CHALLENGE Liberty & Security

Research Paper No. 3

November 2006

The Changing Landscape of European Liberty and Security

Communicating (in)Security: A Failure of Public Diplomacy?

Juliet Lodge

Abstract

This paper attempts to unravel elements of the problem of communicating security to citizens in the EU and to show how it is tangled up in the misleading dichotomous rhetoric of security or liberty. The resulting failure of public diplomacy leads to sub-optimal policy outcomes and accountability deficits. The paper i) explores these effects in the context of problems of communication in spaces of disconnection arising between political agents of territorial power and the creation and maintenance of citizens' affective loyalties; ii) briefly examines issues arising from the introduction of biometric identifiers to show how liberty and security are portrayed as alternative rather than complementary options; and iii) relates this portrayal to aspects of managing communication. It concludes that imprecision among elites as to what they mean by 'security' and what they think they communicate aggravates accountability deficits, public trust and confidence in the EU.

Juliet Lodge is Director of the Jean Monnet European Centre of Excellence (JMECE) and Institute of Communication Studies at the University of Leeds in the UK. This work was carried out in the context of *CHALLENGE* – programme *(Changing Landscape of European Liberty and Security)*, a research project funded by the Sixth Framework Programme of the European Commission's DG for Research (www.libertysecurity.org). Special thanks are due to Leeds Challenge research assistant Bruno Fransen for preparing the interview data and comments.

An Integrated Project Financed by
the Sixth EU Framework Programme

ISBN 92-9079-680-4

Available for free downloading from the CEPS website (http://www.ceps.be)

Contents

COMMUNICATING (IN)SECURITY: A FAILURE OF PUBLIC DIPLOMACY?

JULIET LODGE

Introduction

Some 17% of all European Commission legislative proposals relate to freedom, security and justice. Somewhat surprisingly, in confronting the need to balance liberty with security, inadequate attention has been paid to the need to communicate the purposes of security convincingly to citizens. Instead, there is a failure of public diplomacy that mirrors but is exacerbated by the public diplomacy failure in respect to communicating Europe.

This paper attempts to unravel elements of the problem of communicating security to citizens in the EU and shows how it is tangled up in the misleading dichotomous rhetoric of security or liberty. The resulting failure of public diplomacy leads to sub-optimal policy outcomes and accountability deficits, which appear to upset the balance between implementing security measures while sustaining liberty in the EU setting. First, this paper begins by placing this issue within the context of disconnection between the political agents of territorial power and citizens' affective loyalties. Second, it illustrates how liberty and security are portrayed as alternative rather than complementary options by briefly examining aspects of the introduction of biometric identifiers. Third, it relates this portrayal to managing communication. It concludes that imprecision among elites as to what they mean to communicate as well as over what they think they communicate undermines public trust and confidence in the EU.

1. Problems of communication in spaces of disconnection

Political communication is varied in scope and intent, but it is an essential element of public diplomacy. Public diplomacy concerns the communication of political messages by the governing political authorities to the public. The content of the message is subject to several determinants beyond those associated with political context, time, degree of crisis and organisational politics. These include the size of the target audience, the nature of political leadership, politico-legal constraints,[1] organisational and communication cultures, framing structures, intervening mediation and brokering between political agencies and the communication establishments.[2] The EU's claim that it is 'listening' implies feedback from the public in response to its public diplomacy initiatives in communicating Europe (and its policy goals). These issues are outside the scope of this paper. Instead, we focus on problems resulting in a lack of clarity and leadership in the communication of messages and claims about 'security', and specifically sustaining freedom, security and justice in the EU. That the EU

[1] See on leadership problems in general: OECD (2003), Challenges for E-government Development, 5th Global Forum on Reinventing Government, Mexico City, 5 November (retrieved from http://unpan1.un.org/intradoc/groups/public/documents/un/unpan012241.pdf); United Nations (2003), World Public Sector Report: E-government at the Crossroads, New York, United Nations, (retrieved from http://unpan1.un.org/intradoc/groups/public/documents/un/unpan012733.pdf).

[2] B. Bimber (2000), "The Study of Information Technology and Civic Engagement", *Political Communication*, Vol. 17, No. 4, pp. 329-33; S. Albrecht (2006), "Whose voice is heard in online deliberation?: A study of participation and representation in political events on the internet", *Information, Communication and Society*, Vol. 9, No. 1, February, pp. 62-82.; J. Hands, (2006), "Civil Society, cosmopolitics and the net: The legacy of 15 February 2003", *Information, Communication & Society*, Vol 9, No. 2, April, pp. 225-243.

Commission has identified a need to 'communicate Europe' to the public marks a recognition of a communication gap as well as low public interest in or attachment to the EU. The EU Commission's 'Plan D' aims to reconnect the citizen with the EU by enhancing democracy, dialogue and debate and prepare the citizen for e-governance 2020 when it is assumed that ICT (information and communications technology) will have a far greater direct impact and tangibility for citizens in their everyday experience of the government services.[3] The EU and member states cannot afford to allow the accountability deficit + digi-divide + digi-exclusion + unconvincing muddled claims on e-security to exacerbate a trust deficit in ways that aggravate a sense of distance and disconnection and fail to bring the citizen closer to the Union.

1.1. Disconnection, deficits and affective loyalties

Theories variously explain citizen disconnectedness from their territorial governments in terms of globalisation theories, centreless societies, social movements and interconnected cosmopolitan networks.[4] Yet in the EU, power and authority continue to be regulated through territorially-based institutions seen to be imbued with values that are supposed to illustrate continuity with past traditions of liberal democracy and exemplify common aspirational values that transcend member state boundaries. While they may not be universal or reflect a single understanding of those values, they broadly reflect acceptance or passive acquiescence over society and how through the exercise of authority the allocation of scarce resources, prioritisation of goals, and attainment of security are to be affected. However, old assumptions that citizens' loyalty to their state of residence could be broadly taken for granted are increasingly challenged by new political spaces of governance. The opportunities offered by multi-media communication lead to an environment in which mediated governance challenges the idea of rational two-way communication among those who exercise political power and those subject to it. Neither political authority nor the public is coherent and cohesive, integrated or common if not uniform. That they are not is recognised by the Commission and member governments in their attempts (such as the Convention on the Future of Europe and the post-Constitution referenda) to bring citizens to discuss the organisation and allocation of power among EU institutions in a defined geopolitical space. The idea is that in doing so citizens may begin to re-think of themselves as citizens communicating in a non-nation state, a supranational space of common values centred arround the four freedoms: liberty, the rule of law, justice and security.

The EU exercise in communication therefore does not illustrate how citizens influence the shape and priorities on the agenda. Instead, it shows how deploying ICT can facilitate interaction over a pre-determined set of core values connected to pre-selected political priorities that crucially depend on sustainable security. Realising e-governance 2020 highlights this, but ducks the critical discussion over legitimising policy goals and means that many citizens find disproportionate and unacceptable. This is especially clear in respect to the introduction of biometric data and identity cards (or their shadows) for which no legal basis exists in the treaties and over which there has not been public debate in the European or national parliaments.

---

[3] DG Communication, (2005), Action Plan to improve communicating Europe by the Commission, July 2005; DG Communication, Action plan - annex with 50 measures.

[4] N. Scandamis, (2006), *Normative parameters of exceptionalism: Community governance patterns in the field of security and its implications for a future global governance as responding to the internal rules of globalization, existing or to be*, paper for Challenge, University of Athens, January.; Anheier H., M. J. Kaldor & M Glasius (eds) (2005), *Global Civil Society 2005/6*, London: Sage.; Hoffman J. (2004), *Citizenship beyond the State*, London: Sage.; James P. (2004), *Globalization and Violence*, London: Sage.; Grant, David, Cynthia Hardy, Cliff Oswick & Linda Putnam (eds) (2004), *The SAGE Handbook of Organizational Discourse*, Thousand Oaks, CA: Sage Publications.

There is a tendency to conflate information-giving with communication. The former is passive and associated with making information available (the claims of transparency). From the Commission's point of view, this has to be presented in as politically neutral a manner as possible to avoid treading on the toes of governments. Such a passive communication strategy is essentially problematic because it avoids deliberation and cannot capitalise on the emerging non-territorial clusters expressing socio-political interests and values that both transcend and continue to find some expression in the more traditional tensions between political parties and groups within member states. Moreover, a passive communication strategy is especially problematic in relation to 'security' because of the imprecision of what security means, and the cultures of secrecy that surrounds international diplomacy as well as internal security. These underlying factors contribute to the difficulties of communicating clearly about security in the EU. Such passive communication becomes a vehicle that provides access to some information for citizens to find out about the goals of their political masters. The objective of all players in this situation is not necessarily informed discourse. Rather it is about persuasion. While mediatisation may blur the boundaries between space and dimensions of space, the legitimacy of the information source in such a setting is vital to promoting understanding and distilling consensus over both the legitimacy of the rulers to rule and the justness of the particular issue on which they have pronounced. When parliaments were seen to hold executives democratically accountable, there was an understood ultimate locus of political contestation, polarisation and advocacy, and an ultimate source of political authority and democratic legitimacy. This concept is increasingly challenged.

Interestingly during the EU presidencies of Austria to Finland, national parliaments have held parallel responsibility for coordinating common national parliamentary activities, such as input reflecting the draft Constitution. Ensuring that their voice is broadcast, heard and heeded is more complicated. Persuasion in cyber-space *sans frontiers* without traditional political interlocutors – the national political classes and MPs – is problematic. The authoritative mediators of public opinion – MPs themselves – are as insufficiently engaged either with the civil society networks or with the supranational institutional framework where they might be expected to play a role in shaping outcomes and making themselves heard. The EU's guidelines on strengthened partnerships with national parliaments[5] endorsed by the June 2006 European Council gives MPs a right to receive draft Commission proposals directly and comment on them (in a manner akin to the old non-elected European Parliament) but without a guarantee that they will be influential and without an effective mechanism to coordinate a common view.

The task of persuasion is all the more onerous if one goes beyond the immediate problems associated with communicating Europe to the more specific and more contentious realm of communicating EU security. This is already seriously hedged by rules on secrecy and exceptionalism. Secrecy can be seen as a derogation from transparency. Not surprisingly, the European Parliament's Committee on Civil Liberties, Justice and Home Affairs challenges any steps that do not explicitly provide for proper accountability to the EP. In September 2006, it accordingly pressed for the mandate of the Fundamental Rights Agency, the successor to the European Monitoring Centre on Racism and Xenophobia, to be extended to integrate cooperation on policing, justice, immigration and counter-terrorism – all slippery areas where transparency and parliamentary accountability have been non-existent, weak or problematic.[6]

---

[5] "Guidelines on Strengthened Partnership with National Parliaments", 5 May 2006, Rapid press release IP/06/1172, Brussels, 11 September 2006.

[6] Gál Kinga (2005), *Draft Report on the proposal for a Council Regulation establishing a European Union Agency for Fundamental Rights*, (COM(2005)0280-C6-0288/2005-2005/0124(CNS).

The European Data Protection Advisor Peter Hustinx sees openness and accountability as intrinsic to transparency. If practiced responsibly, it is more likely that a culture of transparency – expressed in terms of figures and facts, and norms and values – will be developed even though freedom of information rules vary across the EU. Transparent information presented by agencies lacking trust or of dubious provenance cannot contribute to improving understanding and knowledge about an issue, which is one of the key purposes of transparency for accountability. Transparency cannot contribute to a culture of trust if it is not accompanied by clarity over purposes, processes, methods, strategies and political goals, and by the means to implement and crucially challenge them. Nor can it be built when there is concern that the agenda is driven not by informed governments and parliaments but by private non-state interests.[7] Both transparency and accountability are needed to contribute to the process of reducing the public distrust that accompanies secrecy and opacity by government bodies, and the concern over the new tools for enhancing public security that governments claim result from the application of ICT managed by and outsourced to barely visible, let alone politically accountable, private agencies in cyber-space or outside the territorial jurisdiction of state agencies.

In the EU, problems of trust are compounded by institutional complexity that compromises openness and accountability. The resultant unpropitious environment for communicating security – what it means, how it is to be enforced, and how it is to be controlled – aggravates public distrust in government and the agencies of security and law enforcement from the police to migration controls. This is all the more problematic in view of the increasing advocacy of using biometrics (which are often poorly explained and presented) in civil applications rather than merely in respect to crime-busting, or in Eurodac to monitor and control migration. Operationally rational reasons for lowering the age for and taking fingerprints of all persons seeking entry to (and not just asylum in) the EU from states for whom visas are required are also poorly explained, but more easily justified in simplistic terms. It is not surprising that in the public mind, the use of biometrics for controlling 'them' – the out-group – is seen as less threatening to personal liberty than is their application to 'us' – the in-group.[8]

There is continuing contestation over the ultimate locus of authority and legitimacy in the EU (exemplified by the continuing wrangling over the Constitution) and transparency under pillar III. This is exemplified by national parliaments' confusion and highly disparate roles in respect to supervision under subsidiarity rules. All intensify the sense of public disconnection from both national and EU agents of political authority. This complicates the communication of security and is exacerbated by both institutional complexity and a failure in public diplomacy to specify more concretely what security means to the state and to the individual, how it is to be attained domestically, and how and why certain measures enable the state to perform its traditional role *vis-à-vis* its citizens in terms of ensuring their security as best it may. The erosion and permeability of the old differentiation between internal and external security inevitably adds further confusion and complexity.

