inequality and poor governance. EU High Representative Javier Solana's own White Paper on 'Climate Change and International Security', published the week before the UK national security strategy, had used exactly the same language to push for EU policies to address the "international security threats created by climate change".[297] The Solana paper suggests that "Climate change is best viewed as a threat multiplier which exacerbates existing trends, tensions and instability", such as "states and regions which are already fragile and conflict prone", "border disputes", "environmentally-induced migration", "conflict over resources" and "situations of fragility and radicalisation".

It is striking how quickly these 'all risks', all encompassing definitions of homeland security have come to dominate western policy-making circles, and how little opposition there is to the 'national securitisation' of questions of social policies on public health and safety. In Germany in 2008 a cross-party group of four MPs published a 'Green Book' on 'Risks and Challenges for Germany', calling for "a new conception of transnational public security encompassing terrorism, organized crime, information technology, infectious diseases, and security of basic services".[298] The objective of this new definition is to allow "complex processes and [security] systems, on local, national and transnational levels, [to] function as smoothly as possible". "The more resources society and the state can mobilise", argues the Green Book, "the more resilient they are in times of crisis". Similarly, in 2009 a 'multi-stakeholder' National Security Commission convened by the UK Institute for Public Policy Research concluded its two year enquiry with the report 'Shared Responsibilities: A National Security Strategy for the UK'.[299] It adopts the same open-ended definition of security "to protect the UK population from the full range of risks so that people can go about their daily lives freely and with confidence under a government based on consent". Stressing that "*The risks to national security must be defined widely in current conditions, to cover major man-made threats and natural disasters*", the IPPR report argues that "Extensive partnership working within the UK, with the private sector, with community groups and with local government and citizens as individuals, must likewise be a feature of security policy". The report concludes that the UK needs "flexible and well coordinated national capabilities, forging a wide range of policy instruments, military and non-military, *into a coherent whole*" (emphasis added).

'Operational superiority": Project for a New European Securité?

Where the UK and German strategies have focused on expanding the concept of national security, the French White Paper on Defence and National Security of 2008 focuses on the operational measures that are required to achieve a coordinated homeland security capability.[300] It uses the concept of 'Operational superiority' to describe its quest for full spectrum dominance in order to "harness those technologies that ensure operational advantage over all plausible adversaries", including "means of information, communication, space--based assets; force protection, particularly against [chemical, biological, radiological and nuclear] and emerging threats; long-range precision strike; the capability to operate in an urban environment, in contact with the population; naval superiority, especially in littoral waters; air superiority; and air mobility". Crucially, these apparatuses are to be used for domestic security as well as external defence to combat the full range of threats described above. The French White Paper calls for a wide range of national and EU reforms to achieve these objectives.

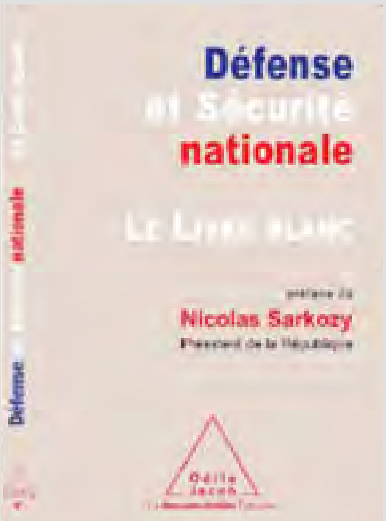


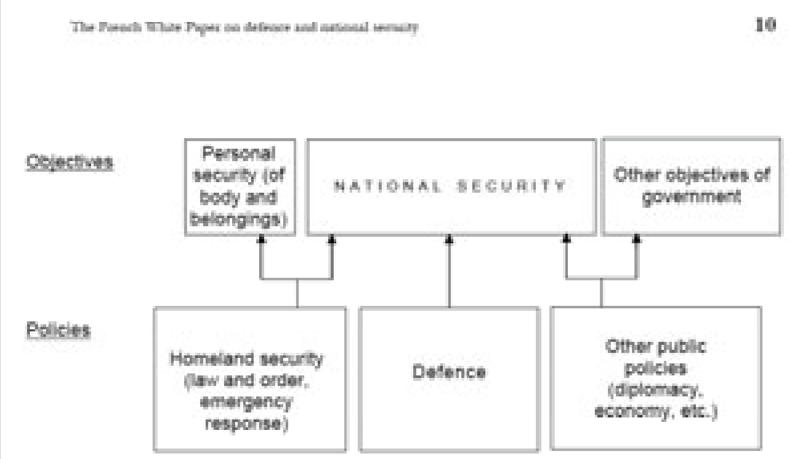
[297] *Climate Change and International Security: Paper from the High Representative and the European Commission to the European Council*, EU Council document S113/08, 14 March 2008, available at: http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/reports/99387.pdf.

