Opinion of the European Economic and Social Committee on the ‘Proposal for a Regulation of the European Parliament and of the Council concerning the European Network and Information Security Agency (ENISA)’

(2011/C 107/12)

Rapporteur: Mr MORGAN

On 19 October 2010 the Council decided to consult the European Economic and Social Committee, under Article 114 of the Treaty on the Functioning of the European Union, on the Proposal for a Regulation of the European Parliament and of the Council concerning the European Network and Information Security Agency (ENISA)


The Section for Transport, Energy, Infrastructure and the Information Society, which was responsible for preparing the Committee’s work on the subject, adopted its opinion on 2 February 2011.

At its 469th plenary session, held on 16 and 17 February 2011 (meeting of 17 February), the European Economic and Social Committee adopted the following opinion with 173 votes in favour and five abstentions.

1. Conclusions and recommendations

1.1 The EESC is very conscious of the scale of dependency which civil society now has on services provided over the internet. The Committee is equally concerned about the relative ignorance of civil society about its own cyber security. It is the opinion of the EESC that the European Network and Information Security Agency (ENISA) is the agency responsible for assisting Member States and Service Providers to raise their general security standards so that all internet users take the steps necessary to ensure their own personal cyber security.

1.2 Accordingly the EESC supports the proposal to develop ENISA for the purpose of contributing to a high level of network and information security within the Union and in order to raise awareness and develop a culture of network and information security in society for the benefit of the citizens, consumers, enterprises and public sector organisations in the Union, thus contributing to the smooth functioning of the internal market.

1.3 The mission of ENISA is vital for the secure evolution of the network infrastructure of EU government, industry, commerce and civil society. The EESC expects the European Commission to set the highest performance standards for ENISA and monitor its performance in the context of evolving and emerging threats to cyber security.

1.4 The cyber strategies outlined by NATO, Europol and the EU Commission all depend on effective cooperation with Member States which themselves have a kaleidoscope of internal agencies dealing with cyber security issues. NATO and Europol strategies are intended to be pro-active and operational. Within the EU Commission strategy, ENISA is clearly an important part of the complex jigsaw of Critical Information Infrastructure Protection (CIIP) agencies and missions. While the new Regulation does not propose an operational role for ENISA, the EESC still sees ENISA as the Agency primarily responsible for CIIP in EU civil society.

1.5 The operational responsibility for cyber security at the Member State level belongs to Member States but standards of CIIP in the 27 Member States are clearly mixed. Bringing the less well equipped Member States up to an acceptable level is the role of ENISA. It must ensure cooperation between Member States and assist them in the application of best practice. In the context of cross border threats, ENISA’s role must be warning and prevention.

1.6 ENISA will also need to be involved in international cooperation with powers outside the EU. Such cooperation will be highly political, involving many EU branches, but the EESC believes that ENISA must find its place in the international scene.

1.7 The Committee believes that ENISA can fulfil a very valuable role in contributing to and initiating research projects in the security domain.

1.8 Within the framework of the Impact Assessment, the EESC will not at present support the full scale implementation of options 4 and 5 which would make ENISA an operational agency. Cyber security is such a huge problem, with threats developing dynamically, that Member States must retain the capability to fight pro-actively against threats. The development
of EU operational agencies usually ends up by de-skilling Member States. In the cyber security domain the reverse is true; Member States must be up-skilled.

1.9 The EESC understands the Commission’s view that ENISA should have a defined and well controlled mission with matching resources. Even so, the EESC is concerned that the finite 5-year mandate of ENISA may restrict long-term projects and jeopardise the development of human capital and knowledge within the Agency. This will be quite a small Agency dealing with a big and growing problem. The scope and scale of ENISA’s mission means that it must employ specialist teams. It will have a mix of work: both short-term tasks and long-term projects. Accordingly, the Committee would prefer that the mandate for ENISA be dynamic and open-ended, confirmed on a rolling basis by periodic assessments and evaluations. Resources could then be allocated progressively, as and when justified.

2. Introduction

2.1 This opinion concerns a Regulation to further develop the ENISA.

2.2 The Commission set out its first proposal for a policy approach to network and information security in a 2001 Communication (COM(2001) 298 final). Mr Retureau prepared a comprehensive opinion (1) in response to the Communication.

2.3 The Commission then proposed a Regulation, to set up ENISA (COM(2003) 63 final). The EESC opinion (2) on this Regulation was written by Mr Lagerholm. The agency was actually established by EC Regulation 460/2004.

2.4 As internet usage continued to increase exponentially, information security became a growing concern. In 2006 the Commission published a Communication outlining a Strategy for a Secure Information Society (COM(2006) 251 final). Mr Pezzini wrote the EESC opinion (3).

