Question for written answer E-003061/2020
to the Commission
Rule 138
Lukas Mandl (PPE)

Subject: EU cyber defence during and beyond the COVID-19 pandemic

The number of cyber attacks against individuals and public institutions has increased sharply since the outbreak of the COVID-19 pandemic. According to Europol, criminals have exploited the crisis to distribute various malware packages. The Czech Republic reported a cyber attack on Brno University Hospital which forced the hospital to shut down its entire IT network and to postpone urgent surgeries. These attacks are coming from criminals but also from state actors. Against this background, I would like to ask the following questions:

1. What concrete measures are being taken by the Commission and the four EU organisations dealing with cyber security (ENISA, EDA, Europol and CERT-EU) to increase resilience and cyber security during the pandemic and beyond?

2. Given their partly overlapping mandates, how does the Commission aim to ensure coherent and effective cooperation among these four organisations?

3. Does the Commission have any concrete proposals on how to increase the EU's cyber defence capability in the military field, and to what extent can the envisaged European Defence Fund contribute to this end?