HOUSE OF LORDS

European Union Committee

17th Report of Session 2010–12

The EU Internal Security Strategy

Report

Ordered to be printed 17 May 2011 and published 24 May 2011

Published by the Authority of the House of Lords

London : The Stationery Office Limited
£price

HL Paper 149

The European Union Committee

The Committee considers EU documents in advance of decisions being taken on them in Brussels, in order to influence the Government's position and to hold them to account.

The Government are required to deposit EU documents in Parliament, and to produce within two weeks an Explanatory Memorandum setting out the implications for the UK. The Committee examines these documents, and 'holds under scrutiny' any about which it has concerns, entering into correspondence with the relevant Minister until satisfied. Letters must be answered within two weeks. Under the 'scrutiny reserve resolution', the Government may not agree in the EU Council of Ministers to any proposal still held under scrutiny; reasons must be given for any breach.

The Committee also conducts inquiries and makes reports. The Government are required to respond in writing to a report's recommendations within two months of publication. If the report is for debate, then there is a debate in the House of Lords, which a Minister attends and responds to.

The Committee has seven Sub-Committees which are:

Economic and Financial Affairs and International Trade (Sub-Committee A)
Internal Market, Energy and Transport (Sub-Committee B)
Foreign Affairs, Defence and Development Policy (Sub-Committee C)
Agriculture, Fisheries and Environment (Sub-Committee D)
Justice and Institutions (Sub-Committee E)
Home Affairs (Sub-Committee F)
Social Policies and Consumer Protection (Sub-Committee G)

Our Membership

The Members of the European Union Committee are:

Lord Bowness
Lord Carter of Coles
Lord Dear
Lord Dykes
Lord Foulkes of Cumnock
Lord Hannay of Chiswick
Lord Harrison
Baroness Howarth of Breckland
Lord Jopling
Lord Maclennan of Rogart
Baroness O'Cathain
Lord Plumb
Lord Richard
Lord Roper (Chairman)
The Earl of Sandwich
Lord Teverson
Lord Tomlinson
Lord Trimble
Baroness Young of Hornsey

The Members of the Sub-Committee which conducted this inquiry are listed in Appendix 1.

Information about the Committee

For information freely available on the web, our homepage is http://www.parliament.uk/hleu
There you will find many of our publications, along with press notices, details of membership and forthcoming meetings, and other information about the ongoing work of the Committee and its Sub-Committees, each of which has its own homepage.

General Information

General information about the House of Lords and its Committees, including guidance to witnesses, details of current inquiries and forthcoming meetings is on the internet at http://www.parliament.uk/business/lords/

Sub-Committee Staff

The current staff of the Sub-Committee are Michael Collon (Clerk), Michael Torrance (Policy Analyst) and Joanna Lukens (Committee Assistant).

Contacts for the European Union Committee

Contact details for individual Sub-Committees are given on the website.

General correspondence should be addressed to the Clerk of the European Union Committee, Committee Office, House of Lords, London, SW1A 0PW

General enquiries 020 7219 5791. The Committee's email address is euclords@parliament.uk

CONTENTS

Evidence is published online at www.parliament.uk/hleuf and available for inspection at the Parliamentary Archives (020 7219 5314)

References in footnotes to the Report are as follows:

Q refers to a question in oral evidence;

ISS 1 refers to written evidence as listed in Appendix 2.

SUMMARY

The security of the Member States is often regarded as being their exclusive preserve, but since 1975 the interior ministers of the European Community have been discussing increased cooperation on internal security matters. Since the Treaty of Maastricht the Union has been given an increasing role. Now, following the Treaty of Lisbon, the Council has been given the power to adopt and implement an internal security strategy. It did so in March 2010, and this was followed in November by a Commission Communication setting out the priorities, and how to implement them.

The Communication sets out "Five steps towards a more secure Europe": the disruption of international crime networks, the prevention of terrorism, security in cyberspace, improved border management, and increased resilience to crises and disasters. We agree that these are the matters on which implementation of the strategy should be focussed. It is this Communication which has been the object of our inquiry.

Progress on these five fronts is designed to lead to a more secure Europe. In each case we have looked in detail at the actions proposed by the Commission to advance security. Most of these will involve increased practical cooperation between the Member States, and some will involve proposals for legislation over the coming three years. We hope that our recommendations may help the Commission when it comes to formulate its proposals. We hope too that the Government—and perhaps also other Member States—may find our views helpful when they come to consider the legislative proposals.

International crime, terrorism, illegal migration and natural disasters have been with us a long time. Cyber-security is a comparative newcomer. Even a few years ago, cyberspace was thought to provide an opportunity only for small-scale criminal acts. It is now clear that, in addition to increasing the outreach of international crime, it can lead to massive disruption of state infrastructure, and can be used for espionage, terrorism, even war. During the course of our inquiry there were major attacks against the EU institutions. It is not surprising that much of the evidence we received concerned the role which the EU might play in fighting cyber-attacks. The Commission's main proposal is to set up a new Cybercrime Centre. This might be no more than a talking shop, but it could become a useful tool for investigating and analysing past attacks, improving law enforcement, and preventing future attacks. Much will depend on whether it is given adequate resources for what could be an important role.

Security knows no borders. We have looked at the way in which the internal security strategy overlaps with national and international strategies, in the hope that they can be mutually supportive. And lastly we have looked at the implementation of the strategy. The Council has an extraordinary number of committees, working groups and other bodies whose tasks overlap and can conflict. It also has one new committee which, under the Treaties, has the duty of coordinating all the work on internal security. Unless it does so effectively, very little will be achieved; if, with the right membership and the right chairmanship, it properly fulfils its mandate, the EU may play a valuable role in protecting the security of its citizens.

The EU Internal Security Strategy

CHAPTER 1: INTRODUCTION

1. In this report we consider how and to what extent the European Union should be involved in the internal security of the individual Member States, covering matters such as terrorism, serious organised crime, civil protection and cyber-security.

The Treaty Background

2. National Security is the sole responsibility of each Member State. Article 4 of the Treaty on European Union, as amended by the Treaty of Lisbon, asserts that this remains the case. However since December 1975 when the Trevi group of interior ministers was established, Member States have been meeting informally to discuss security issues. Trevi began as a regular meeting of the interior ministers of the Member States—then 9, later 12—together with a gradually increasing number of working groups. The first formalisation of this came at Maastricht in 1992 with the Treaty on European Union (TEU), Title VI, entitled "Provisions on cooperation in the fields of Justice and Home Affairs". The "matters of common interest" included immigration and asylum, combating drug addiction and fraud, judicial cooperation in civil and criminal matters, and customs and police cooperation. The Member States were required to consult and to coordinate their actions, and were allowed to adopt joint positions, take joint action, and enter into multilateral conventions.

3. But there was no power for the Council to legislate. Power to legislate in the areas covered by Title VI had to wait for the amendments made by the Treaty of Amsterdam, which came into force on 1 May 1999. In addition for the first time the words "internal security" appear in an EU Treaty, but this is only to state: "This Title [Title VI] shall not affect the exercise of the responsibilities incumbent upon Member States with regard to the maintenance of law and order and the safeguarding of internal security."[1] While the Union's external security policy was the subject of Title V of the TEU—Provisions on a Common Foreign and Security Policy—internal security was seen as remaining largely a matter for the Member States.

4. This changed with the entry into force of the Treaty of Lisbon on 1 December 2009. While Article 72 of the Treaty on the Functioning of the European Union (TFEU) repeats that the Title[2] does not affect the responsibilities of Member States with regard to internal security, Article 71 sets up a standing committee within the Council whose prime aim is "to ensure that operational cooperation on internal security is promoted and strengthened within the Union".[3]

The Stockholm Programme

5. Since the entry into force of the Treaty of Amsterdam, work on JHA matters has been the subject of 5-year programmes agreed by the European Council.

---

1 Article 33 TEU

2 By now this is Title V of Part Three of the TFEU.

3 We consider the role of this Committee in Chapter 6.

The latest of these is the Stockholm Programme,[4] agreed by the European Council on 10 December 2009.[5] It includes an invitation to both the Council and the Commission "to define a comprehensive Union internal security strategy": see Box 1.

BOX 1

Extract from paragraph 4.1 of the Stockholm Programme

> The European Council is convinced that the enhancement of actions at European level, combined with better coordination with actions at regional and national level, are essential to protection from trans-national threats. Terrorism and organised crime, drug trafficking, corruption, trafficking in human beings, smuggling of persons and trafficking in arms, inter alia, continue to challenge the internal security of the Union. Cross-border wide-spread crime has become an urgent challenge which requires a clear and comprehensive response. Action of the Union will enhance the work carried out by Member States' competent authorities and will improve the outcome of their work. The European Council calls upon the Council and the Commission to define a comprehensive Union internal security strategy…

6. It was perhaps a source of confusion for the European Council to invite both the Council and the Commission to define an internal security strategy. In February 2010 the Council, seemingly without any formal consultation of the Commission, prepared its own "Draft Internal Security Strategy for the European Union: 'Towards a European Security Model'",[6] which was agreed by the Council on 25–26 February 2010, and subsequently adopted by the European Council.[7] At the same time the Commission was preparing an Action Plan to "translate the aims and priorities of the Stockholm Programme into concrete actions with a clear timetable for adoption and implementation" which it had been invited to produce.[8] In this Action Plan, submitted to the Council on 22 April 2010,[9] the Commission undertook to formulate a Communication on the Internal Security Strategy by the end of the year. It did so on 22 November 2010 in a Communication entitled: "The EU Internal Security Strategy in Action: five steps towards a more secure Europe".[10]

The Council Strategy and Commission Communication

7. The Council Strategy is an anodyne document, phrased in broad generalities and lacking in specificity. According to the United Kingdom National

---

4 OJ C115 (4 May 2010) p 1

5 This was the subject of our brief report *The Stockholm Programme: home affairs* (25th Report, Session 2008–09, HL Paper 175).

6 Document 5842/2/10

7 Document 7120/10, referred to hereafter as the Strategy or the ISS

8 Paragraph 1.2.10 of the Stockholm Programme

9 "Delivering an area of freedom, security and justice for Europe's citizens: Action Plan implementing the Stockholm Programme" (Document 8895/10). This was the subject of our brief report *Implementing the Stockholm Programme: home affairs* (9th Report, Session 2010–11, HL Paper 90).

10 COM(2010)673 final, document 16797/10. It should be noted that this Communication and the Commission Action Plan of 22 April 2010 to implement the Stockholm Programme both take the forms of Commission Communications to the European Parliament and the Council. References subsequently in this report to "the Commission Communication" or "the Action Plan" are to the document of 22 November 2010 on the Internal Security Strategy.

Security Strategy, "A national security strategy, like 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 the ends)."[11] We agree. By this definition, the Council Strategy is hardly a strategy at all. As the Institute of Civil Protection and Emergency Management (ICPEM) pointed out, the Council document does not match these criteria.[12]

8. The Strategy does however state in its final paragraph that the Commission will adopt a Communication "which will include action-oriented proposals". And so it does. The Communication, in contrast to the Strategy, has a practical and pragmatic focus on five main objectives: the disruption of international crime networks; prevention of terrorism; security in cyberspace; improved border management; and increased resilience to crises and disasters. We have taken it as the main focus of our inquiry. We reproduce it (without its Annex) in Appendix 4.

9. Professor Wyn Rees, Professor of International Security at the University of Nottingham, criticised both documents as having no "big, underlying vision", and little in the way of a "grand objective".[13] We agree that this is true of the Council Strategy; but the Communication does not purport to have either. It will be followed by proposals from the Commission for legislation to implement its objectives. One of these, the proposal for a Directive on the use of PNR data,[14] has already been submitted. Others will be put forward later this year and in the course of the next three years. We therefore hope that our inquiry is well timed to allow our recommendations to be taken into account by those working on such proposals, and by the Government in reacting to them.

Conduct of the inquiry

10. This inquiry has been conducted by the Home Affairs Sub-Committee, a list of whose members is printed in Appendix 1. They issued a call for written evidence in November 2010; this is printed in Appendix 3. In reply they received written evidence from 13 persons and bodies. Between December 2010 and March 2011 they took oral evidence from 20 witnesses, and received supplementary evidence from a number of them. They are listed in Appendix 2. To all of them we are most grateful.

11. Three of the oral evidence sessions were in Brussels. The first of these was with Cecilia Malmström, the Commissioner responsible for the Communication. We particularly appreciate her having made time to speak to us in such a helpful and informative way. The Sub-Committee also obtained valuable informal information from Mr Juan Fernando López Aguilar, the Chairman of the European Parliament's Civil Liberties, Justice

---

[11] A Strong Britain in an Age of Uncertainty: The National Security Strategy (October 2010, Cm 7953), paragraph 0.14

[12] ISS 6

[13] ISS 13

[14] Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, COM(2011)32, Document 6007/11. This was the subject of our report *The United Kingdom opt-in to the Passenger Name Record directive* (11th Report, Session 2010–11, HL Paper 113). The report was debated on 17 March 2011, when the House agreed our recommendation that the Government should opt in to the proposed directive: HL Deb 17 March 2011, col. 433. See further paragraphs 71–72.

and Home Affairs (LIBE) Committee, and from Ms Rita Borsellino MEP, that Committee's rapporteur on the subject.

12. Throughout this inquiry we have had the assistance of Stephen Hawker CB as our specialist adviser. His wide knowledge and experience of counter-terrorism and national security issues in the United Kingdom and overseas have been invaluable to us. We are most grateful to him for all his help.

13. **We recommend this report for debate.**

CHAPTER 2: THE EU'S ROLE IN INTERNAL SECURITY

The EU's role in Internal Security

14. The Council's view of the meaning of "internal security", set out in the Strategy, is all-embracing: see Box 2.[15]

BOX 2

Council definition of "internal security"

> The main crime-related risks and threats facing Europe today, such as terrorism, serious and organised crime, drug trafficking, cyber-crime, trafficking in human beings, sexual exploitation of minors and child pornography, economic crime and corruption, trafficking in arms and cross-border crime, adapt extremely quickly to changes in science and technology, in their attempt to exploit illegally and undermine the values and prosperity of our open societies …
>
> The concept of internal security must be understood 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 such as forest fires, earthquakes, floods and storms.

15. Probably wisely, the Commission does not attempt to define "internal security", and nor do we. However none of our witnesses suggested that any of the five priorities identified by the Commission fell outside a reasonable view of internal security. There was agreement that youth or hooligan violence at sports events, and road traffic accidents, both mentioned in the Council strategy, fell below the threshold for internal security and were rightly excluded from the Communication. We agree.

16. **For the purposes of this report we are treating internal security as the ground covered by the Communication, and believe this provides reasonable and pragmatic boundaries for a strategy and for its implementation.**

17. National security of a State is the responsibility of that State, but it cannot be dealt with by that State acting alone. Many threats to security—and especially to cyber-security—are global in nature, and have to be dealt with in conjunction with other States, including other Member States. **The security of the United Kingdom does not begin or end at the water's edge, and cannot be defended independently of the security of other States.**

18. Whilst it does not necessarily follow that the EU as such has a role to play, in our earlier report *Protecting Europe against large-scale cyber-attacks*[16] we concluded that the EU does have a part to play in cyber-security, and we believe this is true of internal security generally. Hugo Brady, Senior Research Fellow at the Centre for European Reform, put it well: "No other organisation [other than the EU] has the legal or political clout to put minimum judicial standards in place across the continent, to steer the private

---

[15] Document 7120/10, Introduction

[16] March 2010; 5th Report, Session 2009–10, HL Paper 68, Chapter 3

sector in areas like aviation and container security, to get police and prosecutors working together across borders, or to put pressure on foreign countries to crack down on counterfeiters and other malefactors. Hence the EU has a *bona fide* role in some security matters."[17]

19. The threats identified in the Communication do not of course affect all Member States equally. William Shapcott, the former director of SitCen, told us: "You can roughly divide the Member States into three groups: those who are threatened and who really understand it. The UK is clearly in that group, and the Germans and the French are as well. Then there is a group that possibly is threatened but maybe doesn't properly register it, and then maybe some that aren't terribly threatened." He went on to explain that, as the threats changed, so would the groups, which could learn from one another.[18]

20. Member States are jealous of their sovereignty, and retain tight control over their national security. It would not have been difficult for the Commission to trespass on their territory. But it seems to have avoided this trap, for the Home Office stated in their written evidence: "Our view is that neither the Council's ISS nor the Commission's Communication strays into matters of national security; however we will continue to monitor this closely as proposals are brought forward." They added: "The Government largely agrees with the priority threats identified in the strategy …"[19] James Brokenshire MP, the Parliamentary Under Secretary of State at the Home Office, confirmed this: "I think that the strategy does broadly capture the priorities that we would seek to see addressed in an Internal Security Strategy."[20]

21. Mr Shapcott's view was that "the strategy looks at ways in which the EU can help Member States deal with their responsibilities. In my view, it is not an attempt to Europeanise national security; it is an attempt to identify ways in which the Union can assist." Sir Richard Mottram, a former chairman of the Joint Intelligence Committee, without attempting to define either national security or internal security, pointed out that "there is obviously a very substantial overlap which has grown between how national security is defined by those who put labels on things and how internal security is defined by those who basically come from the justice and police environment." He added that the Commission had framed its actions in a way which seemed to be "sensible and achievable". [21]

22. **Member States' national security and the EU's internal security are inextricably linked. We do not believe that these proposals intrude upon or threaten Member States' primary responsibility for national security.**

23. **We welcome the Communication as the first pragmatic attempt to articulate a comprehensive approach to the EU's internal security.**

24. **The five objectives proposed in the Communication, while broad and demanding, are sensible, practical and achievable, with the potential**

---

17 ISS 12

18 Q 51

19 ISS 10

20 Q 406

21 Q 369

to raise standards among Member States and therefore to enhance the EU's security as a whole. All future proposals in this area should be developed on a sound evidential base, with priority given to tackling identifiable threats, and with full impact assessments and cost-benefit analyses.

25. The Home Office said in their written evidence: "The Stockholm Programme was agreed under the previous Administration. The current Government therefore did not sign up to the Stockholm Programme and does not support all the proposals within that document."[22] We accept this. But, they continued, "we believe that future EU JHA measures must at the very least not stray outside the boundary of this Programme, which was agreed by the Heads of Government."[23] This we do not accept.

26. **We believe that it is shortsighted of the Government to criticise some Commission proposals solely on the ground that they go beyond what was agreed in the Stockholm Programme or the Strategy itself. Achieving internal security is a moving target; over the five years covered by this Communication it may well require action beyond what is envisaged in the Stockholm Programme. Each proposal should be assessed on its merits.**

Fundamental rights

27. "What is to be delivered by the Internal Security Strategy? Is it security only or is it liberty, security and justice?" This question, posed by Professor Didier Bigo of King's College London,[24] is one which has exercised us too.

28. The Strategy itself explains that "the values and principles established in the Treaties of the Union and set out in the Charter of Fundamental Rights have inspired the EU's Internal Security Strategy". It states that the EU's accession to the European Convention on Human Rights will also contribute to improved protection for the human rights of people in Europe.

29. The Communication says much the same:

BOX 3

Fundamental rights—the Commission view

> The Internal Security Strategy in Action, and the tools and actions for implementing it, must be based on common values including the rule of law and respect for fundamental rights as laid down in the EU Charter of Fundamental Rights. Solidarity must characterise our approach to crisis management. Our counter terrorism policies should be proportionate to the scale of the challenges and focus on preventing future attacks. 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.

---

22 ISS 10

23 They repeated this mantra on two subsequent occasions: "… we do not endorse legislative proposals that go beyond the Stockholm Programme" (section 5); and "… measures arising from these two documents must not go beyond the Stockholm Programme." (section 12)

24 ISS 7

30. Are these statements more than "formalistic sentences and announcements"? Professor Elspeth Guild and Sergio Carrera of the Centre for European Policy Studies (CEPS) do not think so.[25]

BOX 4

Fundamental rights—the views of CEPS

> Both official documents illustrate how the insecurity concerns enshrined in the ISS are attempting to take over the EU's AFSJ [the Area of Freedom, Security and Justice] 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.

31. The reference here to the whole Area of Freedom, Security and Justice is apposite, because these are questions which arise whenever coercive measures are proposed, at national or international level, and especially when they involve the collection and exchange of information, as many proposals in the Communication do. These are matters we have considered in, among others, our inquiries into SIS II,[26] Prüm,[27] PNR,[28] and Europol.[29] In our report on Money Laundering we were strongly critical of the handling of Suspicious Activity Reports by the Serious Organised Crime Agency, [30] and this has led to an investigation by the Office of the Information Commissioner and a further report.[31]

32. CEPS were not alone. Many witnesses expressed concerns that the "freedom" and "justice" aspects of the Area of Freedom, Security and Justice should not be compromised by placing too much emphasis on "security". For the Home Office Peter Storr, the Director of the International Directorate, would have liked to see greater concentration in the Communication on the issue of information exchange. "Clearly", he said, "there is, as with all data issues, a balance to be struck between the security aspect and the civil liberties and privacy aspects. We felt that that perhaps should have been picked up in the Commission Communication."[32]

33. In her oral evidence to us Commissioner Malmström placed great emphasis on fundamental rights: "I am very aware of the importance of fundamental rights and I do not see it as a trade-off. High security in the European Union

---

25 ISS 2

26 *Schengen Information System II (SIS II)* (March 2007; 9th Report, Session 2006–07, HL Paper 49), Chapter 6

27 *Prüm: an effective weapon against terrorism and crime* (May 2007; 18th Report, Session 2006–07, HL Paper 90), paragraphs 81–98

28 *The EU/US Passenger Name Record (PNR) Agreement* (June 2007;21st Report, Session 2006–07, HL Paper 108), pargraphs 110–123; and *The Passenger Name Record (PNR) Framework Decision* (June 2008; 15th Report, Session 2007–08, HL Paper 106), paragraphs 27–29

29 *EUROPOL: coordinating the fight against serious and organised crime* (November 2008; 29th Report, Session 2007–08, HL Paper 183), Chapter 8

30 *Money laundering and the financing of terrorism* (July 2009; 19th Report, Session 2008–09, HL Paper 132-I), paragraphs 174–183

31 *Money laundering: data protection for suspicious activity reports* (January 2011; 6th Report, Session 2010–2011, HL Paper 82).

32 Q 210

can come only with a very strong safeguarding of individual rights and data protection."[33]

34. The Minister did not like use of the word "balance": "it almost implies that security and the values [of fundamental rights] are, in some way, in conflict ... that being safe and being free are in some way at variance or at odds with each other. I think both are possible …"[34] "Balance" was a word Professor Bigo also disliked: "Security cannot 'balance' liberty. Security is a means to achieve liberty".[35] We agree. But it could be said that some restrictions on liberty are the price to be paid for security which, as the Strategy points out, is itself a basic right.

