ACIG APPLIED CYBERSECURITY & INTERNET GOVERNANCE

NASK

Commentary: The Czech Approach to Supply Chain Security in ICT

Received: 20.10.2022
Accepted: 10.11.2022
Published: 14.11.2022

Veronika Netolická Masaryk University, Faculty of Social Studies, Department of Political Science and National Cyber and Information Security Agency, Cyber Security Policies Department, National Strategy and Policy Unit, Czech Republic, ORCID: 0000-0001-8991-384X

Cite this article as: Example:
V. Netolická, "Commentary:
The Czech Approach to Supply
Chain Security in ICT,"
ACIG, vol. 1, 2022,
DOI: 10.5604/01.3001.0016.0867

Corresponding author:
Veronika Netolická, Masaryk University, Faculty of Social Studies, Department of Political Science and National Cyber and Information Security Agency, Cyber Security Policies Department, National Strategy and Policy Unit, Czech Republic;
ORCID: 0000-0001-8991-384X
E-mail: v.netolicka@gmail.com

Abstract

Supply chain security is one of the challenges many countries are currently addressing. As this topic is a national security prerogative, the systems for screening also vary. The Czech Republic is preparing a legislative framework to protect strategically important infrastructure from high-risk suppliers. This commentary focuses on the Czech Republic's progress in this area, particularly in the European context.

Keywords

national regulation, security, supply chain, the Czech Republic

1. Introduction

The Czech Republic (CZ) is one of the last European countries to prevent and reduce dependencies on high-risk suppliers in its strategically important infrastructure through legal regulation. Despite the proactive Czech approach to this issue and its long-standing importance, CZ has not yet adopted a legislative framework to protect strategically important infrastructure from high-risk suppliers, making it among the last European Union (EU) member states to do (alongside Croatia and Ireland) [1]; as a result, it is one of the last countries not to use its prerogative to interfere in national security matters reserved for EU Member States. For this purpose, the Czech National Security Council has given authorisation to the National Authority for Cyber and Information Security (NUKIB) [2], which is the central administrative body for cyber security (including the protection of classified information in the information and communication systems and cryptographic protection). Before this mandate, CZ, like most European and EU countries, looked at supply chain security chiefly through the lens of the supply chain to 5th-generation (5G) networks. 5G networks, often referred to as technologies with the potential to become the backbone of the economy, were socially accepted as infrastructure that should be protected from misuse [3]. This narrow view which focused only on electronic communications networks—or only on one generation—has primarily (but not exclusively) shifted due to the changing security environment in Europe related to the war in Ukraine. The war in Ukraine has made it clear to the world, and Europe in particular, that supply chain security is important regardless of the sectoral divide or interlocking components for which we require this security. These interlocking components stand for confidentiality, integrity, and availability. Each has its irreplaceable function and needs to be equally protected to achieve the security of the whole security ecosystem. The supply chain of the information and communication infrastructure has the potential to disrupt each of these components. Screening of the supply chain, especially when it comes to infrastructure essential to the functioning of a state, must be the prerogative of each state underlying its technological sovereignty. Regarding the importance of this topic, this commentary focuses specifically on the supply chain of the country's information infrastructure at a strategic level, for which regulation is currently being drafted in CZ and on the basis of which CZ can exclude high-risk suppliers. The path of the CZ in this respect will be described in terms of developments in the international environment, with a primary focus on EU countries. On this basis, the current status quo and the basic ideas of the forthcoming mechanism are set out. Finally, the question of the role of the private sector in this topic is discussed.

2. The Czech Republic's path to the forthcoming regulation

CZ is one of the last remaining EU countries to approach supply chain regulation. However, few comprehensive approaches exist, even in Europe, with partial sectoral regulations prevailing. The German approach is the most comprehensive regardless of the sectoral scope. Its mechanism gives the Federal Ministry of the Interior ex ante powers to restrict the use of a critical component if its operation would affect national security [4]. Germany is followed by countries such as Poland, Slovakia, Romania, Latvia, and Cyprus, which also have legislative powers to deal with supply chain security. Furthermore, countries such as Finland, Denmark, the Netherlands, France, Austria, Estonia, Belgium, Sweden, and Italy, have already adopted specific legislative measures to reduce the risks associated with high-risk suppliers in the electronic communications sector, specifically in response to the security of the 5G networks deployment [5]. The absence of any similar process places CZ among the countries with a lower resilience to these threats; however, CZ is otherwise one of the countries with the most advanced cyber security systems [6]. It should be noted that this is not a topic that is solely dealt with at the level of EU Member States. For example, countries such as the United States of America [7], the United Kingdom [8], or Japan [9] also have mechanisms to address supply chain security.

