WORLD TRADE ORGANIZATION

G/TBT/W/509

19 April 2018

(18-2457)

Page: 1/2

Committee on Technical Barriers to Trade

Original: English

CHINA — CYBERSECURITY LAW

STATEMENT BY THE EUROPEAN UNION TO THE COMMITTEE ON TECHNICAL BARRIERS TO TRADE 21 AND 22 MARCH 2018

The following communication, dated 16 April 2018, is being circulated at the request of the delegation of the European Union.

---

1. The European Union reiterates its concern of the entry into force on 1 June 2017 of the new Cybersecurity Law. The EU has provided written comments in 2016 detailing these concerns and as well raised during the last TBT-meeting in November last year.

2. The EU would like to take the opportunity to emphasize its main concerns again:

- The scope of the requirements is not clear as key terms have not been specified in sufficient detail. Concepts such as "critical information infrastructure" and "secure and trustworthy products" are not clarified, which leads to unclarity as to which sectors are impacted by the measures.

- The EU recalls the importance of using international standards and notes that the law only references national standards. This could lead to lack of interoperability with international standards. In the development of national standards, it would be appropriate to build on existing international standards and to involve all relevant stakeholders (including foreign invested and wholly-foreign owned enterprises) in a non-discriminatory manner in the relevant Technical Committees.

- As regards the certification and security requirements on critical information infrastructure, the EU is concerned that such requirements lead to a de facto ban on products and services from foreign-invested enterprises providing products and services to businesses falling under the notion of "critical information infrastructure". The EU calls on China to implement these provisions in a non-discriminatory manner, respecting the principles of proportionality, necessity and technology neutrality. Moreover, the EU repeats its previous requests for clarifications on the relationship to existing multi-level-protection systems (MLPs) and the expected timeline of implementation.

- As regards data localization, the EU understands that the storage obligation has been replaced by controls on cross-border transfers of data. The EU is concerned that these controls create the same level of restriction than the obligation to store data in China. Moreover, the EU notes with concern that the scope of the relevant obligations has been enlarged to 'network operators' in general (and not only those of critical information infrastructure). The EU appreciates that the date of entry into force of these specific measures has been postponed to 31 December. Moreover, the EU welcomes the opening of TC260 standard defining the concept of 'important data' for public comments. Could China confirm that the specific measures have now entered into force?

3. The EU notes with concern that the Cybersecurity law already applies and is enforceable (including possible fines and sanctions), while the implementing measures that would clarify its

implementation are still not in place. The current situation creates a lot of uncertainty for economic operators. Could China inform when implementing measures will be adopted?

4. The EU kindly requests China to notify draft measures in any subsequent sectoral implementation to the TBT Committee in order to give adequate opportunity for WTO Members and their stakeholders to comment on any subsequent developments.