---

[7] Hayes B. (2006), *Big Brother: The EU's Security Research Programme*, The Transnational Institute, Amsterdam, (retrieved from www.tni.org).; Ashbourn J. (2006), *Societal Implications of the Wide Scale Introduction of Biometrics and Identity Management*, Background Paper for the EuroSci Fourm (ESOF), Munich.

[8] Lodge J. (2003), "Transparency and EU Governance: Balancing Openness with Security", *Journal of Contemporary European Studies*, Vol. 11, No. 1, pp. 95-118.; Lodge J. (2002), "Sustaining Freedom, Security and Justice – From Terrorism to Immigration", *Liverpool Law* Review, Vol. 24, No. 1-2, pp. 41-71.

1.2. Disconnection and institutional complexity

The communication of internal security has two core but inter-linked elements: securitisation and function creep. Communicating security to citizens through multi-media, multiple-channel ports provides diverse means for transmitting information and equally diverse messages as it is enmeshed and communicated via the agendas of data protection, civil liberties and human rights (including the vast migration, asylum and refugee agenda).[9] The multiplicity of bodies involved in security matters – from agenda-setting through legislating implementation measures to operational intelligence, policing and judicial enforcement – means that it is very hard to prioritise and discern if there is a single security message, and if so what single message on security should or could be communicated to the EU public. This leaves too much scope for dominant vested interests to capture and skew the agenda and the communication of security.

A number of factors contribute to this. Where communicating security in general, and specifically within the constraints of pillars II (CFSDP) and III (Justice and Home Affairs) is concerned, they include i) the event-driven – and often crisis-scenario – nature of EU member state responses to security issues ranging from terrorism to immigration and border controls to function creep via biometric IDs introduced ostensibly for security purposes,[10] ii) institutional complexity, multi-agency interests and inter-governmentalism inherent to the constitutional design of pillars II and III; iii) a tendency for national interpretations of security issues to predominate over EU solutions arising from inter-governmentalism and very limited EU resources for security issues; iv) inter-agency disinclination to trust counterparts, share information and collaborate; and v) the adoption of a mix of EU-based tools alongside parallel and sometimes mutually contradictory national or international tools. If the Fundamental Rights Agency is able from 2007 to complement the work of the Council of Europe and coordinate some of the activities of national human rights bodies, this will be a small step in the right direction. Yet, even if there is closer insistence on and adherence to human rights among new or candidate EU members and those linked to the EU through stabilisation and association agreements, making this a practical reality will continue to be problematic and protracted, even with strong political endorsement and follow-up from the European Council and member governments. The more e-security and e-governance initiatives are rolled out, the more difficult it may be for all to be included as front-and back-end technology are out of kilter in different states. Information-sharing among law enforcement agencies even within the EU and the Schengen group suffers from this as well as from the problems of incompatibilities and distrust. This was exemplified in September 2006 by the Visegrad Four's disappointment at the postponement of their entry to Schengen until 2008, ostensibly for technical reasons over Schengen II.

Moreover, at the operational level, member states' internal domestic institutional arrangements and agencies may find it hard or inconvenient to accommodate EU measures in their routine implementation of measures to uphold law, order, justice, security and liberty. Function creep and disparate interpretations of the legitimacy and practice of public data re-use[11] mean that the

---

[9] Hustinx P. (2004), European Data Protection Supervisor Annual Report 2004, (retrieved from http://www.edps.eu.int/publications/annual_report/2004/Annual_Report_2004_EN.pdf); EURODAC (2005), *eGovernment Observatory EURODAC confirmed as a key asylum management tool for the EU*, (retrieved from http://europa.eu.int/idabc/en/document/4385/5860).

[10] House of Lords European Communities Committee (1999), *Fingerprinting illegal immigrants: Extending the Eurodac Convention*, Tenth Report, Session 1998-1999, (retrieved from http://www.publications.parliament.uk/pa/ld199899/ldselect/ldeucom/69/6901.htm).

[11] EU Directive 2003/98/EC on the Re-use of Public Sector Information of the European Parliament and of the Council of 17 November 2003, Official Journal L345, 22/06/2001, p. 90.

political and operational agencies have to adapt to ad hoc crises and work in a fluid environment where borders and jurisdictions are ever-more flexible and eroding.

Heightened concerns over combating international crime and illegal immigration underscore the need for collaboration. However, moving from the rhetoric to the realities of collaboration is difficult. At the EU level, inter-governmentalism facilitates procrastination in decision-making and implementing steps on a consistent, uniform basis. It may be the only way to speed up a common position or responses to new threats. However, it results in new instruments and structures being glued onto or put alongside the existing *acquis* yet outside supranational accountability rules. While justifiable in times of crisis or emergency, function creep begs questions once normalised across increasingly securitised domestic policy areas.

Institutional complexity complicates thinking about security in a Europeanised setting, let alone scrutinising and communicating security within and outside the EU setting. From the EU Council Presidencies, the High Representative and diplomatic missions, special Commission task forces, member government ministers and supranational and national parliaments to local judicial, border, security and police forces, there is ample scope for variation of emphasis, linguistic nuance and the sensitivities of traditional alliance loyalties to intervene in ways that may create the impression of a degree of diversity. This can be exploited by domestic, civil society and external players.

In addition to these constraints are those relating to the relative and discretionary competence of the European Parliament and national parliaments to scrutinise 'security' policies. Under the inter-governmental arrangements of pillars II and III, national parliaments might be expected to play a role. However, traditionally they are excluded from adequately scrutinising national executive action in areas subject to exceptionalism on grounds of public security. This originated historically in relation to secrecy requirements under foreign diplomacy and defence. In the EU, the European Parliament continues successfully to fight for greater legislative authority, but incremental increases have not kept pace with the fast-expanding agenda of internal and external 'security'. Neither the European nor national parliaments have legal instruments to oblige the Commission or Council to disclose information or to consult them before decisions are implemented.[12] The new Constitution would have improved this situation. Similarly, judicial control differs over both policy pillars. The Court of Justice may interpret conventions and resolve disputes between member states where this is expressly provided for in the treaties.

An added layer of obscurity arises from the multiplicity of complex programmes and cooperation arrangements.[13] Groups within the EU also work together on internal security matters, as in the G6 (UK, Germany, France, Italy, Spain and Poland) Heiligendamm March 2006 meeting of the Ministers of the Interior. They too take decisions that may shape EU thinking, but these meetings are not routinely presented to parliaments and receive little publicity in many member states.[14] Yet their discussions on the tensions between data protection and cooperation in police and law enforcement matters are pertinent and a matter of public interest. The European Parliament's LIBE Committee in 2006 tried to insist on safeguards and

---

[12] Monar, J. (1995), "Democratic Control of Justice and Home Affairs: The European Parliament and the National Parliaments", in R. Bieber & J. Monar (eds), *Justice and Home Affairs in the European Union. The Development of the Third Pillar*, Brussels: European Interuniversity Press, pp. 243-257.

[13] Apap, J. & Carrera, S (2003*), Progress and Obstacles in the Area of Justice & Home Affairs in an Enlarging Europe*, CEPS Working Document No. 194, p. 6.

[14] *Behind Closed Doors: the meeting of the G6 Interior Ministers at Heiligendamm*, European Union Committee 40th Report of Session 2005-2006. (retrieved from http://www.publications.parliament.uk/pa/ld200506/ldselect/ldeucom/221/22102.htm).

not just on the principles of proportionality and necessity as criteria for establishing whether the processing (and exchange) of personal data are legitimate, but also on the protection of sensitive information such as biometric and DNA data. Crucially, MEPs wanted consistency between the data protection rules applicable to Europol, Eurojust and the Customs Information System (exempted from the proposal because they have their own systems) and those of the Framework Decision.[15] Such procedural discrepancies are magnified by institutional complexities, and weak accountability and transparency.

This is illustrated by the growth in the establishment of new bodies, such as Commission task forces. The Immigration Task Force first met in September 2006. Coordinated by JHA Commissioner Franco Frattini, its deliberations range across supranational and inter-governmental issues. Its advocacy of new steps to improve EU responses to migration problems, in non-EU states bordering or close to EU frontiers, through the provision of local aid covers numerous sensitive policy areas. Priorities will have to be set if the intended Commission Communication for the December 2006 European Council is to be coherent and workable. Within the EU itself, numerous committees and working groups prepare work done by COREPER. The system of comitology is opaque. Member governments and/or the EU have set up a whole series of non-community agencies, which are loosely entwined in European integration. Different working groups, committees and agencies dealing with similar issues deliberate separately with different reporting mechanisms. The need for effective coordination may be obvious but making it happen is tortuous. Problems in e-governance for routine domestic service delivery are compounded by endemic weak coordination within national administrations[16] and more so in relation to security. Most security-related non-Community agencies, such as the European Defence Agency (CFSP) and Europol or Eurojust (JHA), were set up in secret, thereby adding to the institutional and legal obscurity of the activities they undertake.[17] These practices underscore the lack of accountability present in these pillars. Institutional complexity within the EU itself compounds problems of liaison, opacity, confusion and weak communication.

For citizens, it can be difficult to verify reliably at which level decisions are made, and at times, this suits governments when adopting measures that they know are unpalatable domestically. This puts a greater onus on MEPs to augment their authority at the supranational level and to complement it with much closer cooperation with (sometimes recalcitrant) national parliaments. Even when pressure to require accountability to parliaments sometimes pays off, the situation can still be complicated. In the case of the European Drugs Monitoring Centre in Lisbon, MEPs eventually got membership of the EMCDDA Bureau: a step in the right direction but still far short of mandatory parliamentary accountability. Given that this body also has a cooperation agreement with Interpol on police collaboration, and takes operational initiatives with implications for public policy in the EU, this is not entirely satisfactory. Similarly, initiatives on matters relating to critical infrastructure encroach domestic employment policies and practices (as in the recruitment of maritime and other transport workers) where some states, both inside

[15] EP:Decision on the committee responsible, 1st reading/single reading, CNS/2005/0202:15/5/2006 (available on the European Parliament Legislative Observatory).

[16] Modinis Progress Report (2006), *Breaking Barriers to eGovernment*, August 2006, (retrieved from www.egovbarriers.org).

[17] Den Boer, M. (2004), "The European Convention and its Implications for Justice and Home Affairs Cooperation", in Apap, J. (ed), *Justice and Home Affairs in the EU: Liberty and Security Issues after Enlargement*, Chelthenham: Edgar Elgar.

and outside the EU, may check the legal status of workers against immigration and other databases, as is the case in the US.[18]

It is important to recognise that whereas member governments (and certainly several presidencies since Tampere) seem to have a JHA vision and plans, and while the Commission openly and quietly communicates what initiatives are intended, their implementation may deviate significantly from the ideals and contemporary expectations of parliamentary accountability and legitimacy procedures. Soft instruments of security and soft law mechanisms flourish; voluntarism and framework regulations occupy the spaces where constitutional accountability is evaded, weak or barely existent. The disingenuous claims of enhanced accountability to individuals through the medium of e-participation (notwithstanding the criticisms of democratic inequity, digi-divides and non-inclusion[19]) do not disguise the absence of effective political accountability and judicial scrutiny, review and legal certainty. Heterogeneous legal frameworks with different requirements and variable rules on transparency and freedom of information persist alongside a growth in disparate codes of practice not subject to parliamentary scrutiny and control.[20]

All in practice weaken the claim that public accountability should be demonstrated through representative, elected parliaments. Transparency, open disclosure of information, organisational audits and public reporting are not sufficient substitutes for accountability. They may be elements of political, constitutional and legal accountability, but democratic accountability relies on the existence of the open forum of parliaments to legitimate and challenge political authority and prevent the abuse of power by ensuring that ultimate decisions have to be explained, justified, confronted, judged and debated openly. In the security field, the plethora of forums and arrangements masquerading as guarantees of good governance (such as peer reviews, audit trails, 'transparency' disclosures, reports to parliaments and oversight bodies) results in too many disparate procedures. Interconnected agencies are subject to different rules and oversight. While it may be weakly protested that this is better than nothing, it ultimately does democracy and the principles of constitutional accountability on which it rests a disservice. It does not help to overcome the democratic accountability deficits in the increasingly slippery security domain where disconnection and murky messages may ultimately weaken the sustainability of the democratic polities and territorial political spaces enhanced security policy is supposed to boost.

