SMART FENCES

Calibrating China's role in Ukraine's reconstruction

by
Tim Rühlig

Ukraine's reconstruction bill is now estimated at €500 billion over the next decade. This amounts to nearly three times the country's projected nominal GDP for 2025. The EU alone cannot cover it, and substantial G7 support remains uncertain. This financing gap creates an opening for China. Beijing has the industrial capacity, the capital, and the appetite: it has publicly signalled readiness to participate in Ukraine's post-war reconstruction and recently reiterated its interest – an observation also corroborated by the author's interviews with party officials.

But Chinese involvement in rebuilding Ukraine's critical infrastructure carries serious political and security risks. The EU should act now: equipping Ukraine with a robust toolkit of regulatory instruments and risk-limitation expertise so that reconstruction does not become a vector for dependency, espionage or sabotage. The goal should be to calibrate – not prevent – China's involvement in Ukraine's reconstruction.

Idea

This is a pivotal moment. Decisions taken now on procurement rules, technology standards and investment screening will shape Ukraine's infrastructure for decades. Allowing Chinese firms to embed themselves in critical systems without adequate safeguards could undermine both Ukraine's and Europe's security.

China's interest in Ukraine's reconstruction is not incidental. Beijing has developed a growing global role in post-conflict reconstruction, with a recognisable track record that spans Iraq, South Sudan, Syria, Afghanistan and Ethiopia. In each case, involvement in reconstruction has provided Beijing with commercial footholds, political leverage and strategic influence. For example, in Ethiopia China was among the first to back reconstruction after the Tigray War, resuming the Exim Bank-financed Mekelle City Water Supply Project; in Iraq, its 2019 'oil-for-projects' deal traded twenty years of guaranteed oil supply for concessional credit earmarked for the country's infrastructure development. China's proclivity for mixing commercial and state interests has also sparked security concerns in the EU and is likely to generate similar concerns in Ukraine. The risks cluster around three distinct but related threats.

The first risk is espionage. Chinese companies operate under a domestic legal framework, most prominently the 2017 National Intelligence Law,

that obliges all organisations and citizens to support, assist and cooperate with state intelligence work. Their involvement in building or operating critical infrastructure – transport hubs, energy grids, communications networks – creates opportunities for intelligence collection. Any sensitive information gathered could ultimately benefit Moscow should Beijing choose to share it with Russia.

Sabotage is the second risk. Digital infrastructure, including telecommunications networks and economically vital seaports, is increasingly maintenance-intensive and requires continuous remote servicing by manufacturers. In a conflict scenario, such access could be weaponised to disrupt critical systems. For example, if Russia were to launch another attack on Ukraine, Chinese technology companies could disrupt or degrade Ukrainian communications and transport networks, thereby undermining Ukraine's ability to defend itself.

The third risk is that Chinese-led reconstruction will lock Ukraine into lasting dependencies. The adoption of Chinese technical standards would create long-term reliance on Chinese suppliers, since Chinese technologies and components cannot easily be replaced or serviced by European providers. Once embedded, these dependencies are extremely costly to unwind.

Impetus

To enable Ukraine to benefit from Chinese investment opportunities without compromising its security, the EU should equip Ukraine with a robust protective toolkit. This requires systematically transferring the EU's own regulatory and risk-limitation expertise to Ukraine and embedding it in Ukraine's reconstruction architecture before Chinese actors establish significant footholds. The necessary safeguards should be incorporated into the legal, procurement and investment framework governing reconstruction from the outset. The Ukraine Facility Regulation already restricts procurement and supply financed under the Facility to eligible countries, effectively excluding Chinese firms and goods. But these rules govern only how EU funds are spent; they do not screen Chinese investment in reconstruction financed by Ukraine, other donors or private capital, and they contain no investment-screening, high-risk-vendor or foreign-subsidy mechanism. The task is therefore to strengthen Ukraine's own regulatory instruments and to make the Facility's discretionary security provisions more systematic. This approach would allow pragmatic engagement with Chinese capital and industrial capacity where appropriate, thus contributing to reconstruction and recovery efforts to everyone's benefit, while ring-fencing critical sectors or components.

The EU should share lessons learned from its own risk-assessment activities with Ukraine and discuss the criteria and thresholds it has put in place, both in its 2023 Economic Security Strategy and the four corresponding risk assessments it has launched on supply chain resilience, physical and cyber security of critical infrastructure, technology security and leakage, and the weaponisation of economic dependencies.

Instruments

The EU has in place a cooperation mechanism on investment screening through which Member States and the Commission exchange information on foreign direct investment (FDI) in sensitive sectors. It is therefore in a position to support Ukraine develop its own instruments by sharing lessons learned and institutional experience from both national screening regimes and the EU-level screening mechanism. While the EU cannot share confidential information exchanged through its investment-screening mechanism with Ukraine, it can provide guidance on screening methodologies and implementation. Currently, the EU is expanding and harmonising the sectors subject to mandatory screening, including energy, transport, digital infrastructure, defence, dual-use technology, AI, biotech, critical raw materials, food, media and ports. Ukraine could receive technical assistance to adopt these practices at a pace commensurate with its institutional capacity.

In the area of public procurement and state-subsidised competition, the Foreign Subsidies Regulation empowers the European Commission to investigate distortions caused by non-EU state subsidies in mergers and public procurement above specified thresholds. A similar mechanism is needed in Ukraine to scrutinise Chinese state-backed bids for reconstruction contracts. The International Procurement Instrument allows the

EU to restrict access to public tenders for firms from countries that do not offer reciprocal market access. Meanwhile, the Net-Zero Industry Act has introduced explicit non-price criteria – including sustainability, resilience and supply-source diversification – into procurement evaluation for clean-tech tenders. Similar criteria could be incorporated into Ukraine's reconstruction procurement framework, particularly for tenders in energy and transport.

In the field of cybersecurity and critical infrastructure, the EU's 5G Cybersecurity Toolbox established the 'high-risk supplier' concept that has underpinned Member State decisions to restrict or exclude Huawei and ZTE. The Commission's January 2026 proposal to revise the Cybersecurity Act would translate the Toolbox into binding obligations and extend its logic to fibre-optic and other critical telecommunications infrastructure. Such measures could provide a blueprint for Ukraine's own approach to vendor risk assessment and the exclusion of high-risk suppliers. Drawing on the NIS2 Directive, Kyiv could harmonise cybersecurity obligations across 18 critical sectors and complement this with measures modelled on the Critical Entities Resilience Directive, which strengthens the physical resilience of critical entities in 11 sectors.

Crucially, much of this is not discretionary as cybersecurity and critical infrastructure rules form part of the *acquis*. But the EU should frontload specific instruments such as high-risk-vendor screening, NIS2-style obligations, and CER-style resilience within the reform conditionality.

None of this will work without sufficient institutional capacity. Ukraine lacks the resources to conduct complex screening procedures, foreign-subsidy investigations and high-risk-vendor assessments at the scale that reconstruction will require. The EU can help here with direct technical assistance, not least in the context of Europe's pre-accession assistance.

The costs of building this architecture are modest compared to the cost of inaction: a compromised port, a sabotaged grid, or a decade-long technical dependency on Chinese suppliers would far outweigh any short-term procurement savings, especially once Ukraine has become a member of the EU.