EUROPEAN COMMISSION

Brussels, 11 I 2012
C(2012)41 final

Dear Lord Roper,

The Commission has examined with great interest the report by the House of Lords entitled 'The EU Internal Security Strategy' {COM(2010) 673} and would like to thank the members of the European Union Committee of the House of Lords for its efforts in scrutinising the Commission's proposals to improve the EU's internal security.

The European Commission welcomes the fact that its Communication "The EU Internal Security Strategy in Action: Five steps towards a more secure Europe" is seen as a pragmatic means to articulate a comprehensive approach to the EU's internal security. The Communication aims to put forward a shared agenda for Member States, the European Parliament, the Commission, the Council and EU agencies as well as others, including civil society and local authorities, with the goal of meeting today's internal security challenges.

Your report shows that there is, overall, strong support from the House of Lords for the aim, the priorities and the content set out in the Communication. In the annex to this letter you will find a detailed Commission reply to the points raised by Your Chamber.

I am looking forward to continuing our political dialogue on these important matters, whilst apologising for the undue delay in replying to this report.

Yours sincerely,

Maroš Šefčovič
Vice President

Lord Roper
Chairman of the European Union Committee
House of Lords
London
SW1A 0PW
United Kingdom

ANNEX

COMMISSION REPLY TO the Report of the House of Lords entitled 'The EU Internal Security Strategy'

***Radicalisation and recruitment** (point 223)*

The Commission fully recognises that Member States have the primary role in this field. The priority actions suggested at EU level, such as the production of a handbook to help exchange best practices, aim to support the Member States in that role. The Commission would note that the Council, in its conclusions of 24-25 February 2011 on 'The EU Internal Security Strategy in Action', explicitly and unanimously agreed to the Commission's five strategic objectives, including the one on addressing radicalisation and recruitment.

***The role of armed forces** (point 227)*

Military assets can indeed be useful in supporting civil protection and humanitarian assistance, notably in large-scale natural disasters, as fully acknowledged in EU civil protection legislation[1], as well as in the Commission's most recent policy initiatives related to disaster response, notably its Communication to the European Parliament and the Council 'Towards a stronger European disaster response: the role of civil protection and humanitarian assistance' of 26 October 2010[2] which is linked to the ISS. When deployed outside EU, the use of military assets is governed by the UN's 'Oslo guidelines', and the 'MCDA' guidelines, which notably state that such assets should operate under civilian leadership and be used as a last resort when no civilian alternative is available[3]. Military assets to support EU disaster response can be engaged either through Member States' civil protection contact points or through the EU Military Staff, which facilitate their deployment. These arrangements have been used successfully in a number of emergencies, including in response to floods in Pakistan and the earthquake in Haiti in 2010, and the evacuation of EU citizens and third country-nationals during the Libyan crisis in 2011.

Furthermore, procedures and criteria have been put in place to make information available to the EU Civil Protection Mechanism from the database of military assets and capabilities relevant to the protection of civilian populations against the effects of terrorist attacks. It is the Commission's intention to continue and to build upon these positive practices.

---

[1] Council Decision of 8 November 2007 establishing [EU] Civil Protection Mechanism (recast), 2007/779/EC, Euratom, Article 4 para 5.

[2] COM(2010)600 final, chapter 4.6.

[3] UN Guidelines on the Use of Foreign Military and Civil Defence Assets in Disaster Relief - "Oslo Guidelines" (Revision 1.1, November 2007), and Guidelines on the Use of Military and Civil Defence Assets to Support United Nations Humanitarian Activities in Complex Emergencies, March 2003.

The development of a European emergency response capacity *(point 230)*

In its Communication of 26 October 2010 on disaster response, the Commission also announced the development of the European Emergency Response Centre by merging the Commission's Monitoring and Information Centre (MIC) and the former DG ECHO humanitarian aid crisis rooms into a genuine response centre, operational on a 24 hours basis and responsible for coordinating the EU's civilian disaster response. The Centre will ensure a continuous exchange of information with both the civil protection and humanitarian aid authorities on the needs for assistance and the offers made by EU Member States and other actors. This will ensure that Member States can make informed decisions on funding and offers of additional assistance. For emergencies outside the EU, the Centre would be responsible for collecting information on all available European assistance in-kind and ensuring its coherence vis-à-vis the UN coordination system and the affected country.

