HOUSE OF LORDS

EU SUB-COMMITTEE F (HOME AFFAIRS)
The EU Internal Security Strategy
Written Evidence

Contents

Memorandum by the Association of Chief Police Officers (ACPO) (ISS 8)

This response is compiled from the views of the relevant national leads for the areas being considered. I have broken the response down into four of the five intentions the Commission's Communication describes.

Disrupt international crime networks

Disrupting international crime networks that work across national boundaries will provide a benefit to the UK. Organised Crime Group Mapping is developing in the UK and while this is early days, it is already proving to be effective; however, ACPO's view is that it would be premature to expand this work overseas. Such a focus would be a distraction from ensuring that it is as effective as it can be in the UK while the approach is developing, and we believe that there would be a greater benefit in waiting until we have more evidence on how the approach has worked in the UK and what lessons can be learnt for emulating it elsewhere.

Prevent terrorism and address radicalisation and recruitment

The National Prevent Delivery Unit is embedded within the Association Of Chief Police Officers Terrorism and Allied Matters and has been established over the last few years and its core objective has been around Preventing Violent Extremism.

It was recognised very early on in the UK that acts of terrorism and violent extremism are crimes but due to the overlap of these crimes with polarisation, religious extremism and social segregation, law enforcement agencies alone cannot solve this problem. The threat of international terrorist attacks on society and infrastructure across Europe including the UK is highly likely. This threat is now leading to an offset in balancing integration due to the rise of domestic extremism and in particular right wing and left wing extremism.

Society is dependent on our communities and partners to help stop people becoming or terrorists or violent extremists. The main focus of all activity within the Prevent Delivery Unit has been based on effective engagement with key stakeholders across UK, without which counter terrorism initiatives would not be sustainable.

Experience has shown that the best results are achieved by:

- Partnership working and effective engagement – getting the right people working together
- Understanding the challenge and its context
- Developing an effective action plan
- Managing risk
- Tracking progress and evaluating success
- Sharing learning and best practice
- Local communities should be actively engaged in the partnership and in the development and implementation of programmes of action
- A 'whole community' approach should be taken to ensure that this work does not inadvertently lead to increased pressure on vulnerable sections of the community

Empower communities to prevent radicalisation and recruitment

The Prevent Delivery Unit has primarily focussed on the above work stream and evolved as a national co-ordination centre supporting Counter Terrorism Units across the UK. Our work has been centred around developing community based approaches and prevention policies to enable local authorities and civil society to be empowered to prevent all forms of violent extremism. We have achieved this by using the following approach:

Understanding the threat

The PDU has done an extensive amount of research based on analytical data as well as joint agency work including agencies such as Security Services, Chief Executives from local councils, etc., to map vulnerable communities and understand the nature of the threat within certain sectors of the community. This research has extended into all forms of extremism including understanding the threat towards certain vulnerable infrastructures. Information sharing outside of law enforcement agencies is crucial if we are to achieve full partnership engagement in tackling the threat of violent extremism within our communities.

Community and Partner Engagement

NPDU have also been co-ordinating responsibility for developing initiatives to empower communities and key stakeholders while also specifically addressing activities around education, health, front line sector, women and young people. The team focuses on supporting police forces and partners by developing new and existing products and applying interactive and pedagogy methods of education to raise awareness of radicalisation and recruitment within communities. Products are based on capacity building within communities. These initiatives help break down barriers as well as implement measures to enhance engagement with civil society to strengthen resilience of individuals and communities against radicalisation. The projects help maintain a measure of the impact of counter terrorism initiatives and facilitate a creation of networks which promote a positive narrative which further delegitimizes extremist narratives.

Training of agencies and law enforcement agencies around delivery of products has also been co-ordinated by NPDU in order to ensure consistency in delivery of key messages and allowing agencies to prevent further radicalisation by implementing standard referral and intervention measures.

Education has been a key area in this empowerment phase as recent history has shown that young people may be more vulnerable to prejudices and this can easily lead to radicalisation. Projects used within education can offer opportunities to help young people understand the risk associated with violent extremism and help develop their knowledge, skills and critical thinking ability to challenge the extremist narrative. This form of activity also encompasses the monitoring of local tensions within communities and addresses grievances around the impact of global and national events on local people. The empowerment and engagement techniques allow safe spaces for grievances to be aired as lack of understanding can increase the threat of vulnerability.

Partnership Interventions

The PDU have been instrumental and done a considerable amount of work to strengthen and develop a wide range of partnership interventions around identifying vulnerable individuals and creating support mechanisms for these vulnerable individuals which are community and partner led. This approach is focused on multi-agency interaction and ties intervention into other safe-guarding mechanisms that are already embedded within the

current civic society. This form of intervention enables communities to provide platforms in order to support positive narratives which can balance and negate the need for violence.

Communication

The success of any form of community empowerment relies heavily on open and transparent communication and the use of appropriate terminology. Effective communication is critical to influence attitudes and properly explain how prevention of radicalisation and recruitment needs the active participation of all partners, agencies and communities to succeed. NPDU has worked with cross government departmental agencies to develop guidance and effective methodology in communicating messages in a language that does not alienate those we wish to communicate with.

Raise levels of security for citizens and businesses in cyberspace

We have a general concern that there should be agreed, auditable and enforced controls to protect information shared between members states and with the EU institutions to ensure that the risk to citizens and to member state interests is appropriately managed. The controls should be a combination of procedural, personnel, physical or technical and achieve a common standard acceptable to all those sharing data. It may be that the Police Service needs to seek specific assurances before it agrees to share data which may, for example, assist an investigation in another member state but could if compromised prejudice an investigation in the UK.

Build capacity in law enforcement and the judiciary

PDU have embedded a Counter Terrorism Internet Referral Unit within their structure which enables the public to report unlawful terrorist and violent extremist material which they may come across on the internet. The CTIRU investigates referrals from the public, proactively seeks out illegal material on websites and works closely with industry to make it harder for terrorists to exploit the internet. Tackling terrorism on the internet is a key part of building capacity within law enforcement and the Counter Terrorism Internet Referral Unit play an integral role in helping to tackle terrorist and violent extremists from using the internet for unlawful messages and recruitment. The referrals are reported by the public through a web page and offer the privilege of anonymity to the public and agencies.

Work with industry to empower and protect citizens

It is recognised that communities and agencies such as Social Services, Education, and Youth Offending Teams play a vital role in helping to tackle terrorism over the internet. The internet has become a powerful medium both for terrorist activity as well as presenting itself as an effective platform to send out effective messages. Over the last decade, it has developed from being an academic tool to an integral part of life, socialisation and business. More and more young people are using the internet in new ways to build identities, socialise and share experiences. At the same time, it has become a powerful medium for criminals including paedophiles, terrorists, etc to exploit vulnerability and undermine the credible voice.

The PDU have developed Internet Safety Resources as safeguarding young and old on the internet should be seen in very much the same way as road safety is thought of today, as a vital life skill to be taught early and often and as a critical investment in preventing harm later on. This program of work needs to be supported by projects, using interactive and appealing technology which can be used by educational and vulnerable institutions, communities, prisons, etc. This subject matter will not only tackle radicalisation, but also sexual grooming, human trafficking, etc.

The internet can also be used to ensure credible voices are given a platform to delegitimize violent narratives used by terrorists. This can be done using strong global communities and this form of empowerment can be a useful way of expressing credibility as well as undermining the extremist platform. The internet can be used as an extremely positive communications tool. Other media channels can also be tapped into to promote credible voices. The PDU have spear-headed this form of work but it is still in its early stages. With the help of EU partners and a global structure, this work-stream should be seen as an influential challenge to root out cyber-crime.

The role of the Prevent Delivery Unit has been to enhance trust and confidence within communities and key stakeholders around the Prevention of Violent Extremism in all aspects. Effective civil society engagement has been an integral part of this agenda in order to gain a deeper understanding of the vulnerabilities and drivers that lead to extremism within communities so that we can collectively empower them to increase their own resilience against violent extremism.

Despite the level of threat being a global issue, there has been a disparate lack of global co-ordination in the quality, quantity, value for money and lack of scrutiny and consistency in combating international terrorism. This has enhanced negative media attention and increased misconception amongst Muslim communities as well as created a rise in polarisation and social segregation and consequently a rise in domestic extremism.

Our involvement within the EU Internal Security Strategy development will bring together a wide range of expertise and promote co-ordination, cooperation and mutual understanding through enhanced working relationships. We can bring the expertise that we have developed through existing networks and by implementing proactive initiatives that are intelligence led, using lessons learnt from previous case studies and which can help promote improved information sharing and good practice.

As a result, best practice and developed products can be rolled out into low priority areas cost effectively so that the strategy does not exclude any specific community where the threat level can change overnight as the extremists refocus their targets.

There also needs to be a sustainable balance in managing anti-radicalisation methodology so that all forms of extremism are tackled and methods applied to cater for the diverse demographics, existing white communities as well as new and emerging communities across Europe.

<u>Increase Europe's resilience to crisis and disasters</u>

Following the Indian Ocean Tsunami of 26th December 2004 and the London bombings of July 2005, the UK Disaster Victim Identification (UK DVI) Team was established, which sits under the Association of Chief Police Officers (ACPO) Emergency Procedures Portfolio. This in turn is responsible to the Uniformed Operations Business Area.

Prior to the inception of this team, forces responded to incidents within their own jurisdictions on an individual basis and arranged for additional resources through local and or regional arrangements or through the Police National Information and Coordination Centre (PNICC).

For international incidents, the Metropolitan Police Service (MPS) provided the primary response to requests for assistance from the Foreign and Commonwealth Office (FCO) to

incidents involving fatalities of British nationals overseas where identification issues appeared to be, were apparent, or where the UK intended to offer DVI skills on a humanitarian aid basis.

At the request of the Home Office, ACPO have worked closely with Central Government and other partners in developing a national DVI team, drawn from every UK police force on the basis of proportional representation to enable the Service to provide an effective response to mass fatality incidents.

The purpose of the UK DVI team is twofold. Firstly to supplement local or regional arrangements to a mass fatality incident, and secondly, to assist in the response to a fatality incident overseas when requested to do so by the FCO. The UK DVI team is notional and its members remain in their host force area and are called upon to assist in the event of an incident requiring a DVI response.

The current ACPO DVI Five Year Strategy has a number of key objectives which may change. These are:

- Develop force/regional DVI capacity commensurate with local/national risk assessment.
- Continue to contribute on a proportionate basis to the UK DVI Team. To maintain capability and capacity commensurate with the national risk assessment.
- Develop National Casualty Bureau arrangements that enable an effective and appropriate bureau to be established in accordance with national risk assessment and forthcoming major events.
- Establish three Forensic Matching Centres that can respond commensurate with the national risk assessment.
- Develop a UK DVI CBRN capacity and capability that will enable an effective response commensurate with the national risk assessment.
- Develop DVI capacity and capability to enable an appropriate and effective response to the 2012 London Olympic Games and 2013 G8 Summit.
- Develop an appropriate training and exercise programme that underpins the maintenance and development of DVI capacity and capability within the Service.

UK DVI deployments to date

Only a small number of DVI trained staff have been actively deployed on five international deployments in the past five years.

- Thailand September 2007 (Phuket - One to Go air crash)
- Bangladesh March 2009 (Bangladesh - rifles uprising)
- Air France AF 447 air crash, (Brazil - June 2009)
- Afriqiyah Air 771 air crash (Libya - May 2010)
- Pamir Airways Flight 112 air crash (Afghanistan - May 2010)

21 December 2010

Memorandum by Professor Didier Bigo (ISS 7)

1. As the Committee suggests, one of the key questions concerns the scope, the scale and subsequent priorities of the Internal Security Strategy.

What is to be delivered by the Internal security strategy? Is it security only or is it liberty, security, and justice? Is the new division of labour between the two commissioners limiting their purposes or do they have to work together? If the ambition of the ISS is the three objectives together, then it needs to be readjusted in order to avoid contradictions of objectives. Freedom and fundamental rights are at the core of what has to be promoted. Security cannot "balance" Liberty.[1] Security is a means to achieve liberty, and any claim of a "security gap" makes sense only if the measures to reduce the security gap with more surveillance and detention don't create distrust in institutions and an enlarged liberty-democracy gap. Security is important but cannot be "unlimited".

So the central question for the internal security strategy is to determine the limits to security, and to the actions of the EU itself in this regard, and to determine the appropriate means to achieve security once the limits have been clearly drawn. It seems that the lack of real collaboration of the services and operational agencies attached to Viviane Reding as commissioner on Justice, Fundamental Rights and Citizenship and the ones attached to Cecilia Malmström as commissioner on Home Affairs has given the upper hand to the latter, and especially to some operational agencies (Europol and Frontex).

The discussions in COSI concerning ISS are paradoxically less a dialogue between different opinions as was intended by the Stockholm programme, and more a quasi monopoly of the Department of Home Affairs in a traditional sense of an old boys network of policemen who disregard objections and reaffirm beliefs they have had from the very beginning of the Maastricht period. Have we forgotten Tampere, Amsterdam and Stockholm? Are we back to the first version of the third pillar in Maastricht with the strategy planned for Internal Security? A list of the participants writing the draft of the ISS would be relevant in this regard.

2. The ISS is focused on important questions concerning terrorism, organised crime, cyber crime, border management, resilience to crises, but it does not appear as a strategy that raises questions and opens alternatives. . On the contrary it looks like a list of well known recipes whose results have not been excellent (or are unknown). The ISS seems to pretend that a zero risk society is possible and desirable, but social science and technological research have shown that this is a dangerous illusion. Security is not a technique that can be applied in a straightforward way; security requires judgements about the balance to be accorded to the values of solidarity, freedom, and equality.

A security strategy must take into account how far effective freedom of movement (which is not to be confused with speed of travel under surveillance), the presumption of innocence, and the right to privacy of individuals blocks in practice (or not) the work of law enforcement and intelligence services? Do these agencies require a greater exchange of information? Does data mining and profiling intrude on the right to privacy? How much

[1] Didier Bigo, Sergio Carrera, Elspeth Guild, and Rob Walker, *Europe's 21st Century Challenge: Delivering Liberty and Security.*Ashgate, 2010) and Didier Bigo, Sergio Carrera, and Elspeth Guild, 'What Future for the Area of Freedom, Security and Justice? Recommendations on Eu Migration and Borders Policies in a Globalising World'. *CEPS Policy Brief*, no. 156 (2008): 4 p.

control at borders and beyond national borders, can be implemented without raising serious questions about the invasion of sovereignty and the erosion of reciprocity? To what extent can detention be justified in terms of a threat of danger as opposed to strict culpability? Unfortunately these questions are not addressed in this document (which is considered to contain the the key reflections of the EU on these matters), or in other security document from the EU. So, what is the thinking that would explain the choices to be found in the Internal Security Strategy document?

Strategy supposes options and choices. It is the privilege of the EU commission to be in a position to open a debate and to propose alternatives. Its main advantage is to have the resources of the 27 member states with their traditions, trajectories, and differences to help it create a dialogue. Yet the ISS text reduces this diversity to a "dogma", which is not sustained by the evidences coming from the knowledge based researches of the DG research, DG JLS or FRA on these topics. It seems that the professionals of security in Europe have acted as a guild, resilient to different points of view, and that they use only "corporate" information already framed so as to justify their view of an expanding and interconnecting level of threat at the world level which makes it necessary to collaborate more, to integrate data better, and to find one technology as a solution against all specific threats. The path dependency towards a homeland security adjusted to Europe is strong, even if these ideas were floating about in some member states before 2001. Europe has to find its own strategy and to respect its diversity.

3. For the moment the text of the internal security strategy shuts down options and is driven by only one main narrative guided by a belief in the technologies of identification and surveillance as the solution for any problem of security. This grand strategy's narrative supposes that we are confronting globalised threats, always on the rise, with more and more interconnection between the different forms of threats (reports of Europol, Frontex, Eurojust, proposals from the EC Commission on Eurosur and border surveillance present as facts the idea of a globalised insecurity). From this unexplored assumption, the logical answer seems to require more globalised security (with fewer national or regional sovereign decisions), to require more coordination and integration (with less diversity of vision) and to require more technologies of identification. The leading idea seems to be: we don't have confine ourselves to reaction and protection, but we also have to, focus on prevention, because of the dire consequences of low level probability events (nuclear terrorism, pandemics, now volcanoes, or meteorites falling on the planet…). Each element of this narrative conducted by a coalition or guild of intelligence services" has to be questioned and tested against liberal political choices of acceptance of risk in everyday life. It is important to give voice to alternatives coming from classical security measures, and rule of law oriented approaches. Most of our interviews show a deep resentment of key professionals against this discourse, but who, nevertheless, are uneasy about challenging it openly, as they feel this narrative is what the politicians want as it may help building EU "capabilities".[2] Suggestions coming from them would be that the EU reports should make a clear distinction between national authorities and European Union responsibilities in the statistics themselves and that they should not aggregate national data as EU data. They should have to describe the EU level with specific EU (only) data.

4. It raises the question of roles and responsibilities towards threats, and the interpretation given to the same phenomenon by different agencies, regarding to their interests to centralise information under the label of information exchange. What are the threats against

[2] Didier et als Bigo, ed. *The Field of the Eu Internal Security Agencies* (Paris: Centre d'études sur les conflits/l'Harmattan, 2007).

which the EU is struggling? Are the threats globalised? Are all of them globalised? Certainly it is true only if one accepts the confusion between global, regional, transnational, cross border, and local. But, the different terminologies cannot be fused as if every threat was of global reach and without boundaries. A global scale of threat is exceptional (even for finance). A minority of threats are "glocal" and their local manifestations so diverse that solutions need to be locally configured, even if knowledge can be wider and shared; a majority are just local (including cross border ones) and don't need to be seen as part of a global phenomenon in the making. The list of threats in the Stockholm programme (4-1) has to be re-evaluated by differentiating what is and what is not global. For example the Corsican FLNC is not Al Qaeda and should not be conflated with the fear of nuclear or very serious terrorism, even if they are put under the same label and the same statistics. But, as the report is at pains to demonstrate (with statistics of bombings) the danger of Al Qaeda, these past few years has increased. In order to strengthen their case, they add to the terminology of terrorism many other small scale activities including the ones of the FLNC. This has the effect of making the threat more credible. It is typical of Europol reports, to connect the two, by insisting on the danger of the threat of terrorism in general shown by large numbers and statistics of hundreds of bombings, and by developing a narrative about radicalisation of Muslim communities not sustained by the very same statistics. Either FLNC is purely local, or it is the most dangerous threat of the EU in terms of statistics, and if so why focus only on the Muslim communities? Why not ask for a special European operation on Corsica. The ambiguous language is always there. What is local is seen as part of a global element. This discourse did not simply emerge in a mysterious fashion. It is the result (rather than a conscious strategy) of the pressure to cooperate brought to bear on different agencies which have to gather the local threats into a global one in the making, in order to show that they effectively collaborate and that they are improving their co-operative exchanges.

The intensity of collaboration may depend on the scale, but the interest of each EU agency (or transatlantic committee) is to present its own mission against a threat as an important one, and to use the keywords "global", and "common". It is important to limit EU activity to a certain scale and to resist the tendency to speak about all threats as global. Subsidiarity is more important than worst-case scenarios. Budgets have to be calibrated. Limits have to be placed on the ability of security concerns to expand to include all things.

5. If not globalised, are the different threats interconnected? Is terrorism linked with organised crime, with illegal migration, with asylum seekers, with overstayers? Is any flow of movement an internal security "competence"? Are the distinctions of Amsterdam erased? Are we coming back to an extensive vision of JHA including legal border crossings, visas, migration, asylum, plus now external actions and foreign affairs on any assumption of overflows? The interconnection argument is a different question to the one about globalisation (of one threat). To point to the interconnection of local events is not to make them global. We have to understand what a network is, what are its limits and its nodes. A discourse insisting on the interconnection of the different threats has emerged as a reaction against freedom of movement of people inside the EU, and then against mobility in general (Single act, end of cold war, post 201 and 2004). Its accuracy in terms of knowledge has been very limited. Some specific connections and nodes may exist, but it is not a complete fusion. We don't have a merging between war and crime at the world level. Nevertheless, if this narrative of an "insecurity continuum" has been successful, it is because we have more and more, after the end of the cold war, witnessed entanglements between the universes of policing and that of military activity. This has lead to the rise of the "intermediary agencies": police with military status, border guards, immigration services, and intelligence services.

This may explain how in a situation of uncertainty concerning their missions, each agency tries to promote its struggle against a threat, as the central one, by explaining that it is interconnected to the other ones and will solve the other problems too. The appeal to some technologies (such as biometric systems, databases, traceability, profiling, and data mining) by the security industry, which present these as solutions against many threats (from identity theft to terrorism), follows the same logic. Mapping the field of the security agencies, their contacts, oppositions and alliances, gives reasonable answers to their beliefs, interests and why they develop (or not) a discourse concerning a global insecurity (see bibliography). The field needs to be regulated instead to accept any form of networking to be developed. It has incidence at the transatlantic level, and even more when cooperation goes beyond democratic regime collaboration under the pretext of "sharing information" which may have value in the future.

6. When it comes to information, more is not always best. The accumulation of information whose reliability is diverse can create error on intelligence and obliges those collecting it to rely more and more on software to sort out the most important cases. This takes time and often there is an imperative to act before the process is completed. . The future of human actions cannot be deciphered through profiling technology. Knowledge certainty cannot be merged with astrological reasoning by the magic of technology. The seriousness of the terminologies of prevention and anticipation regarding the results has to be addressed in detail. During our interviews, no one example given resisted the test of success in anticipating human behaviour, and this confidence was often based on the results of statistical correlations, often not accurate about a previously unknown individual. . . A better option is to avoid to overload the system with information and to rely more on human beings capacity. It goes against the theology of the "unknown unknowns" of the neo conservatives and the total information awareness they wanted. But it goes against with good reason for both freedom and efficiency on security missions. Asking for an internal survey about the optimal level of information (and not the maximum) will certainly permit a better appreciation of the difference between the need for data, and the strategies to accumulate them. Once again, the technologies are not the solution to security problems. These technologies need to be supplemented with a discussion of the political and democratic issues involved in security questions. The Information management strategy has to be revised to take this into account. It is central to present alternatives to Eurosur, to the European entry and exist system and a technologisation which confuses speed of travel with freedom of movement.

12 December 2010

Memorandum by the Centre for European Policy Studies (CEPS) (ISS 2)

Introduction

The Centre for European Policy Studies (CEPS) is among the most experienced and authoritative think tanks operating in the European Union today. CEPS serves as a leading platform for debate on EU affairs. Its most distinguishing feature lies in its strong in-house research capacity, complemented by an extensive network of partner institutes throughout the world. Researchers in the Justice and Home Affairs Section at CEPS examine the main issues and dilemmas related to the construction of an Area of Freedom, Security and Justice (AFSJ) in the EU, its internal and external dimensions and how these impact on the liberty and security of individuals.[3] It is an honour and a pleasure to submit evidence to the Select Committee on the EU on this important aspect of EU policy.

1. The EU Internal Security Strategy (ISS) was adopted by the Council in February 2010 under the auspices of the Spanish Presidency with a view to setting out a common European Security Model.[4] This initial document followed the entry into force of the new treaty setting of the EU, brought about by the entry into force of the Lisbon Treaty and the Stockholm Programme setting out the new five-year plan for the development of the EU's Area of Freedom Security and Justice (AFSJ) in December 2009. The AFSJ was created by the Amsterdam Treaty amendments to the EU treaties in 1999. In its original form, the AFSJ comprised the fields of borders, immigration, asylum and judicial cooperation in civil matters in a legally binding form (previously called the EU's "first pillar"), and policing, terrorism and judicial cooperation in criminal matters in the more intergovernmental venue of the EU (formerly known as the "third pillar"). The Lisbon Treaty formally abolished the old pillar structure in Justice and Home Affairs (JHA) policies and brought (to varying degrees and subject to several exceptions) the different policy fields of the AFSJ into one fairly homogeneous legal and institutional framework. However, the ISS and the Commission's vision outlined in the Communication offer evidence that the old third-pillar spirit and intergovernmental ways of thinking and working (police-led, secretive and unaccountable) are still very much in favour and can be expected to be expanded through their practical implementation.

