

Can Sweden's new public procurement legislation mitigate "China risk"?

Björn Cappelin

Summary

- The Swedish government has proposed revising the legislation on public procurement to make it possible to exclude bidders from non-EU countries, making specific reference to security considerations.
- There has been public debate in Sweden concerning several cases of public procurement where Chinese suppliers have been considered a source of risk, chiefly in the context of data or infrastructure integrity. In some cases, Chinese suppliers have been excluded, while in others the procurement has gone forward. The nature of the risk has not always been clearly defined, and the risk is often potential rather than evidenced.
- The revised legislation will give public actors new possibilities to de-risk from China. Challenges arise, however, when the procuring actor must bear the responsibility for determining the nature of both supplier and security risk. Work is needed to improve analyses of China-related risks. Responsible agencies should consider communicating more clearly the nature of such risks.

The need to increase security in procurement

In January 2026, the Swedish Government [presented a proposal](#) on revising public procurement legislation, specifically highlighting new possibilities to exclude bidders from "antagonistic states". While the definition of an antagonistic state is vague, China is mentioned in [the most recent public threat assessment](#) by the Swedish Security Police as one of the main threats to Swedish security. Several cases of China-related risk in public procurement have come to light in recent years, which makes it useful to examine these risks and how

they could be mitigated. This Brief examines whether the proposed revised procurement legislation could provide Swedish stakeholders with better tools to handle China-related security risks in the context of public procurement.

China as a risk factor

An answer to this question requires an understanding of the nature of such risks. The specific risks associated with China, as set out in publications by the Swedish security services and in the Swedish Government's 2024 [National Security Strategy](#), align quite well with the broad categories outlined in the European Commission's 2023 proposal for an [EU economic security](#) strategy. These categories are: (i) the resilience of supply chains; (ii) the physical and cyber security of critical infrastructure; (iii) technology security and technology leakage; and (iv) the weaponisation of economic dependencies or economic coercion.

The EU and its member states have begun to address some of these risks, notably research security and the risks associated with Foreign Direct Investment (FDI). However, procuring products and systems that process sensitive information or could give a service provider access to such information also creates risks for states. The [Chinese national intelligence law of 2017](#), which obliges all Chinese citizens and companies to supply information to the Chinese authorities when requested, is a particular risk factor in the context of sensitive information. Giving a foreign actor a key role in a system or process can also lead to undue influence and risks of coercion. Foreign sourcing of strategically important products, for instance for medical use, can constitute a supply chain weakness. All the four main categories of risk outlined in the Commission's strategy could therefore be present in public procurement, but the security risks related to public procurement are not covered by comprehensive EU regulation.

This Brief aims to answer the following questions:

- What is the current understanding of security risks related to Chinese actors in public procurement processes in Sweden?
- Will the current proposal to revise procurement legislation address such security risks?

The analysis¹ examines several noteworthy Swedish cases in which China-related security risks have been highlighted in the media and the public debate. It is followed by an overview of the proposed revised legislation and the public comments that have been made regarding the proposal by concerned stakeholders.

¹ The debate on public procurement and China has also highlighted risks associated with environmental issues and human rights, but these are outside the scope of this text. The EU's use of the International Procurement Instrument (IPI) to exclude Chinese companies from EU government purchases of medical devices is also not discussed here, since it is based on trade policy rules and aims to counter China's discriminatory practices.

Challenges in assessing China-related security risks in procurement cases

There are very few known instances of a “smoking gun” where Chinese action has led to actual security breaches in the context of a public procurement process in Sweden. At the same time, however, several cases have involved systems or information that are security-sensitive, and there is increasing evidence from many countries that China has both the means and the motives to exploit such sensitivities.

The exclusion of Huawei from 5G networks in Sweden

In 2020, in a well-known Swedish case of “China risk”, the Swedish Post and Telecoms Agency (*Post- och Telestyrelsen*, PTS) announced that companies bidding for 5G frequencies would be required to exclude network equipment from the Chinese telecom suppliers Huawei and ZTE. This was one of the first cases of a European country officially declaring a Chinese telecom company a security risk.