A consolidated Emergency Response Centre will also facilitate operational coordination with other EU actors. This would involve sharing information and analysis with the geographic departments of the European External Action Service (EEAS) (including the Situation Centre, where appropriate) and EU delegations. It would also concern cooperation with the EEAS crisis management structures. In addition, the Centre should be a point of liaison with relevant parts of the EEAS, including in view of CFSP/CSDP missions deployed in third countries. The Centre will be linked to the situation awareness arrangements being developed as part of the ISS and will thus contribute to increase Europe's resilience towards disasters.

In terms of links between the EU and NATO's disaster response tools, NATO's Euro-Atlantic Disaster Response Coordination Centre (EADRCC) regularly informs the MIC on its response to major emergencies. The MIC also exchanges information with the EARDCC when both have been activated for the same emergency.

The Commission takes note of the concerns expressed by the House of Lords and would like to emphasise that the proposed Emergency Response Capacity in the form of a pool of Member States' assets committed to EU operations is envisaged as a fully voluntary system. Member States would remain free to decide whether or not they want to participate in the arrangements, which aim to improve European disaster response through better planning, for which a degree of predictability is needed as to which assets can be relied upon. If a Member State does choose to commit some of their assets to the pool, there would be an expectation that these assets would be made available for European operations, unless the Member State in question were to have specific reasons for not deploying (e.g. due to a domestic emergency). Even when deployed in European operations, the teams would remain under national direction and control. This proposal is a part of the Commission's bottom-up approach of strengthening the EU's disaster response system by building on Member States' assets.

Cyber-security: the challenge *(points 231/232)*

The Commission shares the view that it is now time for a change in the way the EU addresses cyber-security issues, considering the importance of the Internet for our economy and society, the constantly increasing level of threats and the potential damage that incidents and disruption could inflict on the EU and Member States. The Commission has, therefore, called on the Member States to strengthen their commitment to reinforcing their national cyber-security capabilities.

The EU institutions, bodies and agencies have taken an important step to counter the threat of cyber attacks against their own information systems and networks by setting up a joint Computer Emergency Response Team (CERT) Pre-configuration team on 1 June 2011. The team is made up of IT security experts from the EU institutions. Within 12 months, an assessment will be made, ahead of a decision on the conditions for establishing a full-scale CERT for the EU institutions.

***Cyber-security: the role of the EU** (point 233)*

The Commission is committed to increasing the level of cyber-security in Europe. The Digital Agenda for Europe[4], under its Trust and Security pillar, launched 14 actions in this respect.

On 31 March 2011, the Commission adopted a Communication on Critical Information Infrastructure Protection (CIIP)[5]. It describes the next steps for action at both European and international level. A number of areas were identified where reinforced efforts are needed to strengthen national cyber-security capabilities: the establishment of National/Governmental CERTs and the creation of a well-functioning network of National/Governmental CERTs in Europe; the development of national cyber incident contingency plans and of a European cyber incident contingency plan; the organisation of regular national and pan-European cyber incident exercises.

***Improving response capabilities** (Point 239)*

In its 2011 Communication on CIIP[6], the Commission restated the need for Member States to improve and reinforce their national cyber-security capabilities in order to ensure the highest level of protection within the EU. A notably element was that all Member States should establish their national/governmental CERTs by the end of 2011 with a view to creating a well-functioning network of CERTs in Europe by 2012. The Council Conclusions on CIIP[7], adopted on 27 May 2011, include a commitment to this effect.

***Raising public awareness** (Point 240)*

The Commission encourages a strong working relationship between the public and private sectors in the area of network and information security.

