Question for written answer E-000680/2019
to the Commission
Rule 130
José Blanco López (S&D)

Subject: Spoofing and jamming

Reports on problems with satellite navigation in the Black Sea suggest that Russia could be trying out a new system for spoofing or jamming the GNSS. This could be the first confirmed sign of a new form of electronic warfare potentially available to everyone.

This analysis formed part of a post on 21 September 2017 on the official Galileo website, which made the point that while Russia had previously used techniques of this kind to falsify signals in Moscow, reports such as these would seem to demonstrate that it had started to use them on a much greater scale. What is most worrying here is the apparent ease of accessibility to this technology.

Furthermore, press reports on the effects of GNSS system blockers or the repercussions that interruptions to GNSS could have on vital services are appearing ever more frequently.

1) Has the Commission recorded any new spoofing attacks or been aware of them? Is Galileo capable of resisting attacks of this kind or has it been affected by them?

2) Has the Commission adopted or does it plan to adopt a strategy to counter attacks or interruptions of this kind in order to protect vital EU infrastructure and be able to guarantee provision of timing and geolocation systems?

3) Does it know what strategies other countries with geo-positioning and timing satellite systems use to tackle attacks of this kind?