Commissioner Cañete at the conference on cyber security in the energy sector

Distinguished Guests, Ladies and Gentlemen,

The **energy system** is one of **the most complex and largest infrastructures** in Europe. It is also one of the most critical assets for a modern society and as such **the backbone for its economic activities, welfare and stability**.

The energy system is changing today – in terms of infrastructure and market developments. In particular with the increasing share of renewable energy sources, it is becoming more decentralised, digitalised and decarbonised.

One of the key trends is that the **share of electricity** in our consumption will increase in the coming years and decades and nearly double by 2050. This is one of the lessons of our long-term strategy.

In the **Clean Energy for All Europeans** package with its eight different legislative acts, we have set a clear and common sense of direction with ambitious targets for 2030 for energy efficiency and renewables. All these acts were adopted with a very broad support in the European Parliament and the Council.

With the increasing share of renewables and decentralised generation, we also witness a **continuously increasing degree of digitalisation**, moving towards **smarter grids** and connecting to the **Internet of Things** through smart devices. If we are to reach our targets, which implies that more than half of our electricity will come from renewables already in 2030, this trend will accelerate even further.

With all its advantages – this digitalisation brings new challenges for the sector. New challenges in terms of data management, but in particular with respect to **cybersecurity**. Recent reports state that foreign actors have been allegedly probing or even infiltrating the US, Russian and Asian electrical grids. Disrupting the electrical infrastructure of a region could cause blackouts and disrupt financial markets, transportation and more.

The Union has put in place common general tools to increase cybersecurity. In particular, **the Directive on Security of Network and Information Systems was adopted in 2016** and is currently being implemented. It is the first European law on cybersecurity and focuses on the resilience of essential services. Furthermore, the recent **Cybersecurity Act of 2019** creates a framework for voluntary European cybersecurity certification of products, processes and services.

Let me underline, in cybersecurity one size does not fit all. The energy sector has some particularities that create challenges in terms of cyber security. These particularities include real-time requirements, cascading effects and the mix of legacy technologies with smart and state of the art

technology. The real-time requirements of for example circuit breakers that have to act in milliseconds, do not work with standard security measures such as authentication or encryption. We have to be aware of cascading effects as electricity grids and gas pipelines are strongly interconnected across Europe, and well beyond EU member states. Energy technology operating today was designed and built before cybersecurity was considered and often has a lifetime of 30 to 60 years. Today these legacy systems need to interact securely with recent smart technology and the Internet of Things.

Therefore, within the Clean Energy for All Europeans package we also address cybersecurity:

The **new regulation on electricity risk preparedness of 2019** mandates Member States to develop national risk preparedness plans and coordinate their preparation at regional level, including measures to cope with cyber-attacks.

The recast of the Electricity Regulation calls for the development of a **network code on cyber security,** to increase the resilience of the energy sector and protect the energy systems.

Further, on 3rd April 2019, the Commission adopted a dedicated **Guidance on cybersecurity in the energy sector** to help the sector implement horizontal energy legislation, but also to address smaller operators that are not necessarily covered by these horizontal rules. They might be the weakest link.

In cybersecurity, information-sharing is key. Therefore the Commission supports information sharing at several levels and through different channels:

The Commission kicked off a work stream under the Network and Information Security (NIS) Cooperation Group dedicated to energy to bring together Member State Authorities from the cybersecurity and the energy side. This is the first sectoral work stream under the NIS Cooperation Group.

We have also encouraged enhanced cooperation with specialised entities such as the European Energy Information Sharing and Analysis Centre on cybersecurity and at technical level via expert groups.

And we are also reaching out beyond the EU, for example with an enhanced dialogue with third countries and the group of seven (G7).

Finally, it is throughdedicated events like the one today that we hope to increase awareness for the need to tackle this challenge jointly. Today we see here at the table representatives of Member States, NATO, industry as well as the European institutions. In cybersecurity, we all need to work together.

To conclude, I welcome very much the initiative to discuss cyber-security today with all relevant actors, which tackles an important issue.

When we look forward to the energy world of tomorrow, it is clear that the

technological revolutions underway offer a lot of opportunities for a cleaner and more participative system. But we also need to be prepared for the new risks to our energy security this entails, and we need to address them together.

In that sense, let me wish you a very fruitful discussion.