The creation of these screening mechanisms is the prerogative of each state, even if they are members of the EU. The topic of supply chain security impinges on national security issues that the member states themselves are best equipped to evaluate and ensure. However, the EU is not giving up its efforts to address the topic in a broad plenary of member states. The most significant input has been the 5G EU Toolbox publication in 2020 (Toolbox), which presents a set of measures to mitigate the risks associated with deploying 5G networks. The Toolbox's measures are non-binding, and the decision on the scope and implementation of each measure is thus left to the EU Member States themselves [10]. The next major step at the EU level is in the form of the Council Conclusions on ICT supply chain security [11]. The fact that this is happening under the auspices of the Czech Presidency underlines the importance and priority of this topic for CZ.

Although it may seem that CZ is lagging behind the other EU Member States, this is true only concerning the absence of legal regulation to date, not the lack of consideration of the importance of the topic as such or steps at the level of soft law. First and foremost, in 2018, NUKIB warned against using software and hardware from Huawei Technologies Co., Ltd. and ZTE Corporation [12]. There are also instruments currently in place that feed into the overall framework and will complement the forthcoming legislation. This includes, for example, the legal authorization of the state to screen i) foreign direct investments [13] and ii) the applicants of cloud computing providers for registration in the state catalogue [14]. The upcoming legislation should thus analogously supplement the state's authority in screening supply chains in its strategically important infrastructure, if CZ does not want to give up on ensuring its cyber security and national security.

Just as at the international level, the topic has been highlighted, and measures have been issued, so the first steps have been taken at the Czech national level. The 2018 NUKIB warning declared CZ's position to high-risk vendors, supported by the issuance of a series of recommendations known as the Prague Proposals: The Chairman Statement on cyber security of communication networks in a globally digitalized world in 2019 [15] and developed by the Prague Proposals on Cyber Security of Emerging disruptive technologies (EDTs) [16], and the Prague Proposals on Telecommunications Supplier Diversity in 2021 [17].

In February 2021, as part of the original mandate, NUKIB prepared a white paper for regulating the supply chain verification mechanism solely for the electronic communications sector [18]. In this context, in February 2022, a non-legally binding Recommendation for assessing the trustworthiness of technology suppliers of 5G networks in CZ was issued [19]. These steps towards securing the supply chain to strategically important infrastructure in one individual sector have been followed by the latest decision of the National Security Council authorizing NUKIB to prepare a law to screen high-risk suppliers to strategically important infrastructure regardless of sectoral focus [20]. However, the fact that risks originating from the supply chain also affect sectors other than electronic communications is evident from the warnings issued by the NUKIB in 2022. The first of these warnings was against the use of smart meters from countries with untrustworthy legal environments [21]. The second warning was issued in the context of economic sanctions associated with the Russian Federation [22].

3. Principles and aspects of the forthcoming regulation

Although the legislation is still being drafted, NUKIB is already publicly commenting on the basic principles on which it wants to base the law, and on who will be affected by the regulation. An overall principle of NUKIB's work is openness concerning pending regulation and a high degree of involvement from the private sector and academia. In this context, expert public consultation has also been promised prior to the formal commentary process [23].

From the private sector's perspective, in terms of private entities or associations covered by the national regulation (the Act on Cyber Security), one of the most important questions was who would be affected by the regulation. NUKIB has been transparent in this respect, stating that the regulation will only affect the strategically important infrastructure of CZ. This term is then interpreted by the Act on Cyber Security as critical information infrastructure and operators of essential services—the set of entities is presented concerning the current legislation in force, but this set may change in the context of implementing the NIS2 Directive. The forthcoming legislation will respond to these changes to encompass only a defined set of entities, and not the extended range of entities that the implementation of the Directive will ultimately bring. Thus, the forthcoming law does not expand the group of persons and bodies under its remit but is based on a cross-section that is already familiar to the national format. Another important aspect is the substantive scope of the forthcoming regulation, i.e., what will be subject to scrutiny by the state. In this respect, too, it will not be the entire set of hardware and software subject to the administration of regulated entities. However, it will be those supplies that have relevance to national security. Thus, it only concerns predefined parts of the infrastructure [23].