35. The European Arrest Warrant (EAW) is a measure which demonstrates the problem. It is considered to be a valuable tool in tackling organised crime, and there is the much-cited example of one of the plotters of the failed London bomb attacks on 21 July 2005 having been extradited from Italy within 21 days.[36] But the EAW is now used by some countries as a means of extraditing persons suspected of having committed relatively trivial offences; some 40% of EAWs are issued by Poland. There are proportionality concerns, and Mr Brady thought there should be a *de minimis* rule.[37] These are matters currently being looked at by the Joint Committee on Human Rights.[38] Additionally, the whole question of extradition is being considered by the review chaired by Sir Scott Baker, which is looking among other things at "the operation of the European arrest warrant, including the way in which its optional safeguards have been transposed into UK law". This review is due to report later this year.

36. The lack of prominence given to liberty and justice in the Communication does not necessarily indicate the direction the Commission is likely to take when formulating proposals for legislation to implement its objectives. The Commissioner said: "All the proposals we make will have to be thought through when it comes to proportionality, subsidiarity and data protection."[39]

37. **Enhancing security while at the same time safeguarding fundamental rights is best done by careful scrutiny of the individual legislative proposals as they are brought forward, to see whether too much freedom is being sacrificed to achieve a high degree of security. The European and national Parliaments have an important role to play.**

38. By the time most of these individual proposals are brought forward, the issue of data protection will already have been considered in the round. Currently data protection in relation to matters which, prior to the entry into force of the Treaty of Lisbon, were first pillar matters,[40] are governed by the Data

---

33 Q 3

34 Q 442

35 ISS 7

36 E.g. by Peter Storr, Q 264

37 Q 152

38 Inquiry into the human rights implications of UK extradition policy

39 Q 3

40 i.e. matters previously falling within Title IV TEC: visas, asylum, immigration and other policies related to the free movement of persons.

Protection Directive,[41] while third pillar measures[42] are governed by the Data Protection Framework Decision.[43] It is unsatisfactory to have two such documents; additionally, some of the most important law enforcement measures which rely on the collection, retention, and use of personal data, which should be governed by either the Directive or the Framework Decision, are governed by neither, but have their own data protection provisions.

39. The Commission has therefore embarked on a comprehensive review of the topic. It issued a Communication on 4 November 2010.[44] This was considered by the JHA Council on 24–25 February 2011, and proposals for legislation are expected from the Commission later this year. The Government have already made clear that they do not believe in a "one size fits all" approach, but would like the revised rules to "cater for the operational needs of the specific types of processing such as that done by law enforcement bodies".[45]

40. **We look forward to considering the Commission's proposal for a comprehensive data protection framework when it is published later this year. However there is already some risk that the Council and the Government will pursue a line which could result in different principles governing different measures.**

41 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281 of 23 November 1995, page 31)

42 i.e. provisions on police and judicial cooperation in criminal matters, falling within Title VI TEU prior to its amendment by the Treaty of Lisbon.

43 Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (OJ L 350 of 30 December 2008, page 60)

44 Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A comprehensive approach on personal data protection in the European Union (COM(2010)609; Council Document 15949/10)

45 Letter of 9 March 2011 from the Rt Hon Kenneth Clarke QC MP, Lord Chancellor and Secretary of State for Justice, to our Chairman

CHAPTER 3: THE INTERNATIONAL DIMENSION

41. Just as the security of each Member State individually does not stop at its national borders, so the security of the Member States collectively stretches beyond the borders of the Union. In this chapter we consider the relationship between the internal security strategy and the European Security Strategy; the impact of the formation of the European External Action Service; and the relations with other international organisations and with countries of particular strategic significance.

European Security Strategy

42. In a note of 25 January 2011 to the Standing Committee on operational cooperation on internal security (COSI), the Hungarian Presidency referred to the "plethora of security strategies" which the EU has already adopted.[46] Foremost among these is the document adopted in 2003 whose true title is European Security Strategy (ESS) but which, to avoid confusion with the internal security strategy (ISS), is often referred to as the External Security Strategy.[47] This is what the Stockholm Programme has to say: "The internal security strategy should also take into account the external security strategy developed by the Union as well as by other Union policies, in particular those concerning the internal market. Account should also be taken of the impact it may have on relations with the Union's neighbourhood and particularly with the candidate and potential candidate countries, since internal security is interlinked with the external dimension of the threats."[48]

43. Some of the threats dealt with by the ESS are truly international, and do not overlap with the ISS. These include the proliferation and use by States of weapons of mass destruction, regional conflicts, and State failure. But others, like terrorism and organised crime, are common to both the ESS and the ISS. Sir Ian Andrews, the Chairman of the Serious Organised Crime Agency (SOCA) told us that "it is entirely consistent with the declaration of the Stockholm programme that the heads of Government adopted towards the end of 2009, that there is a seamless relationship between an internal security strategy and an external one".[49] Certainly the relationship between internal and external security threats is seamless; as Professor Paul Wilkinson said, "The threat to Europe's internal security and the global struggle against international terrorism are inextricably intertwined".[50] But whether the relationship between the two strategies is as yet seamless is more open to doubt. It is for those dealing with the implementation of the two strategies to ensure that this is the case. We consider this in Chapter 6.

European External Action Service

44. The EU has had a Common Foreign and Security Policy (CFSP) since the Maastricht Treaty on European Union, but it is only since the entry into

---

46 Council document 5620/11

47 A Secure Europe in a Better World – European Security Strategy, adopted by the European Council in Brussels on 12 December 2003

48 Paragraph 4.1

49 Q 343

50 ISS 1. Professor Wilkinson is Emeritus Professor of International Relations and Chairman of the Advisory Board of the Centre for the Study of Terrorism at St Andrews University.

force of the Treaty of Lisbon that there has been a European External Action Service (EEAS) to assist the High Representative for Foreign Affairs and Security Policy. The EEAS is formed through a merger of the Commission Directorate-General for External Relations (DG Relex), parts of DG Development, and parts of the Council Secretariat, with a significant number of national diplomats and the existing overseas offices of both the Commission and the Council. When we took evidence from Mr David O'Sullivan in Brussels on 7 December 2010 he explained that this was in his capacity as the last Director-General of Relex. At the end of the year he would mutate into the first Chief Operating Officer of the new External Action Service. At that stage the structure, senior appointments, relationship with the Commission and many other matters were still being worked out, and there was a need for the appointment of more persons to deal with internal security matters in the delegations overseas.[51]

45. In December 2010 Professor Wyn Rees told us: "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[52] 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."[53] Matters are still evolving. It is not yet clear to us or (we suspect) to many others whether or how the EEAS will act as the interface between the EU's internal and external security strategies, or how its relationship with the Commission and Council will work in practice.

46. Among the matters still evolving are the future role and positioning of SitCen, the Joint Situation Centre, which is responsible for situation monitoring, for assessing threats from both outside and inside the EU, and for early warning to support EU policy-making in a crisis.[54] Until recently SitCen came under the Council; now it is part of the EEAS. A new Director, Ilkka Salmi from the Finnish Security Intelligence Service, was appointed on 17 December 2010.

47. Another body playing a central role in the EU's response to a crisis is the Political and Security Committee (PSC), which monitors the international situation in the areas covered by the CFSP and CSDP. Its role in relation to external security is, very broadly, equivalent to the role of COSI for internal security. The Communication proposes that COSI and the PSC "should work together and meet regularly"; but Mr O'Sullivan told us that this was not happening.[55]

48. Hugo Brady was pessimistic about the connection between internal security and foreign policy, and did not believe the Communication addressed this well. "There is no real level of political agreement in Brussels or between many of the Member States on how that can best be done … Conceptually,

---

51 QQ 67–76

52 JLS is the French acronym for Freedom, Security and Justice, and was the title of the Commission Directorate-General before it was split into two: Home Affairs and Justice.

53 ISS 13

54 For a fuller description of SitCen's role, see our report *Civil Protection and Crisis Management in the European Union* (March 2009; 6th Report, Session 2008–09, HL Paper 43), paragraphs 12–14

55 Q 94

although the EU has adopted strategies and even action plans on this issue, there isn't a great deal of coherence, even in the Commission for example, between Baroness Ashton and Cecilia Malmström, who are as well disposed to each other as any two colleagues. There is no real agreement at the moment in international forums such as the UN on who leads for the EU on areas such as fraud or even counterterrorism …"[56] But Mr O'Sullivan regarded as "a great success" the role played by Commission delegations in overseas offices; they were "certainly covering the full spectrum of policies emanating from the Commission, including justice and home affairs".[57] The EEAS would have to expand on this, including what was covered by the internal security strategy.

49. **We urge the Commissioner for Home Affairs and the High Representative for Foreign Affairs and Security Policy to work closely together to ensure the close alignment of internal and external security. We believe that structures to ensure that alignment is made a practical reality should be established urgently.**

50. **COSI and the Political and Security Committee should hold regular joint meetings on a similar basis.**

51. **We welcome the appointment of JHA staff to work in some overseas EU missions, and hope that this will be extended so that the EEAS may become an effective means of achieving good cooperation between those responsible for the EU's internal and external security.**

52. **We welcome the recent appointment of the new director of SitCen. We hope that it will continue to develop a wider security assessment role within the new EEAS structure, and will make an effective input to internal security threat assessments.**

Relations with the United Nations and NATO

53. The EU's action on the international scene is built on "respect for the principles of the United Nations Charter",[58] and Professor Wyn Rees told us that the UN, as the premier international security organisation, must be the focus of the effort to make internal security cooperation effective on a global scale. He pointed out that the UN is home of the 2000 Convention Against Transnational Organised Crime, and that in 2001 it passed UN Security Council Resolution 1373 which 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. European governments had regarded the UN as a vital part of an international campaign. He thought that only in this a way would the norms contained within the EU's approach to internal security be diffused throughout the wider international community.[59]

54. Relations between the EU and the UN are good; relations with NATO are not. Dr Paul Cornish, Carrington Professor of International Security at Chatham House, thought there was "a history. 'Bad blood' would probably

---

56 Q 150

57 Q 73

58 Article 21.1 TEU

59 ISS 13

be too strong a term, but they have not collaborated all that well or all that effectively, over the last several decades."[60]

55. This does no more than bear out what we have heard in previous inquiries. In our 2009 report on Civil Protection in the EU we noted the lack of cooperation between the two organisations, especially in their early warning systems, their mechanisms for communicating during a crisis, and their exercises.[61] In Chapter 5[62] we explain the particular effect of this in the field of cyber-security. In our report on Cyberattacks we noted that the Commission Communication on Protecting Europe from large-scale cyber-attacks and disruptions referred to NATO only once, and that there was a considerable overlap between the functions of the two organisations but duplication in their working. We urged the Government to encourage cooperation rather than duplication.[63] The ISS Communication mentions NATO not even once. This does not bode well. Like Sir Richard Mottram, we think that there is "obvious sense in a dialogue with NATO";[64] so obvious that it should not need saying.

56. **Vigorous engagement by the EU with the international community on security matters is crucial in order to tackle new and developing security threats. The EU should use its negotiating weight to influence the agenda accordingly.**

57. **We have repeatedly urged that relations between the EU and NATO should be improved and developed. The current situation cannot be allowed to continue. The Government, as a major participant in NATO, must take urgent steps to improve cooperation and avoid unnecessary duplication.**

Relations with strategically important third countries

58. The part that third countries can play in the security of the EU is recognised in both the Strategy and the Commission Communication. Foremost among these countries is the United States. Professor Rees regards as "striking" the importance attached in both documents 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."[65]

59. In recent meetings of the G6[66] the US Secretary for Homeland Security has always attended part of the meeting. The US was the first State with which the EU concluded an agreement on the exchange of Passenger Name Record

---

60 Q 184

61 *Civil Protection and Crisis Management in the European Union* (6th Report, Session 2008–09, HL Paper 43), paragraphs 21–36

62 Paragraphs 160–164

63 Paragraphs 80–93

64 Q 392

65 ISS 13

66 The informal, usually bi-annual, meetings of the interior ministers of the six largest Member States: France, Germany, Italy, Poland, Spain and the United Kingdom

(PNR) data,[67] and there is an agreement in force on the transfer of financial messaging data for the purposes of the US Terrorist Finance Tracking Program (TFTP). Negotiations are currently taking place on data protection. An EU-US working group on cybercrime has been set up; this was described as a "real step forward" by a member of the Commissioner's Cabinet.[68]

60. As Professor Rees explained, 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.[69] Readmission Agreements, under which third countries agree to accept the return of their own failed asylum seekers or people who have transited across their territory, are in force between the EU and 13 States.[70] Their value has been confirmed in a recent Commission report, which has however recommended a number of changes.[71] Negotiations for an agreement with Turkey have been under way since 2002. In her evidence to us the Commissioner voiced her frustration that a final agreement had still not been concluded.[72] While the negotiations have now been completed, the agreement is still not in force, and it includes a 3-year transitional provision before full implementation.

61. Negotiations have recently begun for an agreement with Belarus. The United Kingdom is a party to all the EU readmission agreements which have so far been concluded, but the Minister for Immigration has written to tell us that the Government have decided not to opt in to the Decision agreeing the negotiating mandate of the EU. Even if, which we doubt, there are good reasons for the United Kingdom not ultimately to be party to the agreement once it is negotiated, there can be no justification for not taking part in the negotiations.[73] Participation in the negotiations, while not in any way requiring the United Kingdom ultimately to be a party to the agreement, would have allowed ministers to stress the importance of protecting the human rights of Belarus citizens.

62. Mr Shapcott explained that for operational matters third countries still tended to deal with individual Member States, but it was the EU's ambition to go further in its relationships with Russia, China, India and Pakistan. Yet with the exception of Pakistan, where there had been fruitful cooperation, this had not got very far. Discussion with the Russians had been rather empty.[74] Professor Rees thought that Russia was resistant to EU incentives because the Kremlin considered itself to be too important to have its policies moulded by Brussels.[75]

---

67 See our report *The EU/US Passenger Name Record (PNR) Agreement,* 21st Report, Session 2006–07, HL Paper 108.

68 Q 80

69 ISS 13

70 Hong Kong, Macao, Sri Lanka, Albania, Russia, Ukraine, Former Yugoslav Republic of Macedonia (FYROM), Bosnia-Herzogovina, Montenegro, Serbia, Moldova, Pakistan and Georgia

71 Communication from the Commission to the European Parliament and the Council: Evaluation of EU Readmission Agreements, COM(2011)76, Council document 7044/11.

72 Q 34

73 Letters of 28 March and 18 April 2011 from Damian Green MP, Minister for Immigration, to the Chairman; replies from the Chairman of 6 April and 11 May 2011.

74 Q 48

75 ISS 13

63. The Director of Europol told us that there were already legal cooperation agreements in force between Europol and some 20 third countries.[76] Negotiations on an agreement between Europol and Russia were ongoing.[77]

64. **We note the continuing importance of EU-US cooperation on security matters, but believe that the EU should also step up its cooperation, however challenging this may be, with other strategically important third countries such as Russia, China, Turkey and Pakistan in order to mitigate the external risks to the EU's internal security.**

65. **We welcome the endorsement by the Council of a readmission agreement with Turkey, but regret the delay in its implementation. We also regret that the Government have decided not to participate in the Decision authorising negotiation of a readmission agreement with Belarus.**

---

[76] QQ 108–109: Albania, Australia, Bosnia-Herzegovina, Canada, Colombia, Croatia, FYROM, Iceland, Moldova, Montenegro, Norway, Russia, Serbia, Switzerland, Turkey, Ukraine, and the USA.

[77] Q 116

CHAPTER 4: THE OBJECTIVES

66. In order to achieve the Strategy's aims, the Communication sets out five strategic objectives, each including a number of specific actions, to be implemented during the period 2011 to 2014. These are to:

(1) Disrupt international crime networks;

(2) Prevent terrorism and address radicalisation and recruitment;

(3) Raise levels of security for citizens and businesses in cyberspace;

(4) Strengthen security through border management; and

(5) Increase Europe's resilience to crises and disasters.

We now consider each of these objectives in turn except security in cyberspace which, because of its particular current significance, is considered in Chapter 5. In practice, the division between these categorisations is not absolute and some of the actions falling under one objective will have an impact on others.

Serious and organised crime

67. The Communication talks of the need for cooperation at EU level, through practical law enforcement cooperation and overcoming divergent legal approaches at Member State level, to "... disrupt criminal networks and combat the financial incentive which drives them." CEPS emphasised the variations in the nature of the threat across Europe and cautioned that "Any one-size-fits-all approach to policy is therefore likely to be highly counterproductive."[78] However, Dr Cornish was more positive, stating that the nature of the international threat in this area was clearer and that therefore international cooperation was "utterly indispensable."[79]

68. Curiously, the Communication does not mention the role of regular common threat assessments in identifying the challenges and deciding the EU's strategic priorities in this area. Since 2006, Europol has produced an annual Organised Crime Threat Assessment (OCTA), which includes an analysis of current and anticipated trends in organised crime across the EU, based upon information provided by the Member States (including contributions from SOCA) and a number of EU agencies.[80] A related development saw the adoption of an "EU policy cycle for organised and serious international crime". This was a Belgian-led initiative, supported by the United Kingdom, the Netherlands and Europol, and adopted by the Justice and Home Affairs Council on 8 and 9 November 2010,[81] following COSI's agreement to establish such a policy cycle. This was welcomed by Rob Wainwright, the Director of Europol, who considered that the OCTA would become the "cornerstone" of the policy-making process.[82] Further information about this initiative—Project Harmony—is in Box 5.

---

78 ISS 2

79 Q 189

80 The 2009 OCTA is available here: http://www.europol.europa.eu/publications/European_Organised_Crime_Threat_Assessment_(OCTA)/OCTA2009.pdf

81 http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/117583.pdf

82 Q 104

BOX 5

Extract from JHA Council Conclusions, 8 and 9 November 2010

The Council concludes to:

Establish and implement a multi-annual policy cycle with regard to serious international and organised crime in order 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 consists of four steps:

Policy development on the basis of a European Union Serious and Organised Crime Threat Assessment (EU SOCTA) that must provide for a complete and thorough picture of criminal threats impacting the European Union.

Policy setting and decision-making through the identification by the Council of a limited number of priorities, both regional and pan-European. For each of the priorities a Multi-Annual Strategic Plan (MASP) needs to be developed in order 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) that need to be aligned to the strategic goals which have been determined in the MASP, building upon the COSPOL framework as the multilateral cooperation platform to address the prioritised threats.

At the end of the policy cycle a thorough evaluation needs to be conducted and will serve as an input for the next policy cycle.

Align the timing and methodology when in the future other policy cycles for areas identified in the Internal Security Strategy were to be created so as to allow the political level to decide at the same time on the priorities.

69. Sir Ian Andrews, the Chairman of SOCA, was enthusiastic about the benefits that cooperation between Member States at EU level can and does provide in this area, and we were encouraged that SOCA has already presented a paper to an early meeting of COSI about the UK's approach in the "disruption and denial" of criminal activities, which we understand was well-received by the other representatives on that body.[83] SOCA has also presented other suggestions for initiatives at the EU level, including tackling organised crime in the Western Balkans.[84]

70. **We welcome the establishment of the organised crime "policy cycle" by the Council and commend SOCA's positive engagement with COSI on organised crime matters.**

Passenger Name Record (PNR) data

71. The Communication makes reference to a forthcoming proposal[85] for a Directive on the collection of passenger name record (PNR) data from

83 Q 318. See Council Document No 11401/10, 22 June 2010

84 Q 342

85 *The EU Internal Security Strategy in Action, Objective 1, Action 1*, p 5

passengers on flights entering or leaving the EU in order to help Member States prevent and prosecute terrorist offences and serious crimes. This proposal was subsequently published by the Commission on 2 February 2011[86] and while many of our witnesses supported it, they considered that it should also apply to intra-EU flights, which the current proposal does not. Mr Brokenshire told us that the Government were arguing in Brussels for the scope of the measure to be extended, and that they had not yet decided whether to opt in.[87] In a separate report we urged the Government to opt in to this proposal, and the House agreed our recommendation.[88]

72. The last day of the three months within which the Government had to opt in if they wished to do so was 9 May 2011.[89] The following day Damian Green MP, the Minister for Immigration, made an oral statement in the House of Commons in which he announced that the Government had informed the Presidency of their decision to opt in to the draft Directive. He added that the Government were making progress in attempting to persuade other Member States that the Directive should apply to intra-EU flights, though it might apply only on those routes thought to present a high risk.[90] **We welcome the Government's decision to opt in to the draft Directive, and support their intention to continue to argue that the Directive should apply to intra-EU flights.**

Money laundering

73. The Communication also supports the revision by 2013 of EU money laundering legislation, in order to enable better identification of owners of companies and trusts.[91] The nature and necessity of further revisions are not clear at this stage and we reserve our position on this point until a more detailed proposal is published by the Commission. We considered the existing EU legislation in this area, as well as the international dimension, in our 2009 report *Money laundering and the financing of terrorism*,[92] which among other things was critical of the fact that the United Kingdom had not yet ratified the Council of Europe's Convention on Money Laundering and Terrorist Financing (the Warsaw Convention)[93] despite having chaired the negotiations. In their evidence to the inquiry which preceded the report, the previous Government suggested that they were on course to have ratified the Convention by September 2010.[94] Nearly nine months after this working deadline has passed the situation remains unchanged.

---

86 Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, COM (2011) 32 final, Council Document 6007/11

87 QQ 436 & 437

88 *The United Kingdom opt-in to the Passenger Name Record directive* (11th Report, Session 2010–11, HL Paper 113). The report was debated on 17 March 2011, when the House agreed our recommendation that the Government should opt in to the proposed directive: Official Report, 17 March 2011, col. 433.

89 The document was dated 2 February 2011, and in our report we stated that 2 May 2011 was the closing date for opting in. Subsequently the Council Secretariat agreed to amend the date from which the three months are calculated, which in the case of this draft Directive put the closing date back by a week.

90 HC Deb 10 May 2011, cols

91 *The EU Internal Security Strategy in Action*, Objective 1, Action 1, p 5

92 19th Report, Session 2008–09, HL Paper 132

93 Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism, Warsaw, 16.V.2005

94 *Money laundering and the financing of terrorism*, paragraph 45

74. **The Government's continuing failure to ratify the Warsaw Convention is inexcusable. We repeat our view that this prevarication sends out a negative message about the Government's commitment to this important matter. We again urge the Government to sign and ratify the Warsaw Convention without further delay**.