2.5 As the concern about information security increased, the Commission came forward in 2009 with a proposal for Critical Information Infrastructure Protection (COM(2009) 149 final). Mr McDonogh wrote the opinion (4) which was approved by the EESC Plenary in December 2009.

2.6 It is now proposed to strengthen and improve ENISA for the purpose of contributing to a high level of network and information security within the Union and in order to raise awareness and develop a culture of network and information security in society for the benefit of the citizens, consumers, enterprises and public sector organisations in the Union, thus contributing to the smooth functioning of the internal market.

2.7 However, ENISA is not the only security agency planned for EU cyberspace. The response to cyber warfare and cyber terrorism is the responsibility of the military. NATO is the main agency in this sphere. According to its new strategic concept published in Lisbon in November 2010 (available at http://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf), NATO will ‘develop further its ability to prevent, detect, defend against and recover from cyber-attacks, including by using the NATO planning process to enhance and coordinate national cyber-defence capabilities, bringing all NATO bodies under centralized cyber protection, and better integrating NATO cyber awareness, warning and response with member nations’.

2.8 Following the cyber attack on Estonia in 2007, the Cooperative Cyber Defence Centre of Excellence (CCD COE) was formally established on the 14th of May, 2008, in order to enhance NATO’s cyber defence capability. Located in Tallinn, Estonia, the Centre is an international effort that currently includes Estonia, Latvia, Lithuania, Germany, Hungary, Italy, the Slovak Republic, and Spain as sponsoring nations.

2.9 Electronic crime at EU level is the responsibility of Europol. The following is an extract from written evidence given by Europol to the House of Lords (see http://www.publications.parliament.uk/pa/ld200910/ldselect/ldeucom/68/ 68we05.htm):

It is clear that law enforcement agencies need to keep pace with the technological development of criminals to ensure that the crimes they perpetrate can be effectively prevented or detected. In addition, given the borderless nature of high-tech crime, capacity must be of a similarly high standard throughout the EU so as not to allow ‘weak spots’ to develop where high-tech crime can flourish with impunity. This capacity is far from homogeneous in the EU. In fact there is clear asymmetrical development; some MS are forging ahead with great advances in certain areas, whilst other MS lag behind in terms of technology. This creates the need to have a centralised service to assist all MS to coordinate joint activities, promote the standardisation of approaches and quality standards and identify and share best practice; only in this way can a homogenous EU law enforcement effort to high-tech crime fighting be assured.

2.10 The High Tech Crime Centre (HTCC) was established at Europol in 2002. It is a relatively small unit but it is expected to grow in the future as the centrepiece of Europol’s work in this area. HTCC plays a major role in coordination, operational support, strategic analysis and training. The training function is particularly important. In addition, Europol has established ECCP, the European Cyber Crime Platform. It is focused on the following topics:

— The Internet Crime Reporting Online System (I-CROS)
— The Analysis Work File (Cyborg)
— The Internet and Forensic Expertise recipient (I-FOREX).

2.11 The EU cyber security strategy is outlined in the ‘Trust and Security’ chapter of the Digital Agenda for Europe. The challenges are outlined as follows:

So far, the internet has proved remarkably secure, resilient and stable, but IT networks and end users’ terminals remain vulnerable to a wide range of evolving threats: in recent years, spam emails have grown to the point of heavily congesting e-mail traffic on the internet – various estimates suggest between 80 % to 98 % of all circulating emails - and they spread a wide range of virus and malicious software. There is a growing scourge of identity theft and online fraud. Attacks are becoming increasingly sophisticated (trojans, botnets, etc.) and often motivated by financial purposes. They can also be politically motivated as shown by the recent cyber-attacks that targeted Estonia, Lithuania and Georgia.

2.12 Actions committed in the Agenda are:

Key Action 6: Present in 2010 measures aiming at a reinforced and high level Network and Information Security Policy, including legislative initiatives such as a modernised ENISA, and measures allowing faster reactions in the event of cyber attacks, including a Computer Emergency Response Team (CERT) for the EU institutions;

Key Action 7: Present measures, including legislative initiatives, to combat cyber attacks against information systems by 2010, and related rules on jurisdiction in cyberspace at European and international levels by 2013.

2.13 In a Communication of November 2010 (COM(2010) 673 final), the Commission has taken the Agenda forward by outlining the EU Internal Security Strategy. It has five objectives and the third of these is to raise levels of security for citizens and businesses in cyberspace. Three action programmes are envisaged and the details of the actions are outlined in the following table (taken from the Communication, available at http://ec.europa.eu/commission_2010-2014/malmstrom/archive/internal_security_strategy_in_action_en.pdf).