1.3. Disconnection and mixed messages: Biometric insecurity

Transparency is a much vaunted goal of government and commercial bodies. Transparency is a precondition of credible communication. In the EU and member states, there is a mismatch between this goal and the set of principles and procedures used to realise internal security objectives. This is a source of inadvertent confusion, ambiguity, distrust and disconnection. It can be illustrated by reference to the introduction and justification used to deploy biometric identifiers for state security purposes and prevent fraud. The tool of biometrics has been poorly communicated with the result that the spectre of 'big brother' can be inferred from steps to

---

[18] *Security Document World Press Release*, 6 April 2006, (retrieved from http://www.securitydocumentworld.com/public/news.cfm?&m1=c_11&m2=e_0&m3=e_0&m4=e_0&subItemID=485#).

[19] *Information, Communication & Society*, special issue on Disability, Identity and Interdependence, 9(3)2006.

[20] Council of Europe (2005), *National Laws: Implementing the Data Protection Convention*, August, (retrieved from http://www.coe.int); Kranenborg, H. &W. Voermans (2005), *Access to Information in the European Union. A Comparative Analysis of EC and Member State Legislation*, Groningen: Europa Law Publishing,

enhance the capacity of existing JHA instruments to contribute to combating international organised crime and thereby enhance EU security. Trafficking in children and illegal migration, (several migrants allegedly claiming welfare benefits for the same child[21]) have all provided governments with a justification for experimenting with biometrics in a way that leaves open the possibility that inter-operability will potentially compromise privacy.

This is especially true in respect to JHA instruments, such as SIS II, Eurodac[22] and the European Automated Fingerprint System (AFIS[23]) which involves central data storage and a means for member states to compare fingerprints.[24] Under JHA provisions, member governments may act on their own initiative. For example, steps can be pioneered to advance cooperation among agencies in two or more member states pending EU-level action as envisaged by the Hague Action Programme even if delayed because it is sensitive and contentious.[25] Under the Prüm Convention, signed by seven member states in 2005, the exchange of fingerprint information proceeds on a bilateral basis pending the adoption of an EU instrument. In this instance, the Commission envisages instruments to link national DNA databases[26] and to link in fingerprint databases as well, something that many member governments condone implicitly and something that the Commission would not have commented on publicly unless the majority of governments agreed. The Council has discussed at what age a child's fingerprints may be compulsorily taken for EU passports. The decision rests not with parliaments, but with a 'comitology' committee meeting in secret – the so-called 'Article 6' Committee. Chaired by the Commission, it comprises 25 government representatives. Its output informs discussion within Council working parties and any resultant documents are not open to effective parliamentary public scrutiny.[27] The line to be taken by the governments is being discussed in Council working parties and the documents are secret.

The problems of weak communication and inadequate accountability are highlighted when consideration is given to the purpose of linkage in e-government applications. There is no point in linking such repositories, unless they are interrogable and therefore inter-operable and accessible by law enforcement authorities with legitimate purposes for seeking access from within and across the member states. The principle of availability, supported by the Hague Programme, underpins these operational requirements for access. However, there is a lack of sufficient clarity over what steps are or would be in place to prevent abuse by corrupt agencies

---

[21] The BBC (retrieved from http://news.bbc.co.uk/1/hi/uk_politics/4773005.stm) reported that the fingerprints of migrant children under 5 years old were being taken to combat fraudulent welfare claims.

[22] Convention determining the state responsible for examining applications for asylum lodged in one of the member states of the European Communities, Dublin Convention, OJ C254, 19 August 1997 (retrieved from http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=41997A0819); Reports that the European Parliament's Committee on Citizens' Freedoms and Rights, Justice and Home Affairs rejected a proposal from the Council to transfer implementation of the Eurodac system from the Commission to the Council. 30 August 2000 (retrieved from http://www.europarl.eu.int/press/sdp/newsrp/en/n000830.htm#3).

[23] Council Regulation (EC) No. 407/2002 of 28 February 2002 laying down certain rules to implement regulation (EC) No. 2725/2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention, OJ L62, 05.03.02 (retrieved from http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_062/l_06220020305en00010005.pdf); Commission communication regarding the implementation of Council Regulation (EC) No. 2725/2000 'Eurodac', OJ C5, 10.01.03. (retrieved from http://europa.eu.int/eur-lex/pri/en/oj/dat/2003/c_005/c_00520030110en00020002.pdf).

[24] http://europa.eu.int/scadplus/leg/en/lvb/l33081.htm

[25] Bigo, D. (2006), "Liberty: whose liberty? The Hague Programme and the Conception of Freedom", in T. Balzacq and S. Carrera (eds), *Security versus Freedom*?, pp. 35-44.

[26] Balzacq T., D. Bigo, S. Carrera & E. Guild, "The Treaty of Prum and EC Treaty: two competing models for EU internal security," in T. Balzacq and S. Carrera (eds), *Security versus Freedom*?, pp. 115-136.

[27] http://www.statewatch.org/news/2006/jul/9403-rev1-06.pdf

from states with somewhat weak judiciaries and records of trust. Respect for law and order is taken for granted in some of the older EU member states. The attendant communication deficit exacerbates a democratic accountability deficit and public cynicism and scepticism over the overarching goal. The absence of a common code regulating liability for data misuse and damage is also problematic.[28]

Inter-operability and accessibility are crucial to maximise the effectiveness and efficiency of the various systems – and especially AFIS, SIS and Eurodac – and their contribution to enhancing the member governments' law enforcement authorities' capacity to meet and deliver JHA goals.[29] By themselves, however, they cannot overcome serious deficiencies arising from disparate practices and laws regarding access to national databases on travel documents, migration, DNA and fingerprints. The trials of fingerprinting under five years of age in the UK, the Swedish plans to fingerprint those under 12, and the German insistence on no fingerprinting under 14 undermine attempts to create a level playing field, but may be justifiable in specific instances. The EU seeks consistency under the Council Regulation No. 2252/2004 of 13 December 2004, which, in line with ICAO recommendations, provides for biometric facial images and two fingerprints. This cannot come into effect until the Article 6 committee has taken its final decision – without parliamentary reference or approval.[30] Even then, while fingerprinting of all people 12 and over will be mandatory, national exceptions will be permissible and will persist.[31]

Inadequately agreed rules on data storage, mining and inter-operability need to be urgently addressed. Similarly, the built-in likelihood of erroneous identifications arising from alphanumeric data entered into the system from false documents and technologies that can read or block RFID chips without the subject's knowledge are problematic.[32] A private British company – RFI-Smart – launched a compliance-testing service for ICAO-based ePassports and Government in August 2006, claiming that in the absence of an international compliance standard this would help ensure security, functionality and inter-operability. However, whereas there is public acceptance of inter-operability in the sense of member states providing for mutual recognition of e-identities, distrust remains *vis-à-vis* the technology, technical capabilities, operational reliability, purposes and goals, administrative practice and political purposes with respect to 'security'.[33]

The Commission acknowledged the desirability of migration and law enforcement agencies[34] to have mutual access to these databases, and to overcome disparities in access arrangements, the problems arising from delays in transmitting fingerprint data to the central unit, and the high

---

[28] De Terwangne, C. (2004), 'Accès à l'information et Organisations Internationales: le cas de l'Union Européenne', *Ethique publique, revue internationale d'éthique sociale et gouvernementale*, Vol. 6, No. 4, pp. 9-22.

[29] European Commission (2005), Schengen: from SIS to SIS II, MEMO/05/188, 01.06.2005 (retrieved from http://europa.eu.int/rapid/pressReleasesAction.do?reference=MEMO/05/188&format=HTML&aged=0&language=EN&guiLanguage=en).

[30] Regulation (EC) No. 1683/95.

[31] EU presidency proposal to delegations on setting the minimum age for recording and storing facial images and fingerprints in the chip of a passport, Doc 9403/1/06 REV 1 LIMITE, Brussels, 26.06.2006, (retrieved from http://www.statewatch.org/news/2006/jul/9403-rev1-06.pdf); (see also http://www.statewatch.org/news/2006/jul/10540-06.pdf).

[32] http://www.elektor-electronics.co.uk/Default.aspx?tabid=1&mid=386&ctl=Details&newsletter=1&ItemID=512.

[33] Modinis Progress Report, op. cit.

[34] European Commission (2004), "EURODAC detects 7% of multiple asylum applications during its first year of activity", Press Release IP/04/581, 5 May 2004 (retrieved from http://europa.eu.int/rapid/pressReleasesAction.do?reference=IP/04/581&format=HTML&aged=0&language=EN&guiLanguage=en).

rejection rate owing to the poor quality data.[35] The political sensitivities over a European Border Guard and the introduction of such a system are communicated weakly so that in some member states the impression of operations by stealth arises. Accountability and transparency being deemed to be weak, the risk is that the public will think that the governments and EU have something detrimental to individual liberty to hide by bringing forth such measures that they justify on the grounds of enhancing security. The lack of clarity over the ultimate source of accountability, responsibility and liability for data misuse, malfunction or malevolent intent underlies the trust tension and deficit. A lack of candour over what happens to the data erodes public trust[36] in the credibility of government claims on security still further.

National governments may take steps that have potentially contradictory and sub-optimal outcomes. For example, when the UK outsources public policy data to private agencies (within and outside the UK borders), political accountability is undermined along with the credibility of government claims as to the security of that data. The publicly visible guarantee that abuse of power (in this case in respect to that data) could be tracked and the authorities held accountable has to be vested in parliament. Where parliament is weak, there is a tendency for government agencies to rely on codes of practice and personal redress mechanisms that are scarcely visible, accessible, transparent or easily used by all citizens.

Whereas the Swedish government has presented proposals to amend the Swedish Personal Data Act to deal with misuse and corruption of an individual's personal integrity in the event of his digi-data being misused, accessed illegitimately or stolen,[37] few states have followed. Instead, unfounded claims as to the security of digi-data abound even though RFID cloning of chipped passports is simple[38] and even though august parliamentary committees[39] have robustly criticised governments for their naiveté and lack of clarity. All this potentially compromises the credibility of claims that new policy instruments will enhance individual and collective security.

The consequences are significant for democratic accountability and transparency of any soft measures taken to advance an obviously advantageous inter-operability in their own right within national settings. They are equally far-reaching at the supranational level where the Commission has mooted the idea of giving the infant European Borders Agency the task of managing large IT systems (such as SIS II, Eurodac and AFIS, which have detected multiple asylum applications, and presumably any other biometric database whether DNA-derived or not).[40] Its lines of accountability and public responsibility are not well known. The European Parliament, for instance, lacks a robust function or responsibility over it.[41]

---

[35] European Commission (2005*), Second annual report to the Council and the European Parliament on the activities of the EURODAC Central Unit*, Commission Staff Working Paper, SEC(2005) 839]20, June 2005.

(retrieved from http://europa.eu.int/comm/justice_home/doc_centre/asylum/identification/doc/sec_2005_839_en.pdf).

[36] Dutton, W.H., G.A. Guerra, D.J. Zizzo & M. Peltu (2005), "The Cybertrust Tension in E-government: Balancing Identity, Privacy, Security"*, Information Polity 10*, pp. 13-23.

[37] On proposals to amend the Swedish Personal Data Act, see www.birdandbird.biz/english/publications/articles/Swedish_Personal_Data_Act.

[38] See Home Office (2004*), Identity Cards: A Summary of Findings from the Consultation on the Legislation on Identity Cards*, CM6358, October (www.computerweekly.com/Articles/2006/08/07/217503/Digital+passports+can+be+cloned.htm).

[39] House of Commons Science and Technology Committee (2006), "Identity Card Technologies: Scientific Advice, Risk and Evidence", Sixth Report of Session 2005-06 (retrieved from www.publications.parliament.uk/pa/cm200506/cmselect/cmsctech/1032/103206.htm).

[40] COM (2005) 597, 24.11.2005, pp. 6-10. DNA is not strictly speaking a biometric, but issues of linkage between DNA databases are akin to those regarding biometric databases.

[41] EP Public Hearing on 'Biometrics', Brussels, 2 March 2004, (retrieved from http://www.edps.eu.int/publications/speeches/04-03-02_Biometrics_en.pdf). EURODAC detected 7% of multiple

Attempts to improve national parliament-European Parliament cooperation over scrutinising internal security initiatives have been troubled by the national parliaments' uncertain understanding of subsidiarity and jealousy over sharing information and control with their natural partner in the game of holding the executive accountable: the European Parliament. The Duff-Voggenhuber proposals for parliamentary forums would not just address the draft Constitution, but core issues, including security and justice. However, greater pragmatism is needed in respect of the reflection period on the Constitution and necessary reform may be some time in the making. Institutional complexity, fuzzy accountability and muddied transparency remain for the time being.