Confiscation of criminal assets

75. The Communication proposes strengthening the EU's existing legal framework for the confiscation of criminal assets, as well as conferring additional functions on the Asset Recovery Offices (AROs), which each Member State is required to establish by 2014.[95] Hugo Brady considered the Commission's focus on this area to be wise as the EU has pre-existing systems in place which continue to play an effective role.[96] However, while the Government were also supportive of the Commission's goals, they believed that the same outcomes could be achieved by improving practical cooperation and by better utilisation of existing powers, rather than by adopting new legislation, which they considered had no basis in the Stockholm Programme.[97] Their view was the same on expanding the role of AROs, which they noted had not yet been established in all Member States.[98]

76. **The establishment of functioning Asset Recovery Offices in each Member State should be given a higher priority before the conferral of additional functions is considered.**

Joint Investigation Teams (JITs)

77. The Communication supports the more extensive use of Joint Investigation Teams (JITs),[99] which consist of judicial and police authorities from at least two Member States. JITs are responsible for carrying out criminal investigations into specific matters for a limited period on a cross-border basis, with expert assistance usually being provided by Europol and Eurojust.[100]

78. The Government consider JITs to be a "valuable tool" in tackling cross-border organised crime and therefore support the Commission's plan to expand their application.[101] Their use throughout the EU already appears to be well established. Mr Wainwright told us that by the end of 2010 Europol had facilitated 13,000 major cross-border operations.[102] SOCA echoed the Government's enthusiasm, and their Head of Strategy in the international department, Mark Bishop, told us that they had recently appointed a

---

95 *The EU Internal Security Strategy in Action*, Objective 1, Action 3, p 6

96 Q 149

97 Q 438

98 According to the Home Office the Member States that have not yet established AROs are Slovenia, Italy, Portugal, Malta and Romania (ISS 18).

99 *The EU Internal Security Strategy in Action*, Objective 1, Action 1, p 5.

100 Council Framework Decision 2002/465/JHA of 13 June 2002 on joint investigation teams (OJ L 162 of 20 June 2002, p 1). This ceased to have effect on the entry into force for all Member States of the Convention on Mutual Assistance in Criminal Matters. See further our report *EUROPOL: coordinating the fight against serious and organised crime* (November 2008; 29th Report, Session 2007–08, HL Paper 183), paragraphs 109–112.

101 ISS 10

102 Q 104

national JIT expert who takes part in the EU level forum for national JIT experts, as well as seconding another member of staff to Eurojust, which has a role in the JIT process, to promote the use of JITs by United Kingdom law enforcement agencies.[103] We also heard about some recent examples of United Kingdom-led JITs operations.[104]

79. **We share the Government's enthusiasm for the work of Joint Investigation Teams and support the greater use of this tool in the fight against cross-border organised crime.**

Counter-terrorism

80. The Communication considers that the terrorist threat to the EU is still significant and is a constantly evolving one, and that therefore any efforts taken at the EU level in response must also evolve and stay ahead of that threat. On a similar basis to its work on threats posed by organised crime, Europol produces regular Terrorism Situation and Trend (TE-SAT) reports,[105] which provide law enforcement officials, policymakers and the general public with facts and figures regarding terrorism in the EU, while also seeking to identify trends and developments. However the Communication considers that Member States have the primary responsibility for achieving this objective, but with the Commission and the Counter-Terrorism Coordinator providing full support.[106]

81. Professor Wilkinson noted that while "... by far the most dangerous of these [terrorist] threats ... is from transnational religio-political terrorism of the Al-Qaida movement and its affiliates, … 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 groups which remain active and capable of attacks."[107] The Communication does not consider the threat posed by the latter type of organisation, possibly because the scope of their activities falls predominantly within the borders of the affected Member States. CEPS and ICPEM suggested that as the most numerous terrorist attacks were still mainly of a local nature, they were best tackled by the Member States concerned.[108] Dr Cornish similarly emphasised the growing problem of "home-grown radicals" and the threat from single issue extremists.[109]

EU Counter-Terrorism Strategy and Counter-Terrorism Coordinator

82. The EU has already been active in this area with the adoption in 2002 of a Framework Decision on combating terrorism[110] which provided for a

---

[103] Q 326

[104] QQ 331–333

[105] These have been produced since 2007 and the most recent 2010 TE-SAT report is available here: http://www.europol.europa.eu/publications/EU_Terrorism_Situation_and_Trend_Report_TE-SAT/Tesat2010.pdf

[106] See paragraphs 81–83

[107] ISS 1. In terms of what should be done in response, Professor Wilkinson goes on to state that "It calls for the highest quality of intelligence, policing and judicial coordination and skill within our national systems, on a pan-European scale and globally."

[108] ISS 2 & ISS 6

[109] Q 205

[110] Council Framework Decision of 13 June 2002 on combating terrorism (2002/475/JHA), OJ L 164 (22 June 2002) p 3

common definition of terrorist offences and minimum penalties, the creation of an EU Counter-Terrorism Coordinator in 2004, and the adoption of an EU Counter-Terrorism Strategy in 2005.[111] More information about these developments is provided in Box 6.

BOX 6

EU Counter-Terrorism Coordinator and Counter-Terrorism Strategy

The position of EU Counter-Terrorism Coordinator was created shortly after the Madrid bombings in March 2004 and the incumbent, Gilles de Kerchove, was appointed in September 2007. He operates within the Council Secretariat and has the following responsibilities: coordinating the counter-terrorism work of the Justice and Home Affairs Council (including a multitude of working groups and working parties); maintaining an overview of the relevant EU instruments in this area; ensuring effective follow-up of Council decisions; monitoring the implementation of the EU Counter-Terrorism Strategy, including making reports to the Council;[112] fostering better communication between the EU and third countries; and ensuring that the EU plays an active role in the fight against terrorism as a whole.

The London bombings on 7 July 2005 provided the impetus for the adoption of an EU Counter-Terrorism Strategy during the United Kingdom Presidency later that year. The Strategy commits the EU to combat terrorism globally, while respecting human rights, and consists of four strands:

- PREVENT people from turning to terrorism;
- PROTECT citizens and critical infrastructure by reducing vulnerabilities;
- PURSUE and investigate terrorists, impede planning, travel, and communications, cut off funding and access to attack materials, and bring terrorists to justice; and
- RESPOND in a coordinated way by preparing to manage and minimise the consequences of a terrorist attack, by improving capabilities to deal with the aftermath and by taking into account the needs of victims.

83. While both the Communication and the Commissioner[113] foresee a continuing role for the Counter-Terrorism Coordinator, it is unclear to us what this will be. Hugo Brady thought that "... at the moment the office plays a valuable role in a number of ways. First, its current occupant [Gilles de Kerchove] has the wonderful genius to be liked and respected by everybody. He is able to bring together professionally sceptical interior ministries and officials dealing with counter-terrorism and get them talking." But, he added, "Now that the EU has a role in internal security, what do we need an inter-governmental Counter-Terrorism Coordinator for?" He concluded that it may eventually become appropriate to abolish the position altogether or alternatively vest its responsibilities elsewhere, possibly within the EEAS, and thus focus its activities on the external dimension of counter-terrorism.[114]

---

111 Council Document No. 14469/4/05, 30 November 2005. The EU Counter-Terrorism Strategy, as well as the various flanking measures which have been adopted by the EU for counter-terrorism purposes, is also considered in the Commission Communication: The EU Counter-Terrorism Policy: main achievements and future challenges, COM (2010) 386 final, 20 July 2010

112 His most recent report to the Council was made in May 2010—see Council Document No. 9685/10.

113 Q 15

114 Q 167

84. **We commend the work of the Counter-Terrorism Coordinator but believe that his role needs to be clarified and reviewed following the entry into force of the Treaty of Lisbon. In the meantime, we believe that he could play a useful role as a bridge between the internal and external aspects of terrorism.**

85. Olivier Luyckx, DG HOME's head of crisis management and the fight against terrorism, has recently advocated the establishment of a new EU internal security body which would pull together a number of existing bodies (CEPOL, COSI, Eurojust, Europol and Frontex) under the Counter-Terrorism Co-ordinator.[115] We do not think this makes very good sense, and it runs contrary to the case we make in Chapter 6 for fewer bodies dealing with internal security, not more.

Radicalisation and recruitment

86. In his written evidence, while asserting that the internet was the most significant "channel" by which Al-Qaida could radicalise and recruit its supporters, Professor Wilkinson also identified additional channels as being "... 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." He concluded by suggesting that these channels can be countered by winning the "battle of ideas" through the construction of "counter-narratives" and working in partnership with moderate Muslim leaders.[116]

87. This issue is related to the ongoing debate about the success or otherwise of multicultural societies in Europe. In a speech to the Munich Security Conference on 5 February 2011 the Prime Minister, the Rt Hon David Cameron MP, talked about the continuing threat of terrorist attacks from a State's own radicalised citizens and the importance of distinguishing Islamist extremism as an ideology from Islam as a religion. He concluded that the "doctrine of state multiculturalism" had failed and that in response what was needed from States was "... less of the passive tolerance of recent years and a much more active, muscular liberalism."[117]

88. The EU has already been active in counter-radicalisation initiatives in the past with the adoption, under the *prevent* strand of the Counter-Terrorism Strategy, of a dedicated EU Strategy for Combating Radicalisation and Recruitment to Terrorism[118] and an associated Action Plan in 2005.[119] Following an initiative by the Counter-Terrorism Coordinator, a number of Member States have been active in taking forward projects which are

---

115 These views were expressed at a European Parliament hearing on 30 March 2011.

116 ISS 1

117 The full speech is available at: http://www.number10.gov.uk/news/speeches-and-transcripts/2011/02/pms-speech-at-munich-security-conference-60293

118 The Strategy was adopted in November 2005 (Council Document No. 14781/1/05) and revised in November 2008 (Council Document No. 15175/08). Its main aims include: disrupting the activities of networks and individuals who attempt to involve people in terrorist activities; ensuring that mainstream opinions prevail and are heard over extremist views; and promoting democracy, security, justice and opportunity for all.

119 Only a partially declassified version of the Action Plan is available (Council Document No. 14782/05) and it contains virtually no substantive content.

designed to facilitate the aims of this strategy, including a project on media and strategic communication in the United Kingdom.

89. The Communication proposes to develop this existing work further through the establishment of an EU radicalisation-awareness network, the organisation of a ministerial conference in 2012 and the adoption of a "handbook" of actions and experiences.[120] The network, in particular, would seek to allow policy specialists and officials from each Member State to share best practice and identify the most effective techniques for challenging terrorist narratives. The Commissioner and Dr Cornish were enthusiastic about the proposed network but considered that the best way to tackle the problem would continue to be at Member State level, which the Communication also acknowledges.[121] Sir Richard Mottram agreed, and suggested that the EU could add further value by sponsoring more academic research in this area, and so raise awareness.[122] He also suggested that the United Kingdom was in a good position to export its knowledge and experience to other Member States, but stressed that it was not a "single problem" with a "single solution" and that it had to be "disaggregated" and tackled at local level.[123] However, other witnesses were less enthusiastic. Hugo Brady was sceptical about the overall efficacy of adopting counter-radicalisation policies at EU level,[124] a view which was shared by Peter Storr from the Home Office.[125] Mr Brokenshire was concerned that any initiatives taken at the EU level might duplicate existing multilateral efforts[126] and considered that the threat was different in each Member State.[127]

90. **The proposal to establish an EU radicalisation-awareness network will be a positive step if its functions are clear and well-defined. However we believe that Member States should continue to have the primary role in this area. We are less convinced that production by the Commission of a "handbook of actions and experiences" would either be practical or add value.**

Preventing terrorists' access to materials and funding

91. The Communication makes reference to past EU initiatives that have been adopted to prevent terrorists acquiring explosives and Chemical, Biological, Radiological and Nuclear (CBRN) substances, as well as more recent measures such as the proposed Regulation to limit the availability of specific chemical precursors which can be used to manufacture explosives.[128]

92. On a similar basis, but in the financial sphere, the Communication states that the Commission will also consider devising a framework for administrative measures to be adopted under Article 75 TFEU to freeze funds of persons

---

120 *The EU Internal Security Strategy in Action*, Objective 2, Action 1, pp 7 & 8

121 QQ 21, 204–206

122 QQ 393–394

123 Q 396

124 Q 169

125 Q 247

126 Q 429

127 Q 430

128 Proposal for a Regulation of the European Parliament and of the Council on the marketing and use of explosives precursors, COM (2010) 473 final, 20 September 2010. The Committee considered this proposal in November 2010 and it remains under scrutiny.

suspected of terrorist activities in the EU as well as developing systems to allow the EU to extract and analyse financial messaging data held on its own territory, possibly through the establishment of an EU Terrorist Financing Tracking Programme (EU TFTP).[129] However, Hugo Brady was not convinced that an EU TFTP was necessary,[130] while the Government were not in favour of the creation of an asset-freezing regime under Article 75 TFEU and instead advocated a softer approach under Article 74 TFEU, which would facilitate administrative cooperation between the relevant departments of the Member States to achieve the same outcomes.[131] The Council already applies restrictive measures against certain persons and entities based on lists of terrorist suspects which are drawn up either by the UN Sanctions Committee or by itself under the CFSP.[132] The EEAS representatives told us about recent legal difficulties which the EU had experienced with the operation of these measures following adverse judgments from the Court of Justice.[133]

93. **We believe there is in principle a case for the establishment of an asset-freezing regime applicable to individuals resident within the EU. To be effective this will require the cooperation of third countries, in particular Switzerland and Liechtenstein.**

Transport security

94. The Communication also looks ahead to the development of an EU regime for aviation and maritime security, as well as the more complicated area of land transport security, including the security of rail passenger services. It considers the possible establishment of a "standing committee on land transport security" as a first step.[134] While we received evidence from the ICPEM stating that the scope of the suggested standing committee should be widened to include "crowded places", little other substantive evidence was received regarding these proposals. The Communication makes reference to a further Communication on Transport Security Policy, which we understand is due to be published by the Commission in October 2011, and we expect that this will contain more detail about the Commission's thinking.

95. **The security of transport networks is a vital component of the security debate. However we reserve judgment on the EU's role in this area pending the publication of the Commission's Communication on Transport Security Policy later this year.**

Border management

96. As the United Kingdom is not a member of the borderless Schengen Area, the Communication's proposals for the enhanced use of new technologies for border checks and surveillance, and greater coordination of Member States'

---

[129] Provision for which was made in the EU-US TFTP Agreement, which after initially being rejected by the European Parliament in February 2010 was eventually approved (after its privacy provisions were enhanced) in July 2010. It entered into force on 1 August 2010.

[130] Q 149

[131] ISS 10

[132] A Council Decision is adopted in each instance, under the CFSP, and then implemented by way of a Regulation.

[133] QQ 98–99

[134] *The EU Internal Security Strategy in Action*, Objective 2, Action 3, pp 8 & 9

efforts through Frontex, will have limited direct impact on the United Kingdom. The creation of the Schengen Area has already necessitated enhanced law enforcement cooperation between the Member States and third countries concerned but while the United Kingdom participates in some of these mechanisms on a partial basis—Frontex, and once it has become operational, the Schengen Information System II[135]—it does not participate in others at all, such as the Visa Information System. Despite this, the Government have in the past emphasised that they will monitor developments in this area so that synergies can be sought between EU policy developments and their own e-Borders programme. We consider this to be a wise approach as enhancing controls at the EU Schengen border is likely to have consequential benefits for the security of the UK borders.

97. This approach is especially appropriate in the light of recent developments, in particular those in third countries bordering the Mediterranean, which will inevitably mean that concerns over border management and frontier control remain high on the agenda of all Member States.[136] These are matters which need to be handled in a manner consistent with an overall policy supporting an increase in democracy, human rights and the rule of law. The Commissioner told us about the deployment by Frontex of the first ever RABIT[137] operation to the Greek-Turkish border, following a request from the Greek authorities.[138] Following increasing levels of irregular immigration resulting from political instability in north Africa, Frontex has also recently deployed another mission to Italy—Operation Hermes.[139]

98. The Government are broadly supportive of the Communication's objectives in this area. However, while they believe that the EU can assist the efforts of individual Member States in the development of an integrated border management strategy to reduce illegal migration and tackle crime at the EU's borders, they have also registered their disappointment that the role of voluntary and forced returns in reducing illegal migration was not emphasised in the Communication, as they consider that "... the only true deterrent to illegal migration into the EU is an enhanced expectation of swift return to the migrant's country of origin." [140]

---

135 SIS II is a database system which will apply to the UK for law enforcement purposes but not for immigration.

136 On 4 May 2011 the Commission issued a Communication on Migration, COM(2011)248, explaining how the events in north Africa, and in particular in Tunisia and Libya, were affecting the EU States of southern Europe, in particular Italy, Malta, Greece and Cyprus, and setting out measures for coping with this in both the short and the longer term.

137 Rapid Border Intervention Teams. They can be deployed to assist Member States in dealing with "urgent and exceptional migratory pressures" and are only intended to provide short-term assistance. See Regulation (EC) No 863/2007 of the European Parliament and of the Council of 11 July 2007 establishing a mechanism for the creation of Rapid Border Intervention Teams and amending Council Regulation (EC) No 2007/2004 as regards that mechanism and regulating the tasks and powers of guest officers, OJ L 199 (31 July 2007) p 30

138 QQ 33–36. The RABIT operation began on 2 November 2010 and involved more than 200 specialist border control personnel, some of whom were armed, from 26 Member States, conducting 24 hour surveillance in an effort to stem a heavy flow of irregular migration. The deployment of the RABIT operation saw a reduction in irregular crossings of approximately 75 per cent. After its mandate expired on 2 March 2011, it was succeeded by Operation Poseidon, which will provide more permanent support from the EU for the remainder of 2011.

139 This operation began on 20 February 2011 and is designed to assist the Italian authorities in managing the inflow of migrants from north Africa, particularly arrivals from Tunisia, on the island of Lampedusa.

140 ISS 10

EUROSUR

99. The Communication refers to a forthcoming legislative proposal for the establishment of a European Border Surveillance System (EUROSUR),[141] which would adopt a technology-based approach to the surveillance of the Schengen border in order to reduce illegal migration, by helping Member States achieve full situational awareness at their external borders and enhancing the reaction capability of their law enforcement services. The establishment of EUROSUR was originally suggested by the Commission in 2008[142] and in the first instance it is likely to concentrate on the southern EU: the Canaries, the Mediterranean and the Black Sea. Emma Gibbons, from the Home Office, anticipated that the United Kingdom's eventual involvement in EUROSUR would be on a similar basis to their engagement with Frontex.[143] Christophe Prince, the Justice and Home Affairs Counsellor at UKREP[144], provided a detailed overview of EUROSUR's current and future development, and confirmed that the United Kingdom would seek to exchange information and cooperate with EUROSUR as it develops, through the United Kingdom National Maritime Intelligence Centre, since the Government consider that it will ultimately benefit controls at the United Kingdom border.[145]

Frontex

100. While both Frontex and Europol collect information about criminal activities during their operations, they are not currently permitted to exchange this information in any way, such as for risk analysis purposes or as the basis for joint operations. However, Frontex does make regular contributions to Europol's annual OCTA report. The Communication proposes to permit such exchanges albeit "... with a limited scope and in accordance with clearly defined personal data management rules."[146] The attainment of this objective is already being pursued through the introduction of a new provision in an existing proposal for the amendment of the Frontex Regulation, which aims to enhance the agency's operational capabilities and its mandate.[147] The Government support this extension of the agency's mandate on condition that it contains "stringent data protection safeguards;" they believe that it should cooperate with other EU agencies, including Eurojust, on the same basis.[148]

101. We noted with interest the inclusion in the Government's Strategic Defence and Security Review of a commitment to make an "effective contribution" to the future work of Frontex.[149] Despite its non-participation in the legal

---

141 *The EU Internal Security Strategy in Action*, Objective 4, Action 1, pp 11 & 12

142 Examining the creation of a European border surveillance system (EUROSUR), COM (2008) 68 final, 13 February 2008

143 Q 433

144 The Brussels office of the United Kingdom Permanent Representative to the EU

145 Q 240

146 *The EU Internal Security Strategy in Action*, Objective 4, Action 2, p 12

147 Proposal for a Regulation of the European Parliament and the Council amending Council Regulation (EC) No 2007/2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders (FRONTEX), COM (2010) 61 final, 24 February 2010.

148 ISS 10

149 Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review, Cm 7948, October 2010, p 63

measures underpinning Frontex, the United Kingdom already makes a financial contribution to its operations, and arrangements are in place for it to participate in the agency's management board.[150] The Government have supported its work since its establishment in 2005 and intend to make a larger contribution to the agency's engagement with third countries and its operational activities in facilitating returns of migrants.[151]

102. **We welcome the Government's commitment to make an effective contribution to the development of EUROSUR and the future work of Frontex. Despite the United Kingdom's inability to participate fully in EUROSUR and Frontex, we believe that their work will make a positive contribution to the protection of the United Kingdom and EU borders.**

Civil protection and disaster relief

103. The Communication calls for improvements in the efficiency and coherence of long-standing crisis and disaster management practices in responding to cross-sectoral threats such as those associated with climate change, terrorist and cyber-attacks on critical infrastructure, hostile or accidental releases of disease agents and pathogens, sudden flu outbreaks and failures in infrastructure. The response to the eruption of the Icelandic volcano Eyjafjallajökull in April 2010 demonstrated the need for a more coordinated approach among Member States in the way that they respond to natural disasters.

104. We considered the operation of the EU Civil Protection Mechanism, the coordination of EU early warning mechanisms, the role of SitCen and other situation centres in crisis management, as well as NATO's work in this area, in our short report on *Civil Protection and Crisis Management in the European Union*, which was published in March 2009.[152] We drew attention to the equivalence between the work of the EU and NATO Situation Centres, and also between the Commission's Monitoring and Information Centre (MIC) and the NATO Euro-Atlantic Disaster Response and Coordination Centre (EADRCC). The ICPEM considered that the Communication did not appear to take account of NATO's and Interpol's existing work in this area and cautioned against any efforts at EU level which would result in further duplication. They also cast doubt on the structure of the Strategy, stating that it appeared that civil protection matters had merely been "bolted" onto an existing security strategy by the Commission.[153]

The role of the armed forces

105. No reference is made in the Communication to the role of the armed forces in civil protection or disaster relief (or indeed in meeting any of the other objectives of the Strategy). The ICPEM considered this to be a serious omission. We also heard from Mr Wainwright that there was minimal engagement between Europol and the military community.[154] Although Dr Cornish thought its exclusion illogical he considered that this was probably due to "... neurosis within the European Union about military matters." He

---

[150] Q 242. These arrangements were previously considered in our report on FRONTEX: the EU external borders agency (9th Report, Session 2007–08, HL Paper 60).

[151] ISS 16

[152] 6th Report, Session 2008–09, HL Paper 43

[153] ISS 6

[154] Q 141

hoped that this would change over time,[155] and this view was echoed by Sir Richard Mottram.[156] Dr Simon Strickland, from the Civil Contingencies Secretariat in the Cabinet Office, stressed that the armed forces fell within the scope of the Solidarity Clause (discussed below) and that they had also played a key part in supporting external relief operations in Haiti after the earthquake. He suggested that the use of the armed forces would only be useful if there was no civilian alternative and that their deployment in a counter-terrorist role would be a matter solely for the Member State concerned.[157] James Brokenshire MP echoed all of these points.[158] The central role which over 100,000 Japanese military personnel, from the country's Self-Defence Forces, played in assisting with search and rescue operations following the earthquake and tsunami in March 2011, illustrates the importance of the contribution that the armed forces can make in such operations.