2. The Stockholm Programme stressed that it "is of paramount importance that law enforcement measures, on the one hand, and measures to safeguard individual rights, the rule of law and international protection rules, on the other, go hand in hand in the same direction and are mutually reinforced."[5] Do the ISS and the Commission Communication 'putting it into action' fulfill this political priority? This submission of evidence argues and provides evidence to the contrary. Both official documents illustrate how the insecurity concerns enshrined in the ISS are attempting to take over the EU's AFSJ agenda. Justice is relegated second to the service of security, and individuals' security and liberty remain absent from the overall objectives of the strategy. The concrete steps presented by the Commission Communication exclusively serve 'internal security' purposes and interests, an approach that positions rule of law and fundamental rights (aside from formalistic sentences and announcements) at the margins. The Communication advocates a

[3] For more information about the JHA Section activities refer to http://www.ceps.eu/content/justice-and-home-affairs as well as the CEPS Activities Report (Review 2009 / Preview 2010) available at http://www.ceps.eu/system/files/article/2009/08/CEPS_Report2009_webversion.pdf

[4] Council of the EU, Draft Internal Security Strategy for the European Union: Towards a European Security Model, Brussels, 23 February 2010, 5842/2/10.

[5] Council of the EU, The Stockholm Programme: An Open and Secure Europe serving and protecting Citizens, 5731/10, Brussels, 3 March 2010, page 9.

predominant 'Home Affairs model', based on a number of 'common threats' that the Union allegedly faces globally and that are said to justify the further integration of security cooperation at EU level in both operations and substance. This home affairs model proposed by the Directorate General Home Affairs of the Commission has not been accompanied by (and in our view remains in tension with) a credible and sound EU citizenship, fundamental rights and justice strategy meeting the liberty-related challenges that a majority of the ISS objectives and policy proposals (especially those related to a proactive, intelligence-based approach and a model for information exchange as well as the call for further operational integration of EU security agencies) will increasingly create to a Europe of law, justice and rights. This, we argue, will constitute one of the main challenges for Europe's future which remains unresolved.

The UK's Position in the AFSJ

3. The UK's position in the AFSJ has been somewhat exceptional. By virtue of Protocols to the Treaties, the UK was, from the beginning, not obliged to participate in EU measures on borders, immigration and asylum. According to the Protocol No. 21 on the position of the UK and Ireland in respect of the AFSJ attached to the Lisbon Treaty, this exception has been extended to criminal justice matters as well. Article 4a of the mentioned Protocol has expanded the 'opt out' to all the Chapters falling within the scope of the new Title V on the AFSJ of the Treaty on the Functioning of the European Union (TFEU) including Chapter 4 on 'Judicial Cooperation in Criminal Matters' and Chapter 5 on 'Police Cooperation'. Yet, according to the second paragraph of that same article, a certain amount of pressure can be exerted on the UK to make it participate in the adoption and implementation of legislative measures that aim at purely amending existing (former EU third pillar) measures where it is participating. Refusal to participate could lead to the cessation of application of that measure to the UK and the financial consequences that would stem from this situation.

4. In practice, the UK has participated in the EU's asylum matters until recently, when the decision was taken to no longer to participate in some of the revised measures. The UK has not participated in any of the border and immigration-related measures with a small number of exceptions that relate to formal matters. The UK expressed interest in participating in the EU's external border agency Frontex, in biometric documents and in the visa database, which the EU is creating (the Visa Information System), but is not entitled to according to refusals by the Council, which have been upheld by decisions of the Court of Justice of the European Union.[6] For the moment the UK participates in the measures adopted before the Lisbon Treaty on judicial cooperation in criminal matters such as the European Arrest and Evidence Warrants.

The Objectives of the Internal Security Strategy

5. The objective of the EU's ISS is to establish a shared agenda on internal security that enjoys the support of all the Member States, the EU institutions, civil society and local authorities, and interestingly enough, the EU security industry. What the ISS does *not* include are institutions and issues that are associated with external security, such as the military, defence and international relations. There is only one cross-over issue: the

[6] C-482/08 *UK v Council*, 26 October 2010; C-137/05, *UK v Council* 18 December 2007; C-77/05 *UK v Council* 18 December 2007.

possible duties of the European External Action Service where a number of suggestions for activities are made in the Commission's Communication (COM (2010) 673).

6. The ISS identified a number of principles and guidelines for action in pursuit of a 'European security model'.[7] The principles included:

    a. Justice, freedom and security policies which are mutually reinforcing whilst respecting fundamental rights, international protection, the rule of law and privacy;

    b. Protection of all citizens, especially the most vulnerable;

    c. Transparency and accountability in security policies;

    d. Dialogue as the means of resolving differences in accordance with the principles of tolerance, respect and freedom of expression;

    e. Integration, social inclusion and the fight against discrimination;

    f. Solidarity between EU Member States; and

    g. Mutual Trust.

    On the basis of these principles, the ISS provided a number of guidelines for action "to guarantee the EU's internal security", which inter alia included a proactive (intelligence-led) approach driven by prevention and anticipation, the reinvigoration of information exchange between law enforcement authorities through the use of EU databases as well as an improved operation cooperation between EU security agencies (Europol, Eurojust, Cepol, Sitcen and Frontex) and ensuring stringent coordination between them by the Standing Committee on Operation Cooperation on Internal Security (COSI). The only guideline presented by the ISS that even partially dealt with rule of law-related aspects was entitled "Ensuring the effective democratic and judicial supervision of security activities". The latter referred in rather general terms to the importance of the involvement of the European Parliament and national parliaments, and referred to the EU's accession to the European Convention on Human Rights.[8] Apart from that, the ISS did not specify the actual ways in which the specific guidelines were going to constitute an implementation of the above-mentioned general principles. Moreover, as we will develop more in detail below, the Commission Communication putting the ISS into action has gone even further by completely neglecting the fundamental rights and rule of law dimensions amongst its five strategic objectives.

7. The Treaty of Lisbon and the Stockholm Programme have provided the legal and political impetus for the ISS to be developed and implemented. The Commission Communication thus comes indeed at a moment when there is much clearer responsibility within the EU institutions on competence for internal security generally; the framework of Member State/EU institution activity is more precisely delineated and the balance of powers among the EU institutions following the augmentation of the European Parliament's competences by the Lisbon Treaty is beginning to become apparent. That notwithstanding the new institutional and legislative framework provided by the Treaty of Lisbon has not meant a formal end to the third pillar 'way of working and thinking' on

[7] Council Document 5842/2/2010, Internal Security Strategy for the European Union: Towards a European Security Model.

[8] Similarly in the Commission Communication "The EU Counter-Terrorism Policy: Main Achievements and future Challenges, COM(2010) 386 final, Brussels, 20.7.2010, the respect for fundamental rights was identified as an 'horizontal issue' in the implementation of the strategy, for instance in what concerns the protection of personal data and the effects on vulnerable groups. See page 11 of the Communication. This element however has not been either incorporated in the Communication putting into action the ISS.

issues of security at EU level. On the contrary, when reading the Communication, it appears as if the old third pillar spirit is not only very much present but it is also now contaminating other (formerly considered) first pillar areas, such as for instance those of external border controls and migration/asylum policies as well as agencies such as Frontex. The 'depillarization' emerging from the Lisbon Treaty is allowing for the extension of the police and insecurity-led (intergovernmental) approach to spread over the entire EU's AFSJ and not – as it might have been originally expected – the other way around (the Community method of cooperation logic to expand over internal security matters). This, of course, raises concerns over the greater effectiveness, democratic accountability and judicial control as well as rule of law/fundamental rights consequences that the end of the pillar divide in JHA policies was expected to bring at EU level and that seem to be now at stake.

8. The former 'third pillar' policies (police and criminal justice) are amongst those in the new Title V of the Treaty on the Functioning of the European Union (TFEU) where more exceptions to the general rules and 'flexibility' mechanisms have been allowed in European cooperation. This will further enhance the intergovernmental and 'police-led' motif of future EU security measures. Not only the maintenance of law and order and the safeguarding of internal security remain exclusively a matter of national competence under the Treaties, but there are a number of important derogations from the expansion of the Community method of cooperation over these domains. As a way of illustration, "cooperation between police, customs and other specialized law enforcement services in relation to the prevention, detection and investigation of criminal offences" remains under unanimity and mere consultation with the European Parliament. This goes along with the possibility offered to EU Member States to use 'emergency brakes' and/or enhanced cooperation (such as for instance in relation to the setting up of the European Public Prosecutor Office). Or the limited jurisdiction of the Court of Justice to review the validity and proportionality of operations carried out by the police and other law-enforcement authorities and the Protocol 36 on Transitional Provisions (Article 10).[9] Overall, the exceptions permitted by the Treaty of Lisbon on EU AFSJ (security) policies will not only allow for the continuation of 'Third Pillar' ways of working in JHA domains. It is also expected to increase the insecurity and vulnerability of the individual, which depending on her/his geographical location in the EU will be facing different degrees of European rights and freedoms.

A Shared Agenda: The starting point

9. Not surprisingly, the Commission's position on an EU ISS commences with a series of arguments that move in one direction only: first, there is a need for 'more security' (never defined but quite clearly not including social security), and secondly the EU 27 Member States share a common framework based on convergence of 'security threats' which provides the objective framework for a common ISS.

10. It is our view that these assumptions need to be examined on the basis of the available evidence. One shortcoming of the Communication is a tendency for assertions about factual matters to be included which lack any indication of the evidential basis on which they repose. It is critically important that the EU develop policy on the basis of the best research, analysis and evidence available in whichever field is under discussion. Indeed,

[9] According to this provision , as a transitional measure, the powers of the Commission and the Court of Justice in relation to acts dealing with 'police cooperation and judicial cooperation in criminal matters" will continue to be 'as they were' in the EU Third Pillar for a period of five years after the entry into force of the Treaty of Lisbon.

the EU itself is an important actor in funding research on all the areas of its competences (and many others) which is carried out at universities and research institutes across the world. Much EU (social sciences) research attention and funding has been directed at security-related issues. It would well behoove the EU institutions (and particularly the European Commission) to examine this body of knowledge in the formulation of policy and to address the existing gap between the findings of these research projects and the ISS. It is also central that the EU continues to support independent social sciences and humanities research projects, which while perhaps not being 'policy-driven' (already-decided) by EU policy priorities of the day, might however be extremely 'policy-relevant' in pointing out main issues and dilemmas of these very policy choices, and offer independent evidence calling at times for a reconfiguration and reframing of the priorities and agendas.

11. As regards the issue of security and the people, we cannot resist commencing with an anecdote: a middle-aged man finds himself in a foreign city late at night on a quiet street. He sees a policeman and he is reassured. The same man finds himself again on the same street late at night and sees two policemen walking together. He is reassured. The same man is once again on the street of the foreign city late at night and he sees 50 policemen coming towards him; he turns and runs as fast as he can in the opposite direction. The purpose of this anecdote is to set the stage – 'more security' is not always reassuring for the EU citizen.

Rule of Law and Fundamental Rights

12. The Commission's Communication on the ISS highlights at the beginning of the document the importance it attaches to the rule of law, fundamental rights and the EU Charter of Fundamental Rights. The EU is indeed, according to its treaty, founded on the principle of rule of law and the respect for fundamental rights. Although the UK has a somewhat *sui generis* protocol which purports to limit the application of the EU's Charter of Fundamental Rights in the EU, as the Charter itself states that it does not more than bring together in one place rights which people already enjoy in the EU by virtue of other treaties, for the purposes of this submission, the exact status of the Charter in the UK is only marginally relevant. Sadly, the Communication does not return to this matter which is perhaps the most important one to consider. The sensitive issues that are dealt with in the Communication include a number which have been the subject of important judgments of the European Court of Human Rights (ECtHR) – for instance on privacy the decision in *S & Marper v UK*[10] where the ECtHR found the UK's DNA and other biometric information database inconsistent with the right to privacy in Article 8 ECHR. Similarly, the same court found, in *Quinton and Gillan v UK,*[11] that the wide anti-terrorism measures permitting the police stop and search powers unfettered by the need for a reasonable suspicion too wide to be compatible with the same provision of the European Convention on Human Rights (ECHR). More attention to the matter of correct application of fundamental rights duties of Member States in the internal security policies would help states to avoid these errors in the application of their national policies.

13. The Commission identifies five key themes (strategic objectives) which form the pillars of the ISS and around which it is structured:

[10] Case numbers 30562/04; 30566/04; 4 December 2008.

[11] Case number 4158/05; 12 January 2010.

a. Organised crime;
b. Terrorism;
c. Cybercrime;
d. External borders; and
e. Natural disasters.

14. The first question that needs to be addressed is the extent to which these five issues, all of which are concerns for at least some Member States, are concerns *for all* EU Member States and the extent to which the issues share common aspects in the 27 Member States at all.

Organised Crime in the EU 27

15. As regards organised crime, it is apparent that there are very wide differences regarding this across the Member States. The EU Organised Crime Threat Assessment (OCTA) was established following the recommendation of the Hague Programme (the five-year plan for the AFSJ 2004-09).[12] In its 2009 report it states that there are five criminal hubs with a wide influence on criminal market dynamics in the EU. These are the North West criminal hub which acts as a distribution centre for heroin, cocaine and synthetic drugs but influences the UK, Ireland, France Spain, Germany and the Baltic and Scandinavian countries. The South West hub is formed around the Iberian Peninsula and the issues for this hub are cocaine, cannabis, trafficking in human beings and illegal immigration. The North East hub, which borders the Russian Federation, and Belarus, engages in human trafficking (women for sex) irregular immigrants, cigarettes, counterfeit goods, synthetic drugs and heroin. The Southern criminal hub is based in Italy; where in addition to drugs and irregular migration it is involved in genuine and counterfeit cigarettes and the production and distribution of counterfeit euros. The South East criminal hub centred in Bulgaria and Romania is involved in drugs, heroin, counterfeit euros and payment card fraud.[13] What is interesting from this summary for the purposes of the ISS around organised crime is the wide differences across the EU, which are evident even in a report designed to highlight synergies and homogeneity in the Union. There is clearly much competition in the field of organised crime and different parts of the EU face very different challenges. Any one-size-fits-all approach to policy is therefore likely to be highly counterproductive.

Terrorism in the EU

16. Turning then to terrorism, there do not appear to be very many Member States that are touched by terrorist acts and those that are appear to be concerned primarily with local terrorism. According to TE-SAT 2010, the EU's Terrorism Situation and Trend Report,[14] in 2009, six Member States[15] reported a total of 294 failed, foiled or successfully perpetrated terrorist attacks and the UK reported 124 attacks in Northern Ireland. Only one 'Islamist' attack was reported (in Italy), while France reported 89 Separatist attacks and Spain 148. The next largest category of attacks was under the heading 'Left Wing'

[12] Brussels European Council, Presidency Conclusions, 4 and 5 November 2004, 14292/1/04, Brussels, 8 December 2004, Annex I, "The Hague Programme: Strengthening Freedom, Security and Justice in the European Union", point 1.5. 2005/C53/01, OJ C53/1, 3.3.2005.

[13] Europol, OCTA 2009 pp 13 – 15.

[14] Europol, TE-SAT 2010 pp 6 – 8.

[15] Austria, France, Greece, Hungary, Italy and Spain.

with 15 in Greece and 23 in Spain. Clearly, the vast majority of terrorist acts reported in the Member States relate to various separatist groups active primarily in particular parts of the affected Member States. The issues are so intricately related to specific local or national political issues which are only fully accessible to the national and local authorities that to call terrorism in the EU a common issue is problematic. Certainly there is political violence in the EU, but a single common approach is unlikely to capture the specificities of the national and local situations. Further it is an issue that affects less than a third of the Member States which raises questions about the appropriateness of EU budgetary expenditure on the subject.

Cybercrime and the EU

17. Data regarding cybercrime are fairly limited. The Commission produced a Communication towards a general policy on the fight against cybercrime in 2007,[16] in which it most helpfully sought to clarify what it is (including computer crime, computer-related crime, high-tech crime and other possible synonyms). Most importantly, it covers traditional forms of crime (such as forgery and fraud) carried out over electronic communications networks, the publication of illegal content and crimes to electronic networks such as attacks on information systems, denial of service and hacking. The Commission, rightly, identified the problem as one for the criminal justice systems of the Member States as the issues that hamper coercive action against cybercrime relate to the jurisdictional limitations of criminal justice systems. The Communication also recognizes that by its very nature, cybercrime is not limited to Member States but may commence on the other side of the world. It can only be classified as crime if the places where it takes place have in their criminal code offences that encompass the activities which some EU Member States consider crimes. The current situation regarding the 2010 WikiLeaks revelations, which are subject to very different legal regimes depending on which country is host to the WikiLeaks activities, highlights the problem.

18. The private sector is particularly engaged with this aspect of the ISS. Cybercrime is most problematic for industry, although of course it touches citizens as well. The Commission's Communication finishes with an ambitious list of activities to be undertaken. However, according to the Council's document base, not much appears to have happened. There are Conclusions in September 2008 which call for a working strategy against cybercrime and enhanced public-private partnership regarding the issue. In 2009 the Dutch Delegation presented its position on fighting cybercrime which places particular importance on coordination of the action with the Council of Europe. However, on 14 and 15 June 2010, following a conference in the Hague, a European Union Cybercrime Task Force has been established under the aegis of Europol.

The EU's External Borders

19. For the UK, the issue of the external borders of the EU is a delicate matter as it does not participate in the EU's common actions and indeed is excluded from participation in the EU's external border agency Frontex. For the rest of the Member States, the EU's external border commences at the UK's border. Thus common issues of border controls are somewhat irrelevant for the UK as regards to EU's Internal Security Policy as it is on the outside.

[16] COM(2007) 267

20. According to the Council, there were an estimated 355 million entries by persons into the Schengen area in 2009.[17] Of these people entering, about 105 million were third country nationals (approximately 61 million non-visa nationals and the rest visa nationals). According to Frontex, over the first three months of 2010, 14,200 detections of irregular external border crossings were reported.[18] A yearly figure on that basis is 56,800 irregular external border crossings. Further irregular border crossings in the first three months of 2010 dropped by 36% in comparison with the final quarter of 2009. The disproportionate nature of the two figures – the 61 million third country nationals who enter the Schengen area annually, against the approximately 56,000 people who are treated as entering irregularly most graphically indicates that border crossing by individuals is not a security issue in the EU. It is a matter of trade and tourism, industry and family relations. To the extent that there is a security dimension at all, this is in relation to travel infrastructure. The external border of the EU most properly facilitates the entry and exit of people who seek to enter the EU whether they are citizens of the Union or third country nationals. The number of people who are treated as inadmissible and thus seeking to enter irregularly is statistically insignificant. In an EU of over 500 million people, there is a real need for a sense of proportion regarding the policy area of irregular migration.

Natural Disasters

21. Natural disasters are a subject where there is perhaps greater scope for common approaches. The eruption of a volcano in Iceland certainly showed many EU citizens, wherever they were in the world, the need for more consistent and coherent consular protection and assistance in the face of such disasters. The fact that many EU citizens were stranded in far-off countries, were provided highly misleading information by government departments of some Member States and felt abandoned by their authorities and unable to access the assistance of the authorities of other Member States leads to the conclusion that we could do much better in this regard.

Conclusions: Towards a European Liberty Strategy

22. A European ISS must be built on the basis of evidence and analysis of the security interests of the people of Europe as well as the added value and effects of new (internal security) policy strategies. It must not be promoted on the basis of a lack of information and data or a willful misrepresentation of the available data. This has been also highlighted by the European Data Protection Supervisor (EDPS), which has called for a systematic approach in these areas (ensuring consistency and clear relations between all policies and initiatives in the area of home affairs and internal security) instead of an 'incident-driven policy-making'.[19] Moreover, it may be easy for some parts of the media (and sadly also some EU leaders and politicians) to fan fears about irregular migrations, terrorist threats and organised crime among the people of Europe, but such irresponsible behaviour helps neither EU citizens to understand their world, nor policy-makers to promote sound and measured policy responses.

[17] Council Document 13267/09.

[18] FRONTEX, News release: Irregular immigration hits net low in first quarter of 2010, facilitator detections up 13%, 7 July 2010.

[19] Opinion of the European Data Protection Supervisor (EDPS), on the Communication from the Commission "The EU Counter-Terrorism Policy: Main Achievements and Future Challenges, 24 November 2010, Brussels.

23. All five strategic objectives that the Commission Communication proposes as core pillars reveal substantial variations across the Member States whether it regards relevance to some Member States at all, fundamental heterogeneity or insignificance. This, in our view, challenges assertions referring to a common EU model on internal security. Another issue of concern is that the strategy proposed by the Council and followed up by the European Commission is to bring back (through the back door) the old 'third pillar' logic of cooperation on JHA (police and insecurity-driven policies) and spread it throughout the Freedom, Security and Justice domains, including policies and EU agencies dealing with migration, asylum and external borders.

24. Will the ISS make the EU more secure or insecure? The ISS offers little in terms of new or innovative policy initiatives towards meeting the challenges that the Union will increasingly face in delivering liberty and security to individuals across the EU. The field of an ISS which touches all Member States and touches a central concern of the people of Europe is the one least developed in the specific actions – promoting the Rule of Law and fundamental rights as the central planks of an EU ISS. By not addressing these elements, the strategy will lead to more insecurity for the individuals subject to these public policy responses. In light of this, the strategy could therefore be re-labelled: the European Insecurity Strategy. Indeed, as the former UN Commissioner for Human Rights, Mary Robinson, has so eloquently explained, the essential element for any community to be secure is the uncompromising championship of Rule of Law and human rights. When people know that their rights are protected by law, law enforcement officials are secure in the knowledge that their actions are fully compatible with fundamental rights and the accused are guaranteed a fair trial, a truly effective Internal Security Strategy will be achieved. In such an environment, criminal gangs are unable to extort money from people as the police will defend the citizen, corrupt officials cannot prosper as the fundamental right of the citizen to transparency will uncover the corruption and law enforcement agents will act in the interest of the Rule of Law.

25. Formalistic statements on the way in which Europe guarantees and respects human rights and the rule of law are not enough and call for constant (evolving) efforts at meeting the liberty-related challenges posed by new EU and national public policy responses. The EU's ISS should be built around the objective of delivering to everyone living in the EU the twin rights of Rule of Law and protection of Fundamental Rights. A solid rule of law and liberty strategy (model) should be jointly devised by the Directorate General of Justice, Citizenship and Fundamental Rights of the European Commission along with the one put forward on 'insecurity' by Home Affairs. Such a strategy should be not only focus on the development of better (fundamental rights) monitoring and – *ex ante* and *ex post* – evaluation of EU policies (and practices) and their national implementation.[20] It should also ensure a more integrated cooperation and coordination between EU (freedom) agencies, such as the European Agency for Fundamental Rights (FRA), the European Data Protection Supervisor (EDPS), the European Ombudsman, etc. The FRA should make use of its current (post-Treaty of Lisbon) powers to assess the ISS from a fundamental rights perspective and it should also see its competences expanded as regards independent and objective evaluation (not only research activities) of EU policies covering in particular the domains of police cooperation and criminal justice.[21]

[20] Refer to the Commission Communication "Strategy for the effective implementation of the Charter of Fundamental Rights by the European Union", COM(2010) 573 final, 19.10.2010.

[21] Refer to Proposal for a Council Decision amending Decision (2008/203/EC) of 28 February 2008 implementing Regulation (EC) No 168/2007 as regards the adoption of a Multi-annual Framework for the European Union Agency for Fundamental Rights for 2007-2012, COM(2010) 708 final, Brussels, 2.12.2010. The objective of this proposal would be destined to expand the FRA's tasks to these areas.

All this should go hand-in-hand with strengthening the democratic accountability (and EU parliamentary representativeness) in the activities and cooperation by EU security agencies and of the coordination role played by the COSI.

December 2010

Memorandum by the European Network and Security Agency (ENISA) (ISS 5)

The Home Affairs Sub-Committee of the House of Lords Select Committee on the European Union, chaired by Lord Hannay of Chiswick, is conducting an inquiry into the EU's approach to internal security.

This inquiry will concentrate on:

- EU and Member State responsibilities for internal security including the role of COSI (the Committee set up under art. 71 TFEU)
- the scope, scale, priorities and intent of the ISS
- prospects and plans for implementation of the ISS
- the relationship between the ISS and global security initiatives, especially those of the United States
- the relationship between the ISS and other EU strategies, policies and plans
- the balance between better security and greater intrusion into individual privacy.

The Sub-Committee has requested evidence on any aspect of the Internal Security Strategy (ISS) for the European Union, its development and its proposed implementation.

In line with the call for evidence, this note provides feedback from the European Network and Information Security Agency (ENISA) under the following headings:

- Scope, scale and range
- Roles and responsibilities
- Prevention and anticipation
- Information exchange
- Operational cooperation
- Integrated border management

In providing this feedback, ENISA aims to provide the House of Lords Sub-Committee with an objective response to the questions raised, but also highlights the role that the Agency could play in supporting the ISS.

Scope, scale and range

In general, ENISA believes that the scope, scale and range of the ISS are reasonable given the nature of the threat. However, it is clear that as Europe becomes increasingly dependent on the correct functioning of ICT systems to support essential day-to-day operations, proportionately more effort and budget should be dedicated to keeping these systems secure, both at the Member State level and at the pan-European level.

