WORLD TRADE ORGANIZATION

G/TBT/W/590

20 December 2018

(18-8068)

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 14 AND 15 NOVEMBER 2018

The following communication, dated 18 December 2018, is being circulated at the request of the delegation of the European Union.

---

1. The EU would like to reiterate its concern with regard to the entry into force of the Cybersecurity Law on 1 June 2017.

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

3. The EU has concerns when it comes to the standard itself. We note that China released in September 2018 the final version of the secure and controllable standards.

4. We welcome the removal of reference to "source code". However, we maintain our concerns about the revised methodology. While references to source code have been removed from the final version, the mere requirement of providing "relevant materials" to verify the security and controllability of products, could very well imply source code disclosure.

5. The EU recalls the importance of international standards and notes that the law only makes references to 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.

6. The EU would like to request more clarity regarding the myriad of implementing measures following China's Cybersecurity Law. Additionally, the Cyberspace Administration of China's Cross-Border Data Transfer Rules *(Critical Information Infrastructure Protection Regulation and Administrative Measures on Security Assessment of Overseas Transfer of Personal Information and Important Data)* raise concerns about the broad scope of these regulations regarding what is considered as critical information infrastructure and which kinds of cross-border data transfers are affected and ensuing legal uncertainty.

7. As regards the certification and security rerquirements 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".

8. 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 would like to repeat its previous requests for clarifications on the relationship with existing multi-level-protection systems (MLPs) and the expected timeline of implementation.

9. 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 significant uncertainty for economic operators. Could China inform the Committee when implementing measures will be adopted?

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