106. **We are surprised to find no reference to the armed forces in the Communication. They make a major contribution to civil protection and disaster relief, especially in the early stages. Their role must feature in the implementation of the strategy. We urge the EU institutions to give more thought to this.**

The Solidarity Clause

107. The entry into force of the Treaty of Lisbon in December 2009 saw the introduction of a new provision, Article 222 TFEU, which obliges the EU and the Member States to assist each other when a Member State is attacked by terrorists or experiences a natural or man-made disaster. The text of part of the article is reproduced in Box 7.

BOX 7

The Solidarity Clause

Article 222

(1) The Union and its Member States shall act jointly in a spirit of solidarity if a Member State is the object of a terrorist attack or the victim of a natural or man-made disaster. The Union shall mobilise all the instruments at its disposal, including the military resources made available by the Member States, to:

(a) prevent the terrorist threat in the territory of the Member States;

protect democratic institutions and the civilian population from any terrorist attack;

assist a Member State in its territory, at the request of its political authorities, in the event of a terrorist attack;

(b) assist a Member State in its territory, at the request of its political authorities, in the event of a natural or man-made disaster.

(2) Should a Member State be the object of a terrorist attack or the victim of a natural or man-made disaster, the other Member States shall assist it at the request of its political authorities. To that end, the Member States shall coordinate between themselves in the Council.

---

[155] QQ 200, 202 & 203

[156] Q 391

[157] Q 249

[158] QQ 421–423 & 440

108. The Communication makes reference to the implementation of the Solidarity Clause on the basis of a joint proposal from the Commission and the High Representative.[159] However, the Government did not seem at all enthusiastic about this prospect, appearing to be unclear as to what effect its implementation would have on the relationship between civilian and armed forces resources,[160] and considering that it would not necessarily alter Member States' current obligations in this area, legally or otherwise, to any significant degree.[161] We stand by the conclusion in our report on the Treaty of Lisbon,[162] where we said that **the Solidarity Clause does not seem to empower Member States to do anything which they could not do without it, or require them to do anything they would not otherwise be required to do. It does however serve to emphasise the political will of the Member States to stand together in the face of adversity.**

Risk assessments and cooperation between Situation Centres

109. The Communication commits the Commission to develop, with the Member States, a more coherent EU risk assessment policy by the end of 2010 for disaster management, covering all natural and man-made disasters.[163] The Government were enthusiastic about adopting a meaningful all-hazards approach to threat and risk assessment and considered that it might enable appropriate future contingency planning to take place in relation to disasters within the EU.[164] Other witnesses were also positive[165] and only the ICPEM expressed doubts about the utility of such a venture. They considered that achieving such an approach among 27 Member States, each of which tended to focus on the immediate hazards in their territory, would be very challenging.[166]

110. The Communication proposes better coordination between different Situation Centres' early warning systems and information-sharing arrangements, so that a more integrated approach can be adopted based upon common perceptions of a crisis situation.[167] We have already emphasised the need for such an approach in our previous report, including the importance of a close working relationship between the EU and NATO.[168] The Government would welcome moves to streamline what they consider to be a complex array of existing rapid alert and notification processes for crisis management, especially where this would result in the more efficient use of EU disaster management resources.

---

159 *The EU Internal Security Strategy in Action*, Objective 5, Action 1, p 13

160 Q 423

161 Q 248. See also Declaration 37 annexed to the Treaty of Lisbon.

162 *The Treaty of Lisbon: an impact assessment* (10th Report, Session 2007–08, HL Paper 62), paragraphs 6.346–6.349

163 *The EU Internal Security Strategy in Action*, Objective 5, Action 2, p 14. This has now been produced in the form of a Commission Staff Working Paper: Risk Assessment and Mapping Guidelines for Disaster Management, SEC (2010) 1626 final, 21 December 2010.

164 ISS 10

165 Symantec, ISS 14

166 ISS 6

167 *The EU Internal Security Strategy in Action*, Objective 5, Action 3, p 14

168 *Civil Protection and Crisis Management in the European Union*, pp 9–10

111. **We support more coordination between different Situation Centres and repeat our call for a closer working relationship between the EU and NATO situation centres. We also support a reduction in the number of existing rapid alert and notification processes for crisis management.**

The development of a European emergency response capacity

112. The Communication proposes the creation of a European Emergency Response Capacity (EERC) for tackling disasters.[169] It suggests that this will be based on pre-committed assets from Member States, which will be available on call for pre-agreed contingency plans and EU disaster relief operations internally as well as externally. A separate Communication dealing with its external response capacities was issued by the Commission a month before the ISS Communication.[170] As a result, both the ICPEM and the Government questioned whether the different Directorates General in Brussels were working in unison in this policy area.[171] While the Government supported a genuinely voluntary pool of pre-committed civil protection assets, they would "... resist moves to prioritise EU operations over national operations, or to introduce a legal presumption that Member States will pre-commit disaster response assets for EU deployment, or any move to limit the right of Member States to decide asset deployments domestically or internationally."[172] At the domestic level, the Government commissioned Lord Ashdown of Norton-sub-Hamdon to conduct a review of how the United Kingdom should respond to humanitarian disasters and emergencies in future; his report was published on 28 March 2011.[173]

113. When we asked Dr Simon Strickland how crises should be defined as either national or EU, he considered that a national crisis may develop an EU dimension in the following circumstances: "...when the response capability of an affected Member State is overwhelmed to the extent that that State calls for assistance through the civil protection mechanism; secondly, perhaps when designated European critical infrastructure is affected under the terms of the European programme for critical infrastructure protection Directive; and thirdly, when an emergency affects a number of Member States or the whole of the EU to the extent that the EU-level crisis co-ordination arrangements are activated or placed on alert, or are used with a view to political co-ordination of the response."[174]

114. **We have practical concerns about the operation of a European Emergency Response Capacity. We believe that any pre-commitment of assets should be on a voluntary basis, and that Member States should retain a discretion to decide how their assets are best deployed.**

---

169 *The EU Internal Security Strategy in Action*, Objective 5, Action 4, p 15

170 *Towards a stronger European disaster response: the role of civil protection and humanitarian assistance,* COM (2010) 600 final, 26 October 2010

171 ISS 6 & ISS 10. DG Humanitarian Aid & Civil Protection was responsible for the former Communication, while DG Home Affairs was responsible for the latter.

172 ISS 10

173 The Humanitarian Emergency Response Review, which is available at: http://www.dfid.gov.uk/Documents/publications1/HERR.pdf

174 Q 248

CHAPTER 5: CYBER-SECURITY

The challenge

115. Cyber-security is an issue of increasing concern to governments, businesses and individuals. The Government published the first Cyber Security Strategy for the United Kingdom in 2009,[175] and in the 2010 revision of the National Security Strategy (NSS) "hostile attacks upon UK cyber space by other states and large scale cyber crime" were raised to a Tier One priority risk, second only to international terrorism.[176] Professor Joseph Nye has categorised cyber attacks into four categories: (i) cybercrime; (ii) cyber espionage; (iii) cyber terrorism; and (iv) cyber warfare between States.[177] We regard this as a useful distinction.

116. The Communication has as its third objective the "rais[ing of] levels of security in cyberspace"[178] and the actions proposed bear primarily upon the first of Professor Nye's categories, though there are proposals also to improve capability for dealing with and responding to cyber attacks from any source. A recent report for the United Kingdom Office of Cyber Security and Information Assurance (OCSIA) estimated the cost of cybercrime to the United Kingdom on the most likely scenario to be £27 billion per annum.[179] The Director of Europol noted that within the EU over the previous year "approximately €100 billion of VAT fraud was committed by enterprising criminals on line, and that is just one aspect of it". "It [cybercrime] is a very good example of a transnational problem without a natural home."[180]

117. All of our witnesses thought it right that the EU should pay greater attention to cyber threats. We agree, and are glad to see the emphasis placed on cyber-security in the Communication.

118. The Commission had already published in April 2009 a Communication to the Council giving its views as to how the Member States might through the EU strengthen the security and resilience of their critical information infrastructures (CIIs) and develop their defences against cyber-attacks.[181] This was the subject of an earlier inquiry of this Committee which led to our report *Protecting Europe against large-scale cyber-attacks.*[182] In that report we

---

175 June 2009, Cm 7590

176 October 2010, Cm 7953, page 27

177 In a speech at the Munich Security Conference, 5 February 2011

178 *The EU Internal Security Strategy in Action*, Objective 3, p 10

179 *The Cost of Cyber Crime:* A Detica report in partnership with the Office of Cyber Security and Information Assurance in the Cabinet Office, February 2011, http://www.detica.com/uploads/resources/THE_COST_OF_CYBER_CRIME_SUMMARY_FINAL_14_February_2011.pdf

180 Q 135

181 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection: "Protecting Europe from large-scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" (COM(2009)149 final, Council document 8375/09). http://register.consilium.europa.eu/pdf/en/09/st08/st08375.en09.pdf. An assessment of the achievements to date was published on 1 April 2011: Communication from the Commission to the European Parliament, the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, on Critical Information Infrastructure Protection, "Achievements and next steps: towards global cyber-security" (COM(2011)163 final, Council document 8548/11).

182 March 2010; 5th Report, Session 2009–10, HL Paper 68

gave the attacks on Estonia in April and May 2007 as well-known examples of the way even relatively minor attacks can cripple the infrastructure of a State which is ill-prepared for them. Since then Stuxnet has provided a further example of the use of hostile cyber-attack.

BOX 8

Stuxnet

Stuxnet is a computer virus, first reported in June 2010, which is widely thought to have been designed by a major Western power, possibly together with Israel, specifically to disable, and possibly destroy, centrifuges at an Iranian uranium enrichment plant by greatly increasing their speed while disguising the fact that this was happening. President Ahmadinejad acknowledged at a news conference that "they succeeded in creating problems for a limited number of our centrifuges with the software they had installed in electronic parts."[183]

119. A more recent example, closer to home, shows the inadequacy of security measures in some Member States, and how this can be an invitation to cybercrime on a grand scale. The EU Emissions Trading System (ETS) is the largest carbon-trading scheme in the world with a turnover of more than €90bn in 2010. It is dealt with by the 30 national registries of the EEA States. After a number of security breaches in previous months in Austria, Greece, Poland and Estonia, a major cyber-attack on the Czech registry on 18 January 2011 led to the loss of some €30m worth of carbon allowances. The following day the Commission suspended transactions at all national registries until they could provide proof of adequate security measures. The United Kingdom was among the first five States allowed to resume operations on 4 February 2011. But it was only on 20 April 2011, more than three months after the attack, that security in the last five States[184] was thought adequate for them to be allowed to resume trading.

120. In 2012 the EU is to open its own registry for emissions trading, taking over from the national registries. This is likely to be a potential target for cyber-criminals, and it surprises us that, as Sir Richard Mottram told us, the EU does not seem to have realised that it is itself an attractive target, and that it should focus more on the security of its own systems.[185] Neil Thompson, the Director of the Office of Cyber Security and Information Assurance (OCSIA), stressed that EU institutions were not immune; that the EU could eliminate some of the weaknesses in its system by reducing the number of portals it operates; and that whoever had responsibility for the EU ETS had to take responsibility for its IT security. This, he said, was a matter of "basic computer hygiene".[186]

121. When we took evidence from the European External Action Service (EEAS) Mr Lars-Gunnar Wigemark, the Head of Security Policy at the Directorate-General for External Relations at the Commission (DG RELEX, the precursor of the EEAS), emphasised the importance of cyber-security which, he said, was much broader than cybercrime and involved national security

[183] In evidence to us (ISS 14) Symantec explained some of the technicalities of Stuxnet, but without offering views as to the identity of the designers of the virus or its target.

[184] Cyprus, Hungary, Liechtenstein, Lithuania and Malta

[185] Q 376

[186] QQ 298–300

interests. He thought that Member States had been reluctant to develop common positions, but he did not mention the security of the EU institutions.[187] He might have done so if he had known that DG RELEX and the EEAS would on 23 March 2011 be hit by a major cyber-attack which forced them to shut down external access to emails and the institutions' intranet, and required all staff to change their passwords. This was followed by an attack on the European Parliament the next day which was still continuing a week later.

122. **We congratulate the Government on the priority they give to cyber-security in the United Kingdom National Security Strategy. But there is no room for complacency. All Member States, individually and collectively, must devote greater resources and urgency to meeting this challenge, given that their overall security is only as strong as the weakest link.**

123. **The EU institutions should take the lead by ensuring the security of their own networks and agencies. They are a natural target for malicious and criminal attack; weaknesses have been and will be exploited. They must take responsibility for their own cyber-security; it is in the interests of the United Kingdom to help them to do so.**

The role of the EU

124. A number of our witnesses gave their views about the challenges of creating greater security in cyber space. Dr Cornish thought that cyberspace was a largely unregulated no-man's land in which a criminal could work with relative impunity.[188] Mr Thompson talked of the "scale, pace and complexity of the cyber-security challenge", creating what he called a policy lag.[189] He also emphasised the importance of connecting with the private sector;[190] in our earlier report we too stressed the need for a close working relationship between Governments and the private sector.[191]

125. In that report we also stressed that cyber-security is a global matter to combat a global problem, and that the EU had an important role to play in coordinating the parts played by the Member States.[192] Symantec, a worldwide leader in internet security, wrote: "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 …"[193] The danger of a fragmented response by Member States with different legal regimes, different offences and different prosecution systems was explained by CEPS, which gave the Wikileaks affair as an example of the problems raised.[194]

---

[187] Q 86

[188] Q 180

[189] QQ 270, 292.

[190] Q 270

[191] *Protecting Europe against large-scale cyber-attacks*, paragraphs 72–79

[192] *Ibid*, Chapter 3: Is there a role for the EU?

[193] ISS 14

[194] ISS 2

126. **We strongly welcome the emphasis on cyber-security in the Communication and believe that this is an urgent and fast evolving challenge in which the EU can play an important part in raising standards and awareness in the Member States.**

127. The Commission had already proposed, in September 2010, a Cybercrime Directive to replace and bring up to date the 2005 Framework Decision on attacks against information systems.[195] We recommended that the United Kingdom should opt in to this proposal, and the Minister wrote to say that the Government had done so.[196] We welcome this.

The Budapest Convention

128. The Council of Europe has also had a role to play. It is now nearly 10 years since the first international treaty on crimes committed via the internet and other computer networks was signed at Budapest, on 23 November 2001. Its main objective is to pursue a common policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation. It deals in particular with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception.

129. The Budapest Convention entered into force on 1 July 2004, but not for the United Kingdom. Nearly 10 years after the Convention was opened for signature the United Kingdom has still not ratified it. It is in force in every other major Member State except Poland, and in most smaller States. The minister conceded that this "portrayed an indication, maybe wrongly, that this country was not serious on this", and he assured us that ratification would be "this year … we are literally in the final stages of dotting the i's and crossing the t's in relation to ratification".[197]

130. In a speech to the Munich Security Conference on 4 February 2011 the Foreign Secretary, the Rt Hon William Hague MP, said: "We have a major opportunity to promote the Budapest Convention on Cyber Crime, which the UK will look to do when we chair the Council of Europe from November." If the United Kingdom is to promote the Convention, we hope that it will have deposited its instrument of ratification no later than the end of July, since the Convention will not otherwise be in force for the United Kingdom when it assumes the Chairmanship.

131. **We welcome the Government's commitment that the United Kingdom will ratify the Budapest Convention before the end of this year.**

Cybercrime Centre

132. The Commission's first and most significant proposal for action under this chapter is to establish a Cybercrime Centre.

---

[195] Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (COM(2010)517, Council document 14436/10)

[196] Letter of 27 October 2010 from the Chairman to Mr James Brokenshire MP, Parliamentary Under-Secretary of State, Home Office, and reply of 31 January 2011.

[197] Q 414

BOX 9

The Cybercrime Centre

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. The centre will improve evaluation and monitoring of existing preventive and investigative measures, support the development of training and awareness-raising for law enforcement and judiciary, establish cooperation with the European Network and Information Security Agency (ENISA) and interface with a network of national/governmental Computer Emergency Response Teams (CERTs). The cybercrime centre should become the focal point in Europe's fight against cybercrime.[198]

133. It is a matter for some regret that we received more evidence about where this Cybercrime Centre should be located than about whether it would be useful to set up such a body in the first place. However, Dr Cornish had reservations: "… the problem of cyber-security is still too young and too indistinct to be absolutely confident that what is needed right now or by 2012 is a cyber-crime Centre run within the European Union".[199] The Government in its written evidence did not favour setting up such a centre, pointing out that "… the Communication is at variance with the ISS in suggesting the establishment of new EU structures and capacities for tackling cyber crime, including the development of an EU cyber crime centre. We believe that any action to tackle cyber crime arising out of the Commission's Communication should be undertaken within existing structures …"[200]

Functions

134. Symantec, while welcoming "in theory" the setting up of a Cybercrime Centre, thought it was not clear what role the Centre would in fact play; there should be further discussion on the aims and objectives of the Centre, and how its work might be structured. These discussions should include an input from industry: "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".[201]Dr Cornish thought that, if such a Centre were set up, he would also like it "to focus very hard on the problem of cyber forensics and cyber attribution".[202] JANET(UK), while welcoming the idea of a complementary body to gather and promote good practice in dealing with cybercrime, doubted that it should have a direct operational role, since this "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."[203]

---

198 *The EU Internal Security Strategy in Action*, Objective 3, Action 1, p 10

199 Q 178

200 ISS 10

201 ISS 14

202 Q 180

203 ISS 4. JANET(UK) is the operator of JANET, the United Kingdom'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.

135. Most of our other witnesses favoured setting up a Centre with the functions envisaged by the Commission, but thought it should be additional to and not in place of national capacity. Mr Thompson stressed that no Centre or agency could compensate for weak national capacity; the United Kingdom was looked at as one of the stronger European countries, but its own capacity was still weak. He did not think that creating an agency and expecting it to fix the problem was "quite aligned to the reality of where we are now".[204]

Location

136. The Commission Communication did not say expressly where the Centre should be located, but if it is to be "within existing structures" only two already existing bodies are possible: Europol or ENISA, the European Network and Information Security Agency. Since the Commission envisages that the new Centre should "establish cooperation with ENISA" it seems that it must envisage a Centre located within Europol. This was confirmed by Commissioner Malmström: "The Cybercrime Centre would, as I see it, be set up at Europol and build on what already exists in Europol. I am not talking of having a new big agency but of pooling a few resources there, working closely with Member States. Europol already has some capacity and some knowledge on this and it will be natural to build on that and not create anything new … if we want to focus on the crime issue, it would be more natural to put it under Europol."[205]

137. None of our witnesses, not even ENISA in its written evidence, suggested that ENISA would be an appropriate location for the Centre, and nor would we. Even if cybercrime fitted with ENISA's current task of promoting cooperation and best practice in the field of cyber-security, we would not recommend giving these duties to an agency located in Heraklion. In our earlier report we pointed to the many problems caused by the location of an EU agency in Crete,[206] and we are not alone in this view.[207]

138. We remain concerned about the dispersal of EU agencies working in the field of cyber-security and cybercrime, most recently exacerbated by the decision that the new agency to manage the large-scale EU IT systems[208] should be shared between Strasbourg, where the infrastructure remains, and Tallinn, where the management will be.[209] We received no evidence suggesting that the Cybercrime Centre should be a new free-standing agency; all witnesses thought, like the Commissioner, that Europol would be the appropriate location. The most enthusiastic, perhaps not surprisingly, was Europol itself. In its written evidence it stated: "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 [i.e. Europol] could play a primary role in the establishment of the future entity. Dispersion of investigative and

---

[204] Q 278

[205] Q 19

[206] *Protecting Europe against large-scale cyber-attacks*, paragraphs 112–120

[207] This would remain our view even if more of ENISA's activities were moved to a centre in Athens, as is envisaged by the European Parliament.

[208] The Schengen Information Systems (SIS and SIS II), the Visa Information System (VIS), and Eurodac, the fingerprint database for the Dublin Regulation on jurisdiction to examine asylum applications.

[209] Agreed at the Justice and Home Affairs Council on 2 December 2010

analytical capacities in the fight against cybercrime should be avoided in order to safeguard the necessary coordination and cost-effectiveness."[210]

139. In his oral evidence Mr Wainwright was equally emphatic: "We have forensic experts at Europol who can improve the capacity for domestic law enforcement to investigate cybercrime offences. As a package, although rather small-scale at the moment because of our resource limitations, it already holds a key to the future elaboration of the EU cybercrime centre and that is the model that we would like to take forward …"[211] Finally, in a document dated 21 December 2010 addressed to the Commission but shown to the Committee, Europol put in what was in effect a formal bid for the Cybercrime Centre to be hosted by Europol.

140. The Minister, while not expressly supporting the creation of a Cybercrime Centre, told us that if such a Centre were set up, Europol would be the right place for it. He added: "I do not think there is any reason to question that Europol would have the skills and capabilities to develop a centre. The High Tech Crime Centre has been housed in Europol since I think around 2002, and provides valuable experience in this area that can be drawn upon. So I think in that sense it is the obvious place to put this."[212]

141. Cooperation between the new centre and ENISA is envisaged by the Commission in its Communication, and the Commissioner said: "We also want to enlarge the competences of ENISA".[213] Negotiations are currently taking place on a Regulation increasing the scope of ENISA's activities.[214] Our witnesses agreed that such a centre should work alongside ENISA, and Peter Storr supported the extension of ENISA's role to include law enforcement cooperation on cybercrime issues.[215]

Funding

142. In October 2010 the Government announced: "The National Cyber Security Programme will be supported by £650 million of new investment over the next four years".[216] This commitment, which was welcomed on all sides, seems to us to be an express acknowledgement by the Government that, even in times of financial austerity, cyber threats cannot be combated without additional resources. Yet the Government told us in their written evidence that they believed that any action to tackle cyber crime arising out of the Commission's Communication, including the creation of a Cybercrime Centre, should be undertaken not only within existing structures, but also within existing budgets.[217] The Director of Europol told us that some additional resources would be needed, though he did not put a figure on them.[218]

---

[210] ISS 11

[211] Q 135

[212] Q 415

[213] Q 16

[214] Proposal for a Regulation of the European Parliament and of the Council concerning the European Network and Information Security Agency (ENISA) (Document No 14358/10)

[215] Q 255

[216] Strategic Defence and Security Review, Cm 7948, paragraph 4.C.3.