Consequently, it is hard to escape the conclusion that the priority remains adopting soft law 'instruments' – whether on a bilateral basis, slipped through without public debate, or whether on a supranational basis – without considered presentation to and discussion in the European Parliament's relevant committees. Significant operational advances using ICT may thereby be implemented without open, transparent discussion.[42] That is serious in its own right. It is also serious in terms of the precedent set for evading parliamentary scrutiny *ab initio* in this sphere. It can be observed that governments and the Commission no longer see the need to invoke an 'exception' to justify such steps. It is taken for granted that they are necessary to enhance 'security' regardless of any contradictory or challenging political or civil society claims.[43] Had the draft Constitution been in place, this would not have been quite so easy. National parliaments are therefore deeply mistaken in dismissing the European Parliament's efforts to rescue the constitutional core of the institutional reforms in the draft Constitution.

However, it would be misleading to infer from the existence of weak accountability provisions in constitutional and institutional arrangements a desire on the part of the public for them to be augmented and entrenched in a new constitutional design. Such an inference would imply a greater degree of public knowledge about the actual nature of existing checks and also more generalised awareness of what inter-institutional weaknesses exist in relation to enhancing public authorities' ability to improve public security. That is far from the case, as can be illustrated by a set of frustrations encountered by EU level agencies concerned with combating crime and boosting internal security cooperation.

In November 2004, at a meeting of the European Parliament's Intergroup on Law Enforcement, Organised Crime and Terrorism, the President of the European Confederation of Police (EuroCOP) lambasted the member governments' failure to agree for many months on a new Europol director. He accused them of being high on rhetoric and low on delivering results, and of making empty promises and failing to address contradictions and problems promoting collaboration among the various agencies concerned. For example, the anti-terrorism unit set up in Europol after September 11th, 2001 was closed when member states failed to share intelligence, and then reopened after the Madrid bombings. Ratification of the European Arrest Warrant proved tortuous and open to challenge. Coordination among law enforcement agencies

---

asylum applications during its first year of activity [IP/04/581] 05.05.04. See also eGovernment Observatory report on EU biometric identification system for asylum seekers, 06.05.04 (retrieved on http://europa.eu.int/idabc/en/document/2528/350).

[42] European Commission (2004), *The Area of Freedom, Security and Justice: assessment of the Tampere programme and future orientations - List of the most important instruments adopted*, Staff Working Paper, SEC (2004) 680, COM(2004) 401, Brussels, 02.06.04. (retrieved from http://europa.eu.int/comm/justice_home/doc_centre/intro/docs/sec_2004_680_en.pdf). This document identifies Eurodac as an element in the creation of a common EU migration and asylum policy.

[43] *Biometrics at the Borders: Assessing the Impact on Society* (2005), Joint Research Centre for the European Parliament's Committee on Civil Liberties, Justice and Home Affairs, EUR 21585 EN, March (retrieved from ftp://ftp.jrc.es/pub/EURdoc/eur21585en.pdf).

in practice is inordinately complicated: the EU Task Force of Chiefs of Police is not connected to any other body. Gijs De Vries, the EU's Counter-Terrorism Coordinator sits with the European Council rather than with Europol's anti-terrorism unit. None of this is much publicised. So the public may have a general inclination to favour greater collaboration among the member states to combat international crime but very little appreciation of what this would entail in practice. MEPs, too, are unclear as to the balance to be struck between implementing greater collaboration and facilitating parliamentary accountability, transparency and openness. It is not surprising, therefore, that Bill Newton Dunn, MEP, advocated the creation of a 'Euro-FBI' yet condemned EU member governments for the gap between the rhetoric and reality: the hypocrisy of internal security collaboration.[44] Similarly, concerns arise within member states where visa shopping is evident among groups of migrants seeking entry via one state to a destination state which, if initially approached, may be inclined to reject them.

The gap between rhetoric and reality illustrates discrepant and complex institutional arrangements and highlights the potential for inefficiency in combating crime on a cross-frontier basis. Inter-institutional and intra-institutional hypocrisy and communication deficiencies result in and compound the problems of communicating a clear message in the public and wider political arenas.

Institutional complexity and ambiguity make for muddled messages. Multiple differing institutional frameworks with different sets of rules complicate and inhibit clear public communication. The operational requirements of security in practice depend on minimising openness. It is not surprising that disconnection should result. However, this does not excuse inadequate communication and weak public diplomacy. If anything, in the face of the public's low knowledge and understanding about the diverse institutions, governments might be expected to want to improve public diplomacy and communication. In the security field at least, there is reason to suppose that the public would be receptive to the message. Paradoxically, there is strong public support for member governments to work more closely together to deal with common concerns, such as international conflicts, international crime and illegal immigration. However, the very instruments to do that exacerbate public anxiety over the trustworthiness of government at all levels. The introduction of biometric tools, in the name of enhancing security, is not seen by the public to be either appropriate or proportionate to the task.

2. Communicating e-security through biometrics: Clouding the medium and the message?

For some time, the introduction of biometric identifiers in travel documents has been presented as a vital tool for sustainable security. The attendant public diplomacy lacked clarity and credibility. Biometric identifiers in travel documents were presented as a means to combat international crime, but they were not accepted by the public in many states as proportionate given their linkage to the collection of additional data for unclear purposes, and given their linkage to other policy goals that were both inspired by internal security needs and sometimes seemed irrelevant. The lack of clear communication, for example, over biometric identifiers in driving licences, health cards, various smart cards, etc., raised concerns as to the overall implication of introducing relevant measures under the umbrella of claims-making in respect to biometrics.

In July 2005, the UK Presidency proposed making such identifiers mandatory components of identity cards in the EU. This contentious suggestion aggravates public distrust of political and

[44] Bill Newton Dunn, MEP, Press Release, 18 November 2004.

judicial authorities because it is not seen to be proportionate, credible or transparent. Biometric identifiers are easily portrayed in the media as transforming the individual into no more than a human bar code, which can be infinitely manipulated in secret by ICT that eludes public control. While biometrics are no more than a tool of ICT, they are readily conflated in the public eye with the idea of 'big brother': with applications by invisible authorities having the potential to abuse the data entrusted to them for other purposes; or worse that are highly susceptible to hacking. The creation of national ID card systems has been criticised as creating a 'honey pot' target for data thieves and fraudsters.[45] There are significant and legitimate concerns about: weak security and/or outsourcing government databases to third states and private companies; politicisation of authentication technologies that deter innovation; and the absence of adequate or sufficiently good data management regimes in respect to the processing, storage and access to personal data.

Calls for the creation of paradigmatic open data files to enable citizens to see how their data may be handled for purposes of judicial cooperation or security have yet to be transformed into concrete action.[46] The telecities initiative for a Charter of eRights similarly languishes even though strong calls were made for ensuring "the effective recognition and protection of concrete and measurable rights of all citizens in the Information and Knowledge Society".[47] Yet, while a distinction between commercial privacy entitlements and official privacy entitlements might be seen as a means of preventing either sphere from accessing data held in the other,[48] it is disingenuous to think that this is a solution to the entrenched problems of governmental function creep in the application and mandatory collection of biometric data regardless of the needs for transparency and accountability.

The issue of the relationship between an individual's multiple digital identities and appropriate controls and respect for data privacy and protection is too often side-stepped or fudged. Instead human rights concerns rise up the agenda as the introduction of biometric measures is justified by agencies concerned primarily with monitoring migration and combating crime and terrorism. Sight is lost of the goals, means and justifications. The risk of this happening rises when in the absence of a universal ID card, several are introduced incrementally (as in the UK) for ostensibly different purposes, such as access to e-services and socio-economic welfare benefit entitlements, local domestic travel, e-commerce, etc. Mounting public incredulity and skepticism is matched by criticism from IT industry stakeholders over confusion, a lack of clarity, wasted effort and goals outstripping ICT architectural possibilities, and the availability of appropriate technologies, as well as criticism from parliaments over bureaucratic politics and a lack of public accountability.

For instance in the UK, the House of Commons Science and Technology Committee in summer 2006 criticised the government – and especially the isolated Home Office – of miscommunication, and a lack of accountability, regarding the scope, practicalities and procurement of ID schemes. The government set up the Identity and Passport Service without properly considering technical issues of inter-operability. It focused on the use of biometrics and the choice of biometric technology before impartial evidence regarding its capacity for enhancing the performance of the system had been taken and assessed.[49] The inevitable message conveyed to the public is therefore one of at best government incompetence and at worst

---

[45] C.W. Crews Jr. (2002), *Human Bar Code: Monitoring Biometric Technologies in a Free Society*, Policy Analysis, Washington, No. 452, 17 Sep 2002, p. 16.

[46] Danish Board of Technology (2005), *Security, Privacy and active citizens in eGovernment*, Tekno Report 2005/13.

[47] Charter of eRights, Eurocities, Porto, 11/2003.

[48] Crews Jr., op. cit., p. 3.

[49] http://www.publications.parliament.uk/pa/cm200506/cmselect/cmstech/1032/1032302.htm

government concealment. This has been compounded by private industry boasting as to the opportunity for profits and growing market potential, notably in the wake of the UK government foiling of terrorism in August 2006. For example, the US Department of State awarded a $10 million contract for multi-modal biometric recognition (face, iris and fingerprints) to SecuriMetrics, part of Viisage. Several other states accelerated the introduction of digital and chipped biometric e-passports. They vary in terms of data storage capacity (with the US favouring the 64k chip), lifespan and cost. In the US, a one-off security tax helped fund their issue and in other countries the costs keep rising.[50] The market for RFID chips grew by 104% between 2005-2006, spurred by e-passports, contactless payments and personal ID card growth, and it is seen to be highly profitable by the industry.[51]

2.1. Communicating e-security

The communication of e-security has so far been channelled via anti-terrorism discourses and instruments. These include: biometric identifiers and passports; passenger name data retention and transfer; telephony transactions; and potentially inter-operable databases remotely and anonymously accessing data stored on individuals without the intervention of the individual subject. Most have received poor press. The credibility of claims as to their security and contribution to maximising state security are disputed because of discrepancies over the choice of biometrics and technology, the lack of political consensus, and the lack of political agreement over controlling their use, shared applications, supervision, and roll-out.

The European Council and the Council repeatedly underline the importance of using biometrics in databases and travel documents to enhance EU security. Selecting what and how many biometric identifiers to use was problematic because of disagreement among vested interests, partly owing to problems of reliable authentication and verification, and rapid obsolescence. Systems that allow 3-D facial imaging automatically overcome issues of enrolment and authentication[52] but ignore civil liberties and consent. Yet, they represent perhaps state-of-the-art technology. Moreover, governments are proceeding with little regard to EU preferences. The UK's e-borders scheme, for example, not only has requirements for mandatory collection of data and biometrics for everyone entering or leaving the country but is also open-ended in its commitment to "support general police and criminal justice functions".[53] The UK National Identity Register, DNA-databased ID card plans, for example, appears out of line with EU tests of proportionality.[54]

The Prüm Treaty requirement for contracting parties to set up DNA profile databases and wide-scale exchange of personal data, and cross-border policing[55] sets out intentions and operational requirements that several EU member states even now cannot meet for technical and political

---

[50] Security Document World (website) (2006), "SecuriMetrics scores DOD deal", 11 August (http://www.securitydocumentworld.com/public/news.cfm?m1=c_11&m2=e_0&m3=e_0&m4=e_0&subItemId=697).

[51] Security Document World (website) (2006), "ePassports help drive contactless chip growth", 29 August, (http://www.securitydocumentworld.com/public/news.cfm?&m1=c_10&m2=c_5&m3=e_0&m4=e_0&subItemID=718).

[52] See www.technest.co.uk

[53] Statewatch Bulletin (2005), Vol. 15, No. 3/4.

[54] The LSE Identity Project Report (2005), London, June 2005, p. 5.

[55] www.statewatch.org/news/2006/jan07italy-prum-treaty.htm

reasons. Yet borders are being defined as an essential aspect of policing[56] and subject to an overall border management strategy covering all border-related threats. The EU Data Supervisor condemned as disproportionate several recent steps to enhance database inter-operability and accessibility to surveillance authorities. The possibility that pillar I instruments will be accessed under pillar III (non-accountable) practices is of special concern as are proposals on the exchange of judicial data on criminal convictions for prosecuting crime[57] and facilitating e-judicial cooperation. In this instance, the consultation rather than co-decision procedure was used thereby averting amendments or the need to await for approval from the European Parliament, and permitting wide discretion by national governments in maintaining disparate domestic rules on the purposes for which data could be released by and to agencies apart from those directly concerned in a given criminal judicial process. Significantly, too, the Finnish Presidency initiated a discussion on moving aspects of border control, asylum, and visas in full or in part for a transitional period to pillar I in order to enhance legitimacy, minimise deficient implementation and rectify efficiency deficits.

