THE RECOMMENDATION FOR ASSESSING THE TRUSTWORTHINESS OF TECHNOLOGY SUPPLIERS OF 5G NETWORKS IN THE CZECH REPUBLIC

National Cyber and Information Security Agency

MINISTRY OF INDUSTRY AND TRADE OF THE CZECH REPUBLIC

Ministry of Foreign Affairs of the Czech Republic

Prepared by the National Cyber and Information Security Agency, Ministry of Industry and Trade, Ministry of Foreign Affairs, Security Information Service, Office for Foreign Relations and Information, and Military Intelligence

Contents

Executive Summary

- The fifth-generation networks (hereinafter referred to as „5G networks“) have the potential to become the digital communication backbone of our economy and society and enable the development and use of new technologies in completely new ecosystems.
- Long-term sustainable security and resilience of these networks is a strategic interest of the state and society as a whole.
- One of the key prerequisites for ensuring the cyber security of 5G networks technology solutions is the supply chain security. The hardware and software of 5G network technology solutions is already so complex that it is insufficient to reduce the risks associated with suppliers solely by technical means; therefore, the trustworthiness of the supplier is a crucial factor.
- Trust in the supplier must be present both at the level of the final form of the delivered solution, as well as at the strategic level within the business, legal and political environment in which the supplier operates.
- The purpose of this recommendation for assessing the trustworthiness of suppliers of technologies for 5G networks in the Czech Republic (hereinafter the „Recommendation“) is to offer operators – or the entire electronic communications sector – the views of the National Cyber and Information Security Agency, Ministry of Industry and Trade, Ministry of Foreign Affairs, Security Information Service, Office for Foreign Relations and Information, and Military Intelligence (hereinafter referred to as “selected state institutions”) on crucial points for assessing the trustworthiness of suppliers of technologies for 5G networks, and to propose criteria that can contribute to the selection of trustworthy suppliers.

Introduction

The development of new information and communication technologies and digital infrastructure in general is a prerequisite for the successful long-term development of national economies. Future mobile electronic communications networks and especially 5G networks have the potential to become the digital communications backbone of our economy and society.

5G networks include various elements of the network infrastructure for mobile communication technologies used to connect an end subscriber or a device. They do not necessarily need to consist only of elements of new technologies, but as a rule they also use elements of previous generations of mobile networks, such as 4G or 3G networks.

5G networks bring, among other things, substantially higher transfer rate, significantly lower latency, high connection reliability and the ability to connect many devices to the network while using advanced virtualization, decentralization, beam shaping and higher data flow sharing rate. These features allow the development of the potential and the use of new technologies, such as diverse autonomous systems, artificial intelligence and machine learning, the Internet of Things, quantum computing technologies and their integration into new ecosystems. It is this potential that predestines 5G networks to become an essential part of the state communication infrastructure, and they need to be approached as such in both their design and construction, as well as in their operation.

An important part of 5G networks cyber security is the supply chain security. In case of 5G networks, due to their high complexity and high cost, a typical phenomenon in the market with these technologies is the dependency of the customer (i.e. the entity building and operating the 5G network) on the technology supplier and its supply chain. This dependency brings along new cyber threats and increases the risk associated with some existing threats, such as the ability to implement a vulnerability that violates the confidentiality, availability, or integrity of transmitted data in the delivered technological solution. Trust in the supplier and in the technological solutions he supplies is essential in this regard.

Disruption of 5G networks cyber security – and especially the most serious cases such as cyber espionage or large-scale disruption of network availability leading to significant damages – is a major problem for important economic interests and security of the state, as well as for operators and their users. Given the role that 5G networks will play in the coming years in the development of new technologies, communication ecosystems, and the increasing number of connected devices, occurrence of the above-mentioned threats would have far-reaching social consequences.

Long-term sustainable security and resilience of these networks is therefore a strategic interest of the state and of the society as a whole.

