COUNCIL OF THE EUROPEAN UNION

Brussels, 25 March 2013

7847/13

LIMITE

COSDP 273
PESC 339
COPS 123
POLMIL 21

NOTE

from:	Politico-Military Group
to:	Political and Security Committee
Subject:	PMG recommendations on the CSDP aspects of the Cybersecurity Strategy of the European Union

Following the agreement by the Politico-Military Group on 25 March 2013, the Political and Security Committee is invited to agree the PMG recommendations on the CSDP aspects of the Cybersecurity Strategy of the European Union.

PMG RECOMMENDATIONS
ON THE CSDP ASPECTS OF THE CYBERSECURITY
OF THE EUROPEAN UNION

INTRODUCTION

1. On 19 March, the PSC tasked the PMG to provide recommendations on the CSDP aspects of the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (doc. 6225/13 dated 8 February 2013). The aim is to provide the Friends of the Presidency concrete elements for the elaboration of Council Conclusions on the Strategy.

CONSIDERATIONS

2. The PMG welcomes the strong focus in the EU Cybersecurity Strategy on cyber defence in the framework of CSDP, as part of the multidimensional array of EU policies and within the multi-stakeholder model.

3. The PMG stresses that this Strategy should be used to enhance Member States' cyber defence capabilities to effectively protect information systems and infrastructure, including through the development of common standards to ensure compatibility and an adequate level of resilience at the national level. EU cyber defence efforts should focus on strengthening the involvement of the Member States in EU-wide cooperation and integrating cyber defence into the planning and conduct of CSDP missions and operations, capability requirements, concepts, training and exercises. The PMG emphasises the need for synergies between the relevant EU cyber policy areas, in particular network and information systems security, law enforcement and the defence community, but also the link towards capacity building.

4. The PMG stresses the need to implement the CSDP related cyber defence aspects of the Strategy to develop a cyber defence framework, as appropriate, building on ongoing capability development work within the European Defence Agency to develop and launch cooperative projects and programmes, and the EU Military Staff where possible.

5. The PMG notes the progress made in the EDA Project Team Cyber in addressing shortfalls, mapping priorities and identifying potential cyber defence pooling and sharing opportunities. It looks forward to the EDA pursuing its work in close cooperation with all stakeholders, including the Commission, ENISA, the European Cyber Crime Centre, the NATO Allied Command Transformation, the multinational Cyber Defence Centre of Excellence in Tallinn with which the EDA has recently established liaison through an exchange of letters, as well as the private sector and academia.

6. The PMG welcomes the ongoing close cooperation with NATO on the CSDP related cyber defence issues and looks forward to continued cooperation between the staffs within the existing framework. The PMG recalls the need for regular briefings and information exchange on this matter, including through cross briefings with NATO. The PMG also notes that possibilities for reciprocal participation in cyber defence exercises and training should be explored with the aim of maximizing synergies.

7. The PMG underlines the need to address CSDP related cyber defence issues in the preparation for the European Council debate on security and defence foreseen in December 2013, recalling the European Council conclusions on CSDP of 13/14 December 2012, in particular as regards to providing future oriented capabilities and developing the ability to respond to emerging security challenges.

RECOMMENDATIONS

8. The PMG highlights the following issues for consideration in the Friends of Presidency's work on the Council Conclusions on the Cybersecurity Strategy:

   a. The urgent need to <u>implement</u> and take forward the CSDP related cyber defence aspects of the Strategy to develop a cyber defence framework, as appropriate, and define concrete steps in this regard, also in view of the European Council debate on security and defence foreseen in December 2013. A single point of contact should be designated within the EEAS to steer these efforts.

b. The need to strengthen a comprehensive approach fostering the cooperation between EU civilian and military actors, including between public and private sector, in raising EU-wide resilience of critical infrastructures. Reinforcing close cooperation and coordination in responding to cyber incidents by defence actors, law enforcement, private sector and cyber security authorities is also necessary to effectively tackle cyber challenges, including incident management.

c. The need to enhance Member States' cyber defence capabilities, including through the development of common standards, and raising awareness through training and education in cyber security, making use of the European Security and Defence College and further improving training and exercising opportunities for Member States.

d. Using the existing mechanisms for Pooling and Sharing and utilising synergies with wider EU policies to build the necessary cyber defence capabilities in the Member States in the most efficient manner.

e. Research and development. Priority is given to encourage Member States to develop secure and resilient technologies for cyber defence with strong involvement of the private sector and academia, and to strengthen cyber security aspects in EDA research projects on the basis of a collaborative approach and as a good example of a dual use capability to be coordinated between EDA and Commission under the European Framework Cooperation.

f. Early warning and response mechanisms should be reviewed and tested in the light of new cyber threats, through dialogue between the EEAS, ENISA, EDA, Commission and Member States, with a view to seeking synergies and links with the defence community.

g. The need to pursue and strengthen EU-NATO cooperation on cyber defence, identifying priorities for continued EU-NATO cyber defence cooperation within the existing framework, including reciprocal participation in cyber defence exercises and training.

h. Embedding cyber defence aspects in the wider cyberspace policy.

_____