Question for written answer E-014895/2015
to the Commission
Rule 130
Louis Michel (ALDE)

Subject: Cyber security risk in nuclear power plants

The perception of cyber security risk is generally low in the nuclear industry, given that it has little experience in the subject since most nuclear power plants were designed at a time when cyber security risk did not exist. The risk has increased, notably due to the fact that commercial ('off the shelf') systems are now being used instead of heavy systems. In practice, many plants have gradually implemented a form of connectivity, leaving their IT systems at risk of being hijacked using methods that are sometimes very straightforward.

A lack of information sharing and of the transfer of knowledge to developing countries can also be observed. According to the British think tank Chatham House, the weaknesses essentially boil down to the absence of regulatory standards, insufficient training of personnel in the area, budget shortages and the lack of a culture of cyber security. There is a particularly urgent need to rethink the cyber security strategy of nuclear power plants.

What can Europe do to establish harmonised terminology at European level?

What is the EU doing to strengthen international cooperation?