The security and defence implications of China influence on critical infrastructure in the European Union

2023/2072(INI) - 11/12/2023 - Committee report tabled for plenary, single reading

The Committee on Foreign Affairs adopted the own-initiative report by Klemen GROŠELJ (Renew, SI) on the security and defence implications of China's influence on critical infrastructure in the European Union.

China is increasingly gaining access to and exercising influence over European infrastructure and sectors of vital importance for the European Union.

The core of the problem: understanding China's military-civil fusion strategy

China's party-driven political system and economy often require private companies to align their commercial interests with the Chinese Communist Party (CCP) including its military activities, repression, influence and political interference activities. Consequently, Chinese companies' international activities support the CCP's goals of expanding its influence in third countries, undermining geopolitical rivals and increasing China's influence.

The report stressed the repeated warnings by intelligence agencies against the risks of economic dependence, **espionage and sabotage** caused by the economic presence of entities from certain non-EU countries, in particular China, in critical infrastructure and strategic sectors across the EU. Members are, in this regard, concerned by the political pressure asserted in the approval of specific Chinese investments into critical infrastructure, as in the case of the German government's decision to agree to the acquisition of a stake at the port of Hamburg by COSCO, contrary to the advice of the competent institutions.

Consequences of the PRC's military-civil fusion strategy

Members warned of the risk of Chinese companies having any involvement with EU strategic assets, especially those companies that have direct or indirect links to China's political-military or intelligence systems. In this regard, they urged EU Member States to **increase regulatory oversight** and introduce specific background checks over individuals and legal entities with direct ties to the Chinese government.

The Commission and the Member States, in coordination with industry stakeholders are called on to implement the decision to **gradually reduce the dependence on China** by diversifying the sources of critical raw minerals and rare earth elements, establishing strategic partnerships with reliable third countries with a view to ensuring a secure and reliable supply of critical raw materials.

Developing responses: expanding the toolkit to respond to security and defence concerns

The report argued that a key area of EU critical infrastructure is its network of research institutes and research and development facilities, which play an important role in the EU's ability to deliver on its green and digital transition commitments, alongside key arenas such as space defence.

Noting that Chinese companies are already leaders in key technologies used in sectors such as 5G wireless infrastructure, drones, batteries, hypersonic missiles, solar and wind energy, as well as cryptocurrency, Members expressed concerns over the uses of these technologies and the dependencies they create.

Therefore, they urged the EU and European institutions to carry out a **systematic screening** of Chinese companies benefiting directly or indirectly from European programmes of strategic importance for the EU and, where necessary, terminate their participation.

Members considered the TikTok app, owned by Chinese conglomerate ByteDance, to be in breach of the European data privacy framework, making it a potential risk and a source of Chinese-backed disinformation. Therefore, they welcomed the decision of EU institutions and those of several EU Member States to **suspend the use of the TikTok application on corporate devices**, as well as personal devices enrolled in the institutions' mobile device services.

Still concerned that European critical infrastructure, from telecommunications networks to port facilities, is becoming increasingly vulnerable to external influence, Members commended, in this regard, recent legislative steps to enhance the resilience of critical entities in the EU.

Furthermore, Members called on the Commission to share with Parliament, before the end of this parliamentary term, a detailed analysis of the trade risks linked to technologies such as semiconductors, quantum computing, block chains, space, artificial intelligence and biotechnologies and the possible need for EU action in these fields.

The report also expressed regret at the **lack of adequate screening of risks of interference in public procurement** related to security equipment, such as the case of the contract signed by Strasbourg airport to install airport security scanners and gates supplied by the European subsidiary of the Chinese company Nuctech, partly owned by the Chinese government and bound by the 'United Front' policy.

According to Members, a strategic balance must be found between, on the one hand, the openness of the EU single market and its attractiveness for investments, and, on the other, the defence of the EU's critical infrastructure and autonomy, considering the EU's security vulnerabilities, especially as regards economic coercion or threats to the integrity of the EU's critical infrastructure.

The Commission, in coordination with the Member States, are called on to design a **rapid response mechanism** for the detection of the dual use, or misuse, of infrastructures in the EU under Chinese ownership, participation or concession, that could be used to terminate the rights of concession and/or suspend the capacity of domain in the cases of ownership and participation.

Members also called for:

- further proposals to secure the production and supply chains of critical infrastructure and materials within the EU;

- a new legislative framework to mitigate the security risks coming from the suppliers of **undersea cable systems**, including through stricter monitoring and frequent review of the ownership structures of such suppliers, their previous investments in undersea cable systems and the proximity of the undersea cable systems to European and allied military bases.

Internal-external nexus: strengthening the resilience of the EU's closest partners

The report expressed concern regarding the PRC's penetration of the EU market and its wider neighbourhood. It called on the Commission and the European External Action Service (EEAS) to ensure that the measures taken to strengthen the resilience of the EU in the face of Chinese influence, including de-risking, diversification and reduction of critical dependencies, are also extended to the EU's closest partners, in particular accession countries and those part of the EUs neighbourhood policy.

Members underlined that the risks of espionage are highest when Chinese civilian commercial assets are located in logistical hubs close to EU and NATO naval bases or port operators that have signed agreements to provide logistical support to European companies. Member States are called urgently to address the need to reduce the risks of espionage and sabotage in critical infrastructure, in particular those with a military function, such as ports that are used by NATO. The EU and NATO must work together to develop a long-term plan to counter China’s MCF strategy in Europe.