[217] ISS 10

[218] Q 136

143. Peter Storr told us: "we wouldn't accept that automatically when there is a new mandate it should be accompanied by an increase in resources."[219] He subsequently qualified this: "I don't think I was suggesting that we would block or be opposed to an increase in the Europol budget to deal with cyber-security as a sort of principle … what one would look to Europol to do, as one would look to other European bodies, is to make out a properly costed, well-argued business case …"[220] But the Minister was more explicit: "We think it [Europol] can do that within existing resources."[221]

144. Sir Richard Mottram, while conceding that this addition to Europol's work could "probably not" be done without additional resources, added that he was "always suspicious … of the argument that your highest priority, because it is new and difficult and needs to be tackled, calls for additional resources. It often calls for a reallocation of priorities."[222]

145. We believe that additional resources are needed, but they need not be the "staggering sums" which Mr Thompson said the United States was investing in cyber-security.[223] Mr Wainwright told us: "We [Europol] already have some experts in this field. I hope that we could supplement those with at least some others from national cybercrime centres, including one that will be established in the next year or so at SOCA here in London. Certainly, I will be making those overtures to national agencies like that in order to demonstrate to them that cybercrime investigations centred in the UK will, by their very nature, have a European, if not global, dimension, and that there are many strong reasons—even operational reasons—why they should invest in common European arrangements so that we can better support their work at the national level."[224]

146. **The establishment of a Cybercrime Centre will enhance the EU's ability to contribute in this area. This is not an end in itself, but only one of many measures that must be deployed.**

147. **Europol would be best placed to host such a body. However, we believe that finding staff with the necessary expertise may not be easy. Additional staff and funding will be essential if the Cybercrime Centre, wherever it may be situated, is to achieve its key aims. The Government's view that this can be done within existing resources is unrealistic, and inconsistent with their making additional resources available for the United Kingdom's programme.**

148. **We believe that the Centre should form a close working relationship with ENISA, and we support the extension of that agency's role and mandate to cooperate with law enforcement agencies.**

149. **The dispersal of agencies dealing with cyber matters is especially unfortunate. In particular, we continue to have concerns about ENISA's ability to operate effectively from its geographical location. We endorse the European Parliament's proposal that the agency's operations could be "frontloaded" in Athens.**

---

[219] Q 237

[220] Q 256

[221] Q 415

[222] Q 371

[223] Q 317

[224] Q 139

Improving response capabilities

150. Mr Thompson explained that one of the reasons cybercrime was a growing problem, both nationally and internationally, was that cyberspace gave criminals anonymity; it was very easy to conduct crime in that space, and not enough was done to deter criminals by building up the judicial and legal capacity to deal with criminals when they were detected. But he added that there was agreement that "you could not prosecute your way out of this problem"; States had to raise their cyber-security standards.[225]

151. The Commission's proposals for raising standards centre on computer emergency response teams, or CERTs: "First, every Member State, and the EU institutions themselves, should have, by 2012, a well-functioning CERT".[226] This is a repetition of the recommendation made by the Commission in its 2009 Communication on Protecting Europe against large-scale cyber attacks[227] which was the subject of our earlier report. We discussed CERTs at some length in that report.[228] Then too the Commission appeared to be recommending that each Member State should have a single CERT. We supported this suggestion in the case of those member States, mainly in Eastern Europe, which have inadequate CERTs, or even none at all. But there is no need for this in those Member States which have a well-developed system of CERTs. We explained that in the United Kingdom GovCertUK is the CERT for the public sector, but the majority of the CERTs are in the private sector, in large companies or in organisations with a common interest.

152. JANET(UK) said: "…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".[229] We note the words "at least". Symantec, while supporting the proposal in the Communication, pointed out that "The CERT model is flexible to enable Member States to develop multiple CERTs, or different types of CERTs …"[230]

153. Neither of these witnesses, nor any of those who gave evidence to our previous inquiry, suggested that the United Kingdom (or other States with a well-developed system of multiple CERTs) should abandon this in favour of a single national CERT. We urged the Commission to clarify its position. In its response to the report it stated: "It is not the intention of the European Commission to impose a 'one size fits all' model with regard [to] the organisation of such capability, which is left to the discretion and experience of Member States." We were glad to read this, but regret that this is still unclear in the ISS Communication.

154. As Mr Thompson emphasised, international cooperation is important in terms of sharing best practice and experience, as well as raising the standards in weaker States.[231] This is one of the roles of ENISA, though it is very

---

225 Q 273

226 *The EU Internal Security Strategy in Action*, Objective 3, Action 3, p 11

227 See paragraph 118 above

228 Paragraphs 57–71

229 ISS 4. CSIRT stands for Computer Security Incident Response Team, and is synonymous with CERT.

230 ISS 14

231 Q 283

conscious that its current role is to supplement the responses of Member States which "are best positioned to defend their own infrastructures".[232] ENISA has already coordinated the first pan-European cyber-security exercise (Cyber Europe 2010). The Commission envisages that ENISA should continue to help Member States to develop national contingency plans and to undertake exercises in incident response and disaster recovery.

155. **Many Member States already have an adequate emergency response capacity and do not need to change their existing CERT structure. But it is essential that every Member State should have an adequate emergency response capacity, and this may need to take the form of a national CERT. Where this is lacking, it should be addressed as a matter of urgency. Individual weaknesses will undermine the collective security of the EU.**

Raising public awareness

156. Many of our witnesses regretted the low level of awareness generally of vulnerability to cyber attacks and cybercrime. Dr Cornish considered that there was a very low level of "cyber consciousness" in the United Kingdom; that a lot of "soft" work needed to be done to raise awareness of the threat; that the threat developed so quickly that institutional responses could become obsolete; that a "culture change" was needed across the EU; and that there was a need for the formulation of a "common language and definitions".[233] Mr Thompson considered that the United Kingdom had a "good track record" in addressing cyber-security across Government in cooperation with the private sector,[234] but he thought that the EU could play an important role in raising awareness of the risks among citizens and businesses,[235] including the organisation of an "EU-wide public awareness campaign".[236]

157. Other witnesses too thought that the EU had an important role to play. The Commission's proposal is headed "Work with industry to empower and protect citizens." Sir Richard Mottram emphasised the importance of bringing together government officials, senior industry figures and technical experts to develop a deep understanding of the problem.[237] Mr Thompson mentioned that the EU had done this in the past—bringing together "consortia of academics and industry partners"—and more work in this area would be welcome.[238] ENISA advocated improving cooperation between the public and private sectors as well as raising public awareness through the inclusion of "information security" lessons within the school curriculum. Symantec was one private sector organisation which said it was very willing to work with the public sector in this area. However ways still need to be found to harness private sector expertise effectively.

158. The Communication suggests that all Member States should make it easier for people to report cybercrime incidents, and should encourage them to do

---

[232] ISS 5

[233] QQ 176–177

[234] Q 270

[235] Q 275

[236] Q 285

[237] Q 383

[238] Q 289

so. The information, once evaluated, could then potentially feed in to a European cybercrime platform.[239] The Commissioner has encouraged the private sector to report cyber incidents.[240] This was supported by Mr Thompson, who said that it was already very much the approach of the United Kingdom and other Member States.[241] We accept however that organisations may be reluctant to report such incidents because of concerns that this may reveal weaknesses, undermine public confidence and credence with regulatory authorities, and perhaps increase the likelihood of further attacks.

159. **A strong working relationship between the public and private sectors will be crucial in raising awareness of the threats from cyberspace. This needs to happen at both Member State and EU level through joint forums involving all of the key players. The EU can and should add value in this area by improving public awareness.**

International cooperation

160. We have already explained in Chapter 3 the importance for security generally of improving relations with international organisations and with strategically important third countries. This is particularly true of cyber-security, which almost by definition is a global problem that requires a global response.

161. It was therefore a particular concern to us to hear the evidence of Dr Cornish. Two years previously he had written a report for the European Parliament in which he examined the level of collaboration among a set of organisations—European Union, NATO, OECD[242] and UN—and his broad conclusion was that there was then "next to no collaboration, partly because they had no common understanding of what they were talking about. There was no common lexicon. There was no common doctrine. There was nothing common really. There were lots of good well-intentioned people in good organisations trying to do their best, but there was no coming together." The organisations did not all have to do everything, but the chances that any one institution could solve the problem within its own remit seemed to him to be slim.[243]

162. Dr Cornish told us that the relationship between EU and NATO was "the big problem". His sense was that there was unlikely in the near future to be a good collaborative effort between the two organisations. NATO with its Emerging Security Challenges department was looking at the possibility of cyber-warfare or war, and how NATO would react to it: whether it would invoke Article 5,[244] which was clearly a NATO concern. But NATO did not look at cybercrime as a discrete problem, which the European Union clearly did. This unfortunate situation is no more than the specific application to cyber-security of the general relationship between the two organisations which we have considered in Chapter 3.[245]

---

239 *The EU Internal Security Strategy in Action*, Objective 3, Action 2, p 11

240 Speech at an APCO lunch debate, 8 February 2011

241 Q 281

242 Organisation for Economic Cooperation and Development

243 Q 183

244 Under Article 5 of the North Atlantic Treaty each State undertakes to treat an armed attack on one of them as an attack on all of them.

245 Paragraphs 53–57

163. Cooperation with others seems to be better. As far as the US and the European Union are concerned, Dr Cornish told us that there was a working group on cyber-security running which was to report later this year; he thought this would be "a very high level and a very serious effort."[246] Dr Steve Marsh, deputy director of the Office of Cyber Security and Information Assurance, pointed out that there were other international institutions operating in the area, in particular the International Telecommunications Union and the Internet Governance Forum. Mr Thompson added that the Foreign Office was building additional capacity to deal with these fora.[247]

164. **The global nature of the cyber threat requires an international response. Proactive collaboration within the international community, including the EU, UN and NATO, will be indispensable if agreement is to be reached on the nature of the threat, and on whether it can realistically be addressed.**

165. In his Munich speech to which we have referred in paragraph 127, the Foreign Secretary set out the benefits which the internet could provide, but explained how our reliance on it opened up new channels for hostile governments, enabled terrorist networks to plan atrocities, and provided rich pickings for criminals. He added: "Cyber-security is on the agendas of some thirty multilateral organisations, from the UN to the OSCE and the G8 … But much of this debate is fragmented and lacks focus. We believe there is a need for a more comprehensive, structured dialogue to begin to build consensus among like-minded countries and to lay the basis for agreement on a set of standards on how countries should act in cyberspace … the UK is prepared to host an international conference later this year to discuss norms of acceptable behaviour in cyber-space, bringing countries together to explore mechanisms for giving such standards real political and diplomatic weight." Mr Brokenshire confirmed that the international conference would be held in the autumn of this year, with attendance by invitation only to governments with a "major stake" in the matter as well as international organisations and representatives from the private sector and academia. But he did not want to pre-empt the results of that process by speculating as to whether an agreement would be reached.[248]

166. **We commend the United Kingdom initiative to host an international conference on cyber-security, and hope that a wide range of countries and organisations with a legitimate interest will be invited. We look forward to considering the outcome and the effect it may have on the EU.**

---

[246] Q 183

[247] Q 309

[248] QQ 417–418

CHAPTER 6: IMPLEMENTING THE STRATEGY

167. The Communication states that the responsibility for the implementation of the strategy will be shared between the EU institutions (including the European External Action Service), EU agencies and the Member States.

168. There did not seem to be any appetite among our witnesses for the creation of any new bodies or agencies in this area, as illustrated by the consensus that the cybercrime centre should be established within Europol. The Government's evidence also emphasised that the Strategy's implementation should focus on reinforcing existing structures rather than creating new ones, while adopting a practical rather than a legislative approach.[249] This is consistent with their stance on the Stockholm Programme, which we have considered in a separate report.[250]

169. **We note the Government's emphasis on practical cooperation, but do not believe that this should exclude further EU legislation if that should prove necessary. We reiterate the importance of adopting a flexible approach in order to respond in an effective manner to unforeseen events raising issues of internal security.**

Council and Commission structures

170. The Government's preference is that no new bodies should be created. During our inquiry we became concerned about the number of existing working groups, working parties and other bodies which have a role in EU internal security, and the potentially detrimental impact that this structure may have on the EU's and the Member States' ability to implement the Strategy effectively. Certainly in the past the reaction to a problem seems all too frequently to have been to set up a new body to consider it. **A fundamental culture change within the EU institutions is needed to achieve a more effective approach, including in particular more integrated working and investment in the necessary training**.

171. Professor Mitsilegas considered that there was a "... considerable lack of clarity regarding the mandate, functions and accountability of EU bodies working in the field of internal security"[251] and Hugo Brady talked of the "... plethora of DGs, agencies and bodies dealing with internal security matters" which he considered often failed to work together properly and were suspicious of each other. With regard to the Commission, he considered the lack of coordination between the different Directorates-General to be problematic, stating that DG Enterprise and Industry's control over the security research budget paid little regard to the policy priorities of DG Home Affairs, while the latter DG had only met with DG Transport once to discuss recent concerns over the safety of air cargo controls. He concluded that there was a need for "... radical thinking on how best to coordinate the various pieces of the EU bureaucracy involved in security matters."[252][253]

---

[249] ISS 10

[250] *Implementing the Stockholm Programme: home affairs* (9th Report, Session 2010–11, HL Paper 90)

[251] ISS 15

[252] ISS 12

[253] The Communication refers to "the recently published Digital Agenda for Europe which addresses issues related to cybercrime, cyber security, safer internet and privacy…". This was prepared, not by DG HOME under the responsibility of Commissioner Malmström, but by DG INFSO (Information Society) under the responsibility of Vice-President Neelie Kroes, the Commissioner responsible for the Digital Agenda.

172. The creation of the new Standing Committee on Operational Cooperation on Internal Security (COSI) was intended to reduce, or at least rationalise, the number of Council bodies with a role in internal security. According to the Home Office some limited rationalisation has already taken place following a review of JHA working structures which took place after the entry into force of the Treaty of Lisbon and which was designed to make the Council structures more efficient.[254] However this seems to have resulted only in the merger of the Police Cooperation Working Group and the Europol Working Party into the Law Enforcement Working Party, and in the absorption of the European Police Chiefs Task Force into COSI. While it is not completely clear which bodies continue to exist and which have been subsumed into new arrangements, it appears that a number of other bodies continue to exist. A selection of these bodies which all operate under the aegis of the Justice and Home Affairs Council, as well as those operating outside of the EU structures, are summarised in Box 10. These bodies sometimes meet in "Mixed Committees" with non-EU States. These are usually Iceland, Liechtenstein, Norway and Switzerland.

BOX 10

Council working groups, parties, committees and other bodies

Article 36 Committee (CATS: Comité de l'article trente-six) was established under Article 36, TEU, following the treaty of Amsterdam, and has a coordinating role regarding police and judicial cooperation in criminal matters. Despite the repeal of its treaty base by the Treaty of Lisbon, it will continue to operate as a Council working party until 1 January 2012 at which point its utility will be evaluated by COREPER.

Counter Terrorism Group (CTG) was established in 2001 and is composed of the heads of all Member States' security and intelligence services, as well as their counterparts in Norway and Switzerland. It composes terrorism threat assessments and radicalisation analysis, as well as assisting with the coordination of operational activities. It sits outside EU structures but its chair rotates in accordance with the changing EU Presidency.

Customs Cooperation Working Party (CCWP) was established in 2003 and is responsible for improving cooperation between Member States' customs authorities in order to improve the fight against customs infringements and the control of the movement of goods over the EU's external borders. It occasionally holds joint meetings with the LEWP.

European Police Chiefs Task Force (EPCTF) was established in 2000 as an informal body and consists of national chief police officers. It sat outside of EU structures, with a rotating chair in accordance with the EU Presidency. Its role has now been assumed by COSI, including its work on the Comprehensive Operational Strategic Plan for Police (COSPOL).

Justice and Home Affairs External Working Group (JAIEX) is an information and cooperation group to strengthen relations between the JHA Council and Commission DG RELEX at all levels. It prepares matters to be dealt with in other Council working parties such as the Article 36 Committee and the Committee on Civil Law Matters.

[254] ISS 10 (supplementary memorandum). See also *Implications of the Treaty of Lisbon provisions for the JHA working structures*, Council Document 17653/09, 16 December 2009.

Law Enforcement Working Party (LEWP) was established in 2010, as a result of the JHA working structures review, and is a merger of the Police Cooperation Working Group (PCWG) and the Europol Working Party (EWP). It deals with general issues of police cooperation and law enforcement.

Police Working Group on Terrorism (PWGT) was established in 1979 as an informal body and consists of members of Member States' anti-terrorism units, as well as their counterparts in Norway and Switzerland. Its main tasks are information exchange, intelligence gathering and operational cooperation. It is not a formal Council working group and also sits outside EU structures.

Strategic Committee on Immigration, Frontiers and Asylum (SCFIA) was established in 2000, following the Treaty of Amsterdam, and coordinates the work of the various working groups, including guidelines, in the field of migration, visa, borders and asylum and also has responsibility for the development of a common European asylum and immigration policy. Like CATS, its continuing existence will also be evaluated in 2012.

Terrorism Working Group (TWG) was established following the Treaty of Maastricht, under the old JHA pillar, and consists of representatives from Member States' interior ministries. It focuses on internal security threats and only considers law enforcement cooperation aspects. It occasionally has joint meetings with COTER so that the internal and external threats can be considered in unison.

Working Party on the application of specific measures to combat terrorism (CP 931) was established in 2001 and is responsible for examining proposals for the listing and de-listing of persons, groups and entities on 'terrorism lists'. It is composed of delegates from the interior and foreign ministries of each Member State.

Working Party on Cooperation in Criminal Matters was established in 1992 and is mainly concerned with the mutual recognition of criminal acts and judgments. In this respect it has responsibility for matters concerning the European Arrest Warrant (EAW).

Working Party on General Matters, including Evaluations was reformulated in 2010 as a result of the JHA working structures review and was formerly called the Multidisciplinary Group on Organised Crime (MDG). It has a coordinating role and deals with organised crime matters, excluding terrorism, that are not covered by COSI or other working parties as well as all evaluation mechanisms that will be set up under Article 70 TFEU.

Working Party on Integration, Migration and Expulsion deals with questions relating to third country nationals' entry into, residence in and removal from the territory of Member States. It was previously called the Working Party on Migration and Expulsion and was renamed in 2010.

Working Party on Terrorism (COTER) was established following the Treaty of Maastricht under the CFSP pillar and is composed of officials for Member States' foreign ministries. It focuses on external security threats and also has responsibility for the implementation of UN Conventions, the EU Counter-Terrorism Strategy and the Strategy for Combating Radicalisation and Recruitment to Terrorism.

173. By contrast, other witnesses emphasised the flexibility of the existing system. While William Shapcott referred to an "alphabet soup" of different bodies, he clarified that some were concerned with policy formulation and others with operational coordination, and concluded that it was "... essentially a permissive environment in which Member States can cooperate, liberally and bilaterally, and use these European instruments when they want to."[255] Mr Wainwright on behalf of Europol agreed but did not seem to be aware of the demise of certain bodies, maintaining that the European Police Chiefs Task Force and the Police Cooperation Working Group would continue to work best if they sat outside the formal institutional architecture.[256]

174. The Council's conduct and discharge of its business, including the configuration of different working groups, is the preserve of the Member States. The Home Affairs Commissioner was accordingly reluctant to make representations to the Council, regarding it as a "sensitive" issue.[257]

175. Following the limited review of the Council structures which took place after the entry into force of the Treaty of Lisbon, it continues to be unclear how many bodies are still in existence, what their remits are and how they interrelate with each other. **The work of Council groups involved in internal security should be further streamlined, with a reduction in their number as an overall objective. We also urge the different parts of the Commission to coordinate their work more closely.**

The Standing Committee on Operational Cooperation on Internal Security (COSI)

176. Article 71 TFEU provides for the establishment of a Council standing committee in order to ensure that operational cooperation on internal security is promoted and strengthened within the EU. A Council Decision to establish COSI was duly adopted on 25 February 2010[258] and excerpts from that Decision concerning COSI's functions are reproduced in Box 11.

BOX 11

COSI

Article 2

The Standing Committee shall facilitate, promote and strengthen coordination of operational actions of the authorities of the Member States competent in the field of internal security.

Article 3

1. Without prejudice to the mandates of the bodies referred to in Article 5, the Standing Committee shall facilitate and ensure effective operational cooperation and coordination under Title V of Part Three of the Treaty, including in areas covered by police and customs cooperation and by authorities responsible for the control and protection of external borders. It shall also cover, where appropriate, judicial cooperation in criminal matters relevant to operational cooperation in the field of internal security.

---

255 QQ 42 & 45

256 Q 147

257 QQ 27 & 28

258 Council Decision of 25 February 2010 on setting up the Standing Committee on operational cooperation on internal security, OJ L52 (3 March 2010) p 50

2. The Standing Committee shall also evaluate the general direction and efficiency of operational cooperation; it shall identify possible shortcomings or failures and adopt appropriate concrete recommendations to address them.

3. The Standing Committee shall assist the Council in accordance with the provisions of Article 222 of the Treaty [*the Solidarity Clause*].

Article 4

1. The Standing Committee shall not be involved in conducting operations, which shall remain the task of the Member States.

2. The Standing Committee shall not be involved in preparing legislative acts.

Article 5

1. When appropriate, representatives from Eurojust, Europol, the European Agency for the Management of Operational Cooperation at the External Borders of the EU Member States (Frontex) and other relevant bodies shall be invited to attend, as observers, the meetings of the Standing Committee.

2. The Standing Committee will help ensure consistency of action by those bodies.

Article 6

1. The Standing Committee shall regularly submit a report to the Council on its activities.

2. The Council shall keep informed the European Parliament and the national Parliaments of the proceedings of the Standing Committee.

Preliminary steps

177. COSI's first meeting was held on 11 March 2010, and it has met regularly since.[259] At this point, beyond draft agendas, very little has been published about its activities.[260] Its main role is to coordinate the actions of Member States and EU agencies, as well as acting as the guardian of the Strategy and its implementation, monitoring progress through the publication of annual reports to the European Parliament and Council. Its creation was also intended to avoid duplication and unnecessary overlap between the numerous Council working groups and also to ensure more effective coordination between different EU agencies. However, as we have already seen, while it has assumed the operative role of the European Police Chiefs Task Force, a plethora of other Council bodies continue to exist, and the rationalisation that was foreseen before its creation has yet to be achieved. In the short term it seems that the establishment of COSI has simply added a new layer to an already crowded network.

178. Many witnesses commented on the slow start which COSI had made since its establishment.[261] This may, in part, be explained by the fact that it is a

[259] Subsequent meetings have been held on 30 April, 25 June, 7 September, 5 October, 24 November 2010 and 9 February 2011.