In the meantime, the impression remains that the roll-out of ICT-enabled cooperation and related measures is out-of-step, haphazard and out-of-balance: several institutions are taking parallel and sometimes contradictory steps unilaterally and independently without sufficient regard to EU desiderata or actual practice. The danger is that public trust in political institutions in general will be further compromised. While EU institutions are aware of these risks, if the response is seen as too little too late, it will not help to convince the public to trust either the technology or the public authorities at whatever level. Fine-sounding statements of intent lack credibility.

There has been a failure of public diplomacy that has not been adequately compensated by flanking measures from the Commission. The Commission tried in 2005 to ensure that proportional steps are taken following systematic risk assessments,[58] and to launch discussion on the longer-term shape and content of inter-operable IT systems (such as SIS I, II, Eurodac, VIS, etc.) in the JHA field before more legislative initiatives are undertaken.[59] Its November 2005 Communication examined whether the "technical and operational possibilities are proportionate and compatible with the need to protect the rights of the individual" and observed that the primary role of national governments lay in furthering inter-operability. Such political correctness is somewhat disingenuous. ICT advantages are optimisable in non-territorial space. Cross-border applications in the EU, therefore, presuppose the easy permeability, if not complete irrelevance, of territorial borders. Digi-profiling replaces geographical borders in non-territorial space.

Governments portray security as the precondition for sustainable economic development and global competitiveness, and accordingly justify introducing surveillance-type measures (such as CCTV, tagging, biometric identifiers, etc.) as instruments to enhance their ability to deliver

---

[56] See note from the Finnish Ministry of the Interior to the Informal JHA meeting in Tampere, 20-22 September 2006 on the Development of an EU Integrated Border Management System for External Borders: Management Strategy, appended in the annex.

[57] http://www.statewatch.org/news/2006/aug/01eu-convictions.htm

[58] Communication of 27 April 2005 COM (2005)172 final on the Compatibility of legislative proposals with the charter of Fundamental Rights (setting out a methodology for the internal control of fundamental rights, their integration in impact assessment depending on the scope of the likely impacts and inclusion of a standard recital on the Charter).

[59] Communication from the Commission to the Council and the European Parliament on Improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs (COM (2005) 597, 24.11.2005) (retrieved from http://www.europa.eu.int/eur-lex/lex/LexUriServ/site/en/com/2005/com2005_0597en01.pdf).

security[60] and combat activities that compromise it (such as terrorism, illegal immigration, trafficking, hacking, organised crime, etc.).[61] E-security measures, such as PKI authentication tools and inter-operable databases, are part of this trend. However, concern that these measures are disproportionate is also readily linked to suspicion that the driver is not necessarily security but commercial interests seeking economic gain.[62] Herein lies a further source of public disconnection and distrust. Elected governments and parliaments do not appear to be in control: policy appears not to be initiated by them, but driven by vested private-sector global-player interests which seem to elude parliamentary accountability. Voluntary adherence to good codes of practice is not trusted as a sufficient guarantee of privacy and e-security even though several respected organisations are trying to advance good practice. The credibility gap in relation to the feasibility of e-security grows.

There is an uneasy tension between reconciling the quest for sustainable security, complete with increased surveillance and intelligence mining operations (sometimes dubbed the securitisation of society) and protection of data privacy and human rights. Balancing the two is difficult. Parliaments are the core arena for voicing concerns and ensuring that: the former does not proceed at the expense of the latter; ICT advantages are appropriately used; and individuals' fundamental rights are safeguarded, including personal data, as per the European Convention of Human Rights and the Charter of Fundamental Rights.

Public diplomacy here is again weak. The messages, from diverse sources, have been mixed and have aggravated the very trust deficit that policy-makers claim they are designed to reduce. As a result:

- The public sees these types of measures as disproportionate; the principle of availability is widely misunderstood and mistrusted.
- The public is not convinced that EU officials and governments want or are able to safeguard individual data privacy and integrity.
- The public is concerned that data and identity theft risks are increased by e-security and e-governance measures.
- The public is not convinced that police, legal and law enforcement systems are universally honest across the EU: the fudging of applicant states' ability to meet EU criteria (notably in the JHA realm) does not allay fears that corruption is widespread and jeopardises the integrity of individuals and the state that purports to safeguard them.

---

[60] Green Paper on a European programme for critical infrastructure protection? (COM (2005) 576, 17/11/2005).

This defines prevention as: the range of deliberate, critical tasks and activities necessary to build, sustain, and improve the operational capability to prevent, protect against, respond to, and recover from an incident. Prevention involves efforts to identify threats, determine vulnerabilities and identify required resources. Prevention involves actions to protect lives and property. It involves applying intelligence and other information to a range of activities that may include such countermeasures as deterrence operations; heightened inspections; improved surveillance and security operations; investigations to determine the full nature and source of the threat; public health and agricultural surveillance and testing processes; immunizations, isolation, or quarantine; and as appropriate specific law enforcement operations aimed at deterring, pre-empting, interdicting, or disrupting illegal activity, and apprehending potential perpetrators and bringing them to justice. Prevention involves the stopping of an incident before it happens with effective processes, guidelines, standards and certification. Seamless interactive systems, and comprehensive threat- and vulnerability analysis. Prevention is a continuous process of ongoing actions to reduce exposure to, probability of, or potential loss from hazards. (full text retrieved from http://www.europa.eu.int/eur-lex/lex/LexUriServ/site/en/com/2005/com2005_0576en01.pdf).

[61] COM (2005) 597, 24.11.2005

[62] http://www.odwyerpr.com/members/0127biometrics.htm; http://www.prwatch.org/node/4409; B. Hayes (supra note 2).

- The public is concerned that human rights will be forfeited on the altar of operational requirements for success in maintaining 'security'.
- The public fears that function creep will: compromise any quality or ethical codes of practice in cross-border transfers of information; that governments will justify inadequate controls on grounds of 'exceptional circumstances'; and that outsourcing will not be appropriately regulated or transparent; and national parliaments are not believed to be credible guardians of national security interests or of those issues raised under JHA.

2.2. Communicating e-(in)security

In many member states, there is a two-dimensional trust deficit: both elements of trust are missing. Politically, governments within the EU are not always sufficiently clear and open about the extent to which they envisage ICT being used on an inter-operable basis founded on some degree of central data storage. Technically, emerging common standards are fragile and evermore speedily eclipsed by technological advances. Technical success requires this; political acceptability may rest on obfuscation. Opacity endangers both. Practical experience informs cooperation more generally and reveals the problems of transition between the political strategic goals and the technical and the operational requirements for greater extra-EU and intra-EU inter-agency cooperation, notably in the sphere of internal security, policing immigration and law enforcement.

The technical dilemma of e-policing and e-judicial cooperation is complex and multi-faceted, but parallels the political dilemmas. Central to overcoming the dilemma lie questions of creating the precondition to making judicial cooperation sustainable: trust. From a political perspective as well as a technical one, this requires the creation of mutual understanding, flexible systems, locally enforceable procedures, secure methods of tracking and tracing on-line actions (and auditing them), and ensuring that the procedures and practices comply with local (domestic national and EU-level legislative requirements). Just as in politics, the key questions are who, when, why, how and where?

This is not just about rights and obligations, trading, protection, and tracking and tracing transactions. It is about the creation of strong, secure authentication and authorisation systems that can be used in a context of mutual trust by those committed to a common goal: secure judicial cooperation for security. It is about creating applicable, simple technologies that protect ownership and control over privacy while fostering secure e-judicial transactions. The problem for the EU is that this is not adequately communicated at any level within the member states or by the EU itself. Instead, the public faces a sea of communications and advertising claims about the alleged benefits of more RFID roll-out. The claims-making and experience are out of balance.

The Council of Europe's report in 2005 advanced ideas on how Convention 108 (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data) should be applied to biometric data.[63] A special Eurobarometer report revealed public concern with ensuring that ICT, and especially data protection issues, were adequately regulated and controlled in order to protect them against misuse and abuse. In all countries surveyed, a majority believed that protecting information about private life from misuse and exploitation is

[63] Council of Europe (2005), Progress report on the application of the principles of Convention 108 to the collection and processing of biometric data, February 2005, (retrieved from http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection/Documents/Reports/O-report%20BIOM%202005.asp).

'very important'. The greatest concern was expressed in the Czech Republic (81%), Greece (78%) and the UK (77%). Support for using ICT measures to enhance efforts to combat crime in general is high: over a third of respondents felt that measures to track cars, for example, should only be introduced if strictly regulated.[64] Little linkage is made between abuse between commercial and anti-crime applications, however, unless the issue is directly relevant to civic, ethnic or minority groups in highly visible but sometimes transient circumstances.

3. Communicating internal security

Communicating internal security issues is intrinsically difficult in view of the fuzzy subject matter as to what constitutes internal security and home affairs; and the legitimate (but ever more flexibly interpreted) requirements of secrecy[65] (or non-transparency) to combat fraud and enhance operational success in addressing one of those elements generically known as international crime. The exchange of classified information with international or national agencies provokes suspicion especially when third parties are concerned. The EU tried in September 2006 to clarify this.[66]

Whereas citizens may applaud domestic efforts to improve law and order[67] (however defined), the raft of instruments adopted to augment this through European agencies is neither transparent nor trusted. Imprecision is the norm and not merely because legal convergence is elusive. Public suspicion of disproportionate tools being deployed to combat imprecise but anxiety-inducing goals is typical, and political justification seems increasingly less credible. Communicating security therefore is readily distorted.

Constitutional and institutional weaknesses allow member governments and the EU's executive branch to permit function creep and a progressive securitisation of domestic policy in a way that escapes parliamentary accountability and control. The concomitant absence of public legitimisation of decisions taken and implemented on the basis of soft law instruments contribute to the general public trust deficit in the EU. As in the past when public confidence and approval of the EU has been in decline, member governments have left the Commission to devise a strategy to reverse the trend. In 2005, following the negative votes on the draft Constitution in France and the Netherlands, the Commission expedited its overhaul of its own information dissemination and produced a communication strategy: 'Plan D'. This did not address adequately the key constitutional deficiencies, including internal administrative, organisational and budgetary constraints,[68] nor did it confront the real weaknesses in communicating Europe to citizens within the member states. Equally problematic, it did not

---

[64] Eurobarometer (2005), *Social Values, Science and Technology*, Special Eurobarometer, June, p. 91.

[65] Commission Decision of 2 August 2006 amending Decision 2001/844/EC, ECSC, Euratom (2006/548/EC,Euratom) OJL215/38-43 with annex on common minimum standards for industrial security underlining national security agencies' responsibility for maintaining the security of classified EU information.

[66] Information Note from the General Secretariat of the Council to Delegations on the Exchange of EU Classified Information (EUCI) with third countries and organisations, Council of the EU, Brussels, 1260/70 LIMITE, 8 September 2006.

[67] In December 2005, Eurobarometer reported that for one European citizen out of four, crime is one of the most important issues facing their country (24%). In comparison to spring 2005, more people considered terrorism one of the two most important issues facing their country. However, this increase is limited to a few countries, and in particular those where terrorist attacks or threats took place (UK, NL) and Denmark, despite the absence of attacks or real threats (+20 points). In other countries like Germany (4%) or Portugal (1%) and in the new member states (3%) terrorism is not an important issue.

[68] European Commission (2006), White Paper on European Communications Policy COM(2006) 35 final, 1 February 2006.

address sufficiently the real problem of communicating EU policy matters in an authoritative and trustworthy way to which citizens could relate directly. As a result, the trust deficit has not been tackled head-on. Yet, the trust deficit is the context within which the other steps are taken. This is especially problematic given the accelerating pace for introducing and expanding securitisation instruments that are justified in terms of operational needs of law enforcement authorities.

The failure to acknowledge core elements of this trust deficit is risky. This is compounded by institutional practices that continue to minimise transparency and marginalise the traditional visible guardians of the interests of the people: parliaments. The latter fail to perform three of their chief functions as i) the grand forum, ii) the voice of the people, and iii) education and communication. This failing is general across the member states. Transparency initiatives that disclose the beneficiaries of agricultural funds and regulate lobbying may divert attention from the bigger issue of universal co-decision. They do not mask how governments continue to use the European Parliament as a secondary scapegoat for either their collective evasion of their duty of openness *vis-à-vis* citizens, or their resistance to the universal co-decision to make pillar III subject to open, democratic accountable parliamentary control at the EU level, and national parliamentary scrutiny at the level of the member states.

