Question for written answer P-003732/2011
to the Commission
Rule 117
Ivailo Kalfin (S&D)

Subject: Europe's response action plan following a number of serious and targeted cyber attacks in the EU

Just before the last European Summit (23-24 March 2011), the Commission and the Parliament were hit by targeted and extremely serious cyber attacks aimed at particular European bodies. The European External Action Service appears to have been particularly affected by this recent attack.

Critical information infrastructures and strategic European data and information networks can best be protected by an optimum level of resilience. As it is very hard to recover data and identify potential intruders and the information stolen, effective prevention measures include a fast and effective capacity to respond to unexpected malicious threats.

This is unfortunately not the first time that EU Member States' strategic systems have been jeopardised. Other examples include the attacks on the French finance ministry networks prior to the G20 Summit in Paris, and the massive and numerous security breaches into the EU Emissions Trading System (ETS), which all resulted in considerable financial thefts. Intrusions into electronic registries have been reported in Austria, Greece, Germany and, most recently, in the Czech Republic, which forced the EU to close its ETS for at least a week.

In view of these worrying cyber breaches, does the Commission not consider it vital to enhance the European strategy on cyber security? If so, what steps does it plan to take in this field?

As the Commission is proposing to set up a European Computer Emergency Response Team (CERT), is it also planning further steps for the coordination and exchange of information with and between governmental CERTs? In this regard, what is the Commission's view on introducing minimum safety and resilience standards and terminology in close cooperation with the Member States' CERTs?