

**Question for written answer E-001293/2018  
to the Commission**

Rule 130

**Lambert van Nistelrooij (PPE) and Esther de Lange (PPE)**

Subject: European cybersecurity strategy and a certification scheme for ICT products and services

The cybersecurity market presents a huge opportunity for Europe to place itself in the vanguard in the promotion of ICT security and also to make the European digital infrastructure more resilient against hacking, ransomware and DDOS attacks.

In the Netherlands, the Cyber Security Council (CSR) has published a report stating, in particular, that 'Internet of Things' (IoT) devices are vulnerable to cyberattacks. IoT applications are often poorly secured at present and thus a threat to our security and privacy. The CSR makes half a dozen recommendations on how to secure them better, including minimum requirements for IoT devices through a European certification scheme<sup>1</sup>.

What is the Commission's response to the analysis by the CSR indicating that poorly secured IoT devices pose a threat to the security and privacy of consumers and businesses, and what does it think of the idea of minimum security requirements for IoT devices, if nothing else?

Does the Commission consider it realistic to assume that a voluntary certification scheme for ICT services and products will reduce the security risks, and would it not be a logical consequence of a voluntary scheme that many ICT products and services, such as IoT devices, would not be covered, making them potentially unsafe, so that there would be a greater likelihood of attacks similar to the Mirai botnet attacks?

Does the Commission agree that the only option is to make the certification scheme compulsory for ICT products and services within the European Union? If not, why not?

---

<sup>1</sup> <https://www.nu.nl/gadgets/5083034/cyber-security-raad-pleit-keurmerken-iot-apparaten.html>