In line with the 2009 action plan on CIIP[8], the Commission has set up a European Public Private Partnership for Resilience (EP3R) with the aim of supporting information sharing and dissemination of good practices between public and private stakeholders. The EP3R will contribute to international cooperation on cyber-security, in particular by supporting the activities of the EU-US Working Group on Cyber-security and Cyber-crime, where public-private partnerships are one of the priority areas.

---

[4] *COM(2010)245.*
[5] *COM(2011)163.*
[6] *COM(2011)163.*
[7] *http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/trans/122265.pdf.*
[8] *COM(2009)149.*

International cooperation *(Points 241/242)*

The Commission agrees that an "EU-only" solution to the challenges of cyber-security is not possible. International cooperation on cyber security is indispensable and its efficiency can be ensured only by reinforcing partnerships and intensifying collaboration with strategic players.

A significant step in this direction has been made with the agreement (in November 2010) between the EU and US to strengthen trans-Atlantic cooperation by creating an EU-US Working Group on Cyber-Security and Cyber-Crime. The Working Group deals with four specific priority areas, namely cyber incident management, public-private partnerships, awareness raising and cybercrime. In addition, this Working Group may consider options for cooperation with other regions or countries addressing similar issues, so as to share approaches and activities, and to avoid duplication of effort. It could also facilitate a joint approach in international forums.

The Commission welcomes the UK's recent initiative to organise an international conference on cyber-security.

Transparency and parliamentary oversight, in particular in relation to the work of Europol *(Point 250)*

On 17 December 2010, the Commission adopted a Communication on parliamentary scrutiny of Europol, which paves the way for a more robust parliamentary oversight of the agency's activities. Over more than a decade, the European Parliament – and also to a certain extent, the national Parliaments – have expressed the wish to exercise closer supervision of Europol's work. The Lisbon Treaty calls for the establishment of scrutiny procedures associating the European and national Parliaments. This is why the Commission wished to kick-start a discussion with the EU institutions and with national parliaments on this aspect of Europol's future framework, by presenting its initial views in a Communication. These procedures will be enshrined in the future regulation governing Europol's structure and missions.

The Commission welcomes the opinions expressed by the House of Lords as a valuable contribution – alongside those from other national Parliaments and other institutional stakeholders – in preparing the content of the procedures for parliamentary scrutiny which will form part of the future legislative proposal on Europol.

EU agencies *(Point 251)*

The agencies are very important actors in operational support for the implementation of the ISS. The Commission agrees that the potential of the agencies can be best exploited if they do not act alone, but rather in close co-operation and coordination with each other agencies, with Member States and with all the EU institutions.

The Commission is willing to take a lead in establishing an administrative platform for multilateral cooperation between the agencies and to be involved at an early stage in all activities related to increasing the coherence of the work of the JHA agencies, including reporting on the cooperation of the JHA agencies.

The Action Plan implementing the Stockholm Programme already provides for development of a methodology based on common parameters for analysis of threats at European level, where full use should be made of Europol, the Joint Situation Centre (SitCen) and Eurojust in the fight against terrorism. It also tasks the Commisison to come

up with a proposal on information exchange between Europol, Eurojust and Frontex. The Action Plan further states that the European Asylum Support Office should develop methods to better identify those individuals within mixed migration flows who are in need of international protection, and to cooperate with Frontex wherever possible. A Communication on possible measures to promote the exchange of information between Member States, and with Europol, on travelling violent offenders in connection with major events is also planned in 2012.

Furthermore, in line with an inter-institutional debate between the European Parliament, the Council and the Commission on a common approach on how to improve the functioning of the agencies, their coherence and effectiveness, the Commission will endeavour to ensure coherence and complementarity when revising the agencies' legal bases (in particular Frontex, Europol, Cepol).

***Research** (Point 254)*

The Commission is examining options for reinforcing and better coordinating research activities in order to respond both to present and future security challenges. The future EU funding programme for research and innovation, Horizon 2020[9], will offer a good opportunity for a comprehensive approach to technological and socio-economic research and innovation.

[9] http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/11/435&format=HTML&aged.