Cyber security and defence

2012/2096(INI) - 17/10/2012 - Committee report tabled for plenary, single reading

The Committee on Foreign Affairs adopted an own-initiative report by Tunne KELAM (EPP, EE) on cyber security and defence. The main recommendations contained in the report are the following:

Actions and coordination in the European Union (EU): given that cyber threats and attacks against government, administrative, military and international bodies are a rapidly growing menace and occurrence in both the EU and globally, the report underlines, therefore, the need for a **global and coordinated approach to the question of cyber security** which should:

- establish a **common definition** of cyber security and defence and of what constitutes a defence-related cyber attack;
- a **common operating vision** and;
- take into account the **added value** of the existing agencies and bodies; as well as **good practices** from those Member States which already have national cyber security strategies.

The report calls on the Commission and the High Representative of the Union for Foreign Affairs and Security Policy to consider the possibility of a serious cyber attack against a Member State in their forthcoming proposal on the arrangements for the implementation of the Solidarity Clause (Article 222 TFEU).

The Council and the Commission are urged to unequivocally recognise **digital freedoms** as fundamental rights and as indispensable prerequisites for enjoying universal human rights, and together with the Member States, to elaborate a **White Paper** on Cyber Defence.

EU level: the Members stress the importance of **horizontal cooperation and coordination** on cyber security within and between EU institutionsand agencies.

The EU institutions are called on to: i) develop their cyber security strategies and contingency plans with regard to their own systems in the shortest time possible; ii) include in their risk analysis and crisis management plans, the issue of cyber crisis management.

The report also underlines the importance of:

- the efficient development of the **EU Computer Emergency Response Team** (EU-CERT) and of national CERTs as well as the development of national contingency plans in the event that action needs to be taken;
- to create as soon as possible at European level the Critical Infrastructure **Warning Information** Network;
- of **pan-European exercises** in preparation for large-scale network security incidents;
- and the definition of a **single set of standards** for threat assessment.

The report underlines the importance for Member States of **close cooperation with the European Defence Agency (EDA)** on developing their national cyber defence capabilities. It encourages the EDA to deepen its cooperation with NATO, national and international centres of excellence, the European Cybercrime Centre at Europol contributing to faster reactions in the event of cyber attacks.

The Member States, for their part, are urged to:

- develop and complete their respective **national cyber security and defence strategies** without further delay and ensure a solid policy-making and regulatory environment, comprehensive risk management procedures and appropriate preparatory measures and mechanisms;

- create **designated cyber security and cyber defence units** within their military structure**,** with a view to cooperating with similar bodies in other EU Member States;

- introduce **specialised courts** at regional level geared to ensuring that attacks on information systems are punished more effectively;

- develop **national contingency plans** and to include cyber crisis management in crisis management plans and risk analysis;

- make **research and development** one of the core pillars of cyber security and defenceand to encourage the training of engineers specialised in protecting information systems.

The Commission and Member States are urged to **come forward with programmes** to promote and raise awareness among both private and business users ingeneral safe use of the Internet. The Members propose that the Commission launch a **public pan-European education initiative** in this regard, calling on the Member States to include education on cyber security in school curricula from the earliest possible age;

Finally, the report:

- underlines the crucial role of meaningful and complementary cyber security **cooperation between the public authorities and the private sector**, both at EU and national level, with the aim of generating mutual trust;

- calls for the **speeding up of cooperation** and exchange of information on how to tackle cyber security issues **with third countries**;

- urges all relevant bodies in the EU dealing with cyber security and defence to **deepen their practical cooperation with NATO** with a view to exchanging experience and learning how to build resilience for EU systems;

- believes that the EU and the **US** should deepen their mutual cooperation to counter cyber attacks and cybercrime, since this was made a priority of the transatlantic relationship following the 2010 EU-US Summit in Lisbon.