**Question for written answer E-010268/2014**
**to the Council**
Rule 130
**Sophia in 't Veld (ALDE), Cecilia Wikström (ALDE), Morten Helveg Petersen (ALDE), Angelika Mlinar (ALDE), Louis Michel (ALDE), Filiz Hyusmenova (ALDE), Nathalie Griesbeck (ALDE) and Gérard Deprez (ALDE)**

Subject: Regin malware used in cyber attacks on EU institutions and Belgacom

In spring 2011, the Commission discovered that its network had been hacked and infected with a sophisticated type of malware. In June 2013, *Der Spiegel* revealed that EU offices had been bugged and hacked by – allegedly – the US National Security Agency (NSA).

In September 2013, *Der Spiegel* published documents indicating that Belgacom had been hacked, allegedly by the UK Government Communications Headquarters (GCHQ), under the codename 'Operation Socialist', possibly affecting the European institutions as users of Belgacom's services.

Last week, computer researchers found that both highly sophisticated attacks had involved a piece of malware called Regin; they strongly suspected the NSA and GCHQ of being the source.

How will the Council address these findings with the UK and US authorities?

Will the Council request that the Computer Emergency Response Team (CERT-EU), the EU Agency for Network and Information Security (ENISA), the EU Intelligence Analysis Centre (IntCen) and/or Europol's Cybercrime Centre investigate the above-mentioned attacks? What role will each of these bodies play as regards the prevention and detection of, and investigations into, future cyber attacks?

What further steps will the Council take to safeguard EU institutions, bodies and agencies from cyber attacks and espionage carried out by its own Member States or by the intelligence services of third countries?