Pending constitutional reform, there is a need for particular vigilance on the part of MEPs and a high degree of detailed knowledge about how soft law instruments are used to expand the remit, authority and scope of application of law enforcement agencies. This was exemplified by the problems in opening up the Council when it acted in legislative mode, and the insufficiency of inter-institutional candour in December 2005 on the proposed directive on data retention.[69] In theory, some MEPs are well placed to discover and communicate identifiable deficiencies and seek transparent discussion, justification and communication. In practice, civil society watchdogs and parliamentarians have to work more closely together in order to discover and challenge new steps, where necessary. As a result, MEPs continue a two-pronged process of seeking to promote, advance and facilitate transparency and openness on the constitutional trajectory. If they fail to do so, the practice of democracy in the EU is endangered and undermined in general, and in particular where pillar III and associated internal security measures are concerned.

Public diplomacy weakness is inevitable in a system where inter-governmental practice allows governments to use their discretion in setting goals before discussing the means to achieve them. The muddled or discretionary communication of security has implications that go beyond the crucial matters of civil liberties and respect for human rights. Weakness in communicating security may be due to the tendency for transparency criteria to be used as a blanket term to justify non-disclosure of information. In times of crisis, this may be legitimate and necessary for operational reasons. Traditionally, the blanket exceptionalism applied to security matters meant that non-disclosure was the norm. Disclosure in some states on identical issues now is ad hoc, inadvertent or entrenched practice. In some states, administrative bureaucratic practices and constitutional rules do not require openness and co-decision, perhaps because exceptionalism legitimatises non-disclosure and minimal transparency. This is problematic in the EU because of the implicit requirements of a uniform administrative culture to inform and communicate security matters to EU residents. This is clearly absent. It is problematic too because internal and external security cannot be compartmentalised and subject therefore to the traditional caveat of a state's sovereign right to act in complete independence. This is incompatible with being part of an ever-integrating EU.

---

[69] Peers, S. (2005), "The European Parliament and data retention Chronicle of a 'sell-out' foretold?" Statewatch Analysis (retrieved from http://www.statewatch.org/news/2005/dec/sp_dataret_dec05.pdf).

3.1. Communicating security: A problem of management or a problem of mediated governance?

Managing communication at whatever level, but notably at the level of officials and particularly *vis-à-vis* the public domain, raises problems typical of mediated governance. Openness and secrecy are not necessarily contradictory since more openness, meaning less obscurity, could clarify when and why security is needed. A wide and diverse agenda characteristic of the traditional conduct of international diplomacy as well as bureaucratic and agency management of the kind and content of information to be put into the public domain have to be taken into account to counter facile assumptions about communicating security. They can be broadly typified as i) the cultural framework; ii) the organisational framework with its socio-economic-politico culture of managing competition over resources; and iii) the perceptual framework of risk.

Cultural framework of secrecy and obscurity

The traditions of secrecy in international diplomacy, crises and interaction are challenged and assisted by mediated governance. The concomitant availability of competing information and disinformation sources mean that even for small unitary societies, deciding what, to and by whom information should be communicated is complex. It is especially so in the multi-layered EU grid. Security risks and crises are normally dealt with in a necessarily rather secretive manner. This principle is contested when exceptionalism and function creep collide with the principles of openness and accountability, de-stabilising the assumed balance between liberty and security, and challenging the sufficiency of government communication of security as well as the justifiability of ever-increasing exceptionalism and attendant measures that potentially limit individual liberty. The communication of security becomes important when public distrust in the message metamorphisises into distrust of the agents of government. The problem is all the greater at the EU level given the absence of a single EU ultimate locus of political authority, the lack of a cohesive, homogeneous European public sphere and civic society, and government ambiguity over the relative authority of supranational over national political agents (usually expressed in terms of sovereignty and subsidiarity claims).

Organisational culture

Communicating information, especially sensitive information, in the security context is a highly delicate task. Strategic, tactical and operational requirements mean that timing, wording, the medium and the target audiences have to be carefully weighed in order not to jeopardise success. This requires knowledge of the agendas as well as the practices and nature of how policy circles work at all levels and *vis-à-vis* operational agencies, such as police and border agencies. It depends on careful planning and an ability to make a fair assessment when deciding whether certain information should be disclosed or kept confidential. Even then, within government departments and media agencies, group think, bureaucratic politics, reliance on sub-optimal, pre-selected options and a tendency not to re-appraise decisions in light of new evidence can inhibit appropriate responses. They can also exacerbate communication deficiencies arising from organisational failures at any level that compromise the flow of information, including inadequate financial and human resources. JHA funding, for instance, though significantly boosted by national funding, officially accounts for no more than 1% of EU expenditure. In such a nascent policy area, the organisational culture is far from homogeneous. Managing internal security with disparate media, new technology tools, human resources and traditions in flexi-territorial spaces as well as in cyber-space challenges governments to rethink the whole area.

The EU is still struggling to create the kind of public ‘loyalty’ that member states take for granted especially when pronouncing on security. Inter-governmentalism inhibits an effective

response, permits diversity and weakens coherent and consistent communication. Sometimes an advantage, its inherent disadvantages are problematic if magnified by public distrust and scepticism. This is problematic not just for governments touting their sovereign credentials, but for the overall credibility of individual and collective claims-making in the security sphere.

Selecting the tools and means to get the message across is an ill-recognised part of the communication problem. The choice affects the content and presentation of policy. These include risk and crisis management, agenda and symbolic management, and network and process management through to mediated governance.

Perceptual culture of risk and crisis

Risk management – identifying and analysing risks and making a selection of policy options and recommendations for action – requires a balance between mapping possible threats, vulnerabilities and risks and assessing possible benefits, competing values and potential costs.[70] Risk assessment can be highly subjective, perceptually skewed, culturally captured, subject to immense time and financial (and other resource) constraints, and technically and managerially complex. Managing risk depends on many criteria including the process of risk selection, knowledge of different players' and stakeholders' preferences, priorities, strengths, weaknesses, proclivity to entertain and evaluate contradictory evidence to one's chosen options, assessment of the reliability and trustworthiness of all concerned. All these criteria become intensely compressed in crises where the tendency to remain with the courses of action chosen at the outset of a crisis are highest.[71] Within an organisation of any size, transparency of procedure even under time constraints may help improve sub-optimal outcomes, provided that it is sufficiently open to new inputs.

A perceptual culture of risk and crisis means that policy and its implementing measures can be viewed through a crisis prism in ways that lead to instruments being chosen that the public sees as disproportionate or inappropriate. Agenda-setting and management require thorough knowledge not just of the political culture of policy and diplomatic circles, but also of the media.[72] By exposing steps, the ground can be prepared for often difficult *démarches*. Symbols and rituals from the projection of images to the processes of security management are designed to prepare the ground for military or diplomatic action; communicating threats to carefully timed releases of committee papers, diplomatic visits, the announcement of unattainable positions to fall-back (acceptable optimisable-bargained outcomes) have a role in communicating policy intentions and goals, especially where broad-stroke generalised security goals are concerned. The more mundane implementing steps are commonly less carefully presented and more easily captured and skewed by agencies, industry and sectoral interests outside the political domain. Yet, effectively communicating the more mundane aspects of security is vital and significant, as experience in the EU shows.

3.2. Mediating security

Trust in the media and trust in the political processes are becoming intertwined. Their mutual dependence affects the process, content and credibility of public diplomacy communication.

---

[70] Lodge, J. with V. Flynn (1998), "The Future of the CFSP: The policy planning and early warning unit", *International Studies*, Vol. 14, pp. 7-22.

[71] Lodge, J. (1979), 'The US and the Berlin Blockade, 1948-1949', in M. Brecher (ed.), *International Crisis Behaviour*, New Brunswick: Transaction Books.

[72] Bennett, L, (2004), "Global media and politics: Transnational communication regimes and civic cultures", *Annual Review of Political Science*, Vol. 7, pp. 125-148.

Quality codes of practice and rhetoric cannot cover up sloppy journalism, poor communication, failings in public diplomacy or in democratic practice.

It is hard to depict how the media influence perception of risks and fears and the so-called 'culture of fear/unease'. Message content and what users receive relate to the structural design and the ethical standards of the media and the psychological and cultural mind-set of its users. The dynamics of the televised press conference or interview, with its emphasis on simplistic sound bites encourages politicians to be more populist and emotive.[73] Media values and structures limit and inhibit how a message is communicated, and so contribute to limiting and skewing of information. Politicians and public managers aware of this set out strategies to deal with the media; keeping them at bay or seeking out their help depending on the crisis at hand and the strategies that have been set up to resolve the situation. As such public knowledge about security issues is mediated through pre-determined filters, they may in turn already have been filtered by others subject to bureaucratic politics, the constraints of group think, sub-optimal decision-making, the socio-psychological, intelligence and organisational dynamics of 'rationality', information overload, pre-selection and perceptual skewing, time, financial, political and military pressure and other considerations including how, if and when the media is to be used to signal always partial information to the target audience.[74]

The credibility of the source of a message is an important element in establishing and sustaining trust. This is a complex arena where foreign stakeholders and media barons with different agendas than that of the EU can be powerful screens in filtering and determining media content and emphasis. This element is easily overlooked in the communication of Europe and especially in communication about open government and security. For the public, finding reliable, dependable and on-going alternative sources of information on-line is haphazard and unpredictable. Media-based preventive diplomacy[75] is not an alternative to the visible channels of democratic decision-making and the authoritative outputs of governments, parliaments and their agencies.

4. Conclusion: 'Legitimacy' – The missing link of EU securitisation

In the EU, much of the debate about the inadequacy of appropriate democratic accountability and responsibility mechanisms has taken place within the discourse of liberty and human and civil rights. Accordingly, attention is paid to the impact of deploying security tools (such as data storage in centralised and possibly inter-operable databases, biometric identifiers, verification, authentication, data privacy, PKI infrastructures, ambient intelligence, RFID and communication retention) on civil liberties. The absence of adequate parliamentary controls and the voluntary or self-regulation by stakeholders of quality codes of practice jeopardise the plausibility of policy-makers' claims that safeguards are both adequate and sufficient to deliver promised security gains and deter security breaches (including identity theft and hacking).

---

[73] Garland, D. (2001), *The Culture of Control: Crime and Social Order in Contemporary Society*, Oxford: OUP, p. 158.

[74] This was well documented by 20th century international relations scholars of communication theory, crisis diplomacy and crisis management. See for example: I. L. Janis, *Victims of Groupthink*, Boston: Houghton Mifflin, 1972; K. W. Deutsch, *The Nerves of Government*, New York: Free Press, 1966; G. T. Allison, *Essence of Decision: Explaining the Cuban Missile Crisis*, Boston: Little Brown, 1971; R. C. North, "The Analytical Prospects of Communications Theory", in J. C. Charlesworth (ed) *Contemporary Political Analysis*, New York: Free Press, 1967, pp. 300-316; I. W. Zartman (ed) *International Multilateral Negotiation: Approaches to the Management of Complexity*, San Francisco: Jossey Bass, 1994.

[75] See the Institute for Preventive Diplomacy (www.mediapeace.org).

The credibility of EU claims is endangered by the fact that most pillar III institutions and actions elude EU budgetary control, are predominantly financed by the member governments, and because any updating – and expansion of – their mandates is not subject to regular justification and authorisation from the European Parliament. Regulatory committees under comitology rule. This produces a disjunction between what the member governments and the EU publicly say and what the law enforcement and security institutions secretly or openly do. The public may well loosely approve of the latter's intentions, but the disjunction has serious consequences for the EU's credibility as the open, benign servant-of-the-people image that it seeks to evoke.

The problem of communicating security has two main elements: one relates to the politico-constitutional construct of managing the internal-external security agendas; the other to the lack of clarity over the nature and tools for effecting accountable security. The first is exemplified by the inter-governmental bargain, which deprives the commons of voice. The second is characterised by competing agendas, none of which seems to enjoy the legitimising support of an ultimate political authority that is accountable and responsive to the public whose security it seeks to ensure. Both contribute to a sense of missing legitimacy in claims that are made in the name of freedom, security and justice and steps that are taken to realise and sustain them.

Disaggregating security tools may help to illuminate what the tools can and cannot do. They are not a substitute for policy content but are easily perceived to be just that. This means that if security is to be communicated effectively, convincingly and credibly, there needs to be greater clarity over the goals themselves, their realisation through specific instruments that are demonstrably proportionate and appropriate, and the way in which they are made accountable. Without clarity of purpose, objectives, overarching goals and means for attaining them, and without effective management of conflicting perception, interests, understanding and operational goals, there is a danger that communicating security will be captured by specific sectoral interests. The risk is that their built-in tendency to skew the message to their own design obscures the overall goals of freedom, security and justice. The communication of insecurity rather than security can well result.