The last accentuated principle according to which NUKIB wants to approach the upcoming regulation is to maintain the current approach to ensuring cybersecurity in CZ,

DOI: 10.5604/01.3001.0016.0867

according to which the administrator knows its system or network best and should therefore be responsible for its evaluation.

Thus, the mechanism will only affect critical parts of strategically important infrastructure while respecting the abovementioned principles. The preparation process is already underway with the involvement of the private sector and the academic sector.

4. Discussion: the role of the private sector

A change in the private sector's approach to increasing security need not always be driven by regulation or otherwise enforced by the state. Companies such as Palo Alto Networks [24] and Microsoft [25] have declared their interest in mitigating untrustworthy vendors. However, these remain exceptions, and even from the Czech perspective the private sector does not have a wholly unified approach. Thus, their position can be divided into two groups as a simplification. The first group follows the principle of short-term economic advantage at the cost of security risk in the medium and long term, while the second group advocates for efficient and sustainable security. As a result, the only adequate response is to shift this responsibility for assessing high-risk suppliers onto the state. Since states are best qualified at a strategic level to assess and evaluate these risks and they can also set (and oversee) a legal environment in which all equally require this element of security improvement, this demand from the private sector is also reasonable. Moreover, although the state is best equipped to make this assessment, despite the published and attributed cases that point to high-risk suppliers, there is not a sufficiently rapid change behind the mindset of using these suppliers, especially concerning the economic benefits they confer. In this regard, the state cannot afford to wait for a change in the attitude and mindset of the operators and administrators of its critical information infrastructure. Supply chain security is a complex issue, and CZ has shown that it endeavours to find a comprehensive solution. The actual result should become apparent in 2023.

REFERENCES

[1] European Court of Auditors. (2022). *Special Report 03/2022: 5G roll-out in the EU: Delays in deployment of networks with security issues remaining unresolved.* [Online]. Available: https://www.eca.europa.eu/en/Pages/DocItem.aspx?did=60614 [Accessed: Oct. 17, 2022].

[2] Government of the Czech Republic. (2021). *Resolution: The National Security Council.* [Online]. Available: https://www.vlada.cz/assets/ppov/brs/cinnost/zaznamy-z-jednani/usn-41-22.pdf. [Accessed: Oct. 17, 2022].

[3] MPO. (2022). *Implementation and development of 5G networks in the Czech Republic towards the digital economy.* [Online]. Available: https://www.mpo.cz/assets/cz/e-komunikace-a-posta/elektronicke-komunikace/koncepce-a-strategie/narodni-plan-rozvoje-siti-nga/2020/1/Implementace-a-rozvoj-siti-5G-v-CR-EN.pdf. [Accessed: Oct. 17, 2022].

[4] CRS. (2022). *Supply Chain Act: Act on Corporate Due Diligence Obligations in Supply Chains.* [Online]. Available: https://www.csr-in-deutschland.de/EN/Business-Human-Rights/Supply-Chain-Act/supply-chain-act.html. [Accessed: Oct. 17, 2022].

[5] European Court of Auditors. (2022). *Special Report 03/2022: 5G roll-out in the EU: Delays in deployment of networks with security issues remaining unresolved.* [Online]. Available: https://www.eca.europa.eu/en/Pages/DocItem.aspx?did=60614. [Accessed: Oct. 17, 2022].

[6] NCSI. (2022). *Czech Republic.* [Online]. Available: https://ncsi.ega.ee/country/cz. [Accessed: Nov. 6, 2022].

[7] Federal Communications Commission. (2022). *List of equipment and services covered by section 2 of the Secure Network Act.* [Online]. Available: https://www.fcc.gov/supplychain/coveredlist. [Accessed: Oct. 17, 2022].

[8] UK Parliament. (2021). *Telecommunications (Security) Act 2021.* [Online]. Available: https://bills.parliament.uk/bills/2806. [Accessed: Oct. 17, 2022].

[9] A. Hiroshi. (2022). *Japan sets guidelines for protecting critical supply chains.* [Online]. Available: https://asia.nikkei.com/Spotlight/Supply-Chain/Japan-sets-guidelines-for-protecting-critical-supply-chains. [Accessed: Oct. 17, 2022].