[298] *Risks and Challenges for Germany: Scenarios and Key Questions*, Green paper of the Forum on the Future of Public Safety and Security, edited by Gerold Reichenbach (SPD), Ralf Göbel (CDU/CSU), Hartfrid Wolff (FDP) and Silke Stokar von Neuforn (Alliance 90/Greens). English version released 8 October 2008, available at: http://www.zukunftsforum-oeffentliche-sicherheit.de/download/27/.

[299] *Shared Responsibilities: A national security strategy for the UK*, IPPR Commission on National Security in the 21st Century, 30 June 2009, available at: http://www.ippr.org.uk/publicationsandreports/publication.asp?id=676.

[300] *The French White Paper on defence and national security*, Presidence de la Republique, June 2008, available at: http://www.globalsecurity.org/military/library/report/2008/livre-blanc_france_2008.pdf.




The French White Paper on defence and national security
10
Objectives
Personal security (of body and belongings)
NATIONAL SECURITY
Other objectives of government
Policies
Homeland security (law and order, emergency response)
Defence
Other public policies (diplomacy, economy, etc.)

The French White Paper on defence and national security: key findings

3. The national security strategy includes five strategic functions which the defence and security forces must master: knowledge and anticipation, prevention, deterrence, protection and intervention. The combination of these five functions must be flexible and evolve over time, adapting to the changes in the strategic environment…

4. Knowledge and anticipation represent a new strategic function and have become a priority. In a world characterised by uncertainty and instability, knowledge represents our first line of defence. Knowledge guarantees our autonomy in decision-making and enables France to preserve its strategic initiative. It is knowledge which must be provided as early on as possible to decision-makers, military commanders and those in charge of internal and civil security in order to go from forecasts to informed action. Intelligence of all kinds, including from space and prospective studies, takes on major importance.

5. … Reinforcing resilience requires a change in the means and methods of surveillance used over the national territory including land, sea, air and now space and to develop a more rapid and wider in scope, response capability for French public authorities. Communication and information systems and civil warning systems lie at the centre of the crisis management and preparedness system. One novel aspect is that operational goals in protection missions are now assigned jointly to both internal security services, civil security services and the armed forces. Coordination between civilian and military departments and agencies is one of the fundamental principles of the new strategy…

8. The European ambition stands as a priority. Making the European Union a major player in crisis management and international security is one of the central tenets of our security policy. France wants Europe to be equipped with the corresponding military and civilian capability… In addition, the White Paper emphasises four priority areas for the protection of European citizens: the reinforcement of cooperation in the fight against terrorism and organised crime; the development of European civil protection capabilities; the coordination of the defence against cyber-attack; and the securing of energy and strategic raw materials supply. Lastly, the White Paper advocates the drafting of a European White Paper on defence and security.

The European Defence Agency aims to establish a **European Framework Cooperation for Security and Defence Research***, together with the European Commission. This new Framework will provide the overarching structure for maximising complementarity and synergy between defence and civilian security-related research activities…*

EDA Press Release, 18 May 2009 [301]

25 The years ahead

The mandate of the European Security Research and Innovation Forum expires at the end of 2009. The group will deliver its final report at 'SRC 09', the annual EU Security Research Conference taking place in Stockholm in September 2009.[302] It remains unclear how the strategic development of the European Security Research Programme will proceed thereafter, but the ESRP is being incorporated into a new five year work programme for EU Justice and Home Affairs (JHA) policy and the European Defence Agency is positioning itself as the long term home of EU security research.

The 'Stockholm programme'

Every five years the EU adopts a five-year plan for justice and home affairs affecting all areas of EU JHA policy: policing, immigration and asylum, criminal law, databases and data protection. The 'Tampere programme' (2000-2004) was followed by the 'Hague programme' (2005-2009), which included the commitment to bring in biometric passports and ID cards and the principles of 'interoperability' and 'availability'. The new programme will be adopted in Stockholm in December 2009. As Tony Bunyan has explained, "the process of deciding the content of these five-year plans is long and complicated and rarely makes it into the mainstream news until they have been adopted – when, of course, it is too late for the public to influence its content or direction".[303]

The Tampere programme was drawn up and negotiated by EU Council and Commission officials, without any consultation with national or European parliaments or civil society, and adopted in closed sessions by the European Council (EU prime ministers). This time a little more information was available. In January 2008 the EU Council set up the 'Future Group', which produced a report on EU home affairs policies.[304] Its proposals, including the new 'principle of convergence' are examined in a special Statewatch report: 'The Shape of Things to Come'.[305]

The European Civil Liberties Network has described the ideology of the Stockholm programme as 'dangerously authoritarian'.[306] To harness what it calls the 'digital tsunami' (see quotation overleaf), the Future Group proposals presage the mass gathering of personal data on travel, bank details, mobile phone locations, health records, internet usage, criminal records however minor, fingerprints and digital pictures that can be data-mined and ap-

[301] *EDA and Commission to work closely together on research*, European defence Agency Press Release, 18 May 2009: http://www.eda.europa.eu/newsitem.aspx?id=471.