Huawei took the PTS to court but the decision was [upheld](#) in all instances of appeal. The case is currently [undergoing international arbitration](#), which will determine whether Huawei has a right to compensation from the Swedish state under the terms of the [1982 Swedish-Chinese Agreement on Mutual Protection of Investments](#). The case continues to cast a shadow over Sweden's bilateral relations with China.

The key risk perceived in this case is also fundamentally the reason for the exclusion of Chinese actors – potential access to important segments of critical information infrastructure. This risk has been [identified in many countries](#) and has led to different forms of exclusion or limits on Chinese involvement in 5G networks.

While the Huawei case illustrates a broadly understood China-related security risk, it is *not* a perfect example in the procurement context. The legal basis for the exclusion of Huawei was not public procurement legislation, but the law on electronic communications, which gives a clear advisory role to the security services on decisions regarding granting access to the radio spectrum.

The list of cases below is not exhaustive. There is no comprehensive overview of the share of Chinese products and services in public procurement in Sweden, mainly due to the absence of a centralised register of public procurements. Nor is there much available research or analysis on the risks posed by foreign companies in public procurement. A [2022 study](#) by the Swedish Defence Research Agency (FOI) attempted to estimate the size of the Russian presence in public procurement. The study concluded that it was difficult to get a full picture and recommended that public procurement should be an area considered for further regulation with regard to security risks. There is therefore no clear view of the size of the potential problem or the number of Chinese bids in public procurement that might or might not lead to security risks.

General matters related to the protection of security interests are currently regulated by the [Protective Security Act \(Säkerhetsskyddslagen\)](#) of 2018. This law requires any public or private sector actor whose operations entail handling security-sensitive information or materials to perform a security assessment within the framework of any procurement process. One issue [that has been raised](#) is that in many cases the responsibility for carrying out such assessments rests with the actor itself, meaning that assessments are not always performed as or when needed.

Publicly debated cases of Chinese participation in public procurement in Sweden

Case	Public reporting	Security risk perception
<i>Tunnelling in the Stockholm metro (2019)</i>	The Chinese company China Railway Tunnel Group (CRTG) was contracted by the region of Stockholm to carry out tunnelling for the Stockholm metro network. At the time, security concerns were raised by some observers specifically regarding access to sensitive infrastructure information. However, the main focus of reporting was labour safety concerns and the perceived risk of price dumping. These concerns were somewhat vindicated in March 2026 when CRTG was suspended from the project because of serious violations of safety standards.	<i>Access to sensitive physical infrastructure</i>
<i>Security scanners at Arlanda airport (2022)</i>	Swedavia, the national airport operator, procured security scanning equipment for Stockholm-Arlanda airport from Chinese provider Nuctech, a company blacklisted in the United States over concerns that its scanning equipment could be used to send sensitive data back to China. According to reports , these concerns had been raised with the Swedish government by the US embassy in Stockholm in 2020. Similar concerns have been voiced elsewhere , but several European countries are nonetheless using the company's scanning equipment. Swedavia argued that it had performed the security assessments required by the Protective Security Act. An inquiry into the procedures by the Swedish Transport Agency (<i>Transportstyrelsen</i>) did not block the procurement and the scanners are now in operation at the airport. According to media reports , Nuctech scanners are also being used in several Swedish court buildings and at customs checkpoints.	<i>Sensitive information could be relayed to China</i>
<i>Monitoring equipment in large electricity grids (2023)</i>	The state-owned Swedish electricity grid operator Vattenfall procured and installed hundreds of thousands of connected household electricity meters from Chinese supplier Sanxing. Media reports raised concerns that the units can relay sensitive information and even be used to shut off the electricity supply. Reporting also focused on the owner of Sanxing's connections to the Chinese Communist Party. The grid operator argued that a security assessment had been undertaken without raising any concerns about the supplier.	<i>Sensitive information could be relayed to China</i> <i>Potential for infrastructure control</i>