[10] NIS Cooperation Group. (2020). *Cybersecurity of 5G networks EU Toolbox of risk mitigating measures.* [Online]. Available: https://ccdcoe.org/uploads/2020/01/EU-200129-Cybersecurity-of-5G-networks-EU-Toolbox-of-risk-mitigating-measures.pdf. [Accessed: Oct. 17, 2022].

[11] Council of the EU. (2022). *The Council agrees to strengthen the security of ICT supply chains.* [Online]. Available: https://www.consilium.europa.eu/en/press/press-releases/2022/10/17/the-council-agrees-to-strengthen-the-security-of-ict-supply-chains. [Accessed: Oct. 17, 2022].

[12] NUKIB. (2018). *Warning. National Cyber and Information Security Agency.* [Online]. Available: https://www.nukib.cz/download/uredni_deska/Varovani_NUKIB_2018-122-17.pdf. [Accessed: Oct. 17, 2022].

[13] MPO. (2022). *Implementation and development of 5G networks in the Czech Republic towards the digital economy.* [Online]. Available: https://www.mpo.cz/en/foreign-trade/investment-screening. [Accessed: Oct. 17, 2022].

[14] MV ČR. (2022). *EGovernment Cloud.* [Online]. Available: https://www.mvcr.cz/clanek/katalog-cloud-computingu.aspx. [Accessed: Oct. 17, 2022].

[15] Government of the Czech Republic. (2019). *Prague 5G security conference announced series of recommendations: The Prague Proposals.* [Online]. Available: https://www.vlada.cz/en/media-centrum/aktualne/prague-5g-security-conference-announced-series-of-recommendations-the-prague-proposals-173422 [Accessed: Oct. 17, 2022].

[16] NUKIB. (2021). *Prague proposals on cyber security of EDTs.* [Online]. Available: https://www.nukib.cz/download/Prague_Proposals_on_Cyber_Security_of_EDTs.pdf. [Accessed: Oct. 17, 2022].

[17] NUKIB. (2021). *Prague proposals on telecommunications supplier diversity.* [Online]. Available: https://www.nukib.cz/download/Prague_Proposals_on_Telecommunications_Supplier_Diversity.pdf. [Accessed: Oct. 17, 2022].

[18] Government of the Czech Republic. (2022). *Resolution: The National Security Council*. [Online]. Available: https://www.vlada.cz/assets/ppov/brs/cinnost/zaznamy-z-jednani/usn-33_2.pdf. [Accessed: Oct. 17, 2022].

[19] NUKIB. (2022). *Recommendation for assessing the trustworthiness of technology suppliers of 5G networks in CZ*. [Online]. Available: https://www.vlada.cz/assets/ppov/brs/cinnost/zaznamy-z-jednani/usn-33_2.pdf. [Accessed: Oct. 17, 2022].

[20] Government of the Czech Republic. (2021). *Resolution: The National Security Council*. [Online]. Available: https://www.vlada.cz/assets/ppov/brs/cinnost/zaznamy-z-jednani/usn-41-22.pdf. [Accessed: Oct. 17, 2022].

[21] NUKIB. (2022). *Warning against using smart meters from countries with untrustworthy legal environments*. [Online]. Available: https://www.nukib.cz/download/uredni_deska/2022-05-30_varovani-smartmetering_final_1.0_podepsno.pdf [Accessed: Oct. 17, 2022].

[22] NUKIB. (2022). *Warning in the context of economic sanctions associated with the Russian Federation*. [Online]. Available: https://www.nukib.cz/download/uredni_deska/2022-03-21_varovani_rusti-dodavatele.pdf [Accessed: Oct. 17, 2022].

[23] NUKIB. (2022). *Increasing the supply chain security of the state's strategic infrastructure is in the interest of the Czech Republic*. [Online]. Available: https://www.nukib.cz/en/infoservis-en/news/1886-increasing-the-supply-chain-security-of-the-state-s-strategic-infrastructure-is-in-the-interest-of-the-czech-republic. [Accessed: Oct. 17, 2022].

[24] M. Coleman. (2020). *NIST highlights palo alto networks supply chain best practices*. [Online]. Available: https://www.paloaltonetworks.com/blog/2020/06/policy-supply-chain-best-practices. [Accessed: Oct. 17, 2022].

[25] Microsoft. (2022). *Supply chain security*. [Online]. Available: https://www.microsoft.com/en-us/research/project/supply-chain-security/publications. [Accessed: Oct. 17, 2022].