1 The aim of the recommendation and the rationale for its need

Based on publicly available documents of the security institutions of the Czech Republic[1], state actors' attacks on the systems that are critical to the functioning of the state are becoming commonplace, affecting the lives of many residents, and functioning of many institutions. The security of these systems is threatened not only by cyber attacks, but also by suppliers and supply chains falling within the sphere of influence of the nation-state threat actors whose interests and international operations are in conflict with the interests of the Czech Republic. These suppliers can thus become a means to pursue political goals.

In recent years, a significant number of documents addressing 5G network security (in particular, the supply chain security and the trustworthiness of 5G network technology suppliers) has been issued at a European and global level. The decisive documents in this aspect are, for example, (i) the Prague Proposals[2], which were adopted at the 5G Security Conference in Prague in 2019, (ii) the EU 5G Toolbox[3], which was issued by the NIS Cooperation Group in January 2020, consisting of representatives of the member states of the European Union (hereinafter also „EU"), the European Commission and the European Union Agency for Cybersecurity (ENISA), (iii) The Joint Statement on the US-Czech Declaration on 5G network security[4] and others[5].

These documents directly or indirectly describe, among other things, how states and operators should approach the construction of 5G networks and the selection of suppliers of technologies that will be used to operate 5G networks in the way to ensure that these networks are secure and resilient.

---

[1] See, for example, the annual reports of the Security Information Service (BIS. Annual reports [online]. Available at: https://www.bis.cz/vyrocni-zpravy/), the annual reports of the Military Intelligence (MILITARY INTELLIGENCE. Annual reports [online]. Available at: https://www.vzcr.cz/vyrocni-zpravy-o-cinnosti-vojenskeho-zpravodajstvi-41) or Reports on the state of cyber security in the Czech Republic (NÚKIB. [online]. Available at: https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/zpravy-o-stavu-kb/)

[2] The Prague Proposals [online]. Praha,3.5.2019. Available at: https://www.nukib.cz/download/5G_site/Prague_Proposals_ENG.pdf

[3] Cybersecurity of 5G networks EU Toolbox of risk mitigating measures [online]. 01/2020. Available at: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=64468

[4] Joint Statement on United States – Czech Republic Joint Declaration on 5G Security [online]. 7. 5. 2020. Available at: https://cz.usembassy.gov/joint-statement-on-united-states-czech-republic-joint-declaration-on-5g-security/

[5] In addition, there are recommendations regarding the use of equipment from high-risk suppliers in the UK's National Cyber Security Center (NCSC. NCSC advice on the use of equipment from high risk vendors in UK telecoms networks [online]. 28. 1. 2020 Available at: https://www.ncsc.gov.uk/guidance/ncsc-advice-on-the-use-of-equipment-from-high-risk-vendors-in-uk-telecoms-networks), the public draft of the Australian Ministry of the Interior´s critical technology supply chain principles (Critical Technology Supply Chain Principles [online] 2020. Available at: https://www.homeaffairs.gov.au/reports-and-pubs/files/critical-technology-supply-chain-principles-discussion-paper.pdf), or the criteria for security and trust in telecommunications networks and services of the prestigious think-tank Center for Strategic and International Studies (CSIS. Criteria for Security and Trust in Telecommunications Networks and Services [online]. 13. 5. 2020. Available at: https://www.csis.org/analysis/criteria-security-and-trust-telecommunications-networks-and-services).

The Strategic Measure No. 3 (SM03) of the EU 5G Toolbox also stipulates that the EU member states shall adopt a framework for the assessment of the risk profile of relevant suppliers at a national level or together with other member states. **Efforts to create such an assessment mechanism at a national level are already under way.** On the basis of the instruction of the State Security Council, a White Paper is being prepared, whose objective is to implement such a mechanism in the Czech Republic.