[260] The draft agendas and some other Council documents are available through CONSILIUM at: http://www.consilium.europa.eu/

[261] E.g. Dr Claudia Hillebrand (ISS 9), William Shapcott (Q 42), Sir Ian Andrews (Q 347), James Brokenshire MP (Q 424).

relatively new body which is still finding its place within the Council apparatus. However, more specifically, William Shapcott suggested that COSI may be being held back and undermined by the continuing existence of its predecessor—the Article 36 Committee (CATS). For this reason he hoped that CATS would "fizzle out" eventually[262] but it seems that the Council will only review its continuing existence by early 2012 at the earliest.[263] CATS was established as a working group by virtue of Article 36 TEU to coordinate activity in a narrower area than that for which COSI now has responsibility: essentially this comprised matters which fell under the old third pillar (police and judicial cooperation in criminal matters). Its treaty base has disappeared following the entry into force of the Treaty of Lisbon, and (unlike COSI) no implementing legislation was adopted in relation to its operation, so it is questionable why this body continues to exist. Mr Wainwright expressed the hope that COSI would "... survive in the institutional treacle of Brussels that is often a problem", while also considering that it suffered from a lack of identity as a result.[264] Peter Storr thought that, in the long term, COSI should emerge as the "only show in town."[265]

179. **We trust that over time COSI will emerge as the lead organisation in all matters of EU internal security, and that this will provide the opportunity for other groups and bodies to be rationalised and their number reduced.**

Membership

180. With regard to COSI's membership, Mr Wainwright remarked that it was currently composed of a mix of senior police officers, interior ministry officials and "even lawyers" which gave it a sometimes complex character that could inhibit the right kind of dialogue from taking place. His preference was for more senior law enforcement officials and police chiefs to attend future meetings rather than interior ministry officials,[266] and SOCA echoed this view.[267] Peter Storr confirmed that the United Kingdom representatives have, in the past, included a senior director of SOCA, and himself as International Director at the Home Office. He also considered that a greater number of law enforcement officials at future meetings would be desirable.[268] We understand that representatives of EU agencies such as Frontex and Europol may also attend COSI meetings, but the Commissioner informed us that she had not yet been invited.[269]

181. **We believe that COSI would benefit from having greater consistency and continuity in its membership. The Home Affairs Commissioner should also be invited to attend each meeting of COSI as a matter of course.**

Chairing arrangements

182. The chair of COSI changes every six months in line with the rotating EU Presidency. We were concerned that this might have a detrimental impact on

---

262 QQ 62–65

263 http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/111615.pdf

264 Q 143

265 Q 234

266 Q 145

267 Q 345

268 Q 227

269 Q 30

its effectiveness and continuity. Peter Storr suggested that this problem was partially solved by the new "trio" approach which the successive EU Presidencies now adopt.[270] We nevertheless considered that there would be benefit in having a more permanent chairmanship. We have considered a similar situation with regard to the chairmanship of Europol Management Board in a separate report.[271]

183. **COSI would benefit from less frequent changes in its chairmanship. It is a less political body than the Council, so there is no conceivable logical connection between the nationality of the person best qualified to chair COSI and the identity of the Member State holding the Presidency. We believe that a suitably qualified chairman of COSI should be appointed for a minimum period of two years, renewable once.**

Transparency and parliamentary oversight

184. Dr Hillebrand from the Department of War Studies at King's College London expressed concern about the lack of transparency surrounding COSI's role and mandate, as well as the lack of public information which was available regarding its work, which she considered undermined its public accountability.[272] Peter Storr conceded that more needed to be done to increase people's understanding of its role[273] and SOCA considered that it should be as "visible and transparent" as any other EU body.[274] In order to boost its profile, Hugo Brady considered that COSI should make public a "list of priorities" as well as maintaining an "EU most wanted list."[275]

185. **There should be greater openness about COSI's activities so that it does not appear to be secretive and lacking in transparency.**

186. Dr Hillebrand also considered that the limited ability of the European Parliament and national parliaments to scrutinise COSI's activities in detail was a serious shortcoming.[276] The Treaty of Lisbon introduced a new provision[277] for the scrutiny of Europol's activities by the European Parliament and national Parliaments, and we have already discussed our preferred mechanisms for such oversight in separate correspondence with the Government and the European Parliament. **We have recommended that inter-parliamentary oversight of the work of Europol could be by bi-annual meetings of the Chairmen of the home affairs committees of national parliaments and the LIBE Committee of the European Parliament. We believe that such meetings could also consider the work of COSI.**

EU agencies

187. COSI has an important role in coordinating and ensuring effective operational cooperation amongst EU agencies which have a role in internal

---

[270] Q 229

[271] *EUROPOL: Coordinating the fight against serious and organised crime* (29th Report of Session 2007–08, HL Paper 183), paragraphs 124 to 137

[272] ISS 9

[273] Q 257

[274] Q 347

[275] Q 164

[276] ISS 9

[277] Article 88 TFEU

security. In this respect, William Shapcott considered that Europol, Frontex and SitCen were "underexploited instruments",[278] while Hugo Brady did not think that they needed any new powers at present, and instead should be allowed time to mature.[279] He observed that despite the existence of cooperation agreements between the agencies, their cooperation was still "sub-optimal, not good, and based on a sense of competition over prerogatives and future ideas coming down the line."[280]

188. It seems that some progress has already been made in this area. Mr Wainwright told us that he had recently chaired an inter-agency meeting between the four principal agencies in this field—Europol, Frontex, Eurojust and CEPOL[281]—in order to improve their operational cooperation regarding internal security.[282]

189. We have already discussed and endorsed the proposed changes to Frontex's mandate to allow it to work more closely with Europol. The Commissioner considered that SitCen should also cooperate more with other EU agencies and bodies.[283] Europol agreed, and suggested that it could cooperate more with SitCen regarding information sharing and the production of joint threat assessments.[284] Peter Storr considered that Europol did not require any additional powers and should instead concentrate on performing its current mandate well.[285]

190. **We welcome the moves already being made for better coordination and cooperation between EU agencies, and hope that the Government will press for further action on this front.**

The Internal Security Fund and security research

191. The proportion of the EU budget spent on home affairs policies currently constitutes only 0.77 per cent of the total spend (€6,449 million) for the period 2007–2013 (see Box 12). We considered this matter in our report on the next multi-annual financial framework (MFF) beginning in 2014, which makes recommendations on funding for the Area of Freedom, Security and Justice (AFSJ) under the next perspective.[286] The Stockholm Programme will expire at the end of 2014, just one year into the period of the next MFF.

Funding

192. In the Communication, the Commission is committed to ensuring that security-related activities, including security research and projects under EU internal security related funding programmes, are coherent with the strategic objectives.[287] The Communication advocates the possible establishment of an

---

278 Q 40

279 Q 163

280 QQ 157–160

281 The European Police College, which is located in Bramshill.

282 Q 130

283 Q 11

284 Q 127

285 QQ 235 & 236

286 *EU Financial Framework from 2014* (13th Report, Session 2010–2011, HL Paper 125), paragraph 134

287 *The EU Internal Security Strategy in Action: Five steps towards a more secure Europe*, COM (2010) 673 final, 22 November 2010

Internal Security Fund (ISF), which was mentioned in the Stockholm Programme "... to promote the implementation of the Internal Security Strategy so that it becomes an operational reality."[288] This will be considered in the context of negotiations on the next MFF when the Commission publishes a legislative proposal in the middle of 2011.

BOX 12

Current internal security funding

The total spend on home affairs policies for the period 2007–2013 falls under Heading 3a of the current MFF entitled "Freedom, Security and Justice". This covers two general framework programmes—"Security and Safeguarding Liberties" and "Solidarity and Management of Migration Flows"—and includes four Funds (the European Fund for the Integration of Third Country Nationals; the European Refugee Fund; the External Borders Fund; and the European Return Fund) as well as funding for the EU agencies falling under the aegis of DG HOME.[289] Each aspect of these funding arrangements has relevance for internal security.

On 12 February 2007, the Council adopted two specific funding programmes under the "Security and Safeguarding Liberties" general programme:

The Prevention of and Fight against Crime (ISEC) programme has a budget of approximately €600 million and its general objective is to fund activities including the fight against terrorism, trafficking in persons and offences against children, illicit drug trafficking and illicit arms trafficking, corruption and fraud.

The Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks (CIPS) programme has a budget of approximately €140 million and its general objective is to support Member States' efforts to prevent, prepare for, and to protect people and critical infrastructure against terrorist attacks and other security related incidents.

193. Hugo Brady considered that the proposal for an ISF was one of the strongest ideas in the Communication which could legitimise COSI's actions and increase its credibility.[290] The Government support the amalgamation of the existing ISEC and CIPS funds to create the ISF with the sum of their current funding levels acting as a ceiling for future allocations to the ISF.[291] We have already suggested that additional funding will be required if the proposed Cybercrime Centre is to achieve its key aims.[292]

194. When we took evidence from the EEAS representatives they emphasised the role of the Instrument for Stability (IfS) in funding strategically important

---

288 *The Stockholm Programme—An open and secure Europe serving and protecting citizens*, OJ C115 (4 May 2010) p 18

289 These are: the European Police College (CEPOL); the European Police Office (Europol); the European Agency for the Management of Operational Cooperation at the External Borders (FRONTEX); the European Asylum Support Office (EASO); and the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA).

290 ISS 12

291 ISS 10

292 See Chapter 5

projects in third countries. They explained that approximately two-thirds of IfS funding was spent on crisis response, spread across the continents, with the remaining third being spent on longer-term threats. With respect to the latter spend, they had recently requested an increase in the budgetary envelope allocated to "trans-regional threats", such as trafficking in drugs, small arms and human beings, as well as organised crime and counter-terrorism, ahead of the negotiations on the next financial perspective.[293] However David O'Sullivan doubted that any increase in funding was likely in the current financial climate. Christophe Prince from UKREP also considered the IfS to be a useful tool for funding counter-terrorism initiatives in third countries,[294] but emphasised that these projects were still at an early stage of development. He stressed that other funds, including development and neighbourhood instruments, were also available which could complement existing initiatives in this area.[295]

195. **We welcome the proposal for the creation of an Internal Security Fund and endorse the proposed amalgamation of the ISEC and CIPS funding streams. We believe that a case may be made for increasing the level of funding for the Internal Security Fund under the next Multi-annual Financial Framework, contingent upon reductions being made in other budget headings.**

Research

196. With regard to security-related research, CEPS was critical of what was perceived to be the lack of evidential base underpinning many of the proposals in the Communication. CEPS suggested that these "knowledge gaps" could be plugged with targeted research funding from the EU to universities and research institutes. William Shapcott emphasised the need for more investment in security research and the importance of committing funds to the right areas based upon an assessment of current and future threats.[296] Sir Richard Mottram emphasised the role of EU research budgets and the importance of identifying research proposals which would add value. He suggested that more coordination was needed between what was being done at Member State, EU and international level.[297] Dr Marsh agreed and stated that more research was needed in order to come up with "innovative solutions" to "some very deep problems." He added that his Office was currently pushing this approach in the negotiations regarding the next framework programme for research and development.[298]

197. This Committee considered this matter in its report on the next MFF, in which we recommended that internal security research should receive a

---

293 Q 90

294 Q 87

295 He stated that so far the Instrument for Stability had funded a €15 million project in Pakistan, a €15 million project in Yemen and a €5 million project in the Sahel.

296 Q 51

297 Q 387

298 QQ 288 & 290. The Commission has presented its proposals for the structure of the next framework programme in a Green Paper: *From Challenges to Opportunities: Towards a Common Strategic Framework for EU Research and Innovation funding*, COM (2011) 48, 9 February 2011. A legislative proposal will follow by the end of 2011.

larger share of funding under the next framework programme on research and development.[299]

198. **EU-funded research projects will continue to play an important role in underpinning future EU internal security action and initiatives. Future funding allocations should be informed by the threat assessments and should also be more closely aligned with the priorities of the relevant Commission Directorates General and EU agencies.**

199. **Priority research areas should include cyber-security and the behavioural aspects and technology involved, as well as the ideological foundations of terrorism.**

Conclusion

200. It will be seen that, overall, we believe that the Commission has chosen the right priorities for an internal security strategy and has suggested sensible ways of achieving the EU's objectives. But ultimately all will depend on effective and sensitive implementation. **We believe these priorities for the Strategy deserve support.**

[299] *EU Financial Framework from 2014* (13th Report, Session 2010–2011, HL Paper 125), paragraph 43

CHAPTER 7: SUMMARY OF CONCLUSIONS AND RECOMMENDATIONS

The EU's role in Internal Security

201. For the purposes of this report we are treating internal security as the ground covered by the Commission Communication, and believe this provides reasonable and pragmatic boundaries for a strategy and for its implementation. (paragraph 16)

202. The security of the United Kingdom does not begin or end at the water's edge, and cannot be defended independently of the security of other States. (paragraph 17)

203. Member States' national security and the EU's internal security are inextricably linked. We do not believe that these proposals intrude upon or threaten Member States' primary responsibility for national security. (paragraph 22)

204. We welcome the Communication as the first pragmatic attempt to articulate a comprehensive approach to the EU's internal security. (paragraph 23)

205. The five objectives proposed in the Communication, while broad and demanding, are sensible, practical and achievable, with the potential to raise standards among Member States and therefore to enhance the EU's security as a whole. All future proposals in this area should be developed on a sound evidential base, with priority given to tackling identifiable threats, and with full impact assessments and cost-benefit analyses. (paragraph 24)

206. We believe that it is shortsighted of the Government to criticise some Commission proposals solely on the ground that they go beyond what was agreed in the Stockholm Programme or the Internal Security Strategy itself. Achieving internal security is a moving target; over the five years covered by this Communication it may well require action beyond what is envisaged in the Stockholm Programme. Each proposal should be assessed on its merits. (paragraph 26)

Fundamental rights

207. Enhancing security while at the same time safeguarding fundamental rights is best done by careful scrutiny of the individual legislative proposals as they are brought forward, to see whether too much freedom is being sacrificed to achieve a high a degree of security. The European and national Parliaments have an important role to play. (paragraph 37)

208. We look forward to considering the Commission's proposal for a comprehensive data protection framework when it is published later this year. However there is already some risk that the Council and the Government will pursue a line which could result in different principles governing different measures. (paragraph 40)

European External Action Service

209. We urge the Commissioner for Home Affairs and the High Representative for Foreign Affairs and Security Policy to work closely together to ensure the close alignment of internal and external security. We believe that structures

to ensure that alignment is made a practical reality should be established urgently. (paragraph 49)

210. COSI and the Political and Security Committee should hold regular joint meetings on a similar basis. (paragraph 50)

211. We welcome the appointment of JHA staff to work in some overseas EU missions, and hope that this will be extended so that the EEAS may become an effective means of achieving good cooperation between those responsible for the EU's internal and external security. (paragraph 51)

212. We welcome the recent appointment of the new director of SitCen. We hope that it will continue to develop a wider security assessment role within the new EEAS structure, and will make an effective input to internal security threat assessments. (paragraph 52)

Relations with the United Nations and NATO

213. Vigorous engagement by the EU with the international community on security matters is crucial in order to tackle new and developing security threats. The EU should use its negotiating weight to influence the agenda accordingly. (paragraph 56)

214. We have repeatedly urged that relations between the EU and NATO should be improved and developed. The current situation should not be allowed to continue. The Government, as a major actor in NATO, must take urgent steps to improve cooperation. (paragraph 57)

Relations with strategically important third countries

215. We note the continuing importance of EU-US cooperation on security matters, but believe that the EU should also step up its cooperation, however challenging this may be, with other strategically important third countries such as Russia, China, Turkey and Pakistan in order to mitigate the external risks to the EU's internal security. (paragraph 64)

216. We welcome the endorsement by the Council of a readmission agreement with Turkey, but regret the delay in its implementation. We also regret that the Government have decided not to participate in the Decision authorising negotiation of a readmission agreement with Belarus. (paragraph 65)

Serious and organised crime

217. We welcome the establishment of the organised crime "policy cycle" by the Council and commend SOCA's positive engagement with COSI on organised crime matters. (paragraph 70)

Passenger Name Record (PNR) data

218. We welcome the Government's decision to opt in to the draft Directive, and support their intention to continue to argue that the Directive should apply to intra-EU flights. (paragraph 72)

Money laundering

219. The Government's continuing failure to ratify the Warsaw Convention on Money Laundering and Terrorist Financing is inexcusable. We repeat our view that this prevarication sends out a negative message about the

Government's commitment to this important matter. We again urge the Government to sign and ratify the Warsaw Convention without further delay. (paragraph 74)

Confiscation of criminal assets

220. The establishment of functioning Asset Recovery Offices in each Member State should be given a higher priority before the conferral of additional functions is considered. (paragraph 76)

Joint Investigation Teams (JITs)

221. We share the Government's enthusiasm for the work of Joint Investigation Teams and support the greater use of this tool in the fight against cross-border organised crime. (paragraph 79)

Counter-terrorism

222. We commend the work of the Counter-Terrorism Coordinator but believe that his role needs to be clarified and reviewed following the entry into force of the Treaty of Lisbon. In the meantime, we believe that he could play a useful role as a bridge between the internal and external aspects of terrorism. (paragraph 84)

Radicalisation and recruitment

223. The proposal to establish an EU radicalisation-awareness network will be a positive step if its functions are clear and well-defined. However we believe that Member States should continue to have the primary role in this area. We are less convinced that production by the Commission of a "handbook of actions and experiences" would either be practical or add value. (paragraph 90)

Preventing terrorists' access to materials and funding

224. We believe there is in principle a case for the establishment of an asset-freezing regime applicable to individuals resident within the EU. To be effective this will require the cooperation of third countries, in particular Switzerland and Liechtenstein. (paragraph 93)

Transport security

225. The security of transport networks is a vital component of the security debate. However we reserve judgment on the EU's role in this area pending the publication of the Commission's Communication on Transport Security Policy later this year. (paragraph 95)

Border management

EUROSUR

226. We welcome the Government's commitment to make an effective contribution to the development of EUROSUR and the future work of Frontex. Despite the United Kingdom's inability to participate fully in EUROSUR and Frontex, we believe that their work will make a positive

contribution to the protection of the United Kingdom and EU borders. (paragraph 102)

Civil protection and disaster relief

The role of the armed forces

227. We are surprised to find no reference to the armed forces in the Communication. They make a major contribution to civil protection and disaster relief, especially in the early stages. Their role must feature in the implementation of the strategy. We urge the EU institutions to give more thought to this. (paragraph 106)

The Solidarity Clause

228. The Solidarity Clause does not seem to empower Member States to do anything which they could not do without it, or require them to do anything they would not otherwise be required to do. It does however serve to emphasise the political will of the Member States to stand together in the face of adversity. (paragraph 108)

Risk assessments and cooperation between Situation Centres

229. We support more coordination between different Situation Centres and repeat our call for a closer working relationship between the EU and NATO Situation Centres. We also support a reduction in the number of existing rapid alert and notification processes for crisis management. (paragraph 111)

The development of a European emergency response capacity

230. We have practical concerns about the operation of a European Emergency Response Capacity. We believe that any pre-commitment of assets should be on a voluntary basis, and that Member States should retain a discretion to decide how their assets are best deployed. (paragraph 114)

Cyber-security: the challenge

231. We congratulate the Government on the priority they give to cyber-security in the United Kingdom National Security Strategy. But there is no room for complacency. All Member States, individually and collectively, must devote greater resources and urgency to meeting this challenge, given that their overall security is only as strong as the weakest link. (paragraph 122)

232. The EU institutions should take the lead by ensuring the security of their own networks and agencies. They are a natural target for malicious and criminal attack; weaknesses have been and will be exploited. They must take responsibility for their own cyber-security; it is in the interests of the United Kingdom to help them to do so. (paragraph 123)

Cyber-security: the role of the EU

233. We strongly welcome the emphasis on cyber-security in the Communication and believe that this is an urgent and fast evolving challenge in which the EU can play an important part in raising standards and awareness in the Member States. (paragraph 126)

The Budapest Convention

234. We welcome the Government's commitment that the United Kingdom will ratify the Budapest Convention on Cybercrime before the end of this year. (paragraph 131)

Cybercrime Centre

235. The establishment of a Cybercrime Centre will enhance the EU's ability to contribute in this area. This is not an end in itself, but only one of many measures that must be deployed. (paragraph 146)

236. Europol would be best placed to host such a body. However, we believe that finding staff with the necessary expertise may not be easy. Additional staff and funding will be essential if the Cybercrime Centre, wherever it may be situated, is to achieve its key aims. The Government's view that this can be done within existing resources is unrealistic, and inconsistent with their making additional resources available for the United Kingdom's programme. (paragraph 147)

237. We believe that the Centre should form a close working relationship with ENISA, and we support the extension of that agency's role and mandate to cooperate with law enforcement agencies. (paragraph 148)

238. The dispersal of agencies dealing with cyber matters is especially unfortunate. In particular, we continue to have concerns about ENISA's ability to operate effectively from its geographical location. We endorse the European Parliament's proposal that the agency's operations could be "frontloaded" in Athens. (paragraph 149)

Improving response capabilities

239. Many Member States already have an adequate emergency response capacity and do not need to change their existing CERT structure. But it is essential that every Member State should have an adequate emergency response capacity, and this may need to take the form of a national CERT. Where this is lacking, it should be addressed as a matter of urgency. Individual weaknesses will undermine the collective security of the EU. (paragraph 155)

Raising public awareness

240. A strong working relationship between the public and private sectors will be crucial in raising awareness of the threats from cyberspace. This needs to happen at both Member State and EU level through joint forums involving all of the key players. The EU can and should add value in this area by improving public awareness. (paragraph 159)

International cooperation

241. The global nature of the cyber threat requires an international response. Proactive collaboration within the international community, including the EU, UN and NATO, will be indispensable if agreement is to be reached on the nature of the threat, and on whether it can realistically be addressed. (paragraph 164)

242. We commend the United Kingdom initiative to host an international conference on cyber-security, and hope that a wide range of countries and

organisations with a legitimate interest will be invited. We look forward to considering the outcome and the effect it may have on the EU. (paragraph 166)

Implementing the Strategy

243. We note the Government's emphasis on practical cooperation, but do not believe that this should exclude further EU legislation if that should prove necessary. We reiterate the importance of adopting a flexible approach in order to respond in an effective manner to unforeseen events raising issues of internal security. (paragraph 169)

Council and Commission structures

244. A fundamental culture change within the EU institutions is needed to achieve a more effective approach to working practices, including in particular more integrated working and investment in the necessary training. (paragraph 170)

245. The work of Council groups involved in internal security should be further streamlined, with a reduction in their number as an overall objective. We also urge the different parts of the Commission to coordinate their work more closely. (paragraph 175)

The Standing Committee on Operational Cooperation on Internal Security (COSI)

246. We trust that over time COSI will emerge as the lead organisation in all matters of EU internal security, and that this will provide the opportunity for other groups and bodies to be rationalised and their number reduced. (paragraph 179)

Membership

247. We believe that COSI would benefit from having greater consistency and continuity in its membership. The Home Affairs Commissioner should be invited to attend each meeting of COSI as a matter of course. (paragraph 181)

Chairing arrangements

248. COSI would benefit from less frequent changes in its chairmanship. It is a less political body than the Council, so there is no conceivable logical connection between the nationality of the person best qualified to chair COSI and the identity of the Member State holding the Presidency. We believe that a suitably qualified chairman of COSI should be appointed for a minimum period of two years, renewable once. (paragraph 183)

Transparency and parliamentary oversight

249. There should be greater openness about COSI's activities so that it does not appear to be secretive and lacking in transparency. (paragraph 185)

250. We have recommended that inter-parliamentary oversight of the work of Europol could be by bi-annual meetings of the Chairmen of the home affairs committees of national parliaments and the LIBE Committee of the

European Parliament. We believe that such meetings could also consider the work of COSI. (paragraph 186)

EU agencies

251. We welcome the moves already being made for better coordination and cooperation between EU agencies, and hope that the Government will press for further action on this front. (paragraph 190)

The Internal Security Fund and security research

Funding

252. We welcome the proposal for the creation of an Internal Security Fund and endorse the proposed amalgamation of the ISEC and CIPS funding streams. We believe that a case may be made for increasing the level of funding for the Internal Security Fund under the next Multi-annual Financial Framework, contingent upon reductions being made in other budget headings. (paragraph 195)

Research

253. EU-funded research projects will continue to play an important role in underpinning future EU internal security action and initiatives. Future funding allocations should be informed by the threat assessments and should also be more closely aligned with the priorities of the relevant Commission Directorates General and EU agencies. (paragraph 198)

254. Priority research areas should include cyber-security and the behavioural aspects and technology involved, as well as the ideological foundations of terrorism. (paragraph 199)

Conclusion

255. We believe the Commission has chosen the right priorities for an internal security strategy, and that these deserve support. (paragraph 200)

256. We recommend this report for debate. (paragraph 13)

APPENDIX 1: SUB-COMMITTEE F (HOME AFFAIRS)

The members of the Sub-Committee that conducted this inquiry were:

Lord Avebury
Lord Blencathra (from 29 March 2011)
Lord Dear
Baroness Eccles of Moulton
Lord Hannay of Chiswick (Chairman)
Lord Hodgson of Astley Abbotts
Lord Judd
Lord Mackenzie of Framwellgate
Lord Mawson
Lord Richard
Lord Tomlinson
Lord Tope

Stephen Hawker CB of SHD Consulting was appointed Specialist Adviser for the inquiry.