[302] See SCR09 conference website http://www.src09.se.

[303] The surveillance society is an EU-wide issue, Guardian, 28 May 2009: http://www.guardian.co.uk/commentisfree/libertycentral/2009/may/28/eu-view-surveillance-society.

[304] *Freedom, Security, Privacy: European Home Affairs in an open world*, Report of the Informal High Level Advisory Group on the Future of European Home Affairs Policy ("The Future Group"), available at: http://www.statewatch.org/news/2008/jul/eu-futures-jha-report.pdf.

[305] Bunyan, T. (2009) *The Shape of Things to Come*. London: Spokesman. Online version available at: http://www.statewatch.org/analyses/the-shape-of-things-to-come.pdf. See also *Statewatch* observatory on the Stockholm Programme: http://www.statewatch.org/stockholm-programme.htm.

[306] Statement on the Stockholm Programme, European civil liberties network: http://www.ecln.org/ECLN-statement-on-Stockholm-Programme-April-2009-eng.pdf.

> *The ability to track the location of any active mobile phone (and to know where it was last switched off and last switched on), this is just the beginning. In the next few years billions of items in the physical world will be connected, using technologies such as radio-frequency identification (RFID), broadband wireless (WiFi, WiMAX), satellite and small area wireless (Bluetooth, wireless USB, ZigBee). This means it will be possible to trace more and more objects in real-time and to analyse their movement and activity retrospectively. We will soon see this with respect to major consumer items such as cars, but this trend is likely to spread quickly to most items of any significant value. In the near future most objects will generate streams of digital data about their location and use – revealing patterns and social behaviours which public security professionals can use to prevent or investigate incidents.*
>
> EU 'Future Group' [307]

The Shape of Things to Come

plied to different scenarios. In the same report, the Future Group also suggests limiting the availability of privacy enhancing technologies on the grounds that they could be 'exploited' by terrorists and criminals. The Future Group proposes that by 2014, the EU needs to create a "Euro-Atlantic area of cooperation with the USA in the field of freedom, security and justice". This would go far beyond current co-operation and mean that policies affecting the liberties and rights of everyone in Europe would not just be determined in Brussels, but in secret EU-US meetings.

ESRP and the Stockholm programme

It is already clear that the aims of the EU security research agenda will be firmly integrated into the Stockholm programme. The Future Group report of June 2008 recommended that "Intensified use should be made of means available in the context of [EU security research] for objectives connected with police cooperation, the fight against terrorism, border management and information and communication technology objectives", and proposes that the EU member states "need to move towards converged networks (or, where necessary, solutions that ensure all their networks can "talk" to each other) and they need to ensure all data streams are digital and capable of being meshed together". ESRIF, suggested the Future Group, should provide the 'collaborative tools'. The "overarching future challenge", it concluded, is "*the further development of new technologies and their link to financing at EU level*, including in the area of security research *and structural funds*" (emphasis added).

The Future Group also recommended the launch of a "European Security Tool Pool… allowing Member State and [EU] institutions to make available secure tools of proven or potential use in the security field for appraisal and/or testing by authorities of other Member States". The new five year EU work programme is also seen as "an opportune moment to go beyond the limited perspective of a case-by-case approach and aim for a holistic objective in law enforcement information management", based on the "professional, business-oriented and cost-effective use of information technology and information networks".

[307] Future Group report, above (see page 6): http://www.statewatch.org/news/2008/jul/eu-futures-jha-report.pdf.

The first draft of the actual Stockholm programme, released in June 2009, takes things even further, proposing that "if national players are gradually to come to regard Europe as the natural theatre of their operations, there will have to be greater mutual trust".[308] It calls for joint training courses and exercises based on "ambitious targets", for example "to train one third of European police officers and border guards in European affairs over the next five years". The need for cultural 'interoperability' is matched by a desire for greater interoperability at the EU level to "ensure that the technical solutions adopted at national level are interoperable with existing or future European systems, and that they develop in a coherent fashion… This architecture will also allow economies of scale as the systems concerned come on stream. It will also make it possible to programme at national level the investments that serve the objectives of the [EU's] internal security strategy". Put another way: if uniform, national systems are developed in accordance with EU requirements, it will be a lot cheaper to develop the EU apparatuses described above.

Beyond ESRIF: towards an EU security and defence council?

It is as yet unclear how the strategic development of the European Security Research Programme will proceed following the expiry of the ESRIF mandate. DG Enterprise and Industry will retain overall responsibility for the programme, but there is still no clear legal basis for continued cooperation with the EU's defence and security apparatus. Another informal, *ad hoc* group of personalities in the mould of ESRAB and ESRIF may follow, but in the longer term, if the EU wants to continue to 'synergise' its R&D, security and defence policies, a more permanent solution must be found. While the FP7 programme is only recently underway (and runs until 2013), the architects of the ESRP are now thinking about funds for the years beyond, and ways to fund procurement as well as R&D in security technologies. In its first draft of the Stockholm programme, the European Commission has suggested that "in due course consideration might be given to setting up an Internal Security Fund".

