Question for written answer E-006374/2020
to the Commission
Rule 138
Elissavet Vozemberg-Vrionidi (PPE)

Subject: Funding for European companies seeking to improve cyber security

The EU has seen an increase in cyber threats since the beginning of the COVID-19 pandemic. Businesses providing essential services in the Member States, including those needed by the healthcare sector, are the principal targets of such malevolent attacks. According to a recent survey, four out of ten undertakings were affected in the last 12 months by a security incident, while data release blackmail rose by 35%. In the period 2014-2019, the number of such offences rose by 67%, resulting in 40% of businesses having suffered cyber attacks with increased costs and recovery times.

Serious cyber-security incidents can in fact cause so much damage as to jeopardise the very survival of a business or, in any event, significantly disrupt its activity, undermining its credibility, causing it financial loss, shutting down its production and pirating its intellectual property.

As a result of the pandemic, public bodies and businesses have become increasingly digitalised. However, this has not been accompanied by a corresponding security systems upgrade and review. In view of this:

1. Can the Commission indicate the cost of cyber attacks in the EU? To what extent does it believe that European businesses as a whole are able to withstand cyber attacks?

2. Does the EU intend to fund European company initiatives and projects to improve their cyber protection and user safety standards?