References

Albrecht, S. (2006), "Whose voice is heard in online deliberation?: A study of participation and representation in political events on the internet", *Information, Communication and Society*, Vol. 9, No. 1, February, pp. 62-82.

Allison, G.T. (1971), *Essence of Decision: Explaining the Cuban Missile Crisis*, Boston, MA: Little, Brown.

Anderson, M. and J. Apap (2002), *Striking a Balance between Freedom, Security and Justice in an Enlarged European Union*, CEPS, Brussels.

Anderson, P. and A. Weymouth (1999), *Insulting the public?*, London: Longman.

Anheier H., M. J. Kaldor & M Glasius (eds) *Global Civil Society 2005/6*, London: Sage.

Apap, J. and S. Carrera (2003), *Progress and Obstacles in the Area of Justice & Home Affairs in an Enlarging Europe*, CEPS Working Document, No. 194, CEPS, Brussels, June.

Apap, J. (2004), *Justice and Home Affairs in the EU: Liberty and Security Issues after Enlargement*, Cheltenham: Edgar Elgar.

Ashbourn J. (2006), *Societal Implications of the Wide Scale Introduction of Biometrics and Identity Management*, Background Paper for the EuroSci Fourm (ESOF), Munich.

Balzacq, T. & Carrera S. (eds) (2006), *Security versus Freedom?* Ashgate: London.

Balzacq T., D. Bigo, S. Carrera & E. Guild, "The Treaty of Prum and EC Treaty: two competing models for EU internal security," in T. Balzacq and S. Carrera (eds), *Security versus Freedom*?, pp. 115-136.

Banisar, D. (2004), *The Freedominfo.org Global Survey – Freedom of Information and Access to Government Record Laws Around the World*, May (retrieved from http://www.freedominfo.org).

Barber, B. (2003), *Fear's Empire: War, Terrorism, and Democracy*, New York, NY: Norton.

Beck, U. (1996), *Risk Society: Towards a New Modernity*, London: Sage.

Beers, T.A.L. (1996), "National Secrecy Interests Versus Public Access", Conference on Access to Public Information, Stockholm, 27-28 June, (retrieved from http://europa.eu.int/ISPO/legal/stockholm/en/beers.html).

Bennett, S., S. Rhine, R. Flickinger and L. Bennett, (1999) "'Video malaise' revisited: Public trust in the media and government", *Harvard International Journal of Press/Politics*, Vol. 4, No. 4, pp. 8-23.

Bennett, L, (2004), "Global media and politics: Transnational communication regimes and civic cultures", *Annual Review of Political Science*, Vol. 7, pp. 125-148.

Bigo, D. and E. Guild (eds) (2005), *Controlling Frontiers: Free Movement into and within Europe*, London: Ashgate.

Bigo, D. (2006), "Liberty: whose liberty? The Hague Programme and the Conception of Freedom", in T. Balzacq and S. Carrera (eds), *Security versus Freedom*?, pp. 35-44.

Bimber, B. (2000), *"The Study of Information Technology and Civic Engagement", Political Communication, Vol. 17, No. 4, pp. 329-33*

Biometrics at the Borders: Assessing the Impact on Society (2005), Joint Research Centre for the European Parliament's Committee on Civil Liberties, Justice and Home Affairs, EUR 21585 EN, March (retrieved from ftp://ftp.jrc.es/pub/EURdoc/eur21585en.pdf).

Brewer, P., S. Aday, and K. Gross (2003), "Rallies all around: The dynamics of system support", in *Framing Terrorism: The News Media, the Government, and the Public*, New York: Routledge, pp. 229-54.

Bunyan, T. (2002), *Secrecy and Openness in the European Union*, Freedominfo.org, September (retrieved from http://www.freedominfo.org/case/eustudy/index.html).

Burkert, H. (1995), *Public Sector Information: some implications for a European information infrastructure* (retrieved from http://herbert burkert.net/ARCHIV/1995-09-00-Vienna.pdf).

Bunyan, T., D. Curtin. and A. White, (2000), *Essays for an open Europe*, European Federation of Journalists (retrieved from http://www.statewatch.org/secret/essays.htm).

Cappella, J. and K. Jamieson (1997), *Spiral of Cynicism: The Press and the Public Good*. New York, NY: OUP.

Charter of eRights, Eurocities, Porto, 11/2003.

Crews Jr., C.W. (2002), *Human Bar Code: Monitoring Biometric Technologies in a Free Society*, Policy Analysis, Washington, No. 452, 17 Sep 2002, p. 16.

Curtin, D. (2005), *Delegation to EU Non-Majoritarian Agencies and Emerging Practices of Public Accountability*, London: Routledge.

Danish Board of Technology (2005), *Security, Privacy and active citizens in eGovernment*, Tekno Report 2005/13.

Den Boer, M. (2004), *Plural Governance and EU Internal Security: Chances and Limitations of Enhanced Cooperation in the Area of Freedom, Security and Justice*, The European Policy Centre, Brussels (retrieved from http://www.theepc.net).

Den Boer, M. (2004), "The European Convention and its Implications for Justice and Home Affairs Cooperation", in Apap, J. (ed), *Justice and Home Affairs in the EU: Liberty and Security Issues after Enlargement*, Chelthenham: Edgar Elgar.

De Riviera, J. (1968), *The psychological dimension of foreign policy*, Ohio: Merrill.

De Terwangne, C. (2004), "Accès à l'information et Organisations Internationales: le cas de l'Union Européenne", *Ethique publique, revue internationale d'éthique sociale et gouvernementale*, Vol. 6, No. 4, pp. 9-22.

Deutsch, K.W., *The Nerves of Government*, New York, NY: Free Press, 1966; G. T.

De Vreese, C. (2002), *Communicating Europe*, The Foreign Policy Centre, British Council Project, (retrieved from www.network-europe.net).

Dutton, W.H., G.A. Guerra, D.J. Zizzo & M. Peltu (2005), "The Cybertrust Tension in E-government: Balancing Identity, Privacy, Security", *Information Polity 10*, pp. 13-23.

Flakheimer, J. and A. Jansson (eds) (2006), *Geographies of Communication: .The Spatial Turn in Media Studies*, Göteborg: Göteborg University Press.

Garland, D. (2001), *The Culture of Control: Crime and Social Order in Contemporary Society*, Oxford: OUP.

Grant, David, Cynthia Hardy, Cliff Oswick & Linda Putnam (eds) (2004), *The SAGE Handbook of Organizational Discourse*, Thousand Oaks, CA: Sage Publications

Guild, E. (ed.) (2006), *Constitutional Challenges to the European Arrest Warrant*, Nijmegen: Wolf.

Guild, E. and E. Brouwer (2006), *The Political Life Cycle of Data: The ECJ Decision on the PNR agreement between the EU and the US*, CEPS, Brussels.

Hands, J. (2006), "Civil Society, cosmopolitics and the net: The legacy of 15 February 2003", *Information, Communication and Society*, Vol. 9, No.2, April, pp.225-243.

Hayes B. (2006), *Big Brother: The EU's Security Research Programme*, The Transnational Institute, Amsterdam, (retrieved from www.tni.org).

Herman, E.S., and N. Chomsky (1988), *Manufacturing Consent: The Political Economy of the Mass Media*, New York, NY: Pantheon Books.

Hetherington, D. (2005), W*hy Trust Matters*, Princeton N.J.: Princeton University Press.

Hoffman J. (2004), *Citizenship beyond the State*, London: Sage.

House of Lords European Communities Committee (1999), *Fingerprinting illegal immigrants: Extending the Eurodac Convention*, Tenth Report, Session 1998-1999, (retrieved from http://www.publications.parliament.uk/pa/ld199899/ldselect/ldeucom/69/6901.htm).

Hustinx P. (2004), European Data Protection Supervisor Annual Report 2004, (retrieved from http://www.edps.eu.int/publications/annual_report/2004/Annual_Report_2004_EN.pdf); EURODAC (2005), *eGovernment Observatory EURODAC confirmed as a key asylum management tool for the EU*, (retrieved from http://europa.eu.int/idabc/en/document/4385/5860).

Irving, L.J (1972), *Victims of Groupthink*, Boston, MA: Houghton Mifflin.

James P. (2004), *Globalization and Violence*, London: Sage.

Janis, I. L., *Victims of Groupthink*, Boston: Houghton Mifflin, 1972.

Kull, S., C. Ramsay and E. Lewis (2003–2004), "Misperceptions, the Media, and the War in Iraq", *Political Science Quarterly*, Vol. 118, No. 4, pp. 569-598.

Kickert, W.J.M., E.H. Klijn, and J.F.M. Koppenjan (1997), *Managing Complex Networks*, London: Sage.

Kinga, Gál (2005), *Draft Report on the proposal for a Council Regulation establishing a European Union Agency for Fundamental Rights*, (COM(2005)0280-C6-0288/2005-2005/0124(CNS).

Kranenborg, H. and W. Voermans, (2005), *Access to Information in the European Union. A Comparative Analysis of EC and Member State Legislation*, Groningen: Europa Law Publishing.

Kuijper, P. (2004), "The evolution of the Third Pillar from Maastricht to the European Constitution: International Aspects", *The Common Market Law Review*, Vol. 41, pp. 609-626.

Lodge, J. (2006), "eJustice-Elusive or Illusionary – five dilemmas of ejudicial cooperation", *Journal of Information, Communication, Ethics and Society*, Paper No. 497, Vol. 4, No. 3, pp. 131-144.

Lodge, J. (2005), "Justice, Security and Biometrics: The EU's proximity paradox, speeding up EU judicial cooperation – problem or panacea?", *European Journal of Crime and Criminal Law and Criminal Justice*, Vol. 13, No. 4, pp. 533-564.

Lodge J. (2002), "Sustaining Freedom, Security and Justice – From Terrorism to Immigration", *Liverpool Law* Review, Vol. 24, No. 1-2, pp. 41-71.

Lodge, J. (2003), "Transparency and EU Governance: Balancing Openness with Security", *Journal of Contemporary European Studies*, Vol. 11, No. 1.

Lodge, J. (2005), "Communicating Europe - From procedural transparency to Grand Forum", in J. Lodge (ed.) *The 2004 Elections to the European Parliament*, London: Palgrave, pp. 61-78.

Lodge, J. with A. Flynn (1998), "The CFSP after Amsterdam: the Policy Planning and Early Warning Unit", *International Relations*, Vol. 14, pp. 7-22.

Lodge, J. (1979), 'The US and the Berlin Blockade, 1948-1949', in M. Brecher (ed.), *International Crisis Behaviour*, New Brunswick: Transaction Books.

Mccullagh, C. (2002), *Media Power: A Sociological Introduction*, New York: Palgrave.

Modinis Progress Report (2006), *Breaking Barriers to eGovernment*, August 2006, (retrieved from www.egovbarriers.org).

Monar, J. (1995), "Democratic Control of Justice and Home Affairs: The European Parliament and the National Parliaments", in R. Bieber and J. Monar (eds), *Justice and Home Affairs in the European Union. The development of the Third Pillar*, Brussels: European Interuniversity Press, pp. 243-257.

Muller-Wille, B. (2004), "Building a European Intelligence Community in Response to Terrorism," *ISIS European Security Review*, Vol. 22.

North, R. C., "The Analytical Prospects of Communications Theory", in J. C. Charlesworth (ed) *Contemporary Political Analysis*, New York: Free Press, 1967, pp. 300-316

Occhipinti, J. (2003), *The Politics of EU Police Cooperation: Towards a European FBI?*, Boulder, CO: Lynne Rienner.

Peers, S. (2004), "Mutual Recognition and Criminal Law in the European Union: Has the Council got it wrong?", *Common Market Law Review*, Vol. 41, pp. 5-36.

Peers, S. (2005), "The European Parliament and data retention Chronicle of a 'sell-out' foretold?" Statewatch Analysis (retrieved from http://www.statewatch.org/news/2005/dec/sp_dataret_dec05.pdf).

Prins, J.E.J. (2006), "Property and Privacy: European Perspectives and the Commodification of our Identity", in L. Guibault and P.B. Hugenholtz (eds), *The Future of the Public Domain, Identifying the Commons in Information Law* (Information Law Series, 16) The Netherlands: Kluwer Law International, pp. 223-257.

Tak, P.J. (2005), *Tasks and Powers of the Prosecution Services in the EU Member States*, Nijmegen: Wolf Legal Publishers.

Rifkin, J. (2000), *The Age of Access*, New York, NY: Tarcher/Puntam.

Sachs, H. (1995), "Computer Networks and the Formation of Public Opinion: an ethnographic study", *Media, Culture and Society*, Vol. 17, pp. 81-91.