In May 2009, EU Ministers of Defence, meeting in their capacity as the European Defence Agency (EDA) Steering Board on 18 May 2009, tasked the EDA with developing concrete proposals for a "European Framework Cooperation for Security and Defence Research". While the management of the defence and security R&D frameworks will remain unchanged, the longer-term intention appears to be to bring the strategic development of the ESRP under the auspices of the EDA. Initially, it is suggested that 'cooperation framework' could assume responsibility for 'situational awareness', from "sensing to command and control of networked assets". "Coordination on investment in research between the Agency and the Commission will save the European taxpayer money, as our actions will be concerted", said Javier Solana, head of the EDA and chair of the EU Defence Council.

At SRC '09, the annual EU Security Research Conference, the European Commission will take the idea one step further, making the case for "widening and deepening" the ESRP by creating a single market for defence and security technology modelled on the Trans-European Networks (TENs) for transport, energy and telecoms. Seen as crucial components of the EC's internal market, TENs are designed to enhance the "interconnection and interoperability of national infrastructure". In addition to specific EU TEN budget lines, the programme also receives Structural and Cohesion Funds, as well as European Investment Bank (EIB) loans.[309]

How would such a fund be governed? The French White Paper on Defence and National Security calls for a 'reorganisation of public authorities' for a new era of integrated defence and national security functions. On this basis, a 'Defence and National Security Council chaired by the President of the Republic' will be created in France. Looking to the future, it would come as little surprise if this model were to emerge as a favoured option for the 'converging' EU security and defence apparatus.

[308] Commission Communication on An area of freedom, security and justice serving the citizen, COM (2009) 262 final, June 2009: http://www.statewatch.org/news/2009/jun/eu-com-stockholm-prog.pdf.

[309] *Trans-European Networks*, European Commission website: http://ec.europa.eu/ten/index_en.html.

PART VIII: TAKING STOCK

We need to take very great care not to fall into a way of life in which freedom's back is broken by the relentless pressure of a security state.

We need to understand that it is in the nature of state power that decisions taken in the next few months and years about how the state may use these powers [of surveillance], and to what extent, are likely to be irreversible. They will be with us forever. And they in turn will be built upon. We should imagine the world we are creating before we build it. We might end up living with something we can't bear.

Ken Macdonald, (outgoing) UK Director of Public Prosecutions, October 2008 [310]

26 Conclusions and recommendations

A NeoConOpticon?

This report set out to examine the development and implementation of the European Security Research Programme while putting the current mania for surveillance and homeland security technology in a broader political and economic context. It has told the story of how a small group of military-industrial companies came together to secure substantial R&D subsidies for EU homeland security, and how rapidly their demands have been incorporated into the fabric of the EU's security and defence policy. The almost complete marginalisation of parliaments, critical NGOs and other 'stakeholders' has meant that at times the research has felt like an investigation into a multi-billion euro corporate coup.

The idea behind the 'NeoConOpticon' was to emphasise both the central role played by the private sector in 'delivering' surveillance-based security policies and the inherently neo-conservative appeal to the 'defence of the homeland' against threats to the 'Western way of life'. The convergence of these ideologies is accelerating the development of a 'surveillance society' in Europe, enhancing the potential for governments to subject the lives of their citizens and non--citizens to incredible scrutiny, transforming the relationship between them and undermining fundamental principles of democracy.

Whereas the ideal of democracy holds that governments are accountable to the people, surveillance-based techniques of governance are transforming this relationship: making people accountable to governments while widening the gap (the so-called 'democratic deficit') between political elites and those they have been elected or, in this case, appointed to serve. Instead of enhancing the EU's political legitimacy, these types of policies can only fuel the sense of alienation that many people now feel from law-makers in Brussels.

Paradoxically, while the overarching concerns of the likes of George Orwell and Michel Foucault about all-seeing and all powerful states are further entrenching themselves in EU policy with every passing year, their concerns are increasingly dismissed as paranoid or groundless, and mean little to new generations. Yet how else can we conceive of a world characterised by mandatory surveillance and wholesale risk profiling; a world policed by computer systems, combat robots and drone planes; and populations, or certain sections of them, subject to full spectrum dominance.

As far as this report is concerned, it must be stressed that the ESRP is very much in its infancy. Six more years and several billion Euros for hundreds of security research projects has already been set aside; the agenda described above merely offers a glimpse of what is to come. Moreover, while the EU's security research programme provides a focal point for the

[310] 'Ken Macdonald: We must not degrade our liberties in the name of defending them', Independent, 21 October 2008: http://www.independent.co.uk/opinion/commentators/ken-macdonald-we-must-not-degrade-our-liberties-in-the-name-of-defending-them-967706.html.

articulation of concerns about contemporary security policies, it is very far from being a single explanatory factor for the emergence and pursuit of those policies. Rather, they are part of a much wider security-industrial complex grounded in a vast array of social, political and economic relations.