However, the preparation of the assessment mechanism is, given its nature, likely to require the adoption of legislative changes. Due to (i) the complexity of the issue, (ii) the need for consultation across selected state institutions, private sector representatives in the electronic communications sector and academia (iii) and given the usual length of the legislative process, **such legislative changes cannot be expected to occur at the current stage of preparations for building 5G networks.** The first implementation of 5G network technologies are already emerging and before the assessment mechanism is adopted, it is necessary for the state to clearly declare national security interests and offer operators criteria for selecting trusted suppliers to 5G networks, at least in the form of a recommendation.

However, the aim of the recommendation is not to propose trustworthiness criteria for a uniform and general application to all suppliers of 5G networks in the Czech Republic. The aim is **to provide guidance especially for the supplies to the information and communication systems of the critical infrastructure of the Czech Republic.** Nevertheless, the proposed criteria are neutral due to the nature and importance of the infrastructure and, at the discretion of individual operators, they can also be applied to suppliers to strategically less important infrastructure.

The aim of the recommendation is not to propose usable conditions of tender documentation in case the supply to the 5G network was the subject of a public commission. In the case of the use of recommendation in a public procurement, it is necessary that the use of criteria in the tender documentation is justified according to the requirements of the relevant legal regulations, and independently of the recommendation. However, the selected state institutions do not assume the use of the recommendation for public procurement, and the recommendation was not prepared for this purpose.

2 The basis of the recommendation

The basis of the recommendation form the rationale of the thought processes of the selected state institutions regarding non-technical aspects of the supply chain security based on the fundamental security interests of the Czech Republic, and also reflect foreign recommendations for cyber security of 5G networks and similar materials mentioned above.

One of the key prerequisites for ensuring the cyber security of 5G network technology solutions, as well as many other systems and networks, is to assess the trustworthiness of suppliers and subcontractors of such solutions. Trust in the supplier must be present both at the level of the final form of the delivered solution as well as at the strategic level, i.e. in the business, legal and political environment in which the supplier operates.

Reducing the risks associated with suppliers to 5G networks by technical means alone is insufficient; the hardware and software of these technological solutions are so complex that they cannot be effectively technically checked for potential vulnerabilities elimination. These vulnerabilities may therefore remain undetected for a long time, or they may be introduced later, for instance as a part of updates. **Trust in the supplier is essential in this regard. The impact of the legal and political environment from which the supplier originates or is influenced by is of considerable importance for trustworthiness, and it is therefore necessary to take it into account to ensure the security of the most important components of 5G networks.**

In this respect, from the selected institutions' point of view, the credibility of suppliers is influenced by (among other things) the fact whether the supplier:

- resides in the state, or is only subject to the laws of the states which:
  - have a democratically elected government, which includes, among other things, existence of an independent opposition, free elections based on which the current government can be replaced, and a functioning principle of so-called brakes and counterweights,
  - have an independent judicial system which is not subject to direct political interference, it respects binding rules, customs and the rule of law, such as the right to a fair trial, incl. respecting the presumption of innocence, the right to a public hearing and the right to be tried without undue delay,
  - whose legislation and public policies are governed by the rule of law and are issued with regards to them,
  - ensure protection of intellectual property,
  - do not violate international law in a long-term or systematic manner, and against whose activities the international and supranational organizations or alliances (of which the Czech Republic is a member) are not officially defined against e.g. in the form of a

United Nations Security Council resolution or a restrictive common foreign and security European Union policy measure,

- maintain a partnership with the Czech Republic and do not carry out activities which run counter to the fundamental interests of the Czech Republic or its allied states,
- do not consider the Czech Republic to be an enemy state,

- is not inappropriately influenced by a foreign government or a state administration body and is capable of ensuring the availability, integrity, and reliability of data in the supplied technological solutions with a sufficient degree of autonomy,
- pursues commercial objectives, conducts business in accordance with international trade practices, and does not have disproportionate advantages (e.g. a state aid significantly distorting competition) from the state in which he resides or under