Roles and responsibilities

The importance of subsidiarity

The principle of subsidiarity is key to ensuring a successful response to an eventual cyber attack or other large-scale disruption of ICT systems. Ideally, subsidiarity should ensure that

the local response to a global issue will be optimal. In other words, Member States are best positioned to defend their own infrastructures.

However, in a global networked environment, subsidiarity will only result in an optimal response if issues that transcend national boundaries are managed and controlled correctly. Without a coordinated global approach to major incidents on the Internet, Member States could find themselves in a situation where local systems cannot function correctly due to issues that are outside their control.

ENISA expects that international coordination in the area of Information Security will grow in importance throughout the next decade as countries become increasingly dependent on ICT functions that are offered and maintained in locations outside national boundaries. The recent phenomenon of Cloud Computing is highly illustrative of this trend.

The role of ENISA

ENISA will continue to liaise closely with stakeholders, such as Member States and industry, to empower and protect citizens by identifying the most important knowledge and skills which are needed to create a safe virtual environment in which European citizens feel protected (as identified as Objective 3, Action 2 in COM(2010) 673). The Agency will continue to assess the key risks and corresponding solutions in areas judged to be important by the Member States in order to provide an information exchange and knowledge sharing platform for the key stakeholders across Europe

New roles

ENISA supports the idea that 'security expertise should be deployed to EU Delegations, particularly in priority countries, including Europol liaison officers and liaison magistrates. Appropriate responsibilities and functions for these experts will be defined by the Commission and the European External Action Service' (COM 2010(673), section 1).

In achieving this, it will be extremely important to ensure that the skill-sets and training are closely matched to the target functions. In addition, this new network of security contacts should be complementary to existing networks (e.g. the ENISA network of National Liaison Officers (NLO)) and potential synergies should be fully exploited.

Increasing dialogue between communities

The ISS clearly foresees the need to bring together actors from different communities in order to increase the effectiveness and efficiency of the security approach. In particular, dialogue between entities that were formerly separated by the 'pillar system' is now explicitly mentioned (e.g. COM 2010(673), Objective 3, action 1 – 'The (cybercrime) centre will ..., establish cooperation with the European Network and Information Security Agency (ENISA) and interface with a network of National /governmental Computer Emergency Response Teams (CERTs).').

ENISA believes that increased dialogue and cooperation between different operational communities is a key requirement for underpinning a new strategy.

Prevention and anticipation

The objectives

The document 'The EU Security Strategy in Action: Five Steps Towards a More Secure Europe' defines five strategic objectives for internal security:

- Disrupt international crime networks.
- Prevent terrorism and address radicalisation and recruitment.
- Raise levels of security for citizens and businesses in cyberspace.
- Strengthen security through border management.
- Increase Europe's resilience to crises and disasters.

Following the coming into force of the Lisbon Treaty, ENISA expects to contribute to objectives 1, 2, 3 and 5 but anticipates that the Agency's most significant contribution will be in the area of objective 3.

At present, the Agency works mainly in the area of prevention, but could also take a more active role in assisting Member States in coordinating the response capability if Member States believe that this is appropriate. At present, a pan-European response to a cyber-incident would be based on bi-lateral arrangements.

The following headings summarise how ENISA expects to contribute to the ISS.

Risk management

A common condition for success for each of the above objectives is the application of proven risk management techniques. Indeed, Information Security can be seen as a form of risk management – where the risks under consideration are taken to be those affecting data and the information systems that process data.

ENISA has significant experience in the area of Risk Management, which has been one of the main components of the work programme in previous years. In 2011 and beyond, the identification of Information Security risks continues to be a central element of ENISA work. Issues of global risk management and risk assessment, emerging threats and dissemination of good practices for Risk Management and IT Contingency are subject of work both within ENISA and the Commission.

Improving resilience at the pan-European level

Where objective 5 is concerned, it should be noted that ENISA is contributing to the Critical Information Infrastructure Protection (CIIP) action plan, as defined in the Commission Communication on Critical Information Infrastructure Protection (CIIP) of March 2009[22]. This action plan will clearly contribute to the goals defined under objectives 3 and 5.

Notable initiatives in this area include the coordination of the first pan-European Cybersecurity exercise (Cyber Europe 2010), support for the European Forum for Member States (EFMS) and the European Public Private Partnership for Resilience (EP3R).

[22] Commission Communication of March 2009, "Protecting Europe from large-scale cyber-attacks and disruptions: enhancing preparedness, security and resilience", COM(2009)149.

In 2011, ENISA plans to build on these initial steps in the following way:

- In the area of exercises the Agency will begin discussions with the Member States on the planning of the second pan European exercise.
- We will gather knowledge, expertise and good practices on the threats and vulnerabilities of Industrial Control Systems (SCADA).
- We will also work with Member States to analyse the interdependencies of Information and Communication Technologies within the Energy, Transport and Finance Sectors.

Working with CERTs

Under OBJECTIVE 3, Action 1, the EC proposes to establish, within existing structures, a cyber crime centre, that should act as operational and analytical capacity for investigations and cooperation for the Member States and international partners. This prospective centre shall

"[...] establish cooperation with the European Network and Information Security Agency (ENISA) and interface with a network of national / governmental [...] CERTs".

ENISA acknowledges the importance of the fight against cyber crime as well as the need for a strong collaboration between CERTs and law enforcement. Since its inception, ENISA has sought to foster a good working relationship with relevant communities in both areas (e.g. by working in close collaboration with the "Forum of Incident Response and Security Teams" (FIRST)).

ENISA is recognised as facilitator and supporter of cooperation, also in operational aspects, by both communities. ENISA experts are invited to closed events organised by law enforcement agencies (like the "Underground Economy" conference organised by Interpol), and is also, since 2008, active in the organisation of the "Financial Information Sharing and Analysis Centre (ISAC)" cooperation activity, that brings together players from the banking sector, CERTs and law enforcement (for example Europol or the Dutch national police) for a vital and trusted information exchange.

A special emphasis is put on a good working relationship between national / governmental CERTs and law enforcement. As such, ENISA has foreseen in its Work Programme for 2011, a dedicated Work Package that aims at establishing (where needed) and fostering these relationships.

Reporting of Serious Incidents - Article 13 a of the new Telecom Package

ENISA is assisting Member States in the implementation of *Article 13 a of the new Telecommunications Regulatory Package*[23] in order to achieve a consistent and harmonized implementation of mandatory incident reporting scheme throughout the EU.

ENISA acts as a facilitator, by identifying the appropriate competent regulatory authorities and engaging them in a structured dialogue on the relevant issues.

The main objectives of this work are to:

[23] Telecommunications Regulatory Package (article 13a. amended Directive 2002/21/EC Framework Directive)

- Identify, disseminate and consolidate the use of good practices in the area of incident collection and reporting.
- Define a unified scheme for reporting that delivers added value to the Member States.
- Work together with Member States and the private sector to increase their level of preparedness by developing minimum security requirements for addressing risks to resilience and security.
- Support the creation of a trusted environment or community for information sharing between Member States.

Improving capability for dealing with cyber attacks

Action 3 of objective 3 is entitled 'Improving capability for dealing with cyber attacks'. In addition to the work being done together with the CERT communities, ENISA regularly undertakes studies that help Member States to identify the key threats and that propose suitable mitigation strategies.

ENISA notes a number of challenges posed by the asymmetric nature of the fight against cybercrime – in particular the flexibility now enjoyed by cybercriminals in moving between jurisdictions, technical solutions and control structures and stresses the importance of a number of measures for dealing with these challenges[24]. In particular:

- Improving the accuracy of information about the level of threat posed in different areas of cybercrime. Current data provides at best estimates based on very limited samples and poorly documented methodology.
- Increasing the efficiency of cross-border legal mechanisms, in particular the time taken to effect sanctions against criminals.
- Enabling and incentivising those in a position to react – for example, by providing tools, support and incentives for ordinary citizens to maintain home systems free of malware.
- Promoting efficient cross-border information-sharing mechanisms between all parties maintaining appropriate levels of confidentiality.
- Putting a focus on addressing all factors contributing to cybercrime including installation of malware on citizen PC's, revenues collected by criminal networks and command and control of botnets.

Supporting European Privacy and Data Protection initiatives

Under the heading 'Security policies based on common values' in section 1 of COM 2010(673), it is noted that 'Where efficient law enforcement in the EU is facilitated through information exchange, we must also protect the
privacy of individuals and their fundamental right to protection of personal data.'

ENISA is currently working together with the European Commission and the European Data Protection Supervisor (EDPS) on the implementation of Article 4 of the ePrivacy Directive. We intend to extend this work during 2011 by assisting the Member States and the Commission in identifying and responding to privacy and security issues related to current and future technology. This will be achieved by promoting methods and tools and standards for recognising and responding to threats, vulnerabilities and risks at both the infrastructure and application levels.

[24] ENISA will publish a report detailing these - Botnets: Detection, Measurement, Disinfection & Defence –in January, 2011.

Increase Europe's resilience to crises and disasters.

Crisis response should assess information technology dependencies and interdependencies. In particular, crisis planning should address not only network infrastructure risks, but risks to the provision of critical IT services whose unavailability affects a significant number of European citizens. Such services might include:

- Single points of failure such as single points of contact for cross border service provision (as required by the services directive).
- IT services such as cloud providers with a market share affecting a significant number of citizens (we note that certain cloud service providers now cover 100's of millions of EU citizens).

The committee may wish to consider the provision of shared information processing resources in the context of a pan European mutual aid and assistance plan for emergencies. For example, the availability of emergency cloud-based IT capacity for emergency response teams.

Information exchange

The importance of information sharing

Information exchange is a fundamental component of any global initiative to improve security. Without effective information exchange mechanisms, European Member States will not be in a position to correctly assess global threats and may therefore put in place procedures and mechanisms that do not respond to the most important risks.

Similarly, poor information exchange mechanisms are likely to result in a duplication of effort and a slower learning curve for implementing approaches, processes and technology for mitigating the key risks once they are understood.

ENISA and information sharing

ENISA has significant experience in promoting the exchange of information related to Information Security between Member States. In the area of Critical Information Infrastructure Protection (CIIP) for instance, the approach has been to work together with Member States in order to identify lessons learned from National approaches and to enable Member States to learn from each other. As a concrete example, the recent Cybersecurity exercise involving all 27 Member States and facilitated by ENISA was prepared in this way.

The Agency developed a good practice guide on Information Sharing using the experience of UK's Centre for the Protection of National Infrastructure (CPNI). The Agency promotes the concept of information sharing in Member States public institutions and private sector. Through this it hopes to increase the number of countries effectively using public private sector information sharing to enhance their cyber security strategy.

In addition, the Agency also exchanges information with countries outside Europe when it clearly makes sense to do so. Recent examples include the work done on Cloud Computing, which involved input from many Member States, but also a collaboration with the Cloud

Security Alliance (CSA) and participation in an international conference in Japan on security and the Internet of Things (IoT).

ENISA and awareness raising

In a more general context, a high-level of awareness of security issues amongst European Citizens can only be achieved if the appropriate information is shared between expert communities and the Citizens themselves. The ENISA Work Programme 2011 includes efforts to enhance European cooperation to generate awareness about NIS, disseminate security relevant information and to assist Member States in coordinating these activities internationally. The Agency is investigating the viability of a European Cyber Security Awareness month partnership to create synergies and mutual benefits at international level and by making use of existing networks and amplifiers. Such an initiative has already met with success in the United States and the Agency aims to build on US experiences. The main concept is to bring basic ideas, tips and practices on NIS to the general public.

Furthermore, as recognised in Council Doc. 7120/10 "Security policies, especially those of prevention, must take a broad approach", ENISA has identified the need to focus on integrating Information Security into the school curriculum and to provide similar opportunities to young people in vocational training.

Operational cooperation

The ISS clearly identifies the need for closer operational cooperation between EU institutions, Member States and between the public and private sector:

'The EU Internal Security Strategy in Action therefore puts forward a shared agenda for Member States, the European Parliament, the Commission, the Council and agencies and others, including civil society and local authorities. This agenda should be supported by a solid EU security industry in which manufacturers and service providers work closely together with end-users.'

A significant part of ENISA's work programme is aimed at improving cooperation between the different actors involved in improving European security. In particular, ENISA works very closely with both the public sector and the private sector and continually strives to align the goals and activities of these two communities in all areas in which the Agency is present.

We therefore fully support the goals of the ISS in this regard.

Integrated border management

This aspect of the inquiry is not within the scope of ENISA's activities. We do not therefore make any comment on this subject.

10 December 2010

Memorandum by Europol (ISS 11)

Scope, scale and range

The scope of the ISS; whether it covers the appropriate range of threats, issues and problems; any gaps and omissions (or inappropriate inclusions); the proportionality and ambition of the approach in relation to the threats and issues identified; the practicability and appropriateness of the proposed European Security Model; priorities for the ISS and its likely impact. How should success be judged?

Europol welcomed the adoption of the Internal Security Strategy as well as the recent publication of the related Commission's Communication. Europol considers the scope of both documents in question as appropriate and comprehensive. They will undoubtedly facilitate and streamline the EU's decision-making in the field of home affairs, especially the coordinative efforts of the **Standing Committee on Operational Cooperation on Internal Security (COSI)** established under art. 71 of the Treaty on the functioning of the EU.

The Strategy and the Communication will enhance the EU position towards its partners, as they make the internal security policy more coherent and clear to the external world.

The Internal Security Strategy maps out the different aspects of internal security policy and lists strategic guidelines for action. Europol fully supports all of them and is convinced that their full implementation will be beneficial to the fight against crime.

Europol ('the Agency') is satisfied to see a proactive, intelligence-led approach (Guideline III) as one of the leading concepts in the field of home affairs. Moreover, the European Council's support for comprehensive information exchange (Guideline IV), focus on operational cooperation (Guideline V) as well as its commitment to innovation (Guideline VIII) fully reflect the Agency's understanding of efficient, modern policing.

Moreover, the Strategy correctly identifies the role of Europol stating that its main aims are to collect and exchange information and to facilitate cooperation between law enforcement authorities in their fight against organised crime and terrorism. It also underlines Europol's role as a provider of regular threat assessments.

The Commission's Communication describes concrete objectives and actions to be taken by Member States, EU institutions and agencies. Three of five objectives listed there, namely the disruption of crime networks (Objective 1), prevention of terrorism (Objective 2) and security of cyberspace (Objective 3), are extensively covered by Europol's mandate. Moreover, strengthening security through border management (Objective 4) is also distinctly related to Europol's core business and is an area where the Agency could add significant value in close cooperation with other EU bodies, especially Frontex. Concrete actions proposed by the Commission in order to meet the objectives indeed mirror the Agency's well- established fields of expertise.

Europol's primary goal is to support Member States in identifying and dismantling criminal networks, facilitating the exchange of relevant intelligence, providing analysis and coordinating multi-national operations. Thus Europol could play a vital role in initiatives under **Objective 1**, Action 1. Concrete proposals made by the Commission under this Action, such as the establishment of **EU Passenger Name Records** or revision of the **EU Anti-Money Laundering legislation**, would undoubtedly facilitate investigations across

the European Union. These improvements could be combined with increasing analytical capabilities at the European level, in order to detect and disrupt transnational criminal activities more effectively.

Attention paid by the Commission to criminal assets, under Actions 1 and 3, is very much welcomed by Europol since it is considered a key element of successful policing and prevention.

Asset Recovery Offices (AROs), mentioned in the Communication, are actively supported by Europol. In 2007 Europol established the **Europol Criminal Assets Bureau (ECAB)** which supports Member States in the identification and confiscation of criminal proceeds. Europol is currently working to facilitate communication between AROs via the **SIENA**[25] system. This provides the Member States with the opportunity not only to exchange information, but also to crossmatch the exchanged data with Europol's databases. Moreover, Europol serves as a secretariat for the **CARIN Network** dealing with asset recovery on a global scale, thus facilitating exchange of information with partners outside the EU.
In order to tackle criminal assets successfully, the development of legal tools for confiscation, and the establishment of AROs equipped with the necessary resources, powers and training, should be combined, in the opinion of Europol, with the mainstreaming of financial investigations. They should be widely applied against serious and organised crime across the EU.

Moreover, the Communication states that the Commission and Member States should continue to ensure effective implementation of the **European Arrest Warrant (EAW)**. The inclusion of Europol in the circulation of EAWs which fall within its mandate would certainly serve the purpose. Information covered by an EAW, especially a description of the circumstances in which the offence was committed, including the time, place and degree of participation by the requested person, are highly valuable from Europol's point of view.

Action 2 focuses on protection of the economy against criminal infiltration and also covers fields where Europol already has vast potential and experience, such as the fight against counterfeit goods. It also encourages the development of policies to engage governmental and regulatory bodies responsible for granting licences, authorisations, procurement contracts or subsidies, known as the **'administrative approach'**, in order to fight organised crime. Europol welcomes this idea which could significantly supplement traditional policing. It is fully in line with Europol's Strategy that encourages crime prevention, pioneering new techniques and advising on new legal or administrative instruments capable of reducing the threat of organised crime. In order to support the approach, the Agency can serve as a platform for the exchange of strategic information and good practices as well as explore the possibilities to facilitate cross-border investigations based on the administrative approach. Exchange of relevant operational information could take place via law enforcement channels already available at Europol.

Objective 2: Preventing terrorism and addressing radicalisation and recruitment is of vital importance to Europol and lies at the heart of its activities. Synergy between new initiatives and current activities should be developed to ensure that actions undertaken are efficient and cost-effective; for example the work of civil society organisations which expose,

[25] Secure Information Exchange Network Application (SIENA), is an IT tool developed by Europol in order to ensure secure communication.

translate and challenge violent extremist propaganda on the internet could benefit from the experience Europol have gained running the ***Check the Web* project,** which has very similar objectives.
Following the signature of the **EU-US Terrorist Financing Tracking Programme (TFTP) agreement**, in 2011 the Commission will develop a policy for the EU to extract and analyse financial messaging data held on its own territory. Europol is of the opinion that the establishment of such a mechanism within the EU would greatly facilitate investigations. Europol is convinced that it could, due to its operational character, analytical capacities and experience in the field of counter-terrorism, be considered a vital element of the future system. Undoubtedly, the debate on the establishment of a EU-wide TFTP system and necessary feasibility studies could take into account Europol's experience in verifying US requests pursuant to article 4 of the current EU-US TFTP agreement. Europol's robust data protection regime and unparalleled expertise in processing large amounts of data offer potential for future common EU data systems.

Under Action 2 the Commission proposes to establish a law enforcement Early Warning System at Europol for incidents related to **Chemical, Biological, Radiological and Nuclear (CBRN)** materials. This idea is considered feasible and could constitute an element of Europol's 24/7 capability.

Moreover, setting up a European network of specialised CBRN law enforcement units proposed under the same Action could also be combined with ongoing networking of experts facilitated by Europol.

Objective 3, which deals with cyberspace security, is also closely related to Europol's mandate. Cybercrime is already a vital element of its Strategy 2010-2014. The Communication rightly underlines the role of **Europol's High Tech Crime Centre (HTCC)** which coordinates operational activities, serves as a communication platform and produces strategic analysis (Europol High Tech Crime Threat Assessment and iOCTA). Action 1 provides for the establishment, within existing structures, of a cybercrime centre, through which Member States and EU institutions will be able to build operational and analytical capacity for investigations and cooperation with international partners.

Taking into account Europol's experience in fighting cybercrime and the unique technical and analytical expertise built in this field, as well as the fact that the centre is supposed to facilitate operational cooperation, **the Agency could play a primary role in the establishment of the future entity.** Dispersion of investigative and analytical capacities in the fight against cybercrime should be avoided in order to safeguard the necessary coordination and cost-effectiveness.

Roles and responsibilities
Clarity of roles and responsibilities between national authorities and the Union; the role of COSI; relationships and interdependencies between the ISS and other strategies and policies, including the external dimension.

The Strategy states that further developing, monitoring and implementing the Internal Security Strategy must become one of the priority tasks of the **Standing Committee on Operational Cooperation on Internal Security (COSI)**. Moreover, according to the document, stringent cooperation between EU agencies and bodies involved in EU internal security (Europol, Frontex, Eurojust, CEPOL and SitCen) is to be ensured by COSI so as to encourage increasingly coordinated, integrated and effective operations. Europol welcomes

this approach and considers the Committee a major improvement provided for by the Lisbon Treaty in the field of overall coordination of operational activities. The Committee is considered an important platform, where Europol's expertise can be used by Member States and the necessary coordination between national services and EU bodies is enhanced.
COSI is also a vital element of the **EU policy cycle for organised and serious international crime**[26] recently established by the Council. Its aim is to tackle the most important criminal threats in a coherent and methodological manner through optimum cooperation between the relevant services of the Member States, EU institutions and EU agencies, as well as relevant third countries and organisations. The policy cycle for serious international and organised crime will consist of four steps. The first step is policy development on the basis of a European Union Serious and Organised Crime Threat Assessment (**EU SOCTA**) that must provide a complete and thorough picture of criminal threats impacting the European Union. The report will be produced by Europol and based on input received from Member States, other EU bodies, third parties and the Agency's own data.

The second step is the policy setting and decision-making through the Council's identification of a limited number of priorities, both regional and pan-European. For each of the priorities a Multi-Annual Strategic Plan (MASP) is to be developed to achieve a multidisciplinary, integrated and integral (covering preventive as well repressive measures) approach to effectively address the prioritised threats.
Implementation and monitoring of annual Operational Action Plans (OAP) is the third step. Europol will seek to integrate the COSPOL projects into the new policy cycle as much as possible, notably by streamlining them with the future action plans in order to provide more coherence to the process. At the end of each policy cycle a thorough evaluation is to be conducted and will serve as input for the next policy cycle.

The Agency considers the adopted model practicable and clear, allowing for the identification of key threats and prioritisation of actions to be taken.
Since the model is based on a thorough threat assessment, it implements the idea of an intelligence-led and knowledge-based fight against crime.
Since it provides for both regional and pan-European measures, it can be flexibly adopted to specific needs of a group of Member States or particular crime phenomenon.
As it is a policy cycle, where results of the previous round influence actions to be taken in the future, regular analysis of achievements and shortcomings is of vital importance. This also contributes to the overall accountability of all entities involved; both decision-making bodies as well as executive agencies. Europol welcomes this approach, since it considers accountability and effectiveness its key values.

Europol fully subscribes to the statement of the Strategy, which says that a concept of **internal security cannot exist without an external dimension**, since internal security increasingly depends, to a large extent, on external security.
The Strategy rightly says that failed states and areas of regional conflict have frequently proven to be breeding grounds for organised crime and terrorism. This evaluation closely corresponds to Europol's own findings, as expressed in Europol's Organised Crime Threat Assessment (OCTA). The first line of defence against such threats must be at the source, and therefore outside the borders of the EU. In this regard Europol would be ready to second its experts to key EU delegations, in order to foster operational cooperation against serious and organised crime.

[26] Doc. 15358/10, COSI 69 ENFOPOL 298 CRIMORG 185 ENFOCUSTOM 94.

Moreover, the Council has established an administrative arrangement allowing for Europol to cooperate and exchange information (excluding personal data) with all CSDP civilian police missions. The Stockholm Programme called for the improvement of these cooperation mechanisms, while the EU Internal Security Strategy encourages law enforcement agencies to strengthen their participation in civilian crisis management missions. Europol can help to improve the performance of Common Security and Defence Policy (CSDP) police missions by providing them with analysis which can allow them to adjust their strategies in response to criminal trends. Equally, **Europol would very much benefit from the expertise and local knowledge gathered by the police missions** to improve its analysis, thereby providing EU decision-making bodies and Member States with a comprehensive picture of criminal threats, both operational and strategic.
In order to enhance coherence between external and internal security, further steps should also be taken to increase Europol's cooperation with the EU Joint Situation Centre, for example with regard to joint threat assessments before CSDP police missions are planned and deployed.

Lastly, Europol supports its Member States wherever they are actively fighting crime, in particular in the framework of regional police initiatives, such as the Maritime Analysis and Operations Centre (MAOC) or the two West African platforms in Ghana and Dakar.

Prevention and anticipation
The systems, mechanisms and processes needed to improve confidence in the early warning of threats and problems; the scope for greater cooperation with non-government actors, including the private and education sectors, and civil society organisations; ways to counter radicalisation and reduce vulnerability and risk.

Europol is of the opinion that **prevention and anticipation are at the heart of efficient and cost-effective law enforcement.**

The recently adopted policy cycle guarantees the permanent monitoring of criminal trends and allows for coordinated countermeasures based on clearly defined priorities. Understanding of criminal trends, which is the objective of Europol's main analytical product - the Organised Crime Threat Assessment - is indispensable for the anticipation of threats and proactive policing.