Shore, C. (2000), *Building Europe: the Cultural Politics of European Integration*, London: Routledge.

Scandamis N., *Normative parameters of exceptionalism: Community governance patterns in the field of security and its implications for a future global governance as responding to the internal rules of globalization, existing or to be*, paper for Challenge, University of Athens, January.

Stone, D. (2002), *Policy Paradox. The art of political decision-making*, New York, NY: Norton.

Stehr, N. (2001), *The Fragility of Modern Societies: Knowledge and risk in the information age*, London: Sage.

Välimäki, M. (2005), "Software Interoperability and Intellectual Property Policy in Europe", *European Review of Political Technologies*, December.

Winston, B. (1998), *Media Technology and Society: A History from the Telegraph to the Internet*, London: Routledge.

Zartman I. W., (ed.) *International Multilateral Negotiation: Approaches to the Management of Complexity*, San Francisco: Jossey Bass, 1994.

Zwan, A. (2003), *The Challenge of Populism*, Amsterdam: Meulenhoff.

Selected Policy Documents and Statistical Data

Council of the European Union (2004), *The Hague Programme*. *Presidency Conclusions of the Brussels European Council*, 4-5 November 2004, 14292/1/0.

European Commission (2006), Proposal for a Council *Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters* (SEC(2005)1241)COM/2005/0475final-CNS2005/0202.

European Commission (2006), COM (2006) 331 final. Communication *Implementing the Hague Programme: the Way Forward*. 28 June 2006.

European Commission (2006), COM (2006) 332 final Communication from the Commission to the Council and the European Parliament. *Evaluation of EU Policies on Freedom, Security and Justice*. 28 June 2006. {SEC (2006) 815}.

European Commission (2006), COM (2006) 333 final Communication from the Commission to the Council and the European Parliament. *Report on the implementation of the Hague Programme for 2005*. 28 June 2006 {SEC (2006) 813}.{SEC(2006) 814}.

European Commission (2005), COM (2005) 490 final. *Proposal for a Council Framework Decision on the Exchange of Information under the Principle of Availability*. 12 October 2005. {SEC (2005) 1270}.

European Commission (2005), COM (2005) 317 final. *Proposal for a Council Decision on the Improvement of Police Cooperation between the Member States of the European Union, especially*

at the Internal borders and Amending the Convention Implementing the Schengen Agreement. 18 July 2005 2005/0131(CNS).

European Commission (2006), *Communication to the Council and the European Parliament on the Interoperability for Pan-European eGovernment Services*, COM (2006) 45 final, 13 February.

Council of the European Union (2006), *Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters – List of data protection provisions in other Title VI instruments*, General Secretariat, Brussels,13958/06 CRIMORG151 ,DROPEN 65, ENFOPOL 170, DATAPROTECT 40,COMIX 831,16 October.

Council of the EU (2006), *Information Note from the General Secretariat of the Council to Delegations on the Exchange of EU Classified Information (EUCI) with third countries and organisations*, Council of the EU, Brussels, 1260/70 LIMITE, 8 September.

Conseil de l'Europe (2003), Groupe des spécialistes sur l'accès aux informations officielles (DH-S-AC), 10ème réunion, Rapport, *l'accès aux documents publics*, (retrieved from http://www.coe.int).

Council of Europe (1991), *The introduction and use of personal identification numbers: the data protection issues*; Council of Europe, Study of the Committee of experts on data protection (CJ-PD)', Strasbourg.

Council of Europe (2005), *National Laws: Implementing the Data Protection Convention*, August, (retrieved from http://www.coe.int).

Data Protection Working Party (2003), *Working Document on E-Government*, adopted on 8 May; Article 29, 10593/02/EN, WP 73.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) Official Journal L 201, 31/07/2002, pp. 0037-0047.

Directive 2003/98/EC on the Re-use of Public Sector Information of the European Parliament and of the Council of 17 November 2003, Official Journal L 345, 22/06/2001, p. 90.

White Paper on European Governance, *Report of Working Group 1a: Broadening and enriching the public debate on European matters*, June 2001.

White Paper on European Governance, *Report of Working Group 4b: Networking people for a good governance in Europe*, May 2001.

Eurobarometer (2004), *Attitudes and expectations of viewers in terms of television programmes with a European content*, November.

Eurobarometer (2002), *Getting information on Europe, the enlargement of the E.U. and support for European integration: European public opinion takes the floor*, Eurobarometer 56.3, May.

Eurobarometer: *Europeans and languages*, September 2005.

Eurobarometer (2005), *Public opinion in the European Union*, Standard Eurobarometer, December.

Eurobarometer (2004), *Citizenship and sense of belonging*, Special Eurobarometer, February.

Eurobarometer (2004), *Justice and Home Affairs*, Flash Eurobarometer, March.

Annex

Ministry of the Interior

Informal JHA Ministerial Meeting

Tampere, 20-22 September 2006

DEVELOPMENT OF THE EU'S INTEGRATED MANAGEMENT SYSTEM FOR EXTERNAL BORDERS; BORDER MANAGEMENT STRATEGY

Significant progress has been made in developing an integrated EU border management system.

Important issues here include: the establishment of Frontex, the External Borders Agency; the adoption of the regulation establishing a community code on the rules governing the movement of persons across borders (the Schengen Borders Code), the regulation laying down rules on local border traffic at the external land borders of the member states, amending the Schengen Convention and the Common Consular Instructions.

To ensure the constant development of EU border management, the Presidency proposes that political strategic guidelines, namely the EU border management strategy, be adopted. The strategy includes the main definitions concerning integrated border management. It also helps to specify the role of the Council, to increase the transparency of border control, to reinforce cooperation between national authorities and to deal with initiatives related to the development of border management. Moreover, the strategy provides an outline for the conduct of external relations in the field of border management.

Definitions: The Presidency aims to define 'integrated border management' as unambiguously as possible. In the Presidency's view, integrated border management should consist of the following dimensions:

- border control (checks and surveillance) as defined in the regulation establishing a community code on the rules governing the movement of persons across borders, including the necessary risk analysis and criminal intelligence investigation of cross-border crime.
- a four-tier access control model (measures in third countries, cooperation with neighbouring countries, border control and control measures within the area of free movement).
- cooperation between the authorities in the field of border management at the national and international level (border control, customs and police authorities, security services and other relevant authorities).
- coordination and coherence of action taken by member states and institutions.

The key principle is that *border management must cover all border-related threats.*

Specifying the role of the Council: In the Presidency' view, the Council should play an active role in providing political and strategic guidelines. The Council should authorise SCIFA, together with representatives of the authorities responsible for integrated border management to continue its work in this field. This work must be carried out in such a way as to support the on-going work of Frontex and other institutions with due regard to the workload arising from previous obligations.

Increasing the transparency of border management: The trust and confidence of citizens in the European Union increasingly requires successful border management. In the Council's view,

border management policy must be implemented at all external borders in a more transparent manner, both between the member states and towards relevant institutions. This will require the development of common risk analysis and evaluation methods.

Cooperation between national authorities: criminal intelligence, implemented in cooperation between the Border Guard, customs, police, and the national security services is the recommended practice according to the Schengen Evaluation Committees. The Presidency proposes this model as a form of 'best practice'.

The external dimension: border management is visible with the external relations of the EU in many ways. It is then appropriate to adopt guidelines, where appropriate, and to guide EU support projects and contacts with cooperation partners with a EU perspective. All of the states in the Western Balkans have been given a perspective of future membership to the European Union. It is important to retain the requirements of specialisation and professionalism, although the creation of too large an administrative capacity should also be avoided. Regional flexibility measures should be introduced.

No exceptions can naturally be allowed in the case of binding provisions, such as the regulation establishing a community code on the rules governing the movement of persons across borders.

The countries participating in the accession process should immediately engage in extensive cooperation with the EU and its member states. The immediate requirements should include, *inter alia*, efficient control of illegal exits from a candidate country to a member state and effective returns. This should be made part of all contacts with EU candidate countries. The Council recommends that the member states and the institutions support permanent professional contacts across the external borders of the Union. The principle of a gradual build-up of professionalism may be used in various projects implemented in third countries (countries without a member state perspective).

Initiatives related to the further development of the border management system: with regard to joint operations, it is necessary to discuss national resources and the criteria for funding and to support the External Borders Agency, Frontex, by issuing appropriate guidelines. In its communications, the Commission stresses the importance of a number of initiatives concerning the further development of the integrated border management system. At present, the most pressing is the initiative on the powers of the expert teams, which operate under the guidance of Frontex in respect to a draft regulation that is already under discussion (the so-called RABIT Regulation).

The Presidency considers it important that swift progress is made in this matter – a simple and efficient system is our goal. Issues relating to the resources of joint operations should also be settled. Other initiatives to be dealt with here include cooperation in the issuing of visas; the establishment of a common entry-exit register of third-country nationals; the creation of a common database for travel documents; a study to assess the so-called Trusted Traveller Programme; and the development of common access to EU databases.

In light of the recent events in the Mediterranean region, the Presidency considers it essential to develop not only joint EU operations, but also regional cooperation between border authorities. The Baltic Sea region has an effective cooperation model in use where all states in the region – both EU Member States and Russia – have been cooperating at an operational level for ten years now. A similar model has been developed for the Mediterranean in the framework of the Medsea project of Frontex.

The Presidency's strategy for border management was discussed at the meeting of the Strategic Committee on Immigration, Frontiers and Asylum (SCIFA) held on 5 July 2006. Based on the

numerous comments received following the meeting, the Presidency drew up a new official document, which was discussed at the informal SCIFA meeting on 3-5 September.

Questions:

1) The Finnish Presidency aims to reach an agreement on the definition of the integrated border management system in a manner that would be appropriate to describe the on-going progress and its results. Another aim is to establish clear criteria for the discussion and joint projects between candidate countries, third countries and other international partners. Do the member states agree on the usefulness and content of the definition?

2) The Presidency requests comments on whether SCIFA should still be obligated to actively monitor the development of the integrated border management system and to discuss the matter, where necessary, together with representatives of the authorities responsible for integrated border management.

3) What are the positions of the member states on the policy guidelines, which deal with the principles of transparency, cooperation between various authorities and external relations?

About CHALLENGE

The familiar world of secure communities living within well-defined territories and enjoying all the celebrated liberties of civil societies is now seriously in conflict with a profound restructuring of political identities and transnational practices of securitisation. CHALLENGE (Changing Landscape of European Liberty and Security) is a European Commission-funded project that seeks to facilitate a more responsive and responsible assessment of the rules and practices of security. It examines the implications of these practices for civil liberties, human rights and social cohesion in an enlarged EU. The project analyses the illiberal practices of liberal regimes and challenges their justification on the grounds of emergency and necessity.

The objectives of the CHALLENGE project are to:

- understand the convergence of internal and external security and evaluate the changing character of the relationship between liberty and security in Europe;
- analyse the role of different institutions in charge of security and their current transformations;
- facilitate and enhance a new interdisciplinary network of scholars who have been influential in the re-conceptualising and analysis of many of the theoretical, political, sociological, legal and policy implications of new forms of violence and political identity; and
- bring together a new interdisciplinary network of scholars in an integrated project, focusing on the state of exception as enacted through illiberal practices and forms of resistance to it.

The CHALLENGE network is composed of 21 universities and research institutes selected from across the EU. Their collective efforts are organised under four work headings:

- *Conceptual* – investigating the ways in which the contemporary re-articulation and disaggregation of borders imply a dispersal of practices of exceptionalism; analysing the changing relationship between new forms of war and defence, new procedures for policing and governance, and new threats to civil liberties and social cohesion.
- *Empirical* – mapping the convergence of internal and external security and transnational relations in these areas with regard to national life; assessing new vulnerabilities (e.g. the 'others' targeted and critical infrastructures) and lack of social cohesion (e.g. the perception of other religious groups).
- *Governance/polity/legality* – examining the dangers to liberty in conditions of violence, when the state no longer has the last word on the monopoly of the legitimate use of force.
- *Policy* – studying the implications of the dispersal of exceptionalism for the changing relationship among government departments concerned with security, justice and home affairs, along with the securing of state borders and the policing of foreign interventions.

The CHALLENGE Observatory

The purpose of the CHALLENGE Observatory is to track changes in the concept of security and monitor the tension between danger and freedom. Its authoritative website maps the different missions and activities of the main institutions charged with the role of protection. By following developments in the relations between these institutions, it explores the convergence of internal and external security as well as policing and military functions. The resulting database is fully accessible to all actors involved in the area of freedom, security and justice. For further information or an update on the network's activities, please visit the CHALLENGE website (www.libertysecurity.org).

An Integrated Project Financed by
the Sixth EU Framework Programme