Declarations of Interests:

A full list of Members' interests can be found in the Register of Lords Interests:

http://www.parliament.uk/mps-lords-and-offices/standards-and-interests/register-of-lords-interests

Interests declared by Members relevant to the inquiry:

Lord Dear
Chairman, Blue Star Capital plc (investment company specialising in homeland security solutions)
Chairman, OmniPerception Ltd (high tech recognition systems)

Lord Hannay of Chiswick
Member, Advisory Board, Centre for European Reform
Governor, Ditchley Foundation

Lord Hodgson of Astley Abbotts
Trustee, Fair Trials International

Lord Judd
Member, Advisory Board, Centre for Study of Human Rights at LSE
Trustee, Saferworld

Lord Mackenzie of Framwellgate
Patron, Association of Security Consultants (ASC)

Lord Mawson
Director, Olympic Park Legacy Company Board

Lord Tope
Member, (EU) Committee of the Regions (allowances)

APPENDIX 2: LIST OF WITNESSES

Evidence is published online at www.parliament.uk/hleuf and available for inspection at the Parliamentary Archives (020 7219 5314)

Evidence received by the Committee is listed below in order of receipt and in alphabetical order. Witnesses marked with * also gave oral evidence. Witnesses marked with ** gave oral evidence and did not submit any written evidence.

Order of receipt

(ISS 1) Professor Paul Wilkinson

(ISS 2) Centre for European Policy Studies (CEPS)

(ISS 3) Foundation for Information Policy Research (FIPR)

(ISS 4) JANET UK

(ISS 5) European Network and Security Agency (ENISA)

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

(ISS 7) Professor Didier Bigo

(ISS 8) Association of Chief Police Officers (ACPO)

(ISS 9) Dr Claudia Hillebrand

* (ISS 10) Home Office

(ISS 11) Europol

* (ISS 12) Hugo Brady, Senior Research Fellow, Centre for European Reform

(ISS 13) Professor Wyn Rees

(ISS 14) Symantec

(ISS 15) Professor Valsamis Mitsilegas

* (ISS 16) Supplementary memorandum by the Home Office

* (ISS 17) Supplementary memorandum by the Serious Organised Crime Agency (SOCA)

* (ISS 18) Supplementary memorandum by James Brokenshire MP, Parliamentary Under-Secretary of State for Crime Prevention, Home Office

* (ISS 19) Further supplementary memorandum by the Home Office

Alphabetical

Association of Chief Police Officers (ACPO) (ISS 8)

Professor Didier Bigo (ISS 7)

* Hugo Brady, Senior Research Fellow, Centre for European Reform (ISS 12)

* James Brokenshire MP, Parliamentary Under-Secretary of State for Crime Prevention, Home Office (ISS 18)

** Civil Contingencies Secretariat, Cabinet Office

** Office of Cyber Security and Information Assurance, Cabinet Office

Centre for European Policy Studies (CEPS) (ISS 2)

** Dr Paul Cornish, Carrington Professor of International Security, Chatham House

European Commission

** Cecilia Malmström, Home Affairs Commissioner

** European External Action Service (EEAS)

European Network and Security Agency (ENISA) (ISS 5)

Europol (ISS 11)

** Rob Wainwright, Director, Europol

Foundation for Information Policy Research (FIPR) (ISS 3)

Dr Claudia Hillebrand (ISS 9)

* Home Office (ISS 10)

* Supplementary memorandum by the Home Office (ISS 16)

* Further supplementary memorandum by the Home Office (ISS 19)

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

JANET UK (ISS 4)

Professor Valsamis Mitsilegas (ISS 15)

** Sir Richard Mottram

* Supplementary memorandum by the Serious Organised Crime Agency (SOCA) (ISS 17)

Professor Wyn Rees (ISS 13)

** William Shapcott, Former director of the Council Joint Situation Centre (SitCen)

Symantec (ISS 14)

Professor Paul Wilkinson (ISS 1)

APPENDIX 3: CALL FOR EVIDENCE

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. The Committee seeks evidence from anyone with an interest.

Written evidence is sought by 22 December 2010. Public hearings will be held in December 2010 and January and February 2011. The Committee aims to report to the House, with recommendations, in April 2011. The report will receive a response from the Government, and may be debated in the House.

The inquiry will focus on two documents:

- the Internal Security Strategy for the European Union which was approved by the Council on 26 February 2010 and endorsed by the European Council on 26 March 2010 (Council doc. 7120/10); 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)

The Internal Security Strategy (ISS) lays out a European security model to integrate action on law enforcement and judicial cooperation, border management and civil protection. Its declared objectives are:

- to raise public awareness of the role and value added by the EU in internal security
- to further develop common tools and policies addressing causes of insecurity as well as effects
- to strengthen law enforcement and judicial cooperation, border management, civil protection and disaster management.

The Commission Communication describes a range of proposed actions intended to:

- 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.

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 would welcome evidence on any aspect of ISS and its development and its proposed implementation. We would particularly welcome comments on:

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?

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.

Prevention and anticipation

The systems, mechanisms and processes needed to improve confidence in 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.

Information exchange

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

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.

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.

APPENDIX 4: THE COMMISSION COMMUNICATION

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

1. The European Security Model: Working together for a more secure Europe

Most Europeans are able to go about their daily lives in relative safety. At the same time, our societies are facing serious security threats that are growing in scale and sophistication. Many of today's security challenges are cross-border and cross-sectoral in nature. No single Member State is able to respond to these threats on its own. This is something that worries our citizens and businesses. Four out of five Europeans want more action at EU level against organised crime and terrorism[300].

Much has been achieved to respond to those emerging threats and to increase Europe's security. With the Lisbon Treaty[301] in force, and with the guidance provided by the Stockholm Programme and its Action Plan[302], the EU now has the opportunity to take further determined action. The Internal Security Strategy, adopted in early 2010 under the Spanish Presidency[303], set out the challenges, principles and guidelines for how to deal with these issues within the EU and called on the Commission to propose actions for implementing the strategy. This communication—the EU Internal Security Strategy in Action—therefore builds on what Member States and EU institutions have already agreed, and proposes how we over the next four years can work together to be more effective in fighting and preventing **serious and organised crime**, **terrorism** and **cybercrime**, in strengthening the **management of our external borders** and in building **resilience to natural and man-made disasters**.

A shared agenda for common challenges

The EU's role in our internal security consists of common policies, legislation and practical cooperation in the areas of police and judicial cooperation, border management, and crisis management. In striving to reach our security objectives, the contribution from both EU internal and external policies is crucial.

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. Our common efforts to deliver responses to the security challenges of our time will also contribute to strengthening and developing the European model of a social market economy put forward in the Europe 2020 strategy.

---

300 Standard Eurobarometer 71.

301 Treaty on the Functioning of the European Union (TFEU).

302 The Stockholm Programme: An Open and Secure Europe Serving and Protecting the Citizens (Council Document 17024/09); Delivering an area of freedom, security and justice: Action plan implementing the Stockholm Programme—COM(2010) 171. The Stockholm Programme is the EU's programme for justice and home affairs for the period 2010–14.

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

Security policies based on common values

The Internal Security Strategy in Action, and the tools and actions for implementing it must be based on common values including the rule of law and respect for fundamental rights as laid down in the **EU Charter of Fundamental Rights**[304]. Solidarity must characterise our approach to crisis management. Our counter terrorism policies should be proportionate to the scale of the challenges and focus on preventing future attacks. 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.

Internal security with a global perspective

Internal security cannot be achieved in isolation from the rest of the world, and it is therefore important to ensure coherence and complementarity between the internal and external aspects of EU security. The values and priorities in the Internal Security Strategy, including our commitment to promoting human rights, democracy, peace and stability in our neighbourhood and beyond, are an integral component of the approach laid down in the European Security Strategy[305]. As that Strategy recognises, relationships with our partners, in particular the United States, are of fundamental importance in the fight against serious and organised crime and terrorism.

Security should be integrated in relevant strategic partnerships, and taken into account in the dialogue with our partners when programming EU funding in partnership agreements. In particular, internal security-related priorities should feature in political dialogues with third countries and regional organisations where appropriate and relevant for combating multiple threats, such as trafficking in human beings, drugs trafficking and terrorism. The EU will moreover pay special attention to third countries and regions which may require EU and Member State support and expertise in the interests of not only the external but also internal security. With the European External Action Service it will be possible to integrate further action and expertise using the skills and knowledge of Member States, the Council and the Commission. Security expertise should be deployed to EU Delegations, particularly in priority countries, including Europol liaison officers and liaison magistrates[306]. Appropriate responsibilities and functions for these experts will be defined by the Commission and the European External Action Service.

2. Five strategic objectives for internal security

This communication identifies the most urgent challenges to EU security in the years to come. It proposes five strategic objectives and specific actions for 2011–2014 which, alongside ongoing efforts and initiatives, will help make the EU more secure.

Serious and organised crime takes a variety of forms: trafficking in human beings, drugs and firearms trafficking, money laundering and the illegal shipment and dumping of waste inside and outside Europe. Even seemingly petty crimes such as

---

[304] 'Strategy for the effective implementation of the Charter of Fundamental Rights by the European Union'—COM(2010) 573.

[305] 'European Security Strategy: A Secure Europe in a Better World' was adopted in 2003 and reviewed in 2008.

[306] In accordance with Council Decision on Eurojust 2009/426/JHA, to be transposed by June 2011.

burglary and car theft, sale of counterfeit and dangerous goods and the actions of itinerant gangs are often local manifestations of global criminal networks. These crimes require concerted European action. Likewise with terrorism: our societies remain vulnerable to the sorts of attacks suffered with the bombings of public transport in Madrid in 2004 and in London in 2005. We must work harder and more closely to prevent new attacks recurring.

Another growing threat is **cybercrime**. Europe is a key target for cybercrime because of its advanced Internet infrastructure, the high number of users, and its internet-mediated economies and payment systems. Citizens, businesses, governments and critical infrastructure must be better protected from criminals who take advantage of modern technologies. **Border security** also requires more coherent action. With common external borders, smuggling and other cross-border illegal activity must be targeted at European level. Efficient control of the EU's external borders is thus crucial for the area of free movement.

Furthermore, in recent years we have seen an increase in the frequency and scale of natural and man-made **disasters** in Europe and in its immediate neighbourhood. This has demonstrated the need for a stronger, more coherent and better integrated European crisis and disaster response capacity as well as for the implementation of existing disaster prevention policies and legislation.

OBJECTIVE 1: Disrupt international crime networks

Despite growing cooperation between law enforcement authorities and the judiciary within as well as between Member States, international crime networks remain highly active, creating vast criminal profits. Alongside corruption and intimidation of local populations and authorities these profits are often used to penetrate the economy and undermine public trust.

To prevent crime it is therefore essential to disrupt criminal networks and combat the financial incentive which drives them. To that end, practical law enforcement cooperation should be strengthened. Authorities across all sectors and at different levels should work together to protect the economy, and criminal profits should be effectively traced and confiscated. We also need to overcome the, obstacles posed by divergent national approaches, where necessary through legislation on judicial cooperation to strengthen mutual recognition and common definitions of criminal offences and minimum levels of criminal sanctions[307].

Action 1: Identify and dismantle criminal networks

To identify and disrupt criminal networks, it is essential to understand their members' methods of operating and their financing.

The Commission will therefore propose in 2011 EU legislation on the collection of **Passenger Name Records** of passengers on flights entering or leaving the territory of the EU. These data will be analysed by the authorities in Member States to prevent and prosecute terrorist offences and serious crimes.

Understanding the criminal source of finances and their movements depends on information about the owner of the companies, as well as the trusts that those finances pass through. In practice, law enforcement and judicial authorities,

[307] Recent proposals for Directives on trafficking in human beings, sexual exploitation of children and cybercrime represent an important first step in this direction. Article 83(1) TFEU lists the following other serious crimes: terrorism, illicit drug trafficking, illicit arms trafficking, money laundering, corruption, counterfeiting of means of payment and organised crime.

administrative investigative bodies such as OLAF and private sector professionals have difficulty obtaining such information. The EU should therefore consider by 2013, in the light of discussions with its international partners in the Financial Action Task Force, revising the **EU Anti-Money Laundering legislation** to enhance the transparency of legal persons and legal arrangements. To help trace the movement of criminal finances, some Member States have set up a central register of bank accounts. To maximise the usefulness of such registers for law enforcement purposes, the Commission will in 2012 develop guidelines. In order to investigate effectively criminal financial transactions, law enforcement and judicial authorities should be equipped and trained to collect, analyse and, where appropriate, share information making full use of national centres of excellence for criminal financial investigation and the European Police College (CEPOL) training programmes. The Commission will propose a strategy in this area in 2012.

Additionally, the international nature of criminal networks calls for more **joint operations** involving police, customs, border guards and judicial authorities in different Member States working alongside Eurojust, Europol and OLAF. Such operations, including **Joint Investigation Teams**[308], should be set up—where necessary at short notice—with the full support of the Commission in line with the priorities, strategic goals and plans established by the Council on the basis of relevant threat analyses[309].

Moreover, the Commission and Member States should continue to ensure effective implementation of and to report on the **European Arrest Warrant**, including its effects on fundamental rights.

Action 2: Protect the economy against criminal infiltration

Criminal networks rely on corruption to invest their profits in the lawful economy, eroding trust in public institutions and the economic system. Sustaining political will to combat corruption is of key importance. Action at EU level and sharing of best practices is therefore necessary, and the Commission will table a proposal in 2011 on how to monitor and assist **Member States' anti-corruption efforts**.

Policies to engage governmental and regulatory bodies responsible for granting licences, authorisations, procurement contracts or subsidies should be developed (the **'administrative approach'**) to protect the economy against infiltration by criminal networks. The Commission will give practical support to Member States by establishing in 2011 a network of national contact points to develop best practices, and by sponsoring pilot projects on practical issues**.**

Counterfeit goods generate large profits for organised crime groups, distort the single market's trade patterns, undermine European industry and put the health and safety of European citizens at risk. The Commission will therefore, in the context of its forthcoming action plan against counterfeiting and piracy, take all appropriate initiatives to foster more effective **enforcement of intellectual property rights**. Meanwhile, to combat the sale of counterfeit goods on the internet, Member States' customs administrations and the Commission should adapt laws where necessary, establish contact points in national customs and exchange best practices.

---

[308] Article 88(2)(b) of the TFEU and Council Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime.

[309] Council Conclusions 15358/10 on the creation and implementation of a EU policy cycle for organised and serious international crime.

Action 3: Confiscate criminal assets

To combat the financial incentive of criminal networks Member States must do all they can to seize, freeze, manage and confiscate criminal assets, and ensure that they do not return to criminal hands.

To this end the Commission will propose **legislation** in 2011 to strengthen the EU legal framework[310] on **confiscation**, in particular to allow more third-party confiscation[311] and extended confiscation[312] and to facilitate mutual recognition of non-conviction-based[313] confiscation orders between Member States.

Member States must[314] by 2014 **establish Asset Recovery Offices** equipped with the necessary resources, powers and training, and the ability to exchange information. The Commission will develop common indicators by 2013, against which Member States should evaluate the performance of these offices. Moreover, Member States should also by 2014 make the necessary institutional arrangements, for example by creating asset management offices, to ensure that frozen assets do not loose their value before they are eventually confiscated. In parallel, the Commission will in 2013 provide best practice guidance on how to prevent criminal groups from reacquiring confiscated assets.

OBJECTIVE 2: Prevent terrorism and address radicalisation and recruitment

The threat from terrorism remains significant and is constantly evolving[315]. Terrorist organisations adapt and innovate, as demonstrated by the 2008 Mumbai attacks, the attempted attack on a flight from Amsterdam to Detroit on Christmas Day 2009 and plots uncovered recently affecting several Member States. Threats now come both from 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. Our efforts to combat terrorism need to evolve to stay ahead of the threat with a coherent European approach including preventive action[316]. Furthermore, the EU should continue to designate critical infrastructure and put in place plans to protect those assets, including transport services and energy generation and transmission, which are essential to the functioning of society and the economy.[317]

Member States have the primary role in delivering on this objective through coordinated and effective efforts, with the full support of the Commission, and assisted by the EU Counter-Terrorism Coordinator.

---

310 Framework Decision 2001/500/JHA on money laundering and confiscation.

311 Third party confiscation involves the confiscation of assets that have been transferred by an investigated or convicted person to third parties.

312 Extended confiscation is the ability to confiscate assets which go beyond the direct proceeds of a crime so that there is no need to establish a connection between suspected criminal assets and a specific criminal conduct.

313 Non-conviction based procedures allow to freeze and confiscate asset irrespective of a prior conviction of the owner in a criminal court.

314 Council Decision 2007/845/JHA requires each Member State to set up at least one Asset Recovery Office on its territory.

315 For the latest figures, see Europol's 2010 Terrorism Situation and Trend (TESAT) Report.

316 EU Counter-Terrorism Strategy Doc. 14469/4/05 of November 2005 sets out a four-fold approach consisting of Prevent, Protect, Pursue and Respond. For a more detailed discussion, see 'The EU Counter-Terrorism Policy: main achievements and future challenges'—COM(2010) 386.

317 Directive on European Critical Infrastructures (2008/114/EC), part of the wider European Programme for Critical Infrastructure Protection, whose scope extends beyond protection against terrorist threats.

Action 1: Empower communities to prevent radicalisation and recruitment

Radicalisation which can lead to acts of terrorism is best contained at a level closest to the most susceptible individuals in the most affected communities. It requires close cooperation with local authorities and civil society and empowering key groups in vulnerable communities. The core of the action on radicalisation and recruitment is—and should remain—at national level.

Several Member States are developing work streams in this area, and certain cities within the EU have developed local community-based approaches and prevention policies. These initiatives have often been successful and the Commission will continue to assist in facilitating the sharing of such experiences[318].

Firstly, by 2011, and in partnership with the Committee of the Regions, the Commission will promote the creation of an **EU radicalisation-awareness network**, supported by an online forum and EU-wide conferences, to pool experiences, knowledge and good practices to enhance awareness of radicalisation and communication techniques for challenging terrorist narratives. This network will consist of policy makers, law enforcement and security officials, prosecutors, local authorities, academics, field experts and civil society organisations, including victims groups. Member States should use ideas generated through the network to create physical and virtual community spaces for open debates which encourage credible role models and opinion leaders to voice positive messages offering alternatives to terrorist narratives. The Commission will also support the work of civil society organisations which expose, translate and challenge violent extremist propaganda on the internet.

Secondly, the Commission will in 2012 organise **a ministerial conference** on the prevention of radicalisation and recruitment at which Member States will have the opportunity to present examples of successful action to counter extremist ideology.

Thirdly, in the light of these initiatives and discussions, the Commission will develop a **handbook of actions and experiences** to support Member States' efforts, from upstream prevention of radicalisation to disrupting recruitment and how to enable disengagement and rehabilitation.

Action 2: Cut off terrorists' access to funding and materials and follow their transactions

The Commission will in 2011 consider devising a framework for administrative measures under Article 75 of the Treaty as regards freezing of assets to prevent and combat terrorism and related activities. The EU action plans for preventing access to explosives (2008) and Chemical, Biological, Radiological and Nuclear (CBRN) substances (2009) need to be implemented as a priority, by way of both legislative and non legislative action. This includes the adoption of a regulation, proposed by the Commission in 2010, limiting general access to chemical precursors used to make explosives. It also means setting up a European network of specialised CBRN law enforcement units, ensuring that Member States take CBRN risks into consideration in their national planning. Another measure is to establish a law enforcement Early Warning System at Europol for incidents related to CBRN materials. These actions require close coordination with Member States, and should involve public private partnerships, where appropriate. To minimise

[318] As part of the EU strategy for combating radicalisation and recruitment to terrorism (CS/2008/15175) the Commission has supported research and the establishment of the European Network of Experts on Radicalisation to study the phenomenon of radicalisation and recruitment, Member State-led projects on for example community policing, communication and radicalisation in prisons, and provided around € 5m for projects on behalf of victims and supports the network of associations of victims of terrorism.

the risk of terrorist organisations and state actors getting access to those items which could be used to make explosives and weapons of mass destruction (biological, chemical or nuclear), the EU should strengthen the dual-use export control system and its enforcement at EU borders and internationally.