There is clearly a need for meaningful debate about the kind of homeland security and surveillance that the EU and its member states are now producing, as well as why it is doing so. However, the burden has fallen to independent civil society to provide a meaningful assessment of the trajectory, implications and pitfalls of the ESRP.

Following the money

This report is based on a simple reading of the capital flows within the European Security Research Programme: economic, political and social. It reveals a programme that has been designed largely by lobbyists, for lobbyists; the product of a structural conflict of interests arising from the failure to separate the development and implementation of the ESRP. Within this framework the companies whose names appear frequently in this report have played a particularly prominent role. This, coupled with an almost entire lack of democratic control over the ESRP, warrants strict auditing and a full review of the projects funded to date. The kind of enquiries conducted by the USA Federal Government Accountability Office (GAO) could provide a suitable model; the EU Court of Auditors could also subject the programme to more rigorous scrutiny should it be deemed necessary.

There is also a pressing need for clarity in the aims and objectives of the ESRP. The programme is predicated on the twin objectives of supporting the emerging European homeland security industry and increasing public safety. What is happening in practice is that multinational corporations are using the ESRP to promote their own profit-driven agendas, while the EU is using the programme to further its own security and defence policy objectives. As suggested from the outset of this report, the kind of security described above represents a marriage of unchecked police powers and unbridled capitalism, at the expense of the democratic system.

As far as the ESRP is concerned, it is also difficult to draw much needed lines between research and procurement, between civilian and military technology control, and between homeland security and defence applications. Amid all this confusion, if the programme is to continue, the parameters of the ESRP must be radically redrawn to put the programme under democratic control, to separate research and procurement and security and defence, to provide impartial objective avenues for research (rather than R&D tailored to the policy objectives of an EU security state), and to put human rights and social justice at the centre instead of the margins of every project.

This is an extremely daunting task that requires an unravelling of the fears – real and imagined – that sustain the demand for new security policies. As the authors of 'Making Threats: Biofears and Environmental Anxieties' have explained: "Unravelling fear is a difficult and complicated project because we have to face squarely the demons of our history, politics, ideologies and economies… In these terror-filled times, the search for just and peaceful solutions depends on seeing through and beyond our fears to new moral choices and political possibilities".[311]

Europe needs limits to police powers and surveillance

Civil liberty concerns about the impact of the 'war on terror', about unchecked surveillance, and about the lack of accountability in EU frameworks for policing and law enforcement cooperation, are well-documented, and have to a limited extent characterised debate about security over the past decade. Sir Ken McDonald, cited on the previous page, is far from a lone voice of 'The Establishment' in his concerns; Sir Richard Dearlove (ex-head of MI6) and Dame Stella Rimington (ex-head of MI5) have also spoken (respectively) of "striking and disturbing" state invasions of privacy, and Britain "becoming a police state".[312] It is remarkable not just how mainstream these concerns have become (at least in Britain), but how little impact they are having on the policy agenda.

Whereas the Obama regime promises 'a break from the past' in the USA, the current politics of the EU are characterised by a significant shift to the right. While it is the Right that has traditionally favoured stricter law and order policies, the political discourse in which the ESRP is embedded now appears to transcend party politics. Among the most revealing trends of the research conducted for this report was how the word 'security' now serves to justify making permanent measures that just a few short years ago appeared 'exceptional'. Despite widespread concerns about civil liberties, we appear to be entering a new era characterised by a shift in emphasis from a 'war on terror' towards the creation of permanent apparatuses for surveillance and social control. Even in countries in Northern Europe and Scandinavia, where the word 'security' hitherto meant a protective cushion provided by the state (or where the words for safety and security are one and the same), national security is steadily coming to provide a mandate for the state to combine and enhance its coercive power to deal rapidly and punitively with all risks.

This shift in emphasis has put surveillance at the centre of EU security and defence policies. If the right to privacy is to survive a generation, then European societies must have a serious discussion about surveillance techniques, their limits and how to control them. A freeze on further measures and a review of existing security policy after a decade of intrusive surveillance legislation will not undermine our security, as is claimed. It is essential to allow Europe the

[311] Hartman, B., Subramaniam, B. & Zerner, C. (2005) *Making Threats: biofears and environmental anxieties.* New York: Rowman & Littlefield (page 250).

[312] 'Ex-spy chief Dame Stella Rimington says ministers have turned UK into police state', *The Times*, 17 February 2009: http://www.timesonline.co.uk/tol/news/politics/article5750713.ece; 'Big Brother HAS gone too far ... and that's an ex-spy chief talking', *Daily Mail*, 2 June 2009.

chance to take stock of where policy and technology is going and devise innovative and robust frameworks for regulating police powers and protecting individual rights and liberties in the 21st century. The regulation of controversial security technologies instead of the generous subsidies currently on offer for their development is an immediate and obvious option for Europe's policy-makers.