<table>
<thead>
<tr>
<th>OBJECTIVES AND ACTIONS</th>
<th>RESPONSIBLE</th>
<th>TIMING</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>OBJECTIVE 3:</strong> Raise levels of security for citizens and businesses in cyberspace</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Action 1:</strong> Build capacity in law enforcement and the judiciary</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Establishment of an EU cybercrime centre</td>
<td>Subject to the COM’s feasibility study 2011</td>
<td>2013</td>
</tr>
<tr>
<td>Develop capacities for investigation and prosecution of cybercrime</td>
<td>MS with CEPOL, Europol and Eurojust</td>
<td>2013</td>
</tr>
<tr>
<td><strong>Action 2:</strong> Work with industry to empower and protect citizens</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Establishment of cybercrime incident reporting arrangements and provide guidance for citizens on cyber security and cybercrime</td>
<td>MS, COM, Europol, ENISA and the private sector</td>
<td>Ongoing</td>
</tr>
<tr>
<td>Guidelines on cooperation in handling illegal content online</td>
<td>COM with MS and the private sector</td>
<td>2011</td>
</tr>
<tr>
<td><strong>Action 3:</strong> Improve capability for dealing with cyber attacks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Establishment of a network of Computer Emergency Response Teams in every MS and one for EU institutions, and regular national contingency plans and response and recovery exercises.</td>
<td>MS and EU institutions with ENISA</td>
<td>2012</td>
</tr>
<tr>
<td>Establishment of European information sharing and alert system (EISAS)</td>
<td>MS with COM and ENISA</td>
<td>2013</td>
</tr>
</tbody>
</table>
2.14 The cyber strategies outlined by NATO, Europol and the EU Commission all depend on effective cooperation with Member States which themselves have a kaleidoscope of internal agencies dealing with cyber security issues. NATO and Europol strategies are intended to be pro-active and operational. Within the EU Commission strategy, ENISA is clearly an important part of the complex jigsaw of Critical Information Infrastructure Protection (CIIP) agencies and missions. While the new Regulation does not propose an operational role for ENISA, the EESC still sees ENISA as the Agency primarily responsible for CIIP in EU civil society.

3. **The ENISA proposal**

3.1 The problem to be addressed by ENISA has seven drivers:

(1) The fragmentation and diversity of national approaches

(2) Limited European early warning and response capability

(3) A lack of reliable data and limited knowledge about evolving problems

(4) A lack of awareness of NIS risks and challenges

(5) The international dimension of NIS problems

(6) The need for models of collaboration to ensure adequate policy implementation

(7) The need for more efficient action against cyber crime.

3.2 The ENISA proposal provides a focal point for both existing policy provisions and the new initiatives outlined in the EU Digital Agenda.

3.3 The existing policies to be supported by ENISA include:

(i) A European Forum for Member States (EFMS) aimed at fostering discussion and exchange regarding good policy practices with the aim of sharing policy objectives and priorities on security and resilience of ICT infrastructure

(ii) A European Public-Private Partnership for Resilience (EP3R), which is the flexible Europe-wide governance framework for resilience of ICT infrastructure, which operates by fostering the cooperation between the public and the private sector on security and resilience issues

(iii) The Stockholm Programme, adopted by the European Council on 11 December 2009, which promotes policies ensuring network security and allowing faster reaction in the event of cyber attacks in the Union.

3.4 New developments to be supported by ENISA include:

(i) Intensifying EFMS activities

(ii) Supporting the European (EP3R) by discussing innovative measures and instruments to improve security and resilience

(iii) Putting the security requirements of the regulatory package on electronic communications into practice

(iv) Facilitating EU-wide cyber security preparedness exercises

(v) Establishing a CERT for the EU institutions

(vi) Mobilising and supporting the Member States in completing and, where necessary, in setting up national/governmental CERTs in order to establish a well-functioning network of CERTs covering all of Europe

(vii) Raising awareness of NIS challenges.

3.5 Five different policy options were examined before this proposal was finalised. Each option had mission and resource options associated with it. The third option was chosen. This involves expanding the functions currently defined for ENISA and adding law enforcement and privacy protection agencies as stakeholders.

3.6 Under option 3, a modernised NIS Agency would contribute to:

— Reducing the fragmentation of national approaches (problem driver 1), increasing data and knowledge/information-based policy and decision making (problem driver 3) and increasing overall awareness of and the tackling of NIS risks and challenges (problem driver 4) by contributing to:

— more efficient collection of relevant information on risks, threats and vulnerabilities by each individual Member State;

— increased availability of information on current and future NIS challenges and risks;

— higher quality NIS policy provision in Member States.
— Improving European early warning and response capability (problem driver 2) by:

— helping the Commission and Member States to set up pan-European exercises, thereby achieving economies of scale in responding to EU-wide incidents;

— facilitating the functioning of the EP3R, which could ultimately lead to more investment triggered by common policy objectives and EU-wide standards for security and resilience.