A long-term policy cycle does not exclude flexible reaction in case of sudden changes in the criminal world and application of new investigative techniques. One of Europol's objectives is to pioneer new policing techniques and react flexibly to new ways of committing crimes, especially in the Hi-Tech area. As indicated above, both strategic documents rightly address developing threats, empowering, for example, civil society to counter radicalisation or proposing the establishment of a law enforcement Early Warning System at Europol for incidents related to CBRN materials.

Moreover, Europol fully recognises the preventive role of confiscating criminal assets and welcomes the attention the Commission attaches to the topic in its Communication. Also, other proposals made by the Commission, such as the increase of security in cyberspace, and the enhanced exchange of financial messaging data or passenger names records, will greatly contribute to overall prevention.

Europol acknowledges the importance of **extending its reach beyond formal official law enforcement channels of cooperation**. The outreach approach is being currently developed at Europol to tackle security threats through building trusted relationships with a variety of partners and other relevant actors. It is to be based on collaboration with academia, private industry and other organisations of both a national and international nature.

Within Europol's overall vision, outreach will create a strategic capability enabling the organisation to benefit from knowledge, information, research and resources held outside of the law enforcement community. It will allow Europol to identify and develop the latest techniques available in combating crime and terrorism and be better informed about current security concerns, phenomena and trends. It will also facilitate the necessary exchange of expertise thus bridging the gap in fields such as IT, where the law enforcement community lacks specific knowledge. On the other hand, close cooperation with industry could have a major preventive dimension - certain new technologies could be discussed before they enter the market, in order to make them 'crimeproof' and to limit the opportunities for criminals to misuse them.

Information exchange

Practical measures to build trust and encourage the timely exchange and appropriate access to data whilst maintaining the right to privacy and the requirements of data protection.

There are numerous communication channels and information systems in the area of freedom, security and justice.[27] Europol enjoys access to many of them and uses them on a daily basis for its operational activities.
The Strategy rightly states that Member States have to share intelligence in time to prevent crime and bring offenders to justice.
Trust and the timely exchange of intelligence are of primary importance to Europol which is, first and foremost, an intelligence hub. The quality and quantity of intelligence is a major factor that determines the effectiveness of the Agency.

Information exchange on the basis of mutual trust, and culminating in the principle of information availability, is rightly named one of the Strategy's key objectives. This is also supported by the explicit statement of the Communication, which says that efficient law enforcement in the EU is facilitated through information exchange. All measures following this reasoning and enhancing intelligence exchange will be welcomed by Europol. At the same **time privacy and data protection are of utmost importance**, constitute a vital element of Europol's culture and are crucial for the Agency's accountability. Europol's robust data protection regime is based on a number of clear values, such as lawfulness of processing, quality of data, proportionality and data security. Europol implements numerous technical and organisational security measures that are appropriate to the risks presented by the processing of data. It also enjoys a well-established system of bodies, both external and internal, supervising the use of data. Observance of the Europol data protection principles is guaranteed and monitored by independent supervisory authorities, both at national and European level. The Europol Joint Supervisory Body (JSB) has powers to rectify or erase data which was processed unlawfully or which is inaccurate or incomplete. Moreover, transparency is one of the guiding principles of Europol's data protection regimes. The data subject has a right to be informed of all data processed at Europol that relates to them, where there are no operational reasons for withholding that data, and they have a right to

[27] Doc. 12579/10, JAI 660 DAPIX 12 DATAPROTECT 60.

correction of that data where it is shown to be inaccurate. The communication of data shall only be refused if such refusal is necessary for law enforcement authorities to fulfil their duties properly, to protect security and public order, or to prevent crime and to protect the rights and freedoms of third parties.

Operational cooperation

The effectiveness of cooperation between EU agencies and bodies involved in EU internal security including Europol, Frontex, Eurojust, CEPOL and SitCen, and measures for the improvement of cooperation; cooperation and support for major and mass international events.

The Strategy calls for stringent cooperation between EU agencies and bodies involved in EU internal security (Europol, Frontex, Eurojust, CEPOL and SitCen) to be ensured by COSI so as to encourage increasingly coordinated, integrated and effective operations. The establishment of COSI indeed enhanced cooperation between the agencies in question, not only by providing a platform where the agencies can communicate with Member States, but also by fostering contacts and coordination among them. Joint reports on the cooperation between Europol, Eurojust, CEPOL and Frontex were produced, and subsequently presented to COSI, leading to concrete recommendations and improvements. Meetings of Heads of JHA Agencies are organised on a regular basis. In 2010 it was Europol that hosted the event.

A common threat assessment is considered a vital prerequisite for more robust coordination between the agencies in question. Indeed, such a document was presented to COSI. The combined report[28] was based on three strategic documents: Europol's Organised Crime Threat Assessment (OCTA), EU Terrorism Situation and Trend Report (TE-SAT), and Frontex's Annual Risk Analysis (ARA).

Major international events, especially sports events are potential targets for organised crime and terrorism. The host Member State is primarily responsible for providing security to such events. However, due to the international character of these events, all other Member States and EU competent bodies have a responsibility to assist and support the provision of such security.

Europol may support coordination of the activities and act as an information hub. Providing intelligence and analytical support to Member States in connection with major international events is explicitly listed in the Europol Council Decision (ECD) as one of Europol's principal tasks.

Europol has provided support to Member States and third parties in the preparation and development of several major international sports events such as the 2004 European Football Championships in Portugal and the 2004 Olympic and Paralympic Games.
On a strategic level, Europol participates in different forums, working groups and initiatives developing policies related to police cooperation in the organisation of these events.
Europol's handbook on support for Member States' Major International Events, that is currently being updated, will cover the whole variety of actions Europol may take.
The Strategy states that progress should be made on the development of a cooperation framework to improve security and safety at major and mass international events. Further developments in this field, contributing to better coordination and more extensive data exchange, could be built on the experience and capacities of the Agency.

[28] Doc. 8849/4/10 REV 4, LIMITE JAI 323 COSI 21.

Integrated border management
The need to reinforce border management mechanisms and share best practice; the case for a European system of border guards; the scope for greater use of technology to facilitate border crossing by citizens whilst maintaining or improving security.

Security at the EU's external border and security inside the European Union are interdependent, thus Frontex and Europol must strengthen their relations, seek **greater synergy of their actions and avoid duplication.** This principle is specifically enshrined in the Commission's Communication and is fully supported by Europol.
Frontex's task is to help Member States organise joint operations at the EU's external borders. Europol is an intelligence agency whose main task is to analyse criminal data sent by Member States' law enforcement authorities, including customs and border guards. Information gathered during Frontex's joint operations is analysed by Europol to support the investigation of organised crime and terrorist networks. Thus the roles of the two agencies are complementary.

Currently, the legal framework of Frontex does not allow the storage of personal data. However, in order to improve this symbiotic relationship, Europol would welcome the strengthening of Frontex's operational capacities. Providing Frontex with the right to process personal data entails, however, some risks of duplication. Therefore Europol supports the possibility of Frontex being able to process personal data, but for the purposes of information exchange with Member States and Europol only.

In practice this means the establishment of an 'information exchange system' at Frontex but with no capacity to store personal data in any 'analysis system', that would duplicate what Europol already does. Such a clear 'purpose limitation clause' would also be attractive in terms of data protection safeguards.

Moreover, Europol could provide Frontex with dedicated access to its analysis work files (AWFs) and Frontex could make use of Europol's SIENA communication system to improve interoperability and cohesion.

The misuse of legal procedures, such as the asylum regimes, is one of the most used modus operandi in the area of illegal immigration. In the absence of any significant harmonisation of standards in asylum systems in the EU Member States, this method will continue to be used or might even become more popular.

Organised crime networks always probe the administrative processes of Member States to find weaknesses and vulnerabilities, and possible opportunities to corrupt, and this will continue.

Thus it is vital for law enforcement authorities to be able to cross-check, store and process information on illegal migrants. This may lead to the identification of suspects or organised crime groups.

Therefore, Europol welcomes the introduction of the new agency - European Asylum Support Office (EASO). Facilitating, coordinating and strengthening practical cooperation amongst the EU Member States in the field of asylum, EASO will complement and support the efforts made by Europol in the fight against illegal immigration.

The Communication states that, by 2014, the Commission will develop, together with Frontex, Europol and the European Asylum Support Office, minimum standards and best practices for interagency cooperation. These shall particularly be applied to joint risk analysis, joint investigations, joint operations and exchanging intelligence. Europol fully supports this initiative and is of the opinion that it should be built on the already-developing cooperation between the respective agencies, especially in the field of strategic threat assessments, and take into account the coordinative role of the COSI Committee.

29 December 2010

Memorandum by the Foundation for Information Policy Research (FIPR) (ISS 3)

The Foundation for Information Policy Research (FIPR) is an independent body that studies the interaction between information technology and society. Its goal is to identify technical developments with significant social impact, commission and undertake research into public policy alternatives, and promote public understanding and dialogue between technologists and policy-makers in the UK and Europe.

We would like to make the following response to the House of Lords inquiry into the EU Internal Security Strategy[29] [30].

We welcome the European Commission's proposals to establish a cybercrime centre and to improve interagency cooperation at national level; we recommended in a report we wrote two years ago for ENISA [3] that Europe needed a "NATO for cybercrime" and while this falls somewhat short of that, at least it's a start. We note the strategy states that "Member States should ensure that people can easily report cybercrime incidents" rather than proposing security-breach reporting legislation as is now in force in most US states. So Europe will still lag the USA in this regard.

Overall, however, these documents are disappointing. The Internal Security Strategy[31] has not been carefully written: for example, at p 5 we find "Terrorism, in any form, has an absolute disregard for human life and democratic values." This is exaggerated: different terrorist organisations have had widely different attitudes towards civilian casualties, with the Provisional IRA generally seeking to minimise them; and while Al-Qaida has staged mass casualty attacks, the recent toner cartridge bombs were aimed explicitly at causing economic damage. If we were to go through the report and examine every sentence for accuracy and relevance, our response would be rather long.

We would like to bring to your attention a public comment by European Digital Rights (EDRi), an organisation of which FIPR is a member[32]. This highlights the security strategy's inconsistency in the way it handles issues such as copyright infringement and unlawful images of child sex abuse. The authorities in many countries are more willing to listen to wealthy complainants, such as the music industry, and take their concerns more seriously than those of the much less vocal and well-resourced victims of child abuse.

The strategy's failure to deal honestly with priorities is compounded by its silence on the real tensions between information sharing and human rights; these were discussed in our "Database State" report last year which found that some EU systems were probably in violation of the European Convention on Human Rights. We also found that the Prüm

[29] Internal Security Strategy for the European Union (Council Doc. 7120/10, 8 March 2010): http://register.consilium.europa.eu/pdf/en/10/st07/st07120.en10.pdf

[30] Communication from the Commission: The EU Internal Security Strategy in Action: Five steps towards a more secure Europe (COM(2010)673 final, 22 November 2010): http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0673:FIN:EN:PDF

[31] Ross Anderson, Rainer Böhme, Richard Clayton and Tyler Moore, *Security Economics and the Internal Market.* ENISA, March 2008: http://www.cl.cam.ac.uk/~rja14/Papers/enisa-short.pdf

[32] ENDItorial: EC Internal Security Strategy – My dog is a cat, EDRi, December 1st 2010: http://www.edri.org/edrigram/number8.23/ec-internal-security-strategy

Framework was almost certainly in breach of the Convention[33]. This is now highly topical in the context of the revision, following the Lisbon Treaty, of the Data Protection Directive. Yet the strategy avoids discussion of this tension, and its general tenor is that privacy must come second to security: this is implied by the 'comprehensive model for information exchange' that we're supposed to develop in order to facilitate 'a proactive, intelligence-led approach'.

The Communication, COM(2010) 673 final, is similarly muddled. It is unclear what PNR legislation has to do with identifying and dismantling criminal networks, or what further IP enforcement measures have to do with protecting the economy against criminal infiltration.

As for new powers, given the current controversy over the European Arrest Warrant, it seems rather courageous of the Commission to propose asset-recovery legislation "to facilitate mutual recognition of non-conviction-based confiscation orders between Member States".

In conclusion, what these documents mostly reveal is a lack of joined-up thinking about security in the Commission. They are a laundry list of policies being pursued by various parts of the Commission for various reasons, good and bad, with varying levels of effectiveness; a strategy, however, they are not.

15 December 2010

[33] Ross Anderson, Ian Brown, Terri Dowty, Philip Inglesant, William Heath, Angela Sasse, *Database State*. Joseph Rowntree Reform Trust, 2009: http://www.cl.cam.ac.uk/~rja14/Papers/database-state.pdf

Memorandum by Dr Claudia Hillebrand (ISS 9)

1. The 1999 Amsterdam Treaty formally set out the aim of the European Union (EU) to create the Area of Freedom, Security and Justice (AFSJ). The policies within this realm refer to, in particular, policing issues, border controls, immigration and asylum, judicial cooperation in criminal and civil matters as well as related fields. Next to external security matters, internal security policies have become an important concern of the Union's efforts. The policies under the AFSJ have been growing throughout the last decade and led to increasing executive action at the EU level. The entry into force of the Treaty of Lisbon reinforced and strengthened the EU's efforts to create an AFSJ.

2. Overall, the Treaty of Lisbon provides for a shift from rather intergovernmental co-operation towards a more Community approach in this field. This implies a strengthened role in the policy-making process for the European Parliament (EP) and new possibilities for scrutiny through national parliaments. The key body in this sensitive field remains the European Council, however, which also, according to Article 68 of the Treaty on the Functioning of the European Union (TFEU), "shall define the strategic guidelines for legislative and operational planning within the area of freedom, security and justice." The European Commission has also taken on an important role in this field over time.

3. From the perspective of democratic governance, the intensified activities of internal security authorities – either directly at the EU level or channelled through EU institutions, continue to pose challenges with respect to democratic accountability. Creating the AFSJ at the Tampere Council in October 1999, the idea was to base the related policies upon the principles of transparency and democratic control to strengthen the acceptance of citizens. While the Treaty of Lisbon brought important changes, the EU's AFSJ policies still do not fully meet those ideals. Both the development of the Internal Security Strategy (ISS) for the EU and the related creation of the Standing Committee on Operational Cooperation on Internal Security (COSI) are examples of the ongoing lack of transparency concerning the EU's field of internal security.

4. The ISS, adopted under the Spanish Presidency in February 2010 and endorsed by the European Council on 25/26 March 2010, presents the first strategy paper concerning the EU's policy field of internal security. Broadly speaking, parliaments have not been involved in the development of this paper. In a written exchange among ministers while at the G6 meeting of 15 March 2009, the Spanish government had announced the development of such a security strategy. A full draft strategy paper was presented on the 3rd of December 2009 and circulated among the EU Member States' governments in preparation for the informal ministerial meeting in Toledo 20-22 January 2010.[34] At least some national parliaments were informed very late about the content of the strategy. For example, the German Bundestag received notice about it in a preparatory report concerning the ministerial meeting in Toledo on the 20th of January 2010 – thus, only on the first day of the meeting.[35]

5. Rather than parliamentary actors, executive authorities have been developing the key features of the ISS. Crucially, Europol, Eurojust and Frontex have done preliminary work on the Strategy. In a Joint Report of July 2010 entitled 'The State of Internal Security in the EU', they described the nature of key common threats, based on the Europol's Organised

[34] See statement by Ole Schröder, Secretary of State in the German Federal Ministry of the Interior, Deutscher Bundestag, 17th legislative period, 23rd session, 24 February 2010 (p. 1977). Online at http://dipbt.bundestag.de/dip21/btp/17/17023.pdf.
[35] Ibid.

Crime Threat Assessment (OCTA) and Terrorism Situation and Trend Report (TE-SAT) as well as Frontex's Annual Risk Analysis (ARA).

6. As a consequence, there has not been a broad discussion about the term 'internal security', for example, which the ISS refers to as "a wide and comprehensive concept which straddles multiple sectors in order to address these major threats and others which have a direct impact on the lives, safety and well-being of citizens, including natural and man-made disasters." This definition seems to allow the EU to include all matters relating to the maintenance of law and public order. As Cecilia Malmström, Commissioner for Home Affairs, pointed out, for the ISS the EU "took inspiration from the comprehensive approach of the US Homeland Security Strategy".[36] As a consequence of such a wide understanding, a great variety of actors is foreseen in the ISS to fulfil the strategy's aims, including law enforcement, border management, judicial coop, civil protection agencies, political/economic/financial/social/private sectors (incl. NGOs) as well as regional and global partners.

7. Concerning the COSI, public information about its composition, function and its work remain scarce. However, a pre-requisite of effective parliamentary – as well as wider public – scrutiny is a certain degree of transparency and adequate access to information. Without information, it is impossible to hold actors to account and to make reasoned judgements about their performance. Decision-making processes should be clear and the information upon which the decision is based ought to be publicly available.

8. In accordance with Article 71 TFEU, the COSI has been created on the basis of a Council Decision.[37] Its basic mandate is "to ensure that "operational cooperation on internal security is promoted and strengthened within the Union. ... (It) shall facilitate coordination of the action of Member States' competent authorities." This mandate is vague and there has not yet been published a more detailed outline of the COSI's functions, powers and mandate. It appears that the COSI's responsibilities stretch from co-operation between police, judicial, customs, border protection personnel. Precise functions, areas of responsibilities and form remain unclear, at least to the wider public. Moreover, it is not clear what the benchmarks are for evaluating the direction, efficiency and effectiveness of operational co-operation.

9. As this body is a crucial product of the changing EU working structures concerning the AFSJ, and it is likely to take on a central role in the EU policy cycle as applied to internal security, it is regrettable that parliaments and the public are marginalized from scrutinizing the work of the COSI. Parliaments, which were not involved in the creation of the COSI, were kept in the dark about the COSI's exact functions until the body was actually set up. Moreover, Article 71 TFEU maintained that, concerning the COSI, "(t)he European Parliament and national Parliaments shall be kept informed of the proceedings." To be merely informed about the proceedings is an insufficient mechanism to ensure effective parliamentary scrutiny. The EP's resolution of 25 November 2009 concerning the Stockholm Programme has therefore to be welcomed in which the EP "calls for the creation of the evaluation system to give Parliament and national parliaments access to information related

[36] Malmström, Cecilia: 'The EU Internal Security Strategy – what does it mean for the United States', Discussion organised by The Center for Transatlantic Relations, Washington DC, 8 December 2010, Doc. SPEECH/10/739.
[37] Council of the European Union: 'Council Decision on setting up the Standing Committee on operational cooperation on internal security', Council Doc. 16515/09, Brussels, 27 November 2009.

to the policies (Article 70 of the TFEU) and activities of the internal security committee (Article 71 of the TFEU)."[38]

10. A crucial limitation of the COSI's mandate is that it is not supposed to conduct operations or prepare legislative acts. However, the COSI is to evaluate the efficiency of operational cooperation and the general direction of this field. This would not only have an effect on the Council's policy priorities in this area, but also on national policing policies. That means it will have at least an indirect impact on legislation on matters of internal security. Moreover, the COSI will also be responsible for the Comprehensive Operational Strategic Plan for Police (COSPOL). Such involvement in intelligence-led policing and strategic planning for law enforcement operations will put the COSI into a position to have a substantial impact on the EU's priority-setting in this policy field.

11. Given the enormous mandate and potentially gigantic workload of the COSI, it is surprising that the group has only met a few times since its meeting in March 2010. Such a slow start might indicate that there is no agreement (yet) by national officials on the way the body is supposed to work.

12. Parliamentary bodies as well as the broader public require a certain degree of transparency and adequate access to information in order to be able to monitor, scrutinize and judge existing structures, institutions and policies. It remains unclear what the terms are in this respect concerning the COSI. For example, will the documents which COSI receives from other EU bodies be accessible to parliamentary bodies, or the public as a whole?

Conclusion

13. The debate about the ISS has to be welcomed as it allows for a wider discussion about the EU's ambitions and efforts in the field of internal security. Usually, AFSJ-related efforts are technocratic and do not gain much public attention.

14. The EU's agenda concerning the AFSJ remains ambitious, also because the field comprises of a diverse set of policy areas. Given the haphazard way of constructing this field so far, the ISS should be welcomed for providing a more coherent overview. It is useful that the EU presents its overall threat assessment and the related policies in one coherent paper, together with confirming the EU's commitment to the Union's principles and values in the field of internal security (in particular "respects for human rights and fundamental freedoms, the rule of law, democracy, dialogue, tolerance, transparency and solidarity").

15. With respect to the COSI, it seems useful to have a body at EU level to avoid duplication and unnecessary overlap of EU internal security bodies and ensure good co-ordination among the agencies involved. However, the lack of involvement of the EP and national parliaments has to be regretted from the point of view of democratic legitimacy. As the AFSJ comprises many policies and measures which can have a direct impact on the rights and freedoms of individuals, a more democratic approach in this area ought to be ensured. Instead, the COSI currently appears to be another rather opaque Council body. However, the supranational nature that the Lisbon Treaty aspires for the AFSJ calls for improved democratic accountability mechanisms as well. It is a serious shortcoming that, given the

[38] European Parliament: 'Multi-annual programme 2010-2014 regarding the area of freedom, security and justice (Stockholm programme)', European Parliament resolution of 25 November 2009 on the Communication from the Commission to the European Parliament and the Council – An area of freedom, security and justice serving the citizen – Stockholm programme, Doc. P7_TA(2009)0090, Brussels.

current legal basis, the EP and national parliaments will not be able to scrutinize the COSI's activities in any detail.

December 2010

Memorandum by the Institute of Civil Protection and Emergency Management (ICPEM) (ISS 6)

Executive Summary

The Internal Security Strategy for the European Union.

The document provides a framework for developing an EU-wide Internal Security Strategy in that it sets out the need for cooperation and coordination between the various internal state organisations.

However, the Institute makes a number of observations:

- It is not a strategy document in the true sense of the word (paragraph 2).
- There is a tendency throughout the document to group law enforcement activities with societal education and civil protection. However, the Institute suggests that they are mutually exclusive and there is a danger that non-law enforcement agencies may exclude themselves from the holistic view put forward in this document (paragraphs 2 and 3).
- It appears that the Commission have taken an existing security strategy and merely 'bolted' on civil protection to the end of certain sections (paragraphs 4, 5, 9 & 29).
- The paper mentions matters, such as road traffic accidents, missing persons, stolen vehicles, which are, in the Institute's view not at the appropriate level for a pan EU internal security strategy (paragraph 6).
- The document claims that evaluation mechanisms have been developed to assess the effectiveness of the EC's actions in the field of terrorism and organised crime but makes no mention of any evaluations in relation to natural and man-made disasters, despite exercises that have taken place in this area (paragraphs 7-9).

The EU Internal Security Strategy in Action: Five steps towards a more secure Europe.

The document focuses on the aspiration of what is to be achieved. It sets out a vision for achieving common efforts and then sets out five strategic objectives and specific actions for 2011-2014 which, if achieved, will help to ensure the security of the population within the EU. The Institute finds these both informative and helpful. Indeed, it goes so far as to suggest that a failure to deliver the key components within the strategy will lead to a Europe that is less safe and more vulnerable to terrorists, criminals, cyber-attacks and disasters (paragraphs 10-12 & 26).

However the Institute makes a number of observations:

- Passenger Name Records (PNR) of passengers on flights, it appears, will only relate to flights entering and leaving the EU, not on internal flights between Member States. It should be extended to include EU internal flights (paragraph 13).
- The objective relating to terrorism appears to concentrate on Al Qaeda motivated or inspired terrorism but neglects to address the threat from domestic groups such as that experienced in Greece, Northern Ireland and Spain. It also fails to address 'single-issue' extremists (paragraph 14).
- The Commission has identified the need to set up a standing committee on land transport security but the Institute feels it ought to be widened to 'crowded spaces' (paragraph 15).

Memorandum by the Institute of Civil Protection and Emergency Management (ICPEM) (ISS 6)

- The Institute feels that greater priority should be given to the setting up of Computer Emergency Response Teams (CERTs) and the cybercrime centre (paragraph 16).
- The solidarity clause in the Lisbon Treat introduces a legal obligation on the EU and its member States to assist each other when a Member State is the object of a terrorist attack or a natural or man-made disaster. The Institute queries as to who has primacy on the disposition of resources in such cases and, in addition to security experts being deployed to EU delegations, there is an opportunity for civil protection expertise to be similarly deployed (paragraph 18 & 19).
- In relation to the development of risk assessment and the mapping of threats, together with the need for situational awareness, issues of focus, trust, transparency and credibility, together with linguistic, cultural and lack of common/integrated technology platforms within a pan-27 member organisation could conspire to render the process almost unworkable (paragraphs 20 & 21).
- In relation to the development of a European Emergency Response Capacity based on pre-committed assets, the Institute points out that providing mutual aid within national borders is often a challenging issue. This multiplies when trying to coordinate external aid (paragraphs 22 & 23).
- Many of the proposals are focused towards reactive measures with little or no focus on proactive measures to reduce risk (paragraph 24).
- There is an absence of a clear commitment on the level of funding and on-going support for funding the initiatives (paragraph 25).