Following the signature of the Terrorist Financing Tracking Programme agreement with the United States, the Commission will in 2011 **develop a policy for the EU to extract and analyse financial messaging data** held on its own territory.

Action 3: Protect transport

The Commission will further develop the EU regime for aviation and maritime security, based on continuous assessment of threats and risks. It will take into account progress in security research techniques and technology, by making use of EU programmes such as Galileo and the GMES[319] initiative on European earth observation. It will work 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; and it will emphasise continued strengthening of the inspections and enforcement regime, including the monitoring of cargo operations. International cooperation is essential and can help to promote improved security standards worldwide, while ensuring efficient use of resources and limiting unnecessary duplication of security checks.

There is scope, and justification, for a more active European approach to the broad and complex area of **land transport security**, and in particular to the security of passenger transport[320]. The Commission intends to extend existing work on urban transport security to cover (a) local and regional rail and (b) high-speed rail, including related infrastructure. To date, EU level activity has been limited to exchanging information and best practice, reflecting subsidiarity concerns and the absence of an international organisation comparable to the International Maritime Organisation or International Civil Aviation Organisation requiring a co-ordinated European approach. The Commission considers that as a first step towards further action, it would be useful to explore the establishment of a standing committee on land transport security, chaired by the Commission and involving experts in transport and in law enforcement, and of a forum for exchanging views with public and private stakeholders, taking account of previous experience in aviation and maritime transport security. Ongoing work to refine and strengthen procedures for monitoring air cargo in transit from third countries has been accelerated in the light of recent events.

Transport security issues will be addressed in detail in a communication on Transport Security Policy to be issued in 2011.

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

Security of IT networks is one essential factor for a well-functioning information society. This is recognised in the recently published Digital Agenda for Europe[321] which addresses issues related to cybercrime, cyber security, safer internet and privacy as the main components in building trust and security for network users.

---

[319] GMES stands for Global Monitoring for Environment and Security.

[320] European Council, March 2004, Declaration on Combating Terrorism.

[321] COM(2010) 245.

The rapid development and application of new information technologies has also created new forms of criminal activity. Cybercrime is a global phenomenon causing significant damage to the EU internal market. While the very structure of the internet knows no boundaries, jurisdiction for prosecuting cybercrime still stops at national borders. Member States need to pool their efforts at EU level. The High Tech Crime Centre at Europol already plays an important coordinating role for law enforcement, but further action is needed.

Action 1: Build capacity in law enforcement and the judiciary

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[322]. The centre will improve evaluation and monitoring of existing preventive and investigative measures, support the development of training and awareness-raising for law enforcement and judiciary, establish cooperation with the European Network and Information Security Agency (ENISA) and interface with a network of national/governmental Computer Emergency Response Teams (CERTs). The cybercrime centre should become the focal point in Europe's fight against cybercrime.

At national level, Member States should ensure common standards among police, judges, prosecutors and forensic investigators in investigating and prosecuting cybercrime offences. In liaison with Eurojust, CEPOL and Europol, Member States are encouraged by 2013 to develop their national cybercrime awareness and training capabilities, and set up centres of excellence at national level or in partnership with other Member States. These centres should work closely with academia and industry.

Action 2: Work with industry to empower and protect citizens

All Member States should ensure that people can easily **report cybercrime incidents**. This information, once evaluated, would feed into national and, if appropriate, the European cybercrime alert platform. Building on the valuable work under the Safer Internet Programme, Member States should also ensure that citizens have easy access to guidance on cyber threats and the basic precautions that need to be taken. This guidance should include how people can protect their privacy online, detect and report grooming, equip their computers with basic anti-virus software and firewalls, manage passwords, and detect phishing, pharming, or other attacks. The Commission will in 2013 set up a real-time central pool of shared resources and best practices among Member States and the industry.

Cooperation between the public and private sector must also be strengthened on a European level through the European Public-Private Partnership for Resilience (EP3R). It should further develop innovative measures and instruments to improve security, including that of critical infrastructure, and resilience of network and information infrastructure. EP3R should also engage with international partners to strengthen the global risk management of IT networks.

The handling of illegal internet content—including incitement to terrorism—should be tackled through guidelines on cooperation, based on authorised notice and take-down procedures, which the Commission intends to develop with internet service providers, law enforcement authorities and non-profit

[322] The Commission will complete a feasibility study for the centre in 2011.

organisations by 2011. To encourage contact and interaction between these stakeholders, the Commission will promote the use of an internet based platform called the Contact Initiative against Cybercrime for Industry and Law Enforcement.

Action 3: Improve capability for dealing with cyber attacks

A number of steps must be taken to improve prevention, detection and fast reaction in the event of cyber attacks or cyber disruption. Firstly, every Member State, and the EU institutions themselves should have, by 2012, a well-functioning **CERT**. It is important that, once they are set up, all CERTs and law enforcement authorities cooperate in prevention and response. Secondly, Member States should network together their national/governmental CERTs by 2012 to enhance Europe's preparedness. This activity will also be instrumental in developing, with the support of the Commission and ENISA, a European Information Sharing and Alert System (EISAS) to the wider public by 2013 and in establishing a network of contact points between relevant bodies and Member States. Thirdly, Member States together with ENISA should develop national contingency plans and undertake regular national and European exercises in incident response and disaster recovery. Overall, ENISA will provide support to these actions with the aim of raising standards of CERTs in Europe.

OBJECTIVE 4: Strengthen security through border management

With the Lisbon Treaty in force the EU is better placed to exploit synergies between border management policies on persons and goods, in a spirit of solidarity and sharing of responsibility[323]. In relation to movement of persons, the EU can treat migration management and the fight against crime as twin objectives of the integrated border management strategy. It is based on three strategic strands.

An enhanced use of new technology for border checks (the second generation of the Schengen Information System (SIS II), the Visa Information System (VIS), the entry/exit system and the registered traveller programme);

an enhanced use of new technology for border surveillance (the European Border Surveillance System, EUROSUR) with the support of GMES security services, and the gradual creation of a common information sharing environment for the EU maritime domain[324]; and

an enhanced coordination of Member States through Frontex.

In relation to the movement of goods, the 2005 'security amendment' of the Community Customs Code[325] laid down a basis for the border to become safer and yet more open for trade of trusted goods. All cargo entering the EU is subject to risk analysis for security and safety purposes based on common risk criteria and standards. Use of resources is more efficient as they focus more on potentially risky cargos. The system relies on advance information of trade movements from economic operators, the establishment of a common risk management framework, as well as an Authorised Economic Operators scheme to be applied to all goods entering or leaving the EU. These instruments are complementary and create a

[323] Article 80 of the TFEU.

[324] Commission communication, 'Towards the integration of maritime surveillance: A Common information environment for the EU maritime domain', COM (2009) 538

[325] Council Regulation (EC) No 648/2005 amending Council Regulation (EC) No 2913/92 establishing the Community Customs Code.

comprehensive architecture, which is being further developed to cope with the increasingly sophisticated criminal organisations that Member States cannot tackle on their own.

Action 1: Exploit the full potential of EUROSUR

The Commission will present a legislative proposal to **set up EUROSUR** in 2011 to contribute to internal security and the fight against crime. EUROSUR will establish a mechanism for Member States' authorities to share operational information related to border surveillance and for cooperation with each other and with Frontex at tactical, operational and strategic level[326]. EUROSUR will make use of new technologies developed through EU funded research projects and activities, such as satellite imagery to detect and track targets at the maritime border, e.g. tracing fast vessels transporting drugs to the EU.

In recent years, two major initiatives on operational cooperation at the maritime borders have been launched—one on human trafficking and human smuggling under the umbrella of Frontex and the second on drugs smuggling in the framework of MAOC-N[327] and CeCLAD-M[328]. As part of the development of integrated and operational action at the EU's maritime border, the EU will launch in 2011 a pilot project at its southern or south-western border, involving those two centres, the Commission, Frontex and Europol. This pilot project will explore synergies on risk analysis and surveillance data in common areas of interest concerning different types of threats, such as drugs and people smuggling[329].

Action 2: Enhancing the contribution of Frontex at the external borders

During its operations, Frontex comes across key information on criminals involved in trafficking networks. Currently, however, this information cannot be further used for risk analyses or to better target future joint operations. Moreover, relevant data on suspected criminals do not reach the competent national authorities or Europol for further investigation. Likewise, Europol cannot share information from its analytical work files. Based on experience and in the context of the EU's overall approach to information management[330], the Commission considers that enabling Frontex to process and use this information, with a limited scope and in accordance with clearly defined personal data management rules, will make a significant contribution to dismantling criminal organisations. However, this should not create any duplication of tasks between Frontex and Europol.

From 2011 onwards, the Commission, with joint input from Frontex and Europol, will present a report by the end of each year on specific cross-border crimes such as human trafficking, human smuggling and smuggling of illicit goods. This annual report will serve as a basis for assessing the need for Frontex and its joint

---

[326] Commission proposals for the development of the EUROSUR system and for the development of a common information sharing environment (CISE) for the EU maritime domain are set out in COM (2008) 68 and COM(2009) 538 respectively. A six step road map for establishing the CISE was recently adopted—COM(2010) 584.

[327] MAOC-N—Maritime Analysis and Operations Centre—Narcotics.

[328] CeCLAD-M—Centre de Coordination pour la lutte antidrogue en Méditerranée.

[329] This project will complement the other integrated maritime surveillance projects such as BlueMassMed and Marsuno, which aim to optimise the efficiency of maritime surveillance in the Mediterranean Sea, Atlantic and the northern European sea basins.

[330] Overview in the area of information management in the area of freedom, security and justice—COM(2010) 385.

operations and joint operations between police, customs and other specialised law enforcement authorities to be carried out from 2012 onwards.

Action 3: Common risk management for movement of goods across external borders

Significant legal and structural developments have taken place in recent years to improve the security and safety of international supply chains and movement of goods crossing the EU border. The Common Risk Management Framework (CRMF), implemented by customs authorities, entails continuous screening of electronic pre-arrival (and pre-departure) trade data to identify the risk of security and safety threats to the EU and its inhabitants, as well as dealing with these risks appropriately. The CRMF also provides for application of more intensive controls targeting identified priority areas, including trade policy and financial risks. It also requires systematic exchange of risk information at EU level.

A challenge in the coming years is to ensure uniform, high-quality performance of risk management, associated risk analysis, and risk-based controls in all Member States. In addition to the annual report on the smuggling of illicit goods referred to above, the Commission will develop EU level customs assessments to address common risks. Pooling information at EU-level should be used to reinforce border security. In order to strengthen customs security to the required level at external borders, the Commission will work in 2011 on options to **improve EU level capabilities for risk analysis and targeting** and come forward with proposals as appropriate.

Action 4: Improve interagency cooperation at national level

Member States should by the end of 2011 start developing **common risk analyses**. This should involve all relevant authorities with a security role, including police, border guards and customs authorities who identify hot spots and multiple and cross-cutting threats at external borders, for example repeated smuggling of people and drugs from the same region at the same border crossing points. These analyses should complement the yearly report by the Commission on cross-border crimes with joint contributions from Frontex and Europol. By the end of 2010 the Commission will finalise a study to identify best practices on cooperation between border guards and customs administrations working at EU external borders and consider the best way to disseminate them. In 2012, the Commission will make suggestions on how to **improve coordination of border checks** carried out by different national authorities (police, border guards, and customs). Further to 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.

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

The EU is exposed to an array of potential crises and disasters, such as those associated with climate change and those caused by terrorist and cyber attacks on critical infrastructure, hostile or accidental releases of disease agents and pathogens, sudden flu outbreaks and failures in infrastructure. These cross-sectoral threats call for improvements to long-standing crisis and disaster management practices in terms of efficiency and coherence. They require both solidarity in response, and responsibility in prevention and preparedness with an

emphasis on better risk assessment and risk management at EU level of all potential hazards.

Action 1: Make full use of the solidarity clause

The solidarity clause in the Lisbon Treaty[331] 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. 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. On the basis of a cross cutting proposal by the Commission and the High Representative—to be presented in 2011—the EU's collective task will be to **put the solidarity clause into practice**.

Action 2: An all-hazards approach to threat and risk assessment

By the end of 2010 the Commission will develop, together with Member States, EU **risk assessment** and mapping guidelines for disaster management, based on a multi-hazard and multi-risk approach, covering in principle all natural and man-made disasters. By the end of 2011, Member States should develop national approaches to risk management, including risk analyses. On this basis, the Commission will prepare, by the end of 2012, a cross-sectoral overview of the major natural and man-made risks that the EU may face in the future[332]. Furthermore the Commission initiative on health security planned for 2011 will seek to reinforce the coordination of the EU risk management and will strengthen the existing structures and mechanisms in the public health area.

On **threat assessment**, the Commission will support efforts to improve mutual understanding of the various definitions of threat levels and to improve communication when these levels are subject to change. In 2012, Member States are invited to produce their own threat assessments on terrorism and other malicious threats. From 2013 the Commission will, in liaison with the EU Counter-Terrorism Coordinator and Member States prepare regular overviews of current threats, based on national assessments.

The EU should establish by 2014 a coherent **risk management policy** linking threat and risk assessments to decision making.

Action 3: Link up the different situation awareness centres

An effective and coordinated response to crises depends on being able to quickly pull together a comprehensive and accurate overview of the situation. Information on a situation inside or outside the EU must be drawn from all relevant sources, analysed, assessed and shared with Member States and the operational and policy branches in EU institutions. With fully networked secure facilities, the right equipment and properly trained staff, the EU can **develop an integrated approach based on a common and shared appreciation in a crisis situation**.

Based on existing capabilities and expertise, the Commission will, by 2012, reinforce the links between sector-specific early warning and crisis cooperation functions[333], including those for health, civil protection, nuclear risk monitoring

---

331 Article 222 TFEU.

332 Council Conclusions on a Community framework on disaster prevention within the EU, November 2009.

333 The Commission will continue to use and further develop ARGUS—see COM(2005) 662—and related procedures for cross-hazard multi-sectoral crises as well as for coordination across all Commission services.

and terrorism, and make use of EU-led operational programmes. These arrangements will help improve links with EU agencies and the European External Action Service, including the Situation Centre, and enable better information sharing and, where required, joint EU threat and risk assessment reports.

Effective coordination between the EU institutions, bodies and agencies requires a coherent general framework to protect classified information. The Commission intends therefore to come forward with a proposal to address this in 2011.

Action 4: Develop a European Emergency Response Capacity for tackling disasters

The EU should be able to respond to disasters both inside and outside the EU. Lessons learnt from recent events suggest that there is room for further improvement in terms of rapidity of deployment and appropriateness of action, operational and political coordination and visibility of the EU's response to disasters internally as well as externally.

In line with the recently-adopted disaster response strategy[334], the EU should **establish a European Emergency Response Capacity** based on pre-committed Member States' assets on-call for EU operations and pre-agreed contingency plans. Efficiency and cost-effectiveness should be improved through shared logistics, and simpler and stronger arrangements for pooling and co-financing transport assets. Legislative proposals will be tabled in 2011 to implement the key proposals.

3. Implementing the strategy

The realisation of the Internal Security Strategy in Action is the shared responsibility of the EU institutions, Member States and EU agencies. This requires an agreed process for implementing the strategy with clear roles and responsibilities, with the Council and the Commission, in close liaison with the European External Action Service, driving progress towards meeting the strategic objectives. In particular, the Commission will support the activities of the Standing Committee on Operational Cooperation on Internal Security (COSI) to ensure that operational cooperation is promoted and strengthened, and that coordination of the action of Member States' competent authorities is facilitated.[335]

Implementation

Priorities shall be reflected both in the operational planning of EU agencies, at national level, and in Commission work programmes. The Commission will ensure that security-related activities, including security research, industrial policy and projects under EU internal security-related funding programmes, are coherent with the strategic objectives. Security research will continue to be funded under the multiannual research and development framework programme. To ensure a successful implementation the Commission will establish an internal working group. The European External Action Service will be invited to participate to ensure consistency with the wider European Security Strategy and to exploit synergies between internal and external policies, including risk and threat

---

[334] 'Towards a stronger European disaster response: the role of civil protection and humanitarian assistance'—COM(2010) 600.

[335] Article 71 TFEU; see also Council Decision 2010/131/EU on setting up the Standing Committee on operational cooperation on internal security.

assessments. For the same purpose, COSI and the Political and Security Committee should work together and meet regularly.

EU funding that might be necessary for the period 2011–2013 will be made available within the current ceilings of the multiannual financial framework. For the period post-2013, internal security funding will be examined in the context of a Commission-wide debate on all proposals to be made for that period. As part of that debate, the Commission will consider the feasibility of setting up an Internal Security Fund.

Monitoring and evaluation

The Commission will, with the Council, monitor progress on the Internal Security Strategy in Action. The Commission will produce an annual report to the European Parliament and the Council on the strategy on the basis of contributions from Member States and EU agencies and using as far as possible existing reporting mechanisms. The annual report will highlight the main developments for each of the strategic objectives, assessing whether actions at EU and Member State level have been effective, and making Commission recommendations as appropriate. The annual report will also include an annex describing the state of internal security. It will be produced by the Commission, supported by contributions from the relevant agencies. The report could inform annually the European Parliament and Council debates on internal security.

Concluding remarks

Our world is changing, and so are the threats and challenges around us. The response from the European Union should evolve correspondingly. By working together to implement the actions outlined in this strategy, we are on the right path. At the same time, it is inevitable that however strong and well-prepared we are, threats can never be entirely eliminated. That is why it is all the more important that we step up our efforts.

With the Lisbon Treaty as a new legal framework, the Internal Security Strategy in Action should become the shared agenda for the EU over the next four years. Its success is dependent on the combined efforts of all EU actors, but also on cooperation with the outside world. Only by joining forces and working together to implement this strategy can Member States, EU Institutions, bodies and agencies provide a truly coordinated European response to the security threats of our time.

APPENDIX 5: LIST OF ACRONYMS AND ABBREVIATIONS

ACPO	Association of Chief Police Officers
AFSJ	Area of Freedom, Security and Justice
ARO	Asset Recovery Office
Article 36 Committee	The Committee of officials of Member States constituted under Article 36 of the TEU prior to its amendment by the Treaty of Lisbon to coordinate work on police and judicial cooperation in criminal matters. The predecessor of COSI.
CATS	Comité de l'article trente-six. The French acronym for the Article 36 Committee, q.v.
CBRN	Chemical, biological, radiological and nuclear substances
CCWP	Customs Cooperation Working Party
CEPOL	European Police College
CEPS	Centre for European Policy Studies
CER	Centre for European Reform
CERT	Computer Emergency Response Team
CFSP	(EU) Common Foreign and Security Policy
CFR	(EU) Charter of Fundamental Rights
CII	Critical Information Infrastructure
CIIP	Critical Information Infrastructure Protection
COREPER	Comité des représentants permanents: the French acronym for Committee of Permanent Representatives of the Member States to the EU
COSI	coopération opérationnelle en matière de sécurité intérieure. The French acronym for the Standing Committee on Operational Cooperation on Internal Security, constituted under Article 71 TFEU. The successor to the Article 36 Committee, q.v.
COTER	A Council working group of national foreign ministry officials which considers external security threats in the context of the CFSP
CP 931	Working Party on the application of specific measures to combat terrorism
CSDP (EU)	Common Security and Defence Policy
CSIRT	Computer Security Incident Response Team (now synonymous with CERT)
CSIRTUK	Combined Security Incident Response Team (UK)
CSS	(UK) Cyber Security Strategy
CTC	(EU) Counter-terrorism coordinator
CTG`	Counter-terrorism group: a Council working group composed of the heads of the intelligence services of the Member States

CTS	The EU counter-terrorism strategy adopted during the UK Presidency in 2005
DG HOME	Commission Directorate-General for Home Affairs
DG INFSO	Commission Directorate-General for Information Society and Media
DG RELEX	Commission Directorate-General for External Relations
EADRCC	NATO Euro-Atlantic Disaster Response and Coordination Centre
EASO	European Asylum Support Office
EAW	European Arrest Warrant
EC	European Community
ECCP	European CyberCrime Platform
ECHR	European Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights)
EEA	European Economic Area
EEAS	European External Action Service
EERC	European Emergency Response Capacity
EGC	European Government CERT Group
EISAS	European Information Sharing and Alert System
EMCDDA	European Monitoring Centre for Drugs and Drug Addiction
ENISA	European Network and Information Security Agency
EPCIC	European Programme for Critical Infrastructure Protection
EPCTF	European Police Chiefs Task Force
ESS	European Security Strategy, or External Security Strategy
ETS	EU Emissions Trading System
EU	European Union
Eurodac	The fingerprint database for the Dublin Regulation on jurisdiction to examine asylum applications.
Europol	European Police Office
EUROSUR	European Border Surveillance System
FIRST	Forum for Incident Response and Security Teams
Frontex	European Agency for the management of operational cooperation at the external borders
GovCertUK	Government CERT UK: the Government CERT for the public sector system
G6	Group of 6. An unofficial group of the interior ministers of the six largest Member States
ICPEM	Institute of Civil Protection and Emergency Management
IfS	Instrument for Stability
IPPR	(UK) Institute for Public Policy Research
ISF	Internal Security Fund

ISP	Internet Service Provider
ISS	Internal Security Strategy
JAIEX	Justice and Home Affairs External Working Group
JANET	Joint Academic Network, a CERT
JCNSS	Joint Committee on the National Security Strategy
JHA	Justice and Home Affairs
JIT	Joint Investigation Team
JLS	Justice, Liberté, Sécurité: the French acronym for the former Commission Directorate-General for Freedom, Security and Justice
LEWP	Law Enforcement Working Party
LIBE	European Parliament Committee on Civil Liberties, Justice and Home Affairs
MFF	Multi-annual financial framework
MIC	Monitoring and Information Centre, Civil Protection Unit, European Commission
NATO	North Atlantic Treaty Organisation
NSS	(UK) National Security Strategy
OCSIA	(UK) Office of Cyber Security and Information Assurance
OCTA	Organised Crime Threat Assessment
OECD	Organisation for Economic Cooperation and Development
PNR	Passenger Name Record
PSC	Political and Security Committee
PWGT	Police Working Group on Terrorism
RABIT	Rapid Border Intervention Teams
SCFIA	Strategic Committee on Immigration, Frontiers and Asylum
SIS	Schengen Information System
SitCen	(EU) Joint Situation Centre
SOCA	Serious Organised Crime Agency
TEC	Treaty establishing the European Community
TE-SAT	Europol's Terrorist Situation and Trend Reports
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union
TFTP	Terrorist Finance Tracking Program: the US means of tracking international financial transactions through SWIFT (Society for Worldwide Interbank Financial Telecommunications) for the prevention of terrorism: the subject of an agreement between the EU and the US
TWG	Terrorist Working Group: a Council working group of national interior ministry officials

UKREP	The Brussels office of the United Kingdom Permanent Representative to the EU
UN	United Nations
VIS	Visa Information System