In democracy's wake

The path to security through profit and technology upon which the EU has embarked is very different to the pursuit of security through democracy. Where the latter ostensibly represents a 'compromise' between the institutions of democracy and the rule of law, the former is based on economic and technological determinism, i.e. is it possible, and is it profitable? It is only after these criteria have been satisfied that democracy and the rule of law come in to play, and often then only as potential 'barriers' to whatever crucial new police power or high-tech solution has become the political imperative of the day.

Some of the EU R&D described above may have verged on the incredulous, but it is nevertheless grounded in the supply and demand of newly viable, if extremely costly and potentially very dangerous, military technologies. The sustainability of this market requires both a hyping up of the 'threat' and a radical reorganisation of the agencies of state into a new integrated framework for defence and national security. Bereft of the political will, mandate and means to make radical contributions to social justice-led policies that could meaningfully address contemporary sources of inequality and insecurity, the EU has retreated behind the only policy area in which the member states can show themselves to be forceful and resolute. Homeland security and defence is now firmly at the centre of the European project.

The principle that security is now a 'common good' shared between the public and private sector is dangerous not because private security is necessarily a bad thing, but because the profit-driven, high-tech vision of security of the private sector is – when examined as whole – demonstrably at odds with the democratic traditions and social justice aspirations of the 'free world'. They have also eclipsed more nuanced social and economic policies designed to address the 'root causes' of complex social phenomenon such as migration, terrorism and underdevelopment.

The new public-private partnership for homeland security is based on a simple *quid pro quo*: profit for companies and power for states, in this case the ability of states to mitigate or neutralise the full spectrum of 'threats' to security, locally, nationally and across borders through communications and surveillance systems overseen by new command and control centres. What will be developed in effect is a network of temporary, permanent and highly mobile state formations at local, regional, national and international levels equipped with latest interoperable military and security technology. Left unchecked, these formations will one day govern a world administered into red zones and green zones.

The overwhelming emphasis of the ESRP on an interoperable EU-wide security architecture is designed to strengthen the nascent European state apparatus, its institutions and agencies. Where the EU speaks of 'pooling sovereignty', and its critics of 'European armies', the real national interest in this kind of European integration is genuine: the international free movement of national law enforcement, security and surveillance efforts within a collective apparatus for security and defence.

This new international form of state has already been established far beyond the confines of the nation-state, systems for accountability, regulation and control, which remain firmly rooted in their old national containers. Instead of 'democratising' the EU's security policy in response to widespread concerns, this apparatus appears to be falling under the increasing control of the even-less-accountable EU security and defence framework and the veil of secrecy that 'national security' affords.

The entire homeland security paradigm is predicated on the idea that western nations face an unprecedented threat to their 'way of life'. Be it pandemics, political violence or protest, the 'problem' is seen as a grave danger and the 'solution' couched in terms that favour the transfer of social policy responses from civilian agencies to law enforcement and militarist proscriptions developed by securocrats and technocrats. This process feeds on much of the recent discourse on globalisation, which asserts that western states, far from becoming more authoritarian and militarised as they plainly are, must defend their 'way of life'. This rhetoric must be challenged head on. There are, of course, genuine threats to security, but all sense of proportion appears to have been lost. In a troubled and desperately unequal world, Europe is already relatively secure.

Full Spectrum Dominance

'Full Spectrum Dominance' may be an extreme way of describing the emerging framework for (global) policing described in this report, but a particularly profound shift in the EU's area of 'freedom, security and justice' appears to be taking place. Whereas the subsidies to transnational security and defence corporations can be traced back to a singular and spectacularly undemocratic EU policy measure (the ESRP), the Full Spectrum Dominance paradigm is built upon more solid foundations.

The political consensus around tough measures on 'illegal' immigration, special powers to combat terrorism, the creation of an international framework to combat organised crime, the embrace of new security technologies, the right of the state to place 'suspects' under sustained and intensive surveillance, and the securitisation of a host of new threats; this discourse is rapidly attaining the status of a 'hegemonic truth' and exerting enormous power over governments of advanced capitalist economies. Put another way, there is a danger that the 'logic of security' is becoming the new orthodoxy or 'common sense', manufacturing both consensus and consent while discrediting alternatives and producing indifference to the harm and inequality it causes. The EU may be more unpopular than ever among those it governs, but its security and defence apparatus is firmly rooted in authoritarian populism. Indeed, neo-liberal globalisation and neo-conservative homeland security policies may ultimately come to be seen as two sides of the same 'globalist' coin.

