PISM | POLSKI INSTYTUT SPRAW MIĘDZYNARODOWYCH
THE POLISH INSTITUTE OF INTERNATIONAL AFFAIRS

NO. 175 (2294), 23 NOVEMBER 2023 © PISM

BULLETIN

Awareness of the Importance of Critical Technologies Growing in the EU

Szymon Zaręba

The proposal to create the Strategic Technology Platform for Europe (STEP) and the adoption of a Recommendation on critical technology areas by the European Commission (EC), announced in recent months, confirm a welcome change in the EU's growing appreciation of the role of technological security. Key to the success of the new initiatives will be their coordination, the identification of the most sensitive technologies, and the selection of response measures adequate to the challenges identified by EU countries, including Poland.

Changing Approach. For several years, there has been a growing awareness among EU states and bodies of the importance of certain technologies beyond their economic value and which are described in EU documents as critical, emerging, or disruptive. However, efforts to date, such as the framework for screening of foreign direct investment into the Union, adopted in 2019, and the 2022 Roadmap on critical technologies for security and defence, which aims to reduce strategic dependencies for some critical technologies, were fragmented and limited in nature. New impulse has been given by the EU Economic Security Strategy announced by the High Representative of the Union for Foreign Affairs and Security Policy and the EC in June this year, identifying risks related to technology security as one of the four main challenges for the EU economy.

Two initiatives announced by the EC in recent months aim to address this challenge. The first is the proposal in June this year for the creation of STEP to support the development of manufacturing capabilities in the EU for critical new technologies that are important for the green and digital transformations and the strategic sovereignty of the Union. The Commission includes in these categories digital technologies (including microelectronics, artificial intelligence, or AI, and 5G connectivity), clean technologies (especially energy- and renewable fuels-related), and biotechnologies. STEP is expected to enable funding of them by around €160 billion. In practice, however, it will mainly redirect available money in the Horizon Europe, Innovation, InvestEU, EU4Health, and European Defence funds. New funding is expected to total around €10 billion (the European Parliament, which backed STEP in October this year, is proposing to increase this amount to €13 billion). Projects eligible for STEP support are to receive a so-called "sovereignty seal" to attract other investors, awarded by a specially created EC expert committee.

The second major initiative is the Recommendation announced by the EC in October this year, which includes a list of 10 technologies critical to the EU's economic security. These are advanced semiconductors, AI, quantum technologies, biotechnologies, advanced connectivity and navigation, sensing, space, energy, robotics and autonomous systems technologies, as well as technologies for advanced materials, manufacturing methods, and recycling. The first four are considered by the EC to be the most sensitive because of their breakthrough ("transformative") economic importance, potential for dual use (i.e., for military purposes), and the risk of their being used to violate human rights. It recommends that EU members conduct a risk analysis on them by the end of 2023. The need for assessments in the remaining categories is to be decided by spring 2024. On the basis of the analyses, the EU bodies are to decide whether restrictions (e.g., export controls and outbound investments) are advisable in a given area or whether risk reduction (e.g., by diversifying suppliers

and supporting the development of the relevant capacities in Europe) is sufficient. The EC also allows for the possibility of changing the list in the future.

Technology vs. Security. The list of critical technologies does not link the threats identified in it to any country. Unofficially, however, EU officials regard it mainly as part of the implementation of the concept of reducing the Union's dependence (derisking) on China. This is linked to concerns about dependence on China that threatens EU security in certain technology areas (e.g., renewable energy), but also the possibility of strengthening China's military capabilities and facilitating human rights violations (e.g., through exports of chipmaking equipment used in weaponry or facial recognition programmes based on AI and used for surveillance of the population). However, the problem is not limited to China, as demonstrated, for example, by the role of Western dual-use components for Russian military equipment used during the aggression against Ukraine. At the same time, the EU list corresponds to analogous actions by some countries. Similar lists have been announced by, among others, the U.S. (starting from 2020), Australia (2021), Japan (2022), and the UK (2023), but also by some non-democratic states, including Russia (from 2002) and China (2015 "Made in China" strategy). They are usually used to identify the main directions to support research and production development, although they are sometimes used to develop separate investment- and trade-control mechanisms.

At the same time, the development of the list and STEP address the need to increase support in areas where EU countries could quickly join the forefront of the technology race or still play an important role in it. The Australian Strategic Policy Institute's 2023 report indicates that China is the world leader in 85% of the 44 key critical technologies highlighted in the report, with the U.S. as runner-up. Only a few EU countries are in the top five: Germany (17 categories), Italy (5), the Netherlands and France (2 each). This raises the need for remedial action. It should be noted that STEP was also initially presented as a European response to the U.S. Inflation Reduction Act, but the amount envisaged, even taking into account very optimistic assumptions about its leveraging with credit and private funds, is half the amount provided by the U.S. for similar purposes.

Conclusions. The evolution of the EU's approach to technology issues, including the publication of the list of critical technologies and the STEP proposal, demonstrates a profound change in EU economic policy thinking. It confirms that the Union recognises more and more the broad dimension of security in economic relations. This is a good step, as the EU needs a long-term policy to support the development of critical technologies, but also their export and control of inbound and outbound investment. The approach so far—mainly reactive, based on imposing sanctions only after the occurrence of undesirable events—needs to be complemented by a preventive one.

A thorough analysis of third-party lists will be important in developing the final list, but also the means of responding to observed dependencies. This may facilitate potential partnerships with like-minded countries and, in the case of others, enable the identification of risks, as the sectors identified in their lists may be obvious targets for third-country sanctions against Union members.

For the Union, it should be important to support the EU capabilities in those technologies where it is still at the global forefront in terms of value chains, as well as to identify and develop areas where EU countries could still quickly join the forefront with appropriate public sector involvement (funding, regulatory changes). Exploiting such interdependencies would increase the potential for deterring economic pressures on EU countries, which the EU institutions are already trying to counter, among others, with the adoption of the Anti-coercion Instrument, which is to enter into force before the end of the year. The STEP fund, among others, could help achieve these goals, although the modest resources allocated to it and the current lack of linkage to the risk analyses recommended by the EC in October 2023 for the list of critical technologies may hinder real progress. It would be desirable to ensure consistency between the selection of technologies supported under STEP and the final outcome of the risk analysis. At the same time, the "sovereignty seal" mechanism seems to be an idea that unnecessarily raises the costs of operating the initiative.

From Poland's perspective, timely completion of the risk analyses recommended by the EC is important, as it may affect the prospects for supporting and protecting the position of domestic companies within existing value chains. Should the investment control standards be tightened on the basis of these analyses, it may also affect the prospects for the development of Polish business abroad. It would therefore be beneficial to include it in the risk analysis recommended by the Commission and for the Polish authorities to be actively involved at the next stage of the discussion of remedial and preventive measures to be introduced.