General Comments

The Institute submits that there are two serious omissions in both documents, viz:

- No mention is made of the role of the military (paragraph 27).
- Although the importance of information exchange is referred to on a number of occasions, neither document deals adequately with the role of intelligence. And yet, it is difficult to see how objectives 1, 2 and 3 can be achieved without appropriate intelligence exchange (paragraph 28).

The Sub-Committee might wish to consider a third document, 'Towards a stronger European disaster response: the role of civil protection and humanitarian assistance', issued one month before the second document to be reviewed. The Institute queries whether the various Directorates-General within the EC are working in unison (paragraph 30).

The two documents under review offer a basis for progress provided the whole process is headed by operationally experienced officials rather than people who are politically driven (paragraph 31).

Introduction

1. This evidence is submitted in response to the above Sub-Committee's call for evidence to assist its inquiry into the EU Internal Security Strategy. The inquiry will focus on two documents:

- the Internal Security Strategy for the European Union (Council Doc. 7120/10, 8 March 2010), hereafter referred to in places as the First Document; and

- the Communication from the Commission: The EU Internal Security Strategy in Action: Five steps towards a more secure Europe (COM(2010)673 final, 22 November 2010), hereafter referred to in places as the Second Document.

The Internal Security Strategy for the European Union

2. This document provides a framework for developing an EU-wide Internal Security Strategy. In the recently published UK National Security Strategy[39] it clearly states what constitutes a 'strategy', viz:

> "...any strategy, must be a combination of ends (what we are seeking to achieve), ways (the ways by which we seek to achieve those ends) and means (the resources we can devote to achieving those ends) ..."[40]

In its current form, it is the Institute's view that the European document does not meet those criteria. Nevertheless, it is a helpful document in that it sets out the common threats and hazards that currently pose a risk to people and institutions within the European Union. Further it sets out the need for cooperation and coordination between the various internal state organisations that respond to those threats and hazards on a national, rather than an international basis. These organisations include law-enforcement and border management authorities, judicial authorities, civil protection agencies and also "political, economic, financial, social and private sectors, including non-governmental organisations."[41] However, notable omissions are the roles played by national security and intelligence agencies and the military (see paragraph 27 and 28 below). In reference to border controls, the strategy seems to have been drafted in the assumption that all EU members are part of the Schengen area.

3. There is a tendency throughout the document to group law enforcement activities, i.e. those associated with counter terrorist and organised crime, with societal education and civil protection.[42] In most cases, the Institute would suggest they are mutually exclusive for very good strategic, tactical and operational reasons, e.g. different skill sets, information requirements, drivers of national legislation, equipment, locations, etc.

4. It follows that many non-law enforcement agencies are likely to exclude themselves from this holistic view on the basis that it involves wider 'security' issues with 'civil protection' providing the all-encompassing safety net at the back end, following the common threats and main challenges for EU internal security. Indeed, the Institute would suggest that what the Commission appear to have done is to take an internal security strategy and merely bolt onto the end of certain parts of it, civil protection. Therefore, although the document acknowledges that "civil protection systems represent an essential element of any modern and advanced security system",[43] the Institute takes the view that the document loses something by not acknowledging, in its title, the link between the two terms and the interdependency of the two functions. Developing a collective understanding that an "Internal Security and Safety Strategy for the EU" might have been more inclusive in accepting that the two span a continuum and that everyone can benefit from the economies

[39] UK Cabinet Office (2010). A Strong Britain in an Age of Uncertainty: The National Security Strategy. London: The Stationary Office.
[40] Ibid, p.10, para.0.14.
[41] Council of the European Union (2010). Draft Internal Security Strategy for the European Union "Towards a European Security Model". Council Doc. 7120/10 dated 8 March 2010, p.10.
[42] Ibid, pp. 2, 7, 8 & 15.
[43] Ibid, p.6.

of scale in most of the key areas highlighted in the 'Response to These Challenges'[44] and the 'Strategic Guidelines'[45] sections.

5. With that in mind, it is the Institute's submission that some of the observations and suggestions in the document apply equally to the civil protection community. Two examples are given here:

a) Training. The paper points out that "a strategic approach to professional training in Europe" is an essential objective in "enabling European law-enforcement training to take a major step forward and become a powerful vehicle for promoting a shared culture amongst European law-enforcement bodies and facilitating transnational cooperation."[46] But why does this only apply to law-enforcement if the document is to provide a holistic approach to all threats? Such training should include those involved in other forms of civil protection and crisis management.

b) Operational cooperation. Again the document focuses on "law-enforcement and border management authorities, including the control and protection of external borders, and when appropriate judicial cooperation in criminal matters".[47] The Institute submits that operational cooperation between civil protection agencies is equally important.

6. Additionally, the document refers to matters which are, in the Institute's submission, not of an appropriate level for a pan EU internal security strategy. For instance, reference is made to road traffic accidents. As the note rightly points out, road traffic accidents do "take the lives of tens of thousands of European citizens ever year",[48] but these are not mass-fatality events, nor do they have a significant economic impact in the short term. Unless, the road traffic accident occurs on an international border or involves multiple Member States by reason of the different nationalities of those involved, it is of little interest to Member States, other than the state in which it occurs. Later in the document, mention is also made, in relation to information sharing and the facilitation of joint investigations and operations of "missing persons ... stolen vehicles and visas which have been issued or refused."[49]

7. The document identifies the importance of planning, programming and handling the consequences of any crisis and mentions the fact that the EU Community Civil Protection Mechanism "coordinates the response of Member States to natural and man-made disasters."[50] This was tested recently during the field exercise 'Orion'. This was, as far as the Institute is aware, the largest and most generously funded exercise that the EU has held. It involved field scenarios, 22 in all, in Liverpool and Portsmouth and Gold level command posts working off those scenarios in Hampshire, Merseyside, Hertfordshire and Lincolnshire, with a co-ordinating control at the Fire Service College and participants acting at national level at the Fire and Rescue Service (FRS) national coordination centre (FRSNCC) in West

44 Ibid, pp. 7-8.
45 Ibid, pp. 10-17.
46 Ibid, p.16.
47 Ibid, p.13.
48 Ibid, p.6.
49 Ibid, p.8.
50 Ibid, p.8.

Yorkshire. In addition, civil servants simulated the Department for Communities and Local Government (DCLG) emergency room and Cabinet Office Briefing Room (COBR).

8. The lessons identified included issues such as having a common language to describe levels of command and control at local, regional, national and EU level. It demonstrated that there are significant differences in the way that assistance will be received in advanced EU Member States as opposed to third party nations, where there has currently been greater experience. When providing assistance to areas devastated by earthquakes, such as Pakistan (2005) and Haiti (2010), the mechanism works well. However, when coping with developed structures and heightened sensitivities found in Member States, the structure and operating assumptions are severely tested, mainly due to the frictions that occur with established laws, constitutions, command structures and organisational cultures. This cannot be ignored if the Five Strategic Objectives mentioned in the Second Document are to be achieved.[51]

9. However, when the document refers to the fact that evaluation mechanisms have been developed to assess the effectiveness of the EC's actions, it merely quotes as examples, "peer-to-peer evaluation exercises in the field of terrorism and organised crime" as "having contributed to the improvement of mutual trust."[52] Again, there is the suggestion here that natural and man-made disasters have been added on to an existing security strategy developed primarily with law-enforcement activities in mind.

The EU Internal Security Strategy in Action: Five steps towards a more secure Europe.

10. The document is more focused on the aspiration of what is to be achieved, that is, "common efforts to deliver responses to the security challenges of our time … to strengthening and developing the European model of a social market economy put forward in the Europe 2020 strategy."[53]

11. It also sets out the vision for achieving these common efforts:

a) "Solidarity must characterise our approach to crisis management."[54] This centres on the concept of mutual aid. The Institute points out, however, that there are enormous challenges in the command, control and coordination of multi-national assets with different standards of training, competency and equipment, as well as the challenges of language, concept of operations and standard operating procedures.

b) "Our counter terrorism policies should be proportionate to the scale of the challenges and focus on preventing future attacks."[55] The Institute suggests this may cause some concern, particularly in the area of harmonisation of national counter terrorism legislation. The UK has amongst some of the most draconian CT legislation in Europe. Attempts to either 'water down'

[51] European Commission (2010). Communication from the Commission: The EU Internal Security Strategy in Action: Five steps towards a more secure Europe (COM(2010)673 final, 22 November 2010, pp. 4-15.
[52] Council of the European Union, op. cit. 3, p.8.
[53] European Commission, op. cit. 13, p.3.
[54] Ibid, p.3.
[55] Ibid, p.3.

UK legislation or bring legislation in other EU countries up to the level of the UK may be a 'bridge too far'.

c) "Where efficient law enforcement in the EU is facilitated through information exchange, we must also protect the privacy of individuals and their fundamental right of protection of personal data."[56] Clearly, the Institute suggests, this highlights the dilemma of 'Security v Privacy'. It is a challenging area and there are no easy solutions. There is likely to be resistance to an EU database, should one be suggested. Also the transfer of personal data between different law enforcement agencies in EU member countries is likely to be controversial.

12. The five strategic objectives and specific actions for 2011-2014 are both informative and helpful. They provide a series of steps to be achieved to help ensure the security of the population within the EU. However, the Institute wishes to make a number of observations in relation to these five strategic objectives.

Objective 1: Disrupt international crime networks

13. Under Action 1, "the Commission will propose in 2011 EU legislation on the collection of Passenger Name Records (PNR) of passengers on flights entering or leaving the territory of the EU."[57] The Institute suggests that, as this only refers to passengers entering or leaving the EU, travelling criminals and/or terrorists from within the EU, who may or may not be EU citizens, would be unaffected by this proposed legislation when they travel from one part of the EU to another, without passing through an external border. Therefore, the Institute submits that PNR should also include travel between EU countries.

Objective 2: Prevent terrorism and address radicalisation and recruitment

14. In the introduction, it states that "threats now come from both organised terrorists and from so-called 'lone wolves', who may have developed their radical beliefs on the basis of extremist propaganda and found training materials on the internet."[58] The Institute suggests that the implication from this statement is that this objective is directed at Al Qaeda motivated or inspired terrorism. This neglects to address the threat from domestic terrorism, such as that experienced in Greece, Northern Ireland and Spain. In addition, the threat of violence from 'single-issue' extremists, e.g. animal rights, is not addressed.

15. Under Action 3, it states that "the Commission considers that as a first step towards further action, it would be useful to explores the establishment of a standing committee on land transport security, chaired by the Commission and involving experts in transport and in law enforcement, and a forum for exchanging views with public and private stakeholders, taking account of previous experience in aviation and maritime transport security."[59] The Institute feels that this is an innovative and welcome initiative to provide a common view of the terrorist threats to the rail infrastructure but it does not go far enough. The Institute's view is that whilst it focuses on passenger and cargo movement by rail and air, it does not appear to consider the movement of freight by road and barge, e.g. container/freight barge traffic on the River Rhine in Germany and other large European rivers. However, by

[56] Ibid, p.3.
[57] Ibid, p.5.
[58] Ibid, p.7.
[59] Ibid, p.9.

restricting it to transport, there would appear to be a gap in the area of 'crowded spaces' Terrorists attack trains because people travel on trains. They also attack hotels, night clubs, shopping malls, etc., because people tend to frequent such places in large numbers. Therefore, rather than confine this initiative to transport, the Institute feels it should be widened to include 'crowded places'.

Objective 3: Raise levels of security for citizens and businesses in cyberspace

16. Under Action 1 it is claimed that "by 2013, the EU will establish, within existing structures, a cybercrime centre, through which Member States and EU institutions will be able to build operational and analytical capacity for investigations and cooperation with international partners ..... and interface with a network of national/governmental Computer Emergency Response Teams (CERTs)" and such a centre "should become the focal point in Europe's fight against cybercrime."[60] Under Action 3, it states that "every Member State, and the EU institutions themselves should have, by 2012, a well-functioning CERT" and that, once they are set up, it is important that "all CERTs and law enforcement authorities cooperate in prevention and response."[61] The Institute sees this as a priority area that needs to be addressed. Although Member States should have a "well-functioning CERT by 2012",[62] the cybercrime centre will not be established until 2013. Given the ease with which hackers have recently closed down Visa, Mastercard and Amazon for periods of time, the Institute believes that this is a priority area.

Objective 4: Strengthen security through border management

17. The Institute has no observations to make in respect of the actions to be taken in relation to this objective.

Objective 5: Increase Europe's resilience to crises and disasters

18. Under Action 1 it is stated that "the solidarity clause in the Lisbon Treaty introduces a legal obligation on the EU and its Member States to assist each other when a member State is the object of a terrorist attack or a natural or man-made disaster" and that "through the implementation of this clause the EU aims to be better organised and more efficient in managing crises, in terms of both prevention and response."[63] The Institute believes that a careful analysis needs to be conducted by any Member State as to the impact of this on national operational discretion. With that obligation comes the responsibility to be competent to manage the response effectively The Institute believes that there is an opportunity to mirror the security sector here by looking to integrate further action and expertise using the skills and knowledge of Members States in the area of civil protection. The European External Action Service suggests that "security expertise should be deployed to EU Delegations, particularly in priority countries, including ... liaison officers".[64] However, the Institute sees an opportunity here for civil protection expertise to also be deployed to EU Delegations. As with the liaison officers providing security expertise, "appropriate responsibilities and functions for these experts could be defined by the Commission and the European External Action Service".[65]

[60] Ibid, p.9.
[61] Ibid, p.10.
[62] Ibid, p.10.
[63] Ibid, p.13.
[64] Ibid, p.3.
[65] Ibid, p.3.

19. Given this "legal obligation", the Institute poses a problem that could arise unless clear lines of authority and decision-making are established. In the event of a major crisis involving all three emergency services, in the UK police resources are likely to be managed by the Police National Information Coordination Centre (PNICC), fire and rescue resources by the Fire and Rescue Service national Coordination Centre (FRSNCC), and the medical services by the Department of Health, and above all of these will be the Cabinet Office Briefing Room (COBR). If urban search and rescue (USAR) resources are required in the EU mainland, but decisions have already been taken by COBR and FRSNCC as to their disposition, which set of priorities will take precedence? Likewise, in the case of a tidal surge which affects the UK east coast at the same time as the Netherlands, who has the final say as to where the UK's High Volume Pump (HVP) resources are to be deployed?

20. Under Action 2, the document mentions the development of risk assessment and mapping guidelines and threat assessment and states that, by 2014, the EU should have established "a coherent risk management policy linking threat and risk assessments to decision-making."[66] The Institute has identified a problem in relation to this and that is one of transparency regarding the threat component. For sound reasons, the detail of the threat assessment in the UK is not as visible and well understood as the non-terrorist components of weather, industrial action, transport mishap, power outage, etc. In the wider EU arena, this issue would be magnified and the effects compounded. In a pan-27 member organisation, issues of focus, trust, transparency and credibility could all conspire to render the process almost unworkable. Solutions could be proposed but at the cost of further erosion of the autonomy of individual Member States. Also, Member States would inevitably focus most strongly on the hazards most relevant to themselves. Investigations during the ongoing EU-funded project ERGO (Evacuation Responsiveness by Government Organisations) being conducted by the Aston Crisis Centre (a part of Aston University in the UK) demonstrate clearly that, despite an ostensible "all-hazards approach", most jurisdictions focus very strongly on the hazard immediately at hand, e.g. Hamburg, Germany, on flooding; Iceland on volcanic activity and glacial flooding; the UK on terrorism. This is understandable and rational, but casts doubt on the achievability, or indeed the sense or value, of a pan-EU consolidated threat and risk assessment.

21. Action 3 relates to situation awareness.[67] Much effort is currently being expended in an attempt to ease the task of building and maintaining situation awareness during a crisis. There is also much debate about the decision-making processes that this supports. How much information is "enough" to base critical decisions on? Do all decision-makers share the same picture of the events that are unfolding as the crisis progresses? Do decision-makers in each Member State perceive the hazards and threats in the same way? Linguistic, cultural and common/integrated technology platforms have challenged the EU for some time. The EU has already funded a number of projects in this area with little or no effective solutions forthcoming.[68] The Institute suggests that there is a need to recognise the likely sensitivity of sharing information across Member States and apply realistic classifications. Open systems often work better and provide more reliability and are more appropriate within the operational environment. Secure systems would need to share risk register

[66] Ibid, p.14.
[67] Ibid, p.14.
[68] For example, a part of Cranfield University based in the UK Defence Academy was involved in a four-year EU project to prove the benefits of integrating Europe's diverse and separate emergency response systems, called OASIS (**O**pen **A**dvanced **S**ystems for D**is**aster and Emergency Management). The project was completed in October 2008 with very little noticeable difference since then.

information, etc.. One centrally funded and properly equipped EU 'situational awareness centre' fed by existing domestic Member State components could be effective – this could interlink with existing EU security/intelligence sharing structures and systems. Law enforcement agencies must recognise that this can be done without compromising security.

22. Action 4 proposes "the development of a European Emergency Response Capacity based on pre-committed member States' assets on-call for EU operations and pre-agreed contingency plans" and goes on to suggest that "efficiency and cost-effectiveness should be improved through shared logistics, and simpler and stronger arrangements for pooling and co-financing transport assets" before stating that "legislative proposals will be tabled in 2011 to implement the key proposals."[69]

23. The Institute points out that providing mutual aid, or 'solidarity' is a challenging issue within a national border, let alone trying to coordinate external aid. So, there has to be a clear willingness for a Member State to accept assistance. This may sound obvious, but some Member States may suffer from misplaced pride as to their ability to cope with any challenge. In addition, there needs to be a clear command and control framework in place, which is accepted by all Member States and incorporated into standard operating procedures of responders in all Member States in order that they can work effectively together without delay, and which has been tested and exercised before resources have to be deployed in earnest. The current draft international standard, ISO 22320 (Societal security – Emergency management – Requirements for command and control) could form the basis for this framework. Therefore, the Institute sees this as an opportunity to develop and promote joint training and cross-border exercises. Uncoordinated and unrehearsed support may make the role of the responders more difficult and, instead of assisting the response and recovery efforts, may actually hinder those efforts.

24. In conclusion in relation to Objective 5, the Institute feels that the proposals are all focused towards reactive measures with little or no focus on proactive measures to reduce risk. Indeed, in the first document, reference is made to the phases of a crisis as being prevention, response and recovery.[70] Thus both mitigation and preparedness, two extremely important phases of the crisis cycle have been omitted.

Implementing the Strategy

25. In terms of implementing the strategy, the document states that "EU funding that might be necessary for the period 2011-2013 will be made available within the current ceilings of the multiannual financial framework". It goes on to say that "for the period post-2013, internal funding will be examined in the context of a Commission-wide debate on all proposals made for that period" before concluding that "as part of that debate, the Commission will consider the feasibility, of setting up an Internal Security Fund."[71] The Institute is of the view that the absence of a clear commitment on the level of funding and on-going support for funding these important initiatives may lead to a lack of commitment, both from the EU institutions and the Member States.

26. In its concluding comments, the document sets out the main challenge to the successful implementation of the strategy when it states that "only by joining forces and working together to implement this strategy can Member States, EU institutions, bodies and

[69] European Commission, op. cit. 13, p.15.
[70] Council of European Union, op. cit. 3, p.14.
[71] European Commission, op. cit. 13, p.15.

agencies provide a truly coordinated European response to the security threats of our time."[72] The Institute feels that a failure to deliver the key components within the strategy will lead to a Europe that is less safe and more vulnerable to terrorists, criminals, cyber-attacks and disasters. Whilst this document may not be "All things to All men",[73] it is a starting point along a long road.

Concluding remarks on both documents under review

27. The Institute submits that there are two serious omissions from the two documents. The first is that neither document refers to the role of the military. At a workshop organised by the Directorate-General for Humanitarian Aid and Civil Protection held in July 2010, it was clear that there was a wide divergence of opinion between Member States on the use of the military. As a result, the Commission would appear to have placed the subject in "the too difficult tray" (but see paragraph 30 below). And yet, the reality is that most, if not all, EU countries will, in response to a natural or man-made disaster, deploy the military when they can add value to the response by the civil authorities. In addition, in a number of EU Member States, the military are part of the response mechanism to counter terrorism.

28. The other serious omission is the failure of either document to deal with the role of intelligence. The need to exchange information is mentioned on a number of occasions but no attempt has been made to explain the difference between information and intelligence. And yet, the Third of the Strategic Guidelines in the First Document highlights the importance of "prevention and anticipation" suggesting what is needed is "a proactive, intelligence-led approach".[74] However, the Fourth of the Strategic Guidelines in the First Document highlights the need to develop "a comprehensive model for information exchange."[75] No attempt is made to differentiate between 'intelligence' and 'information'. Neither is there any mention of the national security and intelligence agencies. Other than that which has just been mentioned, each of the documents makes only one passing reference to intelligence. In the First Document, it merely states that "we should ensure that Member States share intelligence in time to prevent crime and bring offenders to justice."[76] In the Second Document, in relation to Frontex, Europol and the European Asylum Support Office, it merely states that "by 2014, the Commission will develop minimum standards and best practices for interagency cooperation. These shall particularly be applied to joint risk analysis, joint investigations, joint operations and exchanging intelligence."[77] The sharing of intelligence between the different agencies in a single Member State is frequently difficult. The Institute believes, therefore, that the sharing of intelligence between the different agencies in 27 Member States has similarly been placed in "the too difficult tray" for neither document makes any attempt to suggest how this can be organised on an EU basis. And yet, it is difficult to see how the EC can achieve success, particularly in Objectives 1, 2 and 3 under the Five Strategic Objectives for Internal Security[78] without the timely sharing of appropriate intelligence.

29. In addition, whilst the European Security Strategy "recognises relationships with other partners, in particular the United States, are of fundamental importance in the fight

[72] Ibid, p.16.
[73] 1 Corinthians 9.22.
[74] Council of European Union, op. cit. 3, p.14.
[75] Ibid, p.13.
[76] Ibid, p.11.
[77] European Commission, op. cit. 13, p.13.
[78] Ibid, pp. 4-10.

against serious and organised crime and terrorism"[79] both documents are somewhat parochial in that although there is a reference of the need to link in with regional and international organisations,[80] no account seems to have been taken of such bodies as Interpol or the actions taken by NATO under its emergency planning function. As a result, the Institute submits that there would appear to be a danger of duplicating the services that are already supplied by existing organisations.

An additional document that possibly needs to be considered

30. Finally, the Institute wishes to point out that on 26 October 2010, less than one month before the Second Document was issued, the European Commission issued another Communication to the European Parliament and Council entitled 'Towards a stronger European disaster response: the role of civil protection and humanitarian assistance'. COM(2010) 600 final. What this document does is to effectively put some 'meat' on the 'skeleton' that is provided by Objective 5 of the Second Document[81] even to the extent that it claims arrangements have "been developed to facilitate the deployment of Member States' military assets when these are required as part of an overall EU disaster response."[82] However, it makes no reference to the First Document under review by the Sub-Committee, supporting the Institute's view that civil protection has been tagged onto an existing security strategy, and only makes passing reference to the Second Document in claiming that "the proposals for improving response capacity would constitute a major contribution" to it because "increasing Europe's resilience towards disasters is one of the strategic objectives."[83] Similarly, the Second Document makes only a passing reference to the document issued on 26 October when it refers to the establishment of a European Emergency Response Capacity.[84] The fact that the 'meat' was published before the 'skeleton' leads one to ask – how joined up will the various Directorates-General within the European Commission be in achieving what is set out in the two Documents appertaining to the Internal Security Strategy for the European Union?

Conclusion

31. Having said that, it is the Institute's submission that the two documents under review by the Sub-Committee on Home Affairs of the House of Lords Select Committee on the European Union, offer a basis for progress provided the whole process is headed by operationally experienced officials rather than people who are politically driven. Experience of large-scale exercises in the Netherlands (Floodex) and the UK (Orion) demonstrate the benefits which may be derived from better collaboration, shared situation awareness and operational cooperation. However, operational responders, as practically orientated organisations and individuals, do not function well in bureaucratic and over-officious environments; so simplicity and transparency must be the order of the day.

21 December 2010

---

[79] Ibid, p. 3. The 'European Security Strategy: A Secure Europe in a Better World' was adopted in 2003 and reviewed in 2008.
[80] European Commission, op. cit. 13, p.3.
[81] Ibid, pp. 13-15.
[82] European Commission (2010). Communication from the Commission to the European Parliament and Council entitled 'Towards a stronger European disaster response: the role of civil protection and humanitarian assistance'. COM(2010) 600 final, dated 22 October 2010, p.5. Also see p.10, para. 4.6 of the same document.
[83] Ibid, p.3.
[84] European Commission, op. cit. 13, footnote on p.15.