There is a link too between new high-tech forms of repression and the practises of 'extraordinary rendition', the torture of terrorism suspects and the incarceration of men and boys in cages on prison islands that have reappeared in recent years. These phenomena have been presented as the new 'exceptionalism', as the excesses of the architects of the war on terror of a neo-con regime that will soon be confined to history. As Gareth Peirce, the UK human rights lawyer, has explained, these exceptional shows of force also serve another quite deliberate purpose. "The first shocking images of human beings in rows in aircraft, hooded and shackled for transportation across the Atlantic… The captor's humiliation of these anonymous beings - unloaded at Guantánamo Bay, crouched in open cages in orange jumpsuits - was deliberately displayed".[313] These images have inevitably inured dispassionate Europeans to more extreme measures, what Jackie Orr calls the "militarisation of inner space",[314] serving to legitimise in the eyes of the public what are, in the eyes of the legal community, parallel justice systems to deal with 'non-citizens', 'asylum-seekers', 'terrorists' and civil unrest.

The response of the watching world is being used by those in charge of these programmes as a barometer as to what is politically acceptable - a grotesque experiment to test the public appetite for 'extraordinary' measures. When the public 'outrage' reaches a critical mass, these programmes are not dismantled, but simply removed from public view. This is what has happened with the EU's most controversial policies, including mandatory surveillance regimes, defence policy and security research. Once the 'enabling' legislation has been adopted, all the key discussions and decisions about implementation take place deep within the corridors and dossiers of the Council and the Commission.

A whole new language has been invented to disguise the aims of EU policy with the means. In the case of the ESRP this means a set of 'principles' with which everyone can agree: the need to increase security, the need to foster EU industrial competitiveness and create European jobs, the need to do something about instability in the world etc. The actual policies that result are buried deep within a million pages of legislation and communications; the outcomes are even further removed from public scrutiny. Concealed by the mantra that EU cooperation is the best and only course of action available to the member states, scant attention is paid to what that cooperation actually entails.

Another world is compromised

Once enacted, the kind of security apparatuses described in this report will be very difficult to unravel. A decade of counter-terrorism and surveillance-enabling legislation is seen by policy-makers not only as here to stay, but merely the beginning of a revolution in law enforcement. Yet while the scope for state intrusion into private life and public space has changed beyond all recognition, the oft-promised revolutions in government accountability have largely failed to materialise, especially at the EU level.

While civil society has exposed the worst excesses of the 'war on terror': Guantanamo, rendition and torture etc., it has systematically failed to challenge the similar underlying approaches employed in migration control, counter-terrorism and criminal justice systems that have given rise to a new authoritarianism.

What is needed, now more than ever, is a new kind of Europe that puts social justice and human rights above and beyond all other values. This will require substantial reform of the EU system of governance, constructive measures to prevent Europe becoming the kind of militarist power and surveillance society about which so many have warned, and a radical reappraisal of an economic paradigm based solely on the desire for profit and growth. This requires a sustained effort on the part of civil society to educate itself and others about the kind of EU that we already have, and to turn pockets of progressive resistance into tangible vehicles for social and political change. Without such efforts, the EU will surely continue, quietly and secretively, along its current path until it is too late.

[313] Peirce, G (2009) "Make sure you say that you were treated properly', *London Review of Books*, vol 31 no. 9: http://www.lrb.co.uk/v31/n09/peir01_.html.

[314] Orr, J. (2005) 'Making Civilian-Soldiers: The Militarization of Inner Space' in Hartman, B., Subramaniam, B. & Zerner, C. (eds) *Making Threats: biofears and environmental anxieties.* New York: Rowman & Littlefield (page 250).

About the author

Ben Hayes has worked for the civil liberties organisation Statewatch, based in London, since 1996, specialising in EU Justice and Home Affairs law, police cooperation, border controls, surveillance technologies and counter-terrorism policies. Ben also works with the Transnational Institute (Amsterdam), the European Centre for Constitutional and Human Rights (ECCHR, Berlin), and has been retained as a consultant to a number of international human rights, social justice and development organisations. He has a PhD from Magee College (Derry/Londonderry) awarded by the University of Ulster in 2008.