<p><i>Security concerns over Volvo Cars in use by law enforcement agencies (2023)</i></p>	<p>Procurement by government agencies from Chinese-owned companies raised concerns about the Swedish police and customs agencies using connected cars supplied by Chinese-owned Volvo. The concern was that not only movement patterns, but also conversations held inside the cars could be relayed to centralised Volvo networks, and by implication on to China. Volvo claimed that the connectivity features were disabled in cars supplied to law enforcement agencies. A representative of the intelligence community said that sensitive discussions should never be held inside any vehicle due to concerns about what might be recorded and transmitted.</p>	<p><i>Sensitive information could be relayed to China</i></p>
<p><i>The Public Employment Agency said no to Lenovo computers ... (2025)</i></p>	<p>The Public Employment Agency (<i>Arbetsförmedlingen</i>) decided to exclude Chinese suppliers from a bid to procure new computers for the agency. The agency argued that its remit includes tasks related to general societal preparedness and that China is on a list of countries of concern issued by Swedish security police. The Chinese company Lenovo, the world's largest supplier of personal computers, took the decision to court, but the decision was upheld in the first instance of appeal. Swedish industry media raised concerns that the case risked being interpreted as a hostile measure by China and could involve Sweden in the “tech war on China”.</p>	<p><i>Sensitive information could be relayed to China</i></p>
<p><i>...but initially said yes to Chinese AI agents (2025)</i></p>	<p>The Public Employment Agency decided to procure and deploy Alibaba's AI tool, Qwen3, in its internal systems. The decision to deploy Qwen3 is thought to have been made because it was cheaper than many comparable AI tools. After concerns were raised about the security aspects of using a Chinese AI solution for sensitive information, the agency's Director General decided to suspend its use.</p>	<p><i>Sensitive information could be relayed to China</i></p> <p><i>Potential for infrastructure control</i></p>

Revised legislation on public procurement

The Government of Sweden's [proposal](#) to revise the laws governing public procurement is due to enter into force at the beginning of 2027. Swedish procurement legislation has not hitherto differentiated between bidders from EU member states and those from third countries. While the main reason given for the revision is the need to harmonise with EU legislation, the proposal also specifically cites security considerations as an important factor.

The proposal states that the rules governing procurement should not apply to third country suppliers. This means that while they would be able enter a procurement process, they would not be guaranteed access or equal treatment. It would be left to procuring agencies to decide whether to permit such bids. The proposal specifically states that this would allow bidders from an antagonistic state to be excluded. It should be noted that the proposal only covers *suppliers* from third countries and not *goods* or *services* originating in such countries. Moreover, there will still be opportunities for an EU-based bidding party to use subcontractors from a third country.

The proposal's impact assessment argues that the revisions are expected to have only a minor impact on procurement in general. The proposal cites estimates, both national and European, that only about five percent of bidders in public procurement processes are non-EU actors. However, this estimate only refers to the number of procurements, not their monetary value. Based on this low estimate, the proposal argues that the risk that higher prices will result from less competition is marginal. The consequences for trade, and for foreign and security policy are only briefly mentioned in the proposal, focused on the possibility that EU exclusion of third country suppliers could be interpreted as a hostile trade policy measure, leading to retaliation from such countries. The likelihood is considered small, however, as the assumption is that procuring agencies will want competition and therefore not exclude bidders without good cause.