Memorandum by JANET UK (ISS 4)

1. This is JANET(UK)'s submission to the inquiry into the EU Internal Security Strategy[85] by the Home Affairs Sub-Committee of the House of Lords Select Committee on the European Union. JANET(UK)[86] is the operator of JANET, the UK's National Research and Education Network, which connects universities, colleges, research organisations and regional schools networks to each other, to peer research networks in other countries and to the public Internet. Our evidence therefore relates only to Objective 3 of the Strategy – Raise Levels of Security for Citizens and Businesses in Cyberspace – and in particular to pages 9 and 10 of the Commission Communication "ISS in Action" (COM(2010) 673).[87] JANET(UK) has operated a Computer Security Incident Response Team (CSIRT)[88] for its network and customers since 1993 and has participated in CSIRT cooperation activities in the UK, Europe and worldwide, including operating the EuroCERT pilot from 1997 to 1999.

2. In the area of **operational cooperation** we welcome the recognition in Action 3 of the important role of cooperating CSIRTs in dealing effectively with security incidents and promoting good preventive practice. Since many security incidents involve more than one country we strongly support the recommendation to increase the proportion of the European Internet that is covered by a CSIRT by encouraging the creation of at least a national CSIRT in each Member State and a CSIRT for the European Institutions. It is important that such CSIRTs are brought into existing trusted collaboration networks such as the European Government CERTs group,[89] TERENA's CSIRT Task Force[90] and the global Forum of Incident Response and Security Teams (FIRST).[91]

3. Since ENISA has provided, and continues to provide, an important facilitating role by gathering and promoting best practice in the field of Network and Information Security we welcome the proposal in Action 1 to provide a complementary body, working with ENISA, to gather and promote good practice in dealing with cybercrime. However we doubt that a direct operational role for such a body would be helpful since it would at best add an additional layer of organisational complexity and at worst disrupt existing bi- and multi-lateral working relationships between national cybercrime centres. The new body's role, like that of ENISA and the EISAS discussed below, should be to ensure – by developing, documenting and disseminating best practice – that relationships between those centres exist and work effectively, not to replace them.

4. On **prevention and anticipation**, we welcome the focus in Action 2 on dealing with criminally illegal material at source rather than, as has been suggested elsewhere, attempting to create blocks that are likely to be ineffective at the technical level and do

[85] http://www.parliament.uk/business/committees/committees-a-z/lords-select/eu-home-affairs-sub-committee-f-/news/lords-committee-to-investigate-the-eu-internal-security-strategy/
[86] http://www.ja.net/
[87] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0673:FIN:EN:PDF
[88] http://www.ja.net/services/csirt/
[89] http://www.egc-group.org/
[90] http://www.terena.org/activities/tf-csirt/
[91] http://www.first.org/

little either to address the crime or to help its victims. However processes for requiring material to be removed from Internet hosts must have a clear definition of what material is covered and effective and trusted safeguards (as provided, for example, by sections 3 & 4 of the *Terrorism Act 2006*[92] and the Internet Watch Foundation's[93] handling of indecent images of children) otherwise there is a risk, as identified by the Law Commission in 2002 for defamation law,[94] of creating mechanisms that can be used to censor legitimate comment and criticism.

5. On Action 3's proposal to create a European Information Sharing and Alert System (EISAS) we note and support the conclusion of ENISA's 2007 report[95] that the most effective role for the EU is as a facilitator for national Information Sharing and Alert Systems (ISAS) – such as the UK's GetSafeOnline[96] – rather than itself attempting to run an ISAS. This role would provide a clearing house to analyse and promote good practice in running national ISAS and a facilitator of discussions between those national Systems. Provided it is this facilitating role that is intended, we consider that the plan to work with ENISA to establish an operational service by 2013 should be achievable.

December 2010

92 http://www.legislation.gov.uk/ukpga/2006/11/section/3
93 http://www.iwf.org.uk/
94 http://www.lawcom.gov.uk/docs/defamation2.pdf para 1.12
95 http://www.enisa.europa.eu/act/cert/other-work/files/EISAS_finalreport.pdf
96 http://www.getsafeonline.org/

Memorandum by Professor Valsamis Mitsilegas (ISS)

1. Thank you for the invitation to submit written evidence for the purposes of the Committee's inquiry into the EU Internal Security Strategy. This is a timely inquiry, as the recent proposals for the development of a strategy for internal security at EU level have followed the entry into force of the Lisbon Treaty, which has enhanced significantly the Union's institutional capacity to emerge as an actor in the field. On the basis of both the Council (doc. 7120/10) and the Commission (doc. (2010) 673) approaches to internal security, I will attempt to highlight the key strands of the envisaged EU internal security strategy and assess their implications for European citizens in the light of the development of the Union as a security provider.

A wide range of objectives and tools

2. The Commission has identified five strategic objectives for EU internal security: disrupting international crime networks; preventing terrorism and addressing radicalisation and recruitment; raising levels of security in cyberspace; strengthening security through border management; and increasing resilience to crises and disasters. This is a departure from the Council's approach of adopting more concrete strategic guidelines for action. Some of the objectives set out by the Commission are more focused (combating crime and terrorism) than others (security in cyberspace or via border management). The breadth of certain objectives also creates potential overlaps between objectives (for example there is a potential overlap between combating crime and terrorism and security in cyberspace; there is also a potential overlap between combating crime and terrorism and the aim of achieving security via border management). The Commission's list contains a mix of security objectives (e.g. combating crime) and *means* of achieving security (security via border management).

3. The breadth of the internal security objectives set out by the Commission at times sits at odds with the Union's competence to legislate as conferred to it in the Lisbon Treaty. The limits of the Union's powers to act may explain why, on a number of occasions, concrete measures envisaged to achieve EU internal security objectives are 'soft' or non-legislative (examples include measures to prevent radicalisation, measures to combat cyber crime and crisis management measures). Softer measures are coupled with proposals for 'hard' law which largely develop existing EU legislation (in particular legislation on money laundering and confiscation). A striking exception in this context involves measures to combat corruption. The Commission envisages tabling merely a proposal on how to monitor and assist Member States' anti-corruption efforts, notwithstanding the fact that the EU legal framework on criminalising corruption (in particular corruption of public officials) is quite dated and stems from 'old' third pillar instruments which still have limited effect.

The intensification of surveillance

4. A key strategic guideline of the EU internal security strategy is according to the Council prevention and anticipation: a 'proactive, intelligence-led approach'. The focus on prevention dictates the adoption of a series of measures (such as legislation on the transfer of Passenger Name Records (PNR data) to police authorities) which entail essentially the intensification of State surveillance and the continuous monitoring of every day life. This intensification of surveillance is particularly evident in proposals aiming at enhancing the monitoring of movement of persons, goods and capital. Such proposals can be found throughout the

Commission's Internal Security Strategy. The Commission envisages: proposing legislation on the collection of PNR data on flights entering or leaving the EU (under the objective of combating crime); developing an EU policy for extracting and analysing financial messaging data (under the objective of preventing terrorism); developing policies to protect transport, working to 'ensure public acceptance by seeking an ever better balance between the highest possible level of security and travel comfort, cost control, and the protection of privacy and health' (p.8, under the same counter-terrorism objective). The emphasis on the surveillance of movement is also evident in the fact that strengthening security through border management has been elevated by the Commission to a separate, self-standing internal security objective, with concrete proposals including the development of a European Border Surveillance System (EUROSUR).

5. If adopted in their entirety, these proposals will lead to the establishment of wide-ranging surveillance mechanisms at EU level. Surveillance will be generalised: rather than focusing on specific incidents or specific individuals, large-scale collection and analysis of every day personal information (such as passenger records or bank details) will be normalised. Surveillance will not be limited to third country nationals (who are already the target of information databases such as EURODAC and the Visa Information System), but will be potentially extended to EU citizens as well (via the development of PNR transfers and an EU entry-exit system based on registered 'trusted travellers'. Continuous risk-assessment is key to this concept of internal security. However, as is evident, the impact on fundamental rights (in particular privacy and data protection) and citizenship rights may be far-reaching. Monitoring the movement of EU citizens via PNR data may also be in breach of EU free movement law, and is certainly at odds with the development of freedom in a European Union without internal frontiers. In the light of the potentially far-reaching consequences that an EU internal security model based on generalised surveillance may entail, it is submitted that in the development and scrutiny of future EU proposals in the field two main interrelated questions should be asked:

a. is the measure necessary, effective and proportionate?
And, if the answer is in the affirmative,
b: how can the measure in question be designed in order to comply fully with fundamental rights at EU level?

The EU as a global security actor- what place for European values?

6. The external dimension of internal security is a key strategic guideline for the Council, and is also central to the Commission's proposals for an EU Internal Security Strategy. However, EU attempts to emerge as a global security actor post 9/11 have been fraught with difficulties. The controversy surrounding the conclusion of counter-terrorism agreements between the EU and the US on the transfer of Passenger Name Records (PNR data) and on the transfer of financial records (under the so-called US 'TFTP'- Terrorist Finance Tracking Programme) is indicative of the complexities surrounding external relations in the field: EU external action has been repeatedly criticised (by actors including the expert EU data protection bodies and the European Parliament) for failing to uphold European fundamental rights standards in complying with US requirements. In the light of this controversy, it is noteworthy that the Commission is envisaging to adopt US approaches on PNR and TFTP in tabling proposals on *internal* Union law in the field. In view of the significant impact of the adoption of such measures on fundamental rights (in particular data protection and privacy) it is important that the necessity, efficiency and proportionality of these measures are fully explored.

7. In any case, the Lisbon Treaty makes clear that EU external action must take into account the values of the European Union. These are set out in Article 2 of the TEU and include the respect for fundamental rights and the rule of law. According to Article 3(1) TEU, the promotion of these values is a key aim of the Union. The role of the Union in promoting its values is further highlighted with regard to EU external action, with Article 3(5) TEU stating that 'in its relations with the wider world, the Union shall uphold and promote its values and interests and contribute to the protection of its citizens'. The centrality of the values of the Union when the Union acts at the global level is further confirmed by the specific Treaty provisions on external action. According to Article 21(1) TEU 'the Union's action on the international scene shall be guided by the principles which have inspired its own creation, development and enlargement, and which it seeks to advance in the wider world', which include: democracy, the rule of law, the universality and indivisibility of human rights and fundamental freedoms and respect for human dignity. It goes without saying that these provisions also apply to the development of the external dimension of the EU Internal Security Strategy.

Fundamental rights in the EU Internal Security Strategy

8. Respect for fundamental rights, the rule of law and privacy is recognised as a key principle of the European Security Model put forward by the Council. The Commission's Internal Security Strategy also stresses that the tools and actions for implementing it must be based on common values including the rule of law and respect for fundamental rights. The potential impact of measures adopted under the EU Internal Security Strategy on fundamental rights has been highlighted in detail above. The purpose of this section is to stress that, along with the central place fundamental rights occupy in the Union external action after the entry into force of the Lisbon Treaty, fundamental rights are now also even more at the heart of *internal* Union legal and policy developments. This is particularly the case in the light of the explicit introduction of the EU Charter of Fundamental Rights into the EU constitutional framework, and in the light of the forthcoming accession of the European Union in the European Convention on Human Rights. Any measure aimed at furthering the EU Internal Security Strategy must be fully compliant with fundamental rights as enshrined in the Union constitutional framework.

Inter-agency cooperation and operational action

9. A key element of the Council's response to the perceived security challenges facing the Union is the work of EU agencies, institutions and bodies in the field: these include Europol, Eurojust, Frontex, and the EU Counter-terrorism Coordinator. The work of EU bodies and agencies in the field of internal security is also highlighted by the Commission. The Commission strategy is two-prong: to propose the establishment of new structures in Member States or at EU level (see for instance calls for the establishment of Asset Recovery Offices, of an EU radicalisation-awareness network, of an EU cyber-crime centre, of EUROSUR and of a European Emergency Response Capacity); and to further develop existing agencies, in particular Frontex which is envisaged to develop intelligence capacities in the field of organised crime. Interagency cooperation is also prioritised throughout the document.

10. While some of these developments may provide added value in the EU Internal Security Strategy, there remains a considerable lack of clarity with regard to the mandate, functions and accountability of EU bodies working in the field of internal security. Some of these

bodies (such as the Counter-terrorism Co-ordinator) are not founded upon a clear legal basis. Other agencies (such as Frontex) have been established in accordance with detailed legislation, but in practice the extent of their operational capacity – and the division of powers between the EU and the national level- are not always clear. In this light, it is noteworthy that the Commission seems to envisage a clearer criminal intelligence role for Frontex, although this is an agency established under a Treaty legal basis dealing with immigration (and not criminal) law, and although such a development may in practice create an overlap with the work of other bodies in the field (such as Europol). It should be reminded here that, in its most recent Report on Frontex, the Committee stated that 'it would be an unacceptable enlargement of the mandate of Frontex for it to concern itself specifically with counter-terrorism or serious cross-border crime which is not directly linked to illegal immigration (*FRONTEX: the EU external borders agency,* 9th Report, session 2007-2008, HL Paper 60, para. 214).

The importance of parliamentary scrutiny

11. The lack of clarity as to the precise mandate of EU bodies in the field of internal security, the growing shift towards operational and interagency cooperation (including information exchange and the accountability gaps which arise from these developments (which are exacerbated by differences in the purpose and nature of EU bodies in the field of internal security) render the enhanced scrutiny of the work of these bodies by the European Parliament and national parliaments essential. The Lisbon Treaty provides the legal mechanism for such scrutiny as regards the work of Eurojust and Europol. It is submitted that both the European Parliament and national parliaments should assume a proactive role in scrutinising in detail the work of all EU bodies working in the field of internal security, by focusing in particular on the *operational action* of these bodies via the organisation of fact-finding missions. The European Parliament and national parliaments should also ensure that they participate actively in the *development of strategy* on internal security, a role which is largely attributed in the Lisbon Treaty to a new EU Internal Security Committee (COSI). While of immense value, scrutiny which is confined to the examination of EU legislative proposals and calling EU officials to give evidence may not provide the most effective way of parliamentary control over the development of measures implementing the EU Internal Security Strategy if not combined with scrutiny at the level of strategy and operations.

5 January 2011

Memorandum by Professor Wyn Rees (ISS 13)

Introduction

The Internal Security Strategy (ISS) and the Communication from the European Commission represent an attempt to draft a strategy and implement an action plan for the EU's area of internal security. It responds to pressure for a long-sought internal security counterpart to the European (external) Security Strategy (European Council (2003), 'A Secure Europe in a Better World', 12 December, Brussels). The EU has possessed competences in the domain of Justice and Home Affairs (JHA) since the 1993 Treaty on European Union (TEU) but these were weak and divided across the three pillars. Progress in internal security depended upon a complex process of inter-pillar coordination and it was not until the Treaty of Amsterdam (ToA) that major steps were taken to develop this area. The ToA brought to an end the purely intergovernmental nature of JHA by 'communitarising' the fields of asylum, border and immigration policy. Since then the Union has been developing a variety of instruments and agencies that enable it to be a more effective actor in internal security, with a major impetus arising from the post-9/11 threat from international terrorism. The Lisbon Treaty collapsed the separate pillar structure of the Union (thereby leaving the UK with the choice of whether to opt in to future measures) and has made possible the forging of an Internal Security Strategy.

The Contribution of the EU

The EU needs to convince its member states that it has a role to play in internal security. It has sought to make that case by demonstrating 'added value' in relation to security threats that have an explicit transnational dimension. It does this in a number of ways. First, by conducting analysis of the threats at a European level that draws on inputs from its member states. Second, by co-ordinating the responses of its member states through Europe-wide agencies. Third, by reaching out on behalf of its members to other international actors such as the US or the UN. An example of where the EU can add value is by identifying European level Critical Infrastructure, namely infrastructure which, if disrupted, would have serious consequences for two or more member countries.

The fact that the EU role in internal security policy has been growing is evidence that its members appreciate the contribution that it can make. In particular, the increasing number of EU actors and agencies with competences in internal security supports this contention. These include the European Police Office (Europol), the European Judicial Agency (Eurojust), the Police Chiefs Operational Task Force (PCOTF), Frontex, the European Police College (CEPOL) and the Critical Infrastructure Warning Information Network (CIWIN). The most significant recent addition is the Standing Committee on Operational Cooperation in Internal Security (COSI). It is hoped, within the expert community in Brussels, that COSI will play a central role in pulling the strands of internal security policy together and increasing its coherence.

Nevertheless, it is important to appreciate that there continue to be problems and limitations for the EU in this field. Internal security remains a subject over which member states maintain tight control and regard as a key aspect of their sovereignty. Operational powers to conduct arrests and prosecutions still reside with nationally based police and judicial agencies. The constraints imposed upon the EU are illustrated by the slow domestic patterns of implementation of European legislation, some of which has extended over years.

Both of the EU's Counter-terrorism Coordinators (CTC) have drawn attention to this problem. Similarly, member states have found ways to increase patterns of internal security cooperation outside the structures of the Union. The Group of 6, for example, consists of some of the larger members who prefer to share intelligence in an ad hoc forum.

Threats

The section of the ISS pertaining to threat perceptions is distinctly modest. It lists several important problems but it fails to prioritise between them. It would be true to say that the preoccupation with Islamist terrorism over the last decade has led to a neglect of other issues. The ISS attempts to re-assert that balance. It refocuses attention upon the challenge from international organised crime. This is also one of the five threats highlighted in its counterpart, the ESS. The ISS also lists some of the different facets of organised criminal activity: drug trafficking, human trafficking, arms smuggling, money-laundering and the sexual exploitation of women and children.

In both the ISS and Commission documents, particular attention is devoted to the vulnerabilities of borders. Pressure upon the EU's borders is seen to come from illegal migrants entering covertly into the Schengen space or from visitors overstaying visas that have expired. The ESS also identified illegal immigration as one of the foremost threats to the EU. Borders have become more porous to activities such as drug trafficking as organised crime has grown increasingly global in nature. The EU recognises the need to engage proactively with neighbouring countries to address internal security threats before they spill-over the Union's borders. It is no longer sufficient to believe that a common external border will keep out these problems.

The ISS acknowledges that the sorts of threats facing the Union are interlinked in nature and exhibit similar characteristics. These include the threat of violence, risks to the integrity of financial systems, the abuse of vulnerable citizens and the potential for large-scale fraud. For example, the internet can be misused both for the radicalisation of individuals for terrorism as well as for the conduct of cybercrime. Just as the threats are interlinked, so are the responses for dealing with these problems. Law enforcement and judicial instruments can be mobilised to address a range of different security challenges. For example, whilst the European Arrest Warrant (EAW) was originally conceived as a way to deal with international crime, it has proved to be highly effective in combating terrorism. Similarly, the efforts undertaken to protect European critical infrastructure against terrorist attack have spin-offs in promoting resilience in the face of natural disasters.

Both documents emphasise the risks associated with weak and failing states. Such countries act as potential incubators or sanctuaries for actors with malevolent intent, such as drug traffickers, terrorists or people traffickers. This has echoes once again of the ESS: a recognition that states with weak governance or security agencies of limited effectiveness may be a source of instability for all countries. Whilst the US has tended to treat these countries as threats, the EU has tended to offer assistance and expertise. The response from the Union has focused upon helping to build capacity in these countries so that they are capable of rectifying their weaknesses.

The Values of the EU

The principles of transparency and accountability are lauded in these documents. The Lisbon Treaty has created a single, more transparent legal framework and rationalised the complex and overlapping legal bases on which some of the EU's agencies were based. The Treaty has ended the intergovernmental nature of judicial cooperation in criminal matters and in police cooperation and extended majority voting and co-decision between the Council of Ministers and the European Parliament. The aim has been to enhance the role of the Parliament. This is seen as addressing some of the accountability deficits in this policy field, particularly through the involvement of its Committee on Civil Liberties, Justice and Home Affairs. In the past there was much criticism of the fact that the Council of Ministers took decisions on internal security matters behind closed doors. The involvement of the European Court of Justice (EJC), after a transition period of five years, also provides judicial oversight into an area of policy that impacts on the rights of citizens of the EU.

The EU has long been criticised for paying disproportionate attention to issues of security, at the expense of freedom for its citizens. The Stockholm Programme was an avowed attempt to find a better balance between improved security and the rights of European citizens. The experience of cooperation with the US in its War on Terror has been salutary: the EU found itself critical of American policies on the detention of 'non-combatants', extraordinary rendition and torture. This has encouraged the Union to place its commitment its citizens' freedoms and the Charter of Fundamental Rights at the centre of its security policies. For example, particular attention is paid to the issue of data protection – a topic that has been the cause of endless tensions with the United States. The EU still needs to move beyond declarations of intent and demonstrate that it is committed to upholding the interests if its individual citizens. If security of personal information is really to mean something, then it should extend to an individual's right to challenge the information and test its veracity.

Enhancing Practical Cooperation

Much of the Commission's 'Five Strategic Objectives for Internal Security' seek to build upon initiatives that already exist. One of the leading areas, predictably, is counter-terrorism. Since the formulation of the EU Counter-terrorism Strategy of 2005, the Union has initiated a range of measures and has mobilised an array of agencies and actors to carry these out. The Counter-terrorism Strategy contained four elements, all of which are identifiable in the Commission's document. In particular, the 'Prevent' strand is mirrored by Objective 2 on preventing terrorism. This focuses on the risks associated with the radicalisation of young people in European countries that can be drawn into violent activity through the influence of radical preachers and the internet. The Commission had already refined its thinking on this subject in an earlier communication, the 'Strategy for Combating Radicalisation and Recruitment to Terrorism' (Council of the European Union (2005) 14781/1/05 REV 1, 24 November 2005).

Similarly, Action 2 (under Objective 1) seeks to 'Cut off terrorists' access to funding' and this mirrors the 'Pursue' strand of the Counter-terrorism Strategy. This aimed to disrupt terrorist planning by cutting off their access to funding. Action 2 seeks to develop additional financial instruments to seize criminal assets and deny terrorists access to funding through cash and wire transfers. It tries to combat the laundering of money and the use of the charitable sector for the channelling of illegal funds. The Union draws for its inspiration upon the recommendations on Terrorism Funding of the Financial Action Task Force (FATF).

Moving beyond the area of counter-terrorism, another of the objectives in the Commission Communication is to improve the sharing of law enforcement information relating to organised crime. It has long been accepted that intelligence-led policing is the most effective instrument and yet the information shared with Europol is known to be patchy at best. In order to drive forward the concept of sharing information, the 'principle of availability' was introduced, generating the expectation that information would be shared where possible between member state police forces. Such information includes fingerprints, vehicle registration numbers and telephone details. This principle was embodied in the 2005 Treaty of Prum that was subsequently absorbed into the Union. The potential to exploit these opportunities has increased with the introduction of new data management systems and the enhancement of existing systems, such as the Schengen Information System II and the Visa Information System

Securing prosecutions, when criminal activity may have been carried out across several legal jurisdictions, demands the admissibility of evidence between national judicial systems as well as the willingness of courts to respect judicial decisions from neighbouring countries. The Commission document appreciates that multi-jurisdictional prosecutions require careful planning and coordination. For this purpose Eurojust was established in order to facilitate judicial cooperation between member states on complex cases. This is a central part of Objectives to disrupt criminal networks as well as build cross-border judicial capacity.

Integrated border management is another area given prominence by the Commission. At the heart of the Union's strategy is an effort to push out the common external border of the Schengen states. There are echoes here of the US Strategy for Homeland Security. Like the US, the EU has concluded that it must harness the efforts of its neighbours if it is to improve significantly the security of its borders. In relation to its central European members, the EU has learnt the lesson that it has most influence over other countries during the period that they are awaiting accession. The EU has linked overtly the implementation of its internal security requirements with the process of accession. Once states have actually joined the Union, then its power of persuasion diminishes markedly. The EU envisages a more significant role for Frontex in assisting members states and acting as a Europe-wide monitor of immigration-related issues. It is also concentrating its attention upon the screening of goods in transit – unsurprisingly, in the light of the recent scare with goods air freighted from Yemen.

The final issue is that of the security of cyberspace. The EU intends to create a Cybercrime Centre, that will draw upon expertise already built up within Europol. By acknowledging the importance of cybercrime, the Commission is responding to a groundswell of concern amongst its members. The UK's recent Strategic Defence and Security Review, for example, announced £800m in spending to address this challenge. It is evident that the EU needs to involve the private sector in this field. The risk to private enterprise is acute and much of the expertise for addressing the problem also resides there. Cybercrime is an area where the EU can act as an umbrella for all its members and can readily demonstrate its added value.