— Promoting a common global approach to NIS (problem driver 5) by:

— increasing the exchange of information and knowledge with non-EU countries.

— Fighting cybercrime more efficiently and effectively (problem driver 7) by:

— being involved in non-operational tasks relating to NIS aspects of law enforcement and judicial cooperation, such as bi-directional exchange of information and training (e.g. in cooperation with the European Police College CEPOL).

3.7 Under option 3, ENISA would dispose of all resources necessary to perform its activities in a satisfactory in-depth way, i.e. allowing for a real impact. With more resources available (5), ENISA can take a much more pro-active role and take more initiatives to stimulate active participation by the stakeholders. Moreover, this new situation would allow for more flexibility to react quickly to changes in the constantly evolving NIS environment.

3.8 Policy option 4 includes operational functions for fighting cyber attacks and response to cyber incidents. In addition to the activities set out above, the Agency would have operational functions such as taking a more active role in EU CIIP, for example in incident prevention and response, specifically by acting as an EU NIS CERT and by coordinating national CERTs as an EU NIS Storm Centre, including both day-to-day management activities and handling emergency services.

3.9 Option 4 would produce a greater impact at operational level, in addition to the impacts to be achieved under option 3. By acting as an EU NIS CERT and by coordinating national CERTs, the Agency would contribute to higher economies of scale in responding to EU-wide incidents and lower operational risks for business due to higher levels of security and resilience, for example. Option 4 would require a substantial increase in the Agency's budget and human resources, which raises concerns about its absorption capacity and effective use of the budget in relation to the benefits to be attained.

3.10 Policy option 5 includes operational functions for supporting law enforcement and judicial authorities in fighting cybercrime. In addition to the activities listed in option 4, this option would enable ENISA to:

— provide support on procedural law (cf. Convention on Cybercrime): e.g. collection of traffic data, interception of content data, monitoring flows in case of denial-of-service attacks;

— be a centre of expertise for criminal investigation including NIS aspects.

3.11 Option 5 would achieve greater effectiveness in fighting cybercrime than options 3 and 4, with the addition of operational functions in supporting law enforcement and judicial authorities.

3.12 Option 5 would require a substantial increase in the Agency's resources and again raise concerns regarding absorption capacity and effective use of the budget.

3.13 While both options 4 and 5 would have greater positive impacts than option 3, the Commission believes that there are a number of reasons not to pursue these options:

— They would be politically sensitive for the Member States in relation to their CIIP responsibilities (i.e. a number of Member States would not be in favour of centralised operational functions).

— Enlarging the mandate as examined under options 4 and 5 may render the Agency's position ambiguous.

— Adding these new and completely different operational tasks to the Agency's mandate may turn out to be very challenging in the short run and there is a significant risk that the agency would not be able to carry out this kind of task properly within a reasonable time-span.

— Last, but not least, the cost of implementing options 4 and 5 is prohibitively high – the budget required would be four or five times as much as ENISA’s current budget.

(5) The reference to more resources is conditional on the ENISA proposal being approved in its present form.
4. **Provisions of the Regulation**

4.1 The Agency shall assist the Commission and Member States to meet the legal and regulatory requirements of network and information security.

4.2 The Management Board shall define the general direction of the operation of the Agency.

4.3 The Management Board shall be composed of one representative of each Member State, three representatives appointed by the Commission and one representative of each of the ICT industry, consumer groups and IT academia.

4.4 The Agency shall be managed by an independent Executive Director, who will be responsible for drawing up the work programme of the Agency for the approval of the Management Board.

4.5 The Executive Director is also responsible for drawing up an annual budget in support of the work programme. The Management Board must submit both the budget and the work programme for approval by the Commission and the Member States.

4.6 The Management Board, on the advice of the Executive Director, will establish a Permanent Stakeholders’ Group comprising experts from the ICT industry, consumer groups, academia, law enforcement and privacy protection authorities.

4.7 Because the Regulation is still at the proposal stage, there is some uncertainty about numbers. At present the Agency has 44-50 staff and a budget of EUR 8m. Conceptually, option 3 could involve a staff of 99 and a budget of EUR 17m.

4.8 The Regulation proposes a fixed term mandate of five years.

---

Brussels, 17 February 2011.

_The President of the European Economic and Social Committee_

Staffan NILSSON