Public consultation and feedback on the proposal

The proposal underwent public consultation and concerned stakeholders were invited to submit comments. The consultation concluded on 14 April 2026 and [62 replies were received](#). Most of the substantive replies expressed support for the proposed changes, but there was some critical feedback. Suggestions centred chiefly on four points:

- **Challenges in determining a supplier's origin:** The proposal places a heavy responsibility on procuring actors to determine the origin of a supplier. Many replies expressed the need for clearer government guidance in this regard.
- **Absence of a clear definition of an antagonistic state:** There is a risk that individual agencies or local and regional governments might inadvertently engage in foreign policy decision making when deciding on which bidders to permit to proceed. Some replies raised concerns that decisions to exclude third country bidders could be interpreted as economic warfare and provoke retaliation.
- **Third country subcontractors not excluded:** The proposed legislation does not allow for the exclusion of third country subcontractors from a procurement bid. Many replies highlighted the risks associated with the use of goods or services supplied to a bidder by a party in an antagonistic third country. In addition, third country companies could establish subsidiaries in an EU member state and thereby evade the scope of the legislation. Concerns were raised that this constitutes a loophole that could be exploited. One reply (from the airport operator, Swedavia, mentioned above) used China as a hypothetical example of such a situation.
- **Excluding competitive offers:** Excluding bidders from third countries means choosing not to consider bids that could be advantageous in terms of price or quality, meaning that the procurement process could result in more expensive, lower quality or less innovative goods and services.

Conclusions and policy recommendations

In the cases outlined above, the sensitivity of information or infrastructure is often the key consideration regarding China-related security risks. At the same time, however, identification of such risks is vague and based on somewhat sweeping descriptions of potential, but rarely evidenced, actions.

In this context, the new Swedish proposal to revise procurement legislation explicitly states that it will make it possible to exclude antagonistic states from public procurement processes. Many of the risks perceived around Chinese participation in procurement would be completely removed if it was possible to exclude all Chinese bidders from consideration. To that extent, the new law provides concerned parties with a valuable method of de-risking.

The legislative proposal estimates that the consequences of the use of this method of full exclusion would be negligible, given the small share of non-EU actors in public procurement. However, Chinese products are important in certain strategic sectors, such as medical products. It is also reasonable to assume that Chinese tenders will continue to become increasingly competitive in procurement based not just on price, but also on quality. China's progress as an advanced manufacturing economy and its dominant position in many industries make this trend likely to continue or even accelerate. Blanket exclusion of Chinese bidders might be beneficial for economic security but could mean increased costs and occasionally declining the best quality tender. This would be detrimental to the public finances. It could also be interpreted as a hostile trade measure and lead to retaliation.

So, if not a blanket exclusion, how can this new legislation be used to exclude bids from countries of concern? There is a need to understand whether a bidder's nationality constitutes a security risk in a particular case. Knowledge of how China affects national security or an entity's operations is still crucial. The legislative proposal concludes that the new rules place a large responsibility on the procuring agencies, and this is echoed in several of the replies in the public consultation.

Policy recommendations:

- **Public actors** should improve their ability to undertake security risk assessments that involve geopolitical factors. More analysis is needed on the nature of the risks emanating from China. There are specific needs in different sectors and different levels of risk to be weighed against economic and other considerations.
- **Security services and expert agencies** should more proactively engage with stakeholders to improve understanding of the China risk. A clearer, more usable definition is needed of an antagonistic state.
- **Legislators** should look at ways to regulate content (products or services) from third-country subcontractors in public procurement processes, to help further minimise security risks.

Finally, it should be noted that [work is under way in the European Commission](#) to revise the directives on public procurement. The Commission has declared its ambition that this revision will strengthen preferential access for European products and services in procurements in strategically important sectors. It can be expected that these revisions will also include provisions on addressing security risks. Furthermore, in March 2026 the European Commission proposed the [Industrial Accelerator Act \(IAA\)](#), which contains provisions on preferential treatment for EU companies in procurement. The IAA has already met with [strong disapproval from China](#) over concerns about discrimination against Chinese companies.



Björn Cappelin

Björn Cappelin is an Analyst at the Swedish National China Centre.

About NKK

The Swedish National China Centre was established in 2021 as an independent unit at the Swedish Institute of International Affairs (UI). The Centre conducts policy-relevant research and aims to contribute to a long-term improvement in the state of China-related knowledge in Sweden. UI's publications undergo internal quality control. Any views expressed are those of the author.