The Interdependence of Internal and External Security

Both the ISS and the Communication from the European Commission recognise that the Union's internal security has important external dimensions. This in itself is nothing new, it was acknowledged in the ESS and was the subject of an EU paper five years ago (See the Council of the European Union (2005) 'A Strategy for the External Dimension of JHA:

Global Freedom, Security and Justice', 14366/3/05, Brussels, 30 November). It is important to note that in the light of the Lisbon Treaty, this dimension is of increased significance due to the EU's enhanced ability to act. Yet the interface within the EU between external policies, such as the Common Foreign and Security Policy (CFSP) and the Common Security and Defence Policy (CSDP), on the one hand, and JLS on the other, is likely to remain problematic. The Lisbon Treaty preserves the intergovernmental nature of CFSP and CSDP and their separate decision-making methods. No mechanism has been found to form a bridge between internal and external security policies despite the inevitable synergies between them.

The part that third countries can play in the security of the Union is accepted in the two documents. Third countries can export security problems to the EU and therefore the Union has sought to embed internal security provisions in its external policies. For example, the EU places requirements in its trade agreements for countries to enter into counter terrorism cooperation. Similarly, in relation to illegal migration and asylum, the EU has taken steps to obtain cooperation on matters of self-interest from other countries. 'Readmission Agreements' have been imposed under which countries accept the return of their own failed asylum seekers or people who have transited across their territory. The EU has designated certain countries as safe from persecution, with the result that asylum seekers from these states are immediately determined to have an unfounded claim for sanctuary.

The EU has found that countries that have no prospect of joining the Union have been more resistant to its internal security provisions. European Neighbourhood Policy (ENP) countries, for example, have been offered trade agreements in return for supporting EU policies on migration and the Commission has approved measures to speed up the supply of visas for entry into Europe for nationals from compliant states. Yet many ENP countries have regarded Union policies as selfish and have been reluctant to participate. Likewise, the Russian Federation has been resistant to EU incentives, despite the fact that a Common Space of Freedom, Security and Justice was designated with Russia. The Kremlin has considered itself to be too important to have its policies moulded by Brussels.

By contrast, the US has been in a different relationship with the EU. Throughout the ISS and the Communication from the European Commission, it is striking the importance attached to cooperation with the US. In fact, since 9/11, America has been treated as the 28th member of the EU: it enjoys a presence in Europol and Eurojust and has signed a range of agreements with Brussels on internal security matters. Whilst the EU has reacted to a stream of American 'homeland security' initiatives, it is less clear what the Europeans have received in return from Washington. The US has been an important influence on the development of the EU's model of internal security. This may be about to be taken further. Wolfgang Schauble, as German Interior Minister, put forward the idea of a Euro-Atlantic area of internal security and this appears to have been taken up within the Commission as something worth pursuing.

The last aspect of the external dimension that deserves comment is the global perspective discussed in the ISS. This reflects an acknowledgement of the need to build an international architecture to make internal security cooperation effective on a global scale. The UN must be the focus of this effort as the premier international security organisation. For instance, the UN is home of the 2000 Convention Against Transnational Organised Crime. In 2001 it passed UN Security Council Resolution 1373 that declared terrorism to be a threat to international peace and security and created a Counter Terrorism Committee (CTC) to monitor the compliance of its members with existing UN Conventions. Whilst European

governments have been aware of the deficiencies of the UN they have nevertheless been attached to the principles of multilateralism and the rule of law and this has meant that they have regarded the UN as a vital part of an international campaign. Only in such a way will the norms contained within the EU's approach to internal security de diffused throughout the wider international community.

Conclusions

Is there a big, underlying vision in these two documents? The answer is no, there is little in the way of a grand objective in either the Internal Security Strategy or the Communication from the Commission. Rather, these documents seek to draw together a set of established policies into a coherent whole. They build on existing policies and make practical improvements. They marry up the internal security agenda - albeit imperfectly - with the external security agenda embodied in the ESS. It is part of the vision contained in the Stockholm Programme, that is designed to take forward internal security policy over the next five years. Better cooperation among law enforcement and judicial authorities are designed to address malevolent action, such as organised criminal activity and terrorist attacks, whilst close coordination amongst the emergency services of member states are designed to deal with natural disasters.

An 'EU Model of Security', whilst rather grand sounding, is nevertheless an apt description of what is presented in these documents. It is something in its relatively early stages of evolution (hence 'Towards a Security Model' in the title). It deserves the title of a 'model' because this policy area of internal security has seen rapid expansion over the last decade. Justice, Liberty and Security has been one of the most important growth areas in EU activity. Furthermore, it presents an example to surrounding countries because it is being adhered to by 27 individual countries. It is one of the EU's contributions to the creation of a European order. This fact has meant that the Union's neighbours have been forced to conform to its model if they wish to enjoy the benefits of interaction with the EU. The influence that the EU wields means that other countries are drawn into a web of cooperative relationships.

22 December 2010

Memorandum by Symantec (ISS 14)

Symantec welcomes the opportunity to provide input to the Committee's inquiry into the EU's approach to internal security. Both the EU's Internal Security Strategy and the recent Commission's Communication rightly highlight the cyber crime and cyber security risks and challenges being faced by European government, businesses and citizens. Given the ever changing online threat landscape and recent incidents of cyber attacks motivated by specific goals, there is clearly a need to protect the increasingly interconnected and interdependent ICT systems and networks that span across Europe and play a critical role in the ongoing stability and security of the EU as a whole.

Given Symantec's position as the world's leader in internet and information security the follow comments are provided on the overall scope of the ISS as well as the Communication's Communications key objectives which address risks in cyberspace and increasing European resilience to cyber related attacks, namely Objectives 3 and 5. In developing these comments Symantec will touch on the topics of interest outlined in the Committee's call for evidence including the role of information exchange and operational cooperation.

Overall scope of the EU Internal Security Strategy (ISS)

The publication of the Commission's Internal Security Strategy played a key role in not only identifying the cyber security risks facing the EU but more generally outlining a common policy approach and core set of principles. These have provided the foundations upon which the Commission's recent Communication for taking the ISS has been built. Taking a principle based approach will ensure the security strategy remains grounded in its core aims and objectives whilst also enabling a degree of flexibility which will be needed as the ISS itself remains constant while the threat landscape continues to evolve. This flexibility is particularly vital when addressing cyber security given the rate at which the online threat environment changes and matures. According to the latest Symantec Internet Security Threat Report in 2009 alone Symantec created 2,895,802 new malicious code signatures (to combat new malware including computer Trojans, worms and viruses)which represents 51 percent of all malicious code signatures ever created by Symantec. This shows the significant continued increase in the number of new global cyber threats.

The ISS's recognition of the current reality where criminals are taking advantage of "high speed communications" to conduct cyber crime is useful to highlight although this is perhaps not a new revelation to many Member States including the UK. It is important to remember however that different Member States will be at different stages of understanding and perhaps experience, of cyber related threats. The ISS can therefore play an important role in creating a common European understanding and recognition of the threat from cyber criminals who are increasingly organised, coordinated and targeted in their operations which continued to be focused on gaining data and information.

The ISS's acknowledgment that major EU ICT systems and networks are facing cyber security risks and that the strategy moving forward must also protect the security, integrity and available of key networks is particularly supported by Symantec. Particularly given that Member States critical national infrastructures are increasingly built upon and dependent on the continued availability and integrity of advanced ICT and as a result a cyber related security attack on these systems could lead to a disruption in the service provided or lack of

availability of ICT systems in not just one Member State but potentially across a whole region. Recent real life example of the power of cyber related attacks include the Estonia denial of service attack and more recently the Stuxnet attack which specifically targeted energy systems.

The Stuxnet incident provides a real life case study of how such an organised and structured cyber attack on critical infrastructure systems can succeed and how they could be used in the future. While details of the attack are still unfolding, with further analysis currently taking place, it is estimated that at least four zero day vulnerabilities attacks were involved in the incident which allowed attackers to steal confidential Supervisory Control and Data Acquisition (SCADA) design and usage documents for industrial systems such as those used by the energy sector. This is the first time that so many zero-day vulnerabilities have been exploited in one attack and indicates that the people needed to develop and execute such an attack were not amateurs. It is understood that once the attackers gained entry into the targeted systems a root kit was used to hide their presence while they targeted software within the systems used to control industrial assets and processes. The use of zero-day vulnerability, root kit, stolen digital certificates, and in-depth knowledge of SCADA software are all high-quality attack assets and points to an estimated group of at possibly up to ten people were involved in developing this specific, targeted and technically sophisticated cyber attack.

In the past this type of cyber attack focusing on critical national infrastructures were seen by many as theoretically a possibility. It is fair to say that most would have dismissed such an attack as simply a movie-plot scenario. Symantec believe the Stuxnet attack is clear evidence that such attacks are real and a possible threat and are no longer just a theory but a reality that European Member States need to prepare for. According to a recent survey by Symantec 53% of all firms surveyed suspected or were pretty sure that they had experience an attack on their systems waged with a specific goal in mind. The Stuxnet incident has shown that such targeted, organised threats do exist where external actors motivated possibly by organised crime, terrorism or even hostile nations, attempt to gain access to major ICT systems and networks.

The ISS is therefore correct to identify and highlight the security risks facing such systems and networks and how these security risks should be addressed particularly given the potential that such incidents could impact more than one Member State. This is of course also being addressed in the Commission's EP3R initiative which Symantec supports and is involved with given its focus on the protection and resilience of critical national infrastructures.

The ISS is also correct for recognising that unfortunately there will never be a situation when there is "zero risk" facing EU citizens. In the online threat environment there is no such thing as one hundred percent security as threats and risks continue to evolve at an increasingly fast rate. In light of this shifting threat landscape Symantec welcomed the ISS's recognition of the importance of developing trusted relationships between different organisations involved in addressing security challenges. Given the very nature of the online environment, there is no one entity, organisations, law enforcement agency or Member States that alone can be held responsible or address cyber crime or online security risks. The ISS's recognition that Member States government, law enforcement and industry are having a role to play where and when appropriate is supported by Symantec. Addressing online security risks is a joint responsibility that must be shared. For Symantec a partnership approach where governments, law enforcement along with industry and other key

stakeholders work together is key to identifying, addressing and combating cyber security threats.

The ISS and the Commission Communication both highlight the role information sharing and exchange can play and ensuring operational capabilities exist to address situations if and when they occur. The development of Public Private Partnerships is seen by Symantec as playing a key role in helping to develop relationships built on mutual trust which can facilitate the sharing of threat information and intelligence within a trusted community. However, it is suggested that a first step in building a successful partnership is having a common objective or concrete goal that the partnership is under agreement to addressing. The purpose, scope and mandate of the partnership should be clearly outlined at the beginning of the initiative. In addition given the involvement of many different parties in a public private partnership approach, particularly in an EU wide context, it is also important that the rules of engagement are clearly defined to ensure the parameters within which it will operate are clearly understood by all involved. These parameters should include relevant jurisdictional and legal requirements that could be involved such as around the sharing of information and data protection. The ISS provides a good foundation for such partnerships to be built upon and the Commission's Communication goes forward to outline the aims and objectives of such partnerships. In Symantec's view without taking the time to build and then maintain trust, within a partnership approach, the willingness of those involved to share information, experience or insights may be put at risk. Time should therefore be taken to consider which parties should be involved in the ISS's activities going forward and how "mutual trust" can best be developed between the identified partners with the understanding that this may not simply happen overnight but could take time to develop and build.

Looking ahead a key issue for Symantec is how the ISS will be taken forward. The Committee's inquiry asks for input on how the success of the ISS should be judged. This is a fair question which may not be easily answered at this stage. Perhaps an additional question that could be asked to is how the success of the ISS should be measured. For example how will it be determined, or perhaps judged, that the strategy and actions that will be taken forward has had any impact on the security of the EU. While in the case of a natural disaster this may be difficult to measure in an area such as cyber crime it is suggested that a benchmark study on the level of cyber crime across the EU today could be conducted now and then repeated at the end of the ISS's lifecycle in 2014. The results could then be compared to measure the impact of the EU strategy. An understanding of the measure by which success will be determined will however be key. For example metrics related to a specific problem or issue can be useful in determining where a particular project or initiative has resulted in a positive change or impact on a cyber security threat or risk perhaps to a particular sector or section of society.

Objective 3: Raise levels of security for citizens and businesses in cyberspace

Symantec also agrees with the Commission's Communication that encouraging greater cooperation between Member States to address security issues, particularly cyber security is important. Of course Symantec continues to also support the call for continued international cooperation given the fact that cyber security is a global problem that requires a global solution which needs international cooperation and collaboration.

While it is still not fully clear what role the proposed creation of an "EU Cybercrime Centre" would in fact play the proposal is welcomed in theory by Symantec at this time. Clearly the results of the proposed feasibility study are needed to move this idea forward.

On the basis of the results of this study further discussion and debate should be held on the overall aims and objectives of the centre and how the centre's work might be structured. These discussions should include input from industry as Symantec believes a public-private partnership approach should be included in the development of such a centre. Public private partnerships have been shown around the world to play a key tool to addressing cyber security issues and should be integral to the development of any cybercrime centre for Europe. A partnership approach can bring all those impacted by cyber security incidents together to share information and form a common vision of cyber threats as well as share knowledge and information needed to not only identify a threat but also take steps to proactively address such risks. Further discussion and insight would also be welcomed on how the work of an EU Cybercrime Centre could be coordinated or linked with the operations of other bodies currently already undertaking work in this area in the EU including ENISA, Europol and European Defence Agency (EDA).

The proposal to enable EU citizens to report cybercrime incidents and to have access to information on online safety is supported. A European wide reporting capability would be an important step forward, not only for citizens but also to build a clearer picture of the cybercrime landscape across all Member States. It will be important however that when this clear picture does emerge law enforcement bodies in all Member States are allocated sufficient funds and trained individuals to take action accordingly to address the level or types of crimes that may be identified.

Given that the ongoing security of the EU will depend heavily on the continued availability and resilience of critical national infrastructures and therefore the natural cross over in the security aims and objectives between the ISS and EP3R it is seen as important that the activities developed in the EP3R work are recognised and incorporated in the work of the ISS going forward. More importantly the ISS should not seek to duplicate work already being developed by the EP3R but support its efforts.

The action in Objective 3 for all Member States to establish centres of excellence is seen as key to improving the capability within all Member States to be prepared for and where possible prevent cyber security incidents. Member States should be prepared to act if a cyber incident occurs that may impact their citizens. As the ISS states Member States cannot and should not work in isolation. However it is not clear from the Commission Communication whether the activities of these national centres of excellence will be coordinated in any way or to what extent the work of these centres could possibly feed in the work of the proposed EU cybercrime centre. While both Member States activities and the development to a EU wide capacity for addressing cyber security issues are needed in light of the overall objective of the ISS is to encourage greater cooperation and collaboration, it is suggested that activities in the area of cyberspace should (as much as possible) be coordinated and encourage Member States to co-operate, share best practice and learn from each other's experiences.

The Commission's Communication call for all Member States to have a CERT in place by 2012 is particularly welcomed. CERT's play an important role for providing a national focal point for information, guidance, providing warning, reports and alerts. The CERT model is flexible to enable Member States to develop multiple CERTS, or different types of CERTS, depending on the particular requirements and needs based on the type of risk or threat activity that may need to be covered. Although it should perhaps be remembered that many EU Member States already have in place CERTs and have done for some time Symantec supports the Communication's support for CERTS and sees the further development as

envisaged by the Commission's Communication as an appropriate means of sharing information and encouraging a collaborative approach to addressing cyber related issues within, and between, all Member States.

The proposed creation of a European Information Sharing and Alert System (EISAS) is also highlighted in the action plan. It is important to underline that the development of any common European system in this area should recognizes and take into account the current activities of the private sector and the solutions and tools already developed given the current online threat environment. Given the experience of industry in this area it is important that ways are found to involve those in industry with the technical capabilities, skills and expertise in the development of any European approach.

The suggestion that Member States, along with ENISA, should develop national plans to response to cyber incidents that national and EU exercises should be conducted is also supported. Symantec has already participated in cyber security incident exercises across the world and believe such activities play an important role in testing responses and preparing for possible incidents. However any exercises that are planned should not only include the CERT community as proposed, but the wider ICT industry given its role in addressing cyber security incidents. In addition it is highlighted once more that any activities or exercises that are developed should be mindful of and where possible planned and coordinated with activities that may be organised through other EU initiatives such as ENISA and those being proposed in the E3PR project or other bodies such as NATO.

Objective 5: Increase Europe's Resilience to crises and disasters

The overall recognition by the Commission Communication of the risk and threat to EU critical national infrastructures from cyber attack is seen by Symantec as key given the level of threat this risk poses to the future security of all EU Member States and the EU. A shift towards greater interoperability between interconnected European wide IT networks and systems, particularly those involved in provision of critical infrastructures, means a targeted cyber attack on one Member State has the potential to have a cascading effect and impact on other connected systems. It is therefore vital that adequate levels of protection are in place that can identify security risks to major IT and ICT based systems and networks in real time and ensure operational capabilities are deployed to mitigate such security threats quickly and effectively. As outlined earlier in this submission, the recent Stuxnet attack represents a real life example of how threats designed to gain access to and reprogram industrial control networks and systems could have an impact on critical national systems and infrastructure such as energy and utilities.

The emphasis placed on the role of threat and risk assessments at an EU level is supported by Symantec. Only by identifying potential risks and security threats can effective and appropriate prevention measures be put in place to mitigate such risks. Also welcomed is the call for a "coherent" overall risk management policy to be in place by 2014. Clearly this timescale gives the EU and Member States time to take the necessary steps towards having in place an effective risk based policy to increasing resilience and disaster management. It is suggested that the first step that should be prioritised in this process is an EU wide threat assessment. Only by identifying the cyber security threats facing the EU can a risk management policy be put in place that are appropriate to managing these specific risks. To develop an effective risk management approach requires an understanding of the risks involved which requires threat intelligence information to be collected, analysed and evaluated.

For Symantec an appropriate approach to addressing possible security threats requires both prevention against incidents occurring as well as preparedness to act if and when an incident may occur. In this light the call for the need for a "proactive, intelligence-led approach" to addressing security risks is supported by Symantec particularly when it comes to cyber related security risks. A key component of being prepared to deal with a cyber security incident is having the right information at the right time to consider the possible threat or risk and take action as and when necessary. As mentioned above having real time threat intelligence information that can be analysed by experts and shared amongst partners can assist in the assessment of a risk and enable a timely response to the threat situation or incident by deploying appropriate operational capabilities to address specific security risks. However it is not clear as yet from the ISS or the communication how threat intelligence information may be collected and where the responsibility will rest to coordinate such activities and conduct the risk evaluation of the information gathered in order to enable the dissemination of threat intelligence as and when appropriate.

Given the complex cyber ecosystem of the internet it is suggested that the threat information, technical intelligence and cyber security related expertise and advice that may be needed to support such EU efforts to address cyber related incidents will reside across a number of different sources both inside and outside of government. For example it is estimated that 90% of critical national infrastructures that are increasingly reliant on interconnected networks and systems, and therefore a possible target for cyber attacks, are privately owned and managed. As a result public and private sector co-operation and collaboration is seen as a key factor to assisting not only the government but also industry to identify, assess and evaluate the level of seriousness of cyber related incidents and better prepare for and react to a cyber incidents. Symantec believes that information sharing is a fundamental component of a modern cyber security strategy and that the development of trusted information sharing networks and systems a key element to the development of successful public and private cooperation in this area.

Therefore action 3 in Objective 5 to develop situational awareness centres so that the EU can take a more integrated and common approach to crisis situations is welcomed. Although it is not clear from the communication whether the work of these awareness centres might be coordinate with the actions outlined in objective 3 related to cyberspace security. For example situational awareness centres could play a role in providing real time threat analysis information to the activities of CERTs and also provide intelligence and situational awareness to the proposed EU Centre for Cybercrime. Also it is not clear how these situational awareness centres would relate to the development of a common European Information Sharing and Alert System (EISAS). It is suggested that the Commission consider further whether, or to what extent, all these activities could be coordinated in some way going forward.

Symantec supports the Communication's recognition of the importance of having the right technology and solutions in place to address security incidents effectively. Clearly as implementation of the ISS moves forward this will be conducted at a time where all are acutely aware of the cost challenges that we all face in the current economic climate. Organizations across the whole of EU from all sectors are being faced with the same challenges around reducing costs. At the same time however the increase in cyber threats and attacks on high profile organizations and critical national infrastructure systems are also a reality being faced and recognized in the ISS. This reality raises many issues and questions as to how the ISS can be taken forward in a way that is most cost effective and efficient

whilst also achieving the aims and objectives outlined. Clearly cost is going to be a factor for all Member States but so is the need to ensure Member States have in place the necessary technologies and solutions, particularly in the fight against cyber crime and the need to protect and secure critical EU networks, systems and critical infrastructures from potential security challenges from cyber attacks. Given the actions outlined particularly in Objective 3 and 5 Symantec feel it is important that Member States recognize the importance of having in place up to date, effective and appropriate technologies to execute the cyber security strategy effectively and achieve the aims the ISS is seeking.

December 2010

Memorandum by Paul Wilkinson (ISS 1)

Introduction

Terrorism is a special type of political violence,[97] not a synonym for political violence in general. It is the deliberate use or threat of extreme violence to create a climate of fear. It is usually aimed at intimidating a wider target than the immediate victims of terrorist attacks and it involves attacks on civilians, symbolic and random targets as well as elements of the critical infrastructure and the wider economy. It is usually (though not exclusively) aimed at bringing about political change.

It is important to recognise that there are many types of terrorism.[98] Historically the most lethal and destructive has been state or regime terror. In the first half of the 20th century the Hitler and Stalin regimes used the weapon on a colossal scale, both against their own populations and the peoples of countries they had occupied. This reminds us that terror is not always the weapon of the weak. It is precisely because state terror is implemented by the armed forces, secret police and police, with all the weaponry and manpower they can deploy that it is so effective, at least in the short and medium term, in suppressing opposition and sustaining systems of brutal dictatorship and totalitarian one-party rule.[99]

In the post-Cold War world there are still many regimes using the weapon of terror,[100] and, as recent cases have demonstrated, the international community has as yet failed to find effective and democratically legitimate ways of halting, or even radically curtailing the mass violations of human rights by regimes of terror.

In the case of non-state terrorism a basic distinction can be made between internal or domestic terrorism confined to the borders of a single state and international terrorism involving the citizens and/or jurisdiction of more than one state. Terrorism becomes truly transnational when it crosses the borders of numerous states.[101]

It is also useful to categorise terrorism groups by their overall political motivation and objectives. For example, there are ethno-separatist groups such as ETA (Euzkadi Ta Askatasuna, Basque Fatherland and Liberty) and the Real IRA which claim to be struggling for the 'self-determination' of a specific ethnic group. Ideological terrorists are those groups with extreme left or extreme right objectives involving reshaping the political and/or socio-economic systems of their respective countries. Examples would be the Red Brigades in

---

97 For a valuable discussion of the concept of terrorism see Alex P. Schmid, Albert J. Jongman et al, Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories and Literature, Amsterdam, North Holland Publishing Co., 1988

98 David Rapoport provides a useful historical interpretation of different types of terrorism in his article 'The Four Waves of Modern Terrorism' in Audrey Kurth Cronin and James M. Ludes (Eds) Attacking Terrorism: Elements of a Grand Strategy, Washington D.C., Georgetown University Press, 2004. See also Paul Wilkinson 'Why Modern Terrorism? Differentiating Types and Distinguishing Ideological Motivations in Charles W. Kegley, Jr., The New Global Terrorism: Characteristics, Causes, Controls., Upper Saddle River, NJ, Prentice Hall, 2003

99 For classic accounts of totalitarian systems see, for example, Hannah Arendt, The Origins of Totalitarianism, 3rd Edition, London, Allen and Unwin, 1967, and Alexander Dallin and George W. Breslaner, Political Terrorism Communist System, Standard, Calif, Stanford University Press, 1970.

100 The annual reports of Amnesty International give abundant evidence of the continuing use of the weapon of terror by regimes in many parts of the world.

101 Al Qaeda is an example of a truly transnational movement because it has demonstrated its ability to mount attacks in different countries, and aims to change the whole international system. There are many groups which confine their attacks to the countries where their chosen enemy regime is in power but which also employ support networks overseas to supply finance, weapons, and to conduct propaganda and, in some cases, recruitment for their respective groups. These groups would be more accurately designated 'international'.

Italy,[102] the Red Army Faction[103] in Germany and the Vlanmse Militante Orde (VMO) in Belgium. Single issue terrorist groups such as violent animal rights extremists and violent anti-abortion groups are also present in several western countries. The single-issue groups unlike the ideological terrorists seek only to change one aspect of society and public policy. They are not trying to alter the entire political and socio-economic system. Most troubling for both Europe and the wider international community there is the challenge from transnational religio-political terrorism from the Al Qaeda movement and its widely dispersed network of affiliates and support networks around the world.[104]

Europe has experienced terrorist attacks and threats of attacks from all the types of terrorist groups listed above. However, by far the most dangerous of these threats at the time of writing (2010) is from the transnational religio-political terrorism of the Al Qaeda movement and its affiliates and support network.