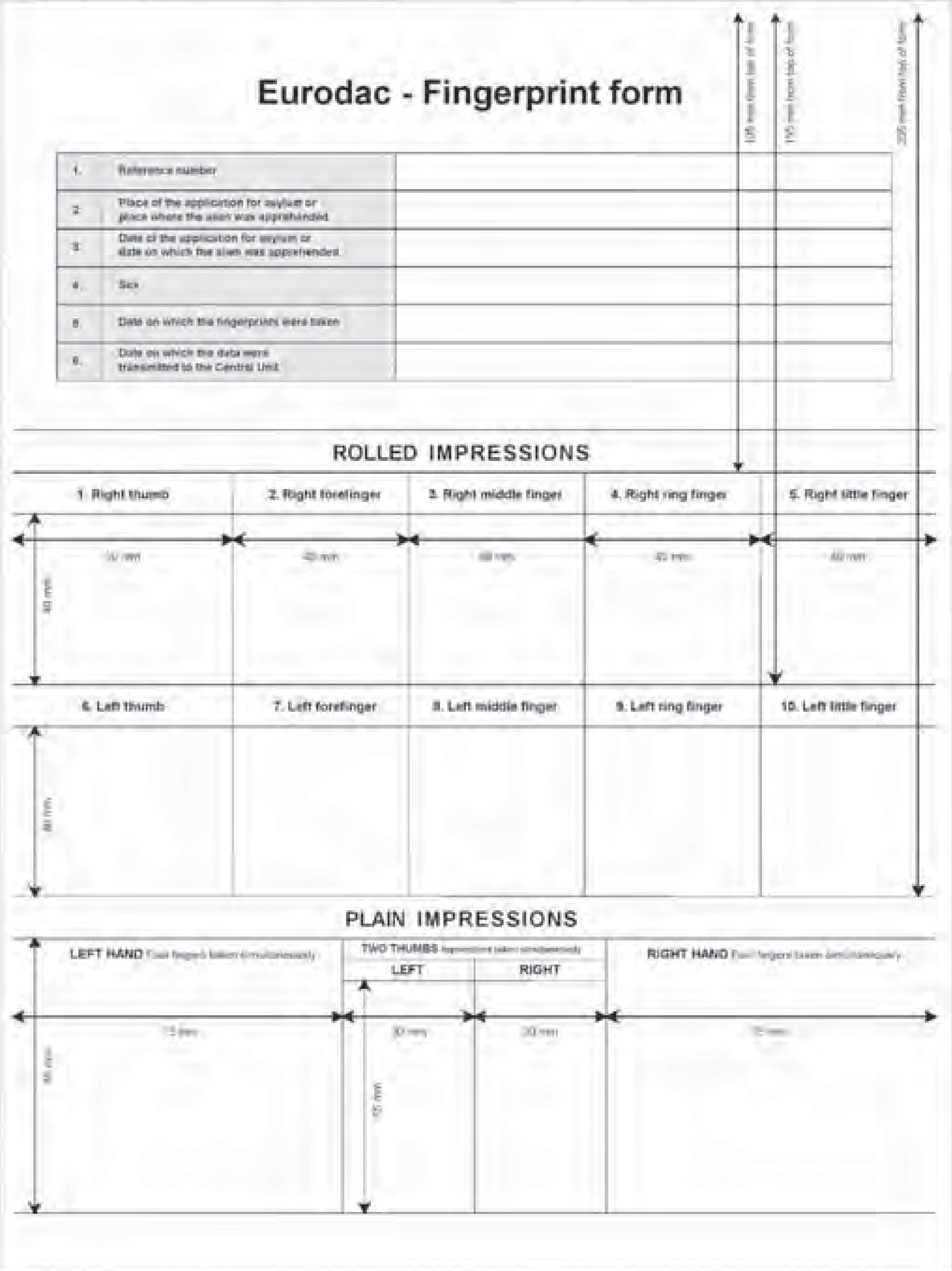
About TNI

Founded in 1974, the Transnational Institute (TNI) is an international network of activist-scholars committed to critical analyses of the global problems of today and tomorrow. We seek to provide intellectual support to those movements concerned to steer the world in a democratic, equitable and environmentally sustainable direction.

About Statewatch

Statewatch is a non-profit-making voluntary group founded in 1991. It is comprised of lawyers, academics, journalists, researchers and community activists with a network of contributors is drawn from 17 countries. Statewatch encourages the publication of investigative journalism and critical research in Europe the fields of the state, justice and home affairs, civil liberties, accountability and openness. For more information see www.statewatch.org.

ANNEX II



Eurodac - Fingerprint form

1.	Reference number	
2.	Place of the application for asylum or place where the alien was apprehended	
3.	Date of the application for asylum or date on which the alien was apprehended	
4.	Sex	
5.	Date on which the fingerprints were taken	
6.	Date on which the data were transmitted to the Central Unit	

ROLLED IMPRESSIONS

1. Right thumb	2. Right forefinger	3. Right middle finger	4. Right ring finger	5. Right little finger
6. Left thumb	**7. Left forefinger**	**8. Left middle finger**	**9. Left ring finger**	**10. Left little finger**

PLAIN IMPRESSIONS

LEFT HAND Four fingers taken simultaneously	TWO THUMBS Impressions taken simultaneously		RIGHT HAND Four fingers taken simultaneously
	LEFT	RIGHT	

Despite the often benign intent behind collaborative European 'research' into integrated land, air, maritime, space and cyber-surveillance systems, the EU's security and R&D policy is coalescing around a high-tech blueprint for a new kind of security. It envisages a future world of red zones and green zones; external borders controlled by military force and internally by a sprawling network of physical and virtual security checkpoints; public spaces, micro-states and 'mega events' policed by high-tech surveillance systems and rapid reaction forces; 'peacekeeping' and 'crisis management' missions that make no operational distinction between the suburbs of Basra or the Banlieue; and the increasing integration of defence and national security functions at home and abroad.

It is not just a case of "sleepwalking into" or "waking up to" a "surveillance society", as the Britain's Information Commissioner famously warned, it feels more like turning a blind eye to the start of a new kind of arms race, one in which all the weapons are pointing inwards. Welcome to the Neo-ConOpticon.