However, it is vital to enter a word of caution at this point. European governments and their counterterrorist agencies cannot afford to neglect continuing threats from the other types of terrorist groups, such as ethno-separatist extremists, ideological groups, single issue groups and state-sponsored terrorist groups which remain active and capable of attacks. Hence, counter-terrorism has to deal simultaneously with 'traditional' terrorist groups, the major challenge of the Al Qaeda movement and its network, and newly emerging groups. The complexity of this task in our open democratic societies in Europe should not be underestimated.

It calls for the highest quality of intelligence, policing and judicial coordination and skill within our national systems, on a pan-European scale,[105] and globally.

In arguing that the threat from Al Qaeda's transnational network is the worst terrorist challenge faced by Europe, I do not mean to imply that it is the worst security threat faced by Europe or by the international community as a whole. It is just as foolish to exaggerate the terrorist threat as it is to underestimate or ignore it. On the global security agenda dramatically rapid climate change and war between nuclear weapon states are clearly far more serious longer term threats to peace and security. This is not in any way to suggest that we can afford to ignore transnational terrorism from the Al Qaeda network. We must bear in mind that Al Qaeda has already succeeded in triggering war in Southwest Asia and that it is showing determined efforts to acquire its own weapons of mass destruction (wmd).[106] We should try to keep a sense of perspective in assessing the terrorist threat.

In analysing trends in terrorism by far the best guide we have is a careful study of the history and track record of particular terrorist movements/networks, their ideologies, objectives,

---

[102] On these European ideological groups, see Donatella della Porta, Social Movements, Political Violence and the State: A Comparative Analysis of Italy and Germany, Cambridge, Cambridge University Press, 1995 and Peter H Merkl, 'West German Left-Wing Terrorism', in Martha Crenshaw (Ed.), Terrorism in Context, University Park, PA, Pennsylvania State University Press, 1995, pp160-210

[103] On ideological terrorism in West Germany see also the perceptive account by Jillian Becker in Hitler's children: the Story of the Baader-Meinhof Gang, St Albans, Granada, 1978

[104] On the development of terrorist networks see Marc Sageman, Understanding Terror Networks, Philadelphia, University of Pennsylvania Press, 2004, Fawaz A. Gerges, The Far Enemy: Why Jihad Went Global, Cambridge, Cambridge University Press, 2005, and Oliver Roy, Globalized Islam: The Search for New Ummah, New York, Columbia University Press, 2006

[105] For a discussion of European cooperation against international terrorism see Paul Wilkinson, 'International Terrorism: The Changing Threat and the EU's Response', Chaillot Paper No. 84, Paris, European Union Institute for Security Studies, October 2005

[106] When allied forces entered former Al Qaeda premises in Afghanistan after the fall of the Taliban regime in late 2001 they discovered documentary and video evidence that Al Qaeda had been studying and experimenting with wmd material. For example, one video, later shown on CBS TV News, showed dogs being exposed to poison gas.

modus operandi and demonstrated capabilities. We must now proceed to apply this to the current Al Qaeda network. By so doing we can gain insights into the characteristics and likely behaviour of the movement, its strengths and weaknesses, and the lessons that can be learned from the brief history of efforts to tackle Al Qaeda terrorism around the world.[107]

All the above are key requisites for an informed assessment of the current and emerging threats from international terrorism. But by themselves they are not going to be enough: we also need to pay attention to significant developments in the global strategic environment and their potential impact on transnational terrorism. For example, what could be the likely effects of a possible change in US presidential leadership? Or suppose several states in possession of nuclear or other forms of wmd began to employ state sponsored terrorism on a major scale, with the danger of the conflict escalating to full-scale interstate war and all the death and destruction emanating from such a conflict? We also need to consider the possibility of an environmental disaster or a major insurgency providing a terrorist group with an unexpected opportunity to acquire wmd material, possibly including weapons grade uranium. Such developments could radically alter the threat assessment relating to the group acquiring such materials, especially in the case of a group which has already acquired the necessary expertise to weaponise them.

Origins and Ideology of Al Qaeda

The key ideas in Al Qaeda's ideology were derived from Sayyid Qutb, an Egyptian Islamist who taught that the world is divided between those who live strictly in accordance with the Shari'a (Islamic religious law) and the infidel (unbelievers) who do not submit to Islamic law and who live in the world of darkness. Qutb believed that all Muslim believers have a duty to wage holy war in order to establish Shari'a rule not only in Egypt but globally. He regarded both the 'infidel' governments of the United States and other western countries, and the secular Arab regimes he accused of collaborating with them, as legitimate targets of jihad. Qutb visited the United States and was outraged by what he saw as the depravity and hedonistic materialism of the American way of life. He returned to the Middle East more determined than ever that it was the duty of all faithful Muslims to wage jihad not only against the west but also against the secular regimes of the Arab world which he regarded as 'apostates' because of their willingness to cooperate with the US and other western states and to allow western secularism and materialism to influence their societies. It should be noted that Qutb's concept of jihad was not limited to a spiritual struggle: he believed that faithful Muslims should prepare for physical confrontation with the western powers and with 'apostate' regimes in the Middle East.[108]

Osama bin Laden came under the influence of Abdallah Azzam, a follower of Qutb's ideas and a teacher of Islamic Law at King Abdul-Aziz University, Jeddah, while he was a student at the same university.[109] Later bin Laden was to become a key figure in the Makhtab al-Khidmat (Services Office) which had been founded by Abdallah Azzam and which was recruiting volunteers and raising funds for the Afghan resistance to Soviet occupation all around the world. This experience provided bin Laden with an ideal opportunity to disseminate the ideas he had acquired from Qutb and Azzam to radical Islamist groups in

[107] An interesting and very constructive analysis on these lines is Daniel Byman's The Five Front War: The Better Way to Fight Global Jihad, Hoboken, NJ, John Wiley and Sons, Inc, 2008.
[108] Quoted in Daniel Benjamin and Steven Simon, The Age of Sacred Terror, New York, Random House,, 2002, p.66
[109] Abdallah stated 'jihad is every man's duty' in cases were foreigners occupy Muslim lands. See Giles Kepel, Jihad: The Trail of Political Islam, Cambridge, Mass, Harvard University Press, P. 318

many countries.[110] In 1988/89 Osama bin Laden and Abdallah Azzam founded Al Qaeda ('The Base') and many of the groups which bin Laden had been in contact with were later to become affiliates and networks in Al Qaeda's global jihad.[111]

From the outset, bin Laden appears to have aimed to be the 'emir' or leader of the Al Qaeda movement. Abdallah Azzam died in rather mysterious circumstances and so Osama bin Laden's one really serious contender for the leadership position was removed from the scene. It is also clear that from the beginning Al Qaeda ('The Base') was seen as the hub of a global network of affiliate militant groups functioning as a transnational movement. Al Qaeda declared a jihad against the US and its allies and set up a 'World Islamic Front for Jihad', declaring that it is the duty of all Muslims to kill US citizens – civilians or military, and their allies everywhere,[112] including Israel and Muslim regimes/governments which Al Qaeda regards as 'apostates' because of their friendly relations with the US and other western countries.

In 1992 Al Qaeda claimed to have mounted bomb attacks against US troops in Aden. In 1993 it claimed to have shot down US helicopters and killed US servicemen in Somalia. Well before the mass lethality attacks against the US on 9/11 2001, Al Qaeda had demonstrated that its chosen method of asymmetric conflict against the US was terrorism. The coordinated no warning suicide bombing attacks on the US embassies in Kenya and Tanzania in August 1998, killing over 240 and injuring over 5,000 should have served as a warning to the US government of worse to come.

In the next section I shall be examining Al Qaeda's track record of terrorist attacks particularly 9/11 and major attacks on European targets. Ultimately Al Qaeda aims to establish a pan-Islamist caliphate (super-state) uniting all Muslims, thus changing the entire international system in accordance with its ideology. As this would necessitate Al Qaeda seizing control of all Muslim countries this seems an utterly unrealistic objective, but we must bear in mind that Al Qaeda militants believe that they are holy warriors fighting for Allah, that Allah is on their side and that this means they will ultimately be victorious over the infidel of the Great Satan and all the lesser Satan's. They work on a different timeline from that of western societies and declare their readiness to continue their struggle however long it may take.

Why the Al Qaeda is the worst Terrorist Threat Faced by the International Community

Brian Jenkins once correctly observed that the terrorist groups of the 1970s and early 80s 'wanted a lot of people watching, not a lot of people dead'[113] Al Qaeda and its affiliates want both a lot of people dead and a lot of people watching. The 9/11 attacks on the World Trade Center and the Pentagon were the most lethal attacks by a non-state organisation in the history of modern terrorism.[114] They have shown no remorse about the number of innocent lives including those of fellow Muslims, they have destroyed. Moreover, their typical weapon has been no-warning coordinated suicide attacks, the most difficult type of terrorism to prevent in 'open' democratic societies such as those in Europe.

---

[110] Peter Bergen, Holy War, Inc. Inside the Secret World of Osama bin Laden, New York, Free Press, 2002

[111] Rohan Gunaratna, Inside Al Qa'ida, New York, Columbia University Press, 2002

[112] Statement issues announcing formation of the 'World Front for Jihad against the Jews and Crusaders', February 1998

[113] Brian M. Jenkins, Will Terrorists go Nuclear?, Santa Monica, Calif, RAND Paper p.5541, p4

[114] For the most thorough investigation into these attacks see Report of the National Commission on Terrorist Attacks upon the United States, The 9/11 Commission Report, New York, N W Norton & Co.

Secondly, Al Qaeda's network has global reach: it is the most widely dispersed international terrorist movement in history with a presence in at least 60 countries.

Although Osama bin Laden and Ayman Zawahiri, his deputy, and Al Qaeda central provide the ideological and strategic direction to the movement, its global network is a complex of cells and affiliated organisations, including support networks, which enable them to mount operations in most parts of the world. For example, their close affiliate in S.E. Asia, Jemaah Islamiyah, has carried out major attacks in Indonesia, and the Egyptian group al-Jihad, led by Ayman Zawahiri, merged with Al Qaeda in 1998 and Zawahiri became Osama bin Laden's deputy. More recent examples of affiliates are Al Qaeda in Iraq, which has recently suffered a major backlash from Iraqi Sunni leaders angry at Al Qaeda's brutal methods and oppression, and Al Qaeda in the land of Islamic Maghreb (AQIM). This affiliate comprises the Salafist Group for Call and Combat (GSPC), the Moroccan Islamic Combatant Group, and the Libyan Islamic Fighting Group. In 2008 it was reported that Al Qaeda-linked cells had been established in Mauritania, Mali, Chad, Senegal and Niger. From open sources alone it has been possible to verify the presence of Al Qaeda-linked groups in 60 countries. The US intelligence community estimates that they are present in 90 countries.

Al Qaeda's global reach is one of the factors which make it particularly difficult to assess their prospects of long term success. Just as they appear to be knocked back in Iraq, at least at time of writing (2010), so they are consolidating their position in the mountainous northwest frontier areas of Pakistan where bin Laden and key members of Al Qaeda 'Central' are thought to be hiding. The Pakistani Army has suffered heavy losses in clashes with Al Qaeda, and the newly established government in Pakistan seems willing to negotiate with the warlords who have been supporting Al Qaeda, much to the fury of the US government.

Another important reason why Al Qaeda is the worst terrorist threat to the international community is that its leaders seem to be incorrigible. That is to say there is no sign of a more pragmatic political strategy emerging in the movement. They are bitterly opposed to democracy, which they see as a despicable western secular idea, and they show no sign of being willing to compromise on their core ideological beliefs and objectives. There have been recent suggestions that the UK government (and presumably other European governments) should start negotiations with Al Qaeda. The harsh truth is that Al Qaeda is not simply a bigger international version of the IRA. The IRA's aims were limited to bringing about radical change in Ireland. They were not trying to change the whole international system. Moreover they had a very active political front which has now succeeded in transforming itself into the largest political party of the Catholic minority in Northern Ireland. Above all the IRA's leaders became convinced that there was a political pathway to gaining some if not all their objectives. There is no comparable political pathway in the case of Al Qaeda, and it is a dangerous misapprehension to assume that bin Laden's network is a suitable partner for negotiations with democratic governments. The only alternative is to combat this particularly lethal terrorist movement by expert internationally coordinated intelligence, police and judicial cooperation, ensuring that the rule of law and the principles of human rights protection are not sacrificed in the name of 'national security'.

Perhaps the most worrying aspect of the Al Qaeda movement, and the most powerful reason for recognising it as posing the most serious terrorism threat to international peace and security is the intense interest it has shown in acquiring the necessary expertise, technology and materials to construct CBRN weapons. In a notorious statement issued as

early as 1998 Osama bin Laden said it was the duty of Muslims to prepare the maximum force to terrorise the infidel enemy. The statement was entitled 'The Nuclear Bomb of Islam'. There have been many reports of Al Qaeda seeking to obtain wmd from former Soviet Union countries and trying to buy uranium, presumably to make an atomic bomb. Most experts on CBRN weaponry emphasise the considerable technological problems involved in trying to construct a viable atomic bomb. However, even if the terrorists were only able to make a relatively crude low-kiloton device it would greatly increase Al Qaeda's ability to blackmail potential targets and to massacre much larger numbers of civilians than can be achieved using conventional weapons. For all these reasons I believe that since the emergence of Al Qaeda the threat of transnational terrorists using some form of CBRN weaponry has increased from low probability to medium probability.[115]

Nor is there any evidence that Al Qaeda's interest in acquiring such a capability has decreased.[116]

Al Qaeda's Track Record and Modus Operandi

In a brief article it is not practicable to include a comprehensive chronology of Al Qaeda attacks, disrupted and pre-empted conspiracies to attack and threats. Clearly many of these events and attacks involve the Middle East, South and South East Asia, Africa and North America. There have been a number of attacks and disrupted pre-empted attacks on European targets, and this should remind us that Al Qaeda certainly regards Europeans and European cities, gathering places, civil aviation, trains, shopping centres and markets, commercial offices and critical infrastructure as legitimate targets.

Al Qaeda-linked groups have also been responsible for killing large numbers of Europeans in its attacks on targets overseas. For example, large numbers died in the 9/11 attacks on New York, the Bali bombings and attacks on overseas embassy and consular buildings.

The general public tend to ignore or forget disrupted and pre-empted attacks, but it should be borne in mind that if it had not been for the successful intervention of the French and German police and intelligence services ,the first mass lethality attack by Al Qaeda against western citizens would not have been 9/11, it would have been the planned attack on the busy market beside Strasbourg Cathedral on New Year's Eve in 2000, a time when the market would have been packed with Christmas and New Year revellers and visitors. Four Algerians accused of plotting the attack were convicted in a Frankfurt court of conspiring to murder.[117]

Among the targets Jemmah Islamiyah (an Al Qaeda affiliate) planned to attack in Singapore in the autumn of 2001 was the British Embassy. When Al Qaeda used a petrol tanker filled with explosives to attack the synagogue at Djerba, Tunisia, in April 2002, 21 people, most of them German tourists, were killed in the attack. And in October 2002 Al Qaeda carried out a suicide attack on a French oil tanker, MV Limburg off the coast of Yemen, killing one member of the crew and injuring 4.

---

115 For interesting discussions of the possibility of nuclear terrorism see Richard Falkenrath, Robert Newman, and Bradley Thayer, America's Achilles Heel, Cambridge MA, MIT Press, 1998, and Graham Allison, Nuclear Terrorism: The Ultimate Preventable Catastrophe, New York, Times Books, Henry Hold & Co. 2004

116 But for interesting views for and against this view see Max Taylor and John Horgan (Eds.) 'The Future of Terrorism in Europe', a symposium published in Terrorism and Political Violence, Vol. 11 No. 4 Winter 1999

117 'Four convicted of Strasbourg bomb plot', http://www.guardian.co.uk/world/2003/mar/10/germany.France

Nor has Europe been spared mass fatality attacks by Al Qaeda-linked cells. In March 2004 a Moroccan cell based in Spain carried out a massive bombing of trains at Madrid railway stations, killing 191 and injuring 2051. In July 2005 an Al Qaeda-linked cell carried out suicide bombings of London Underground trains and a double-decker bus, killing 52 and injuring 700. There was a further bombing attempt in London on 21st July but it failed and the perpetrators were captured and brought to justice.

In 2007, 42 people were convicted of terrorist offences relating to 16 known operations. Half of them pleaded guilty.[118] Some of the plots prevented by the work of the intelligence and police services would have undoubtedly led to large numbers of deaths and injuries. Improved intelligence and police cooperation also led to conspiracies being thwarted in Germany, France, Italy, Germany and Belgium. In June 2008 there was a massive bomb attack on the Danish Embassy in Pakistan. It is believed to have been carried out by Al Qaeda. There is certainly no evidence for believing that European countries and citizens have ceased to be seen as legitimate targets in the eyes of Al Qaeda and Al Qaeda-linked cells.

There have been numerous reminders that Al Qaeda linked groups are determined to attack targets in Europe, including airliners departing from European airports. For example a group of Al Qaeda linked terrorists have been convicted for plotting to blow up 7 airliners leaving Heathrow for north American destinations, using liquid explosives. If their plan had succeeded the death toll might well have matched that of the 9/11 attacks. On Christmas Day 2009, a young Nigerian allegedly attempted to blow up an airliner as it approached Detroit having boarded the plane at Amsterdam. In 2010 European Governments were warned that Al Qaeda planned multiple Mumbai-style attacks on European cities, and in the autumn, Al Qaeda in the Arabian Peninsula (AQAP) threatened to attack civil aviation by planting bombs in air cargo. Devices were found on board an aircraft that landed at East Midlands Airport and on an aircraft bound for Germany, flying from Namibia. Al Qaeda propaganda repeatedly threatens attacks on European NATO states deploying troops in Afghanistan. Intensive efforts by intelligence services and police in close cooperation with foreign intelligence services have helped to thwart or at least seriously disrupt, some major terrorist conspiracies. However, intelligence is an art, not a science. It will not always succeed in pre-empting attacks. Europe is right to play its part in the wider struggle against the Al Qaeda network, a struggle that needs to be waged globally. The threat to Europe's internal security and the global struggle against international terrorism are inextricably intertwined.

Major Conducive Conditions for the Spread of the Al Qaeda Network

Al Qaeda and its affiliates exploit both religious and political motivations in their ideological and propaganda messages to potential recruits and supporters. Potential suicide bombers are told that if they carry out acts of voluntary self-sacrifice or martyrdom they will go to Paradise and be rewarded by Allah. Al Qaeda constantly portrays the Muslim world as being 'victimised' by the US and other western states, and claims that it is true defender of Islam. Hence, wherever there is a religious fault-line between Muslims and non-Muslims around the world Al Qaeda claims to be the only true protector of the Muslim community.

[118] See Home Secretary Jacqui Smith's speech at the first International Conference on Radicalisation and Political Violence in London, called terrorism 'a crime that doesn't discriminate.' 27th January 2008. http://www.homeoffice.gov.uk/about-us/news/ct-speech-08

However, as was noted in the Introduction to this article, Al Qaeda can best be described as a religio-political movement because it also plays on and magnifies hatreds, grievances and resentments against the US and the western world generally. They incite hatred of the US and its foreign policies and allies. They magnify the already latent hatred of Israel and all countries that cooperate with Israel. They blame the US in particular for its major political and financial support for Israel. And they continually stir up hatred and resentment against the regimes in the Muslim world which have in many cases suppressed fundamentalist Islamist movements (e.g. Egypt, Jordan) and those regimes that have blocked them gaining power via the ballot box (e.g. in Algeria in 1991).

It is also very important to take into account a number of sociological influences which have a particularly crucial part in helping Al Qaeda to recruit and mobilise its militant followers. For example, many young men in the Muslim communities in Europe see themselves as being treated as second class citizens and robbed of their identity – i.e. no longer part of the traditional world of Islam, and not accepted as full citizens of countries where they now reside. In many cases the sense of alienation felt through this loss of identity is reinforced by failure to gain employment or to rise up to the socio-economic ladder, even when they have acquired suitable educational and professional qualifications.

Another sociological factor which must not be underestimated is the spread of the internet and other global media of communication enabling individuals anywhere in the world to gain access to Al Qaeda network propaganda, images of conflict and alleged victimisation etc., and to instructions on explosives, weaponry etc. It is surely significant that in all the recent trials of suspected Al Qaeda-linked terrorists in the UK which have resulted in convictions prosecution evidence includes reference to the fact that the accused was accessing substantial amounts of Al Qaeda propaganda and practical guidance via the internet. Indeed it seems theoretically possible for a 'loner' terrorist to obtain all the incitement indoctrination and training required to become an Al Qaeda operative from the internet alone. However, it is necessary to enter a word of caution here. It is quite rare to find a case of loner terrorism of the kind practised by the 'Unabomber' in the US. In almost every case of Al Qaeda attacks and conspiracies small groups or cells have been involved. Terrorism is quintessentially a group phenomenon, with leaders, bomb-makers, couriers and other individuals working together in teams to carry out or support particular operations. Nevertheless in a transnational terrorist movement the value of the internet as a method of communication is particularly significant and serves to make the term 'home-grown terrorist' a contradiction in terms when applied to the Al Qaeda movement.

Triggering Conditions for Recruitment into the Al Qaeda Network

In addition to the above general religious, political and sociological factors which are conducive to Al Qaeda radicalisation and recruitment there are a number of precipitant events or experiences that may be important in pushing an individual in Al Qaeda's direction and making them more vulnerable to being identified, targeted, groomed and indoctrinated.

For example, the individual may be influenced by peer group pressure, particularly from strong charismatic personalities. The individual may want to express their anger and outrage at specific events (e.g. the US/UK invasion and occupation of Iraq). Or they may experience great resentment at what is seen as unjust or repressive treatment of relatives or close friends by the police or other security or government agencies.

Channels for Radicalisation and Recruitment

As we have noted above, the internet is undoubtedly now the most significant channel for Al Qaeda radicalisation and recruitment. However, there are other significant channels including radical leaders based in particular mosques, radical prison imams and militant fellow inmates, campus extremists and visits to family members or friends in Islamic countries, leading in some cases to personal links with extremists overseas, and attendance at terrorist training camps overseas.

A Holistic Strategy to Counter the Al Qaeda Threat

I have addressed the difficult problems of designing an effective response to Al Qaeda terrorism in a number of recent publications.[119] In broad terms I conclude that it is a serious error to place the main responsibility for countering Al Qaeda terrorism on the shoulders of our hard-working and dedicated professional armed services. In some circumstances particular military units (e.g. bomb disposal experts, special forces) may play an invaluable role, but they should be seen as only one part of a broader holistic multi-lateral and multi-pronged strategy involving intelligence services, police, judiciary, private sector, the media and the general public. Unfortunately President George W. Bush's administration decided on a predominantly military response to Al Qaeda, taking the concept of a 'war on terrorism' literally.

This concept of the war on terrorism tended to create false expectations among the US public and gives people the idea that there can be a solution to the terrorism threat by defeating Al Qaeda on the battlefield. This is of course to seriously misunderstand the nature of terrorism. Terrorists learn to hide themselves among the civilian population in cities around the world, and a sophisticated network, such as Al Qaeda, has learned how to disguise its communications from the authorities and how to evade security measures at international borders and regulatory measures designed to suppress terrorist financing. For these and many other reasons a holistic multi-pronged approach which develops much closer and more effective international cooperation is vital.

Priority Tasks

Four particularly important elements of an effective strategy are too often neglected or even overlooked:

1. Comprehensive and rigorous enforcement of counter-proliferation measures to prevent acquisition of CBRN weapons/materials by terrorists and;

2. Long term measures to win the battle of ideas with leaders/mentors of Al Qaeda terrorism.

3. We need to make a major effort to work in partnership with moderate Muslim leaders to help ensure that Al Qaeda's claim to be 'true Islam' is totally discredited. This effort will be helped by Al Qaeda's ruthless and deadly terrorist attacks in which scores of fellow Muslims have been killed – a huge strategic blunder by Al Qaeda.
4. Last but not least, we need to ensure that our own preparedness to emergency mass-casualty terrorist attack is greatly improved. Al Qaeda is still very much in business and

[119] See for example, Paul Wilkinson, Terrorism versus Democracy, 2nd Edition, London and New York, Routledge, 2006 and Paul Wilkinson (Ed), Homeland Security in the UK, London and New York, Routledge, 2007.

is capable of mass casualty attacks not only using tactics such as suicide airliner hijacking and suicide vehicle bombs, but also CBRN materials. It would be foolish to discount the possibility of attacks using chemical or biological materials, or radioactive isotopes used to make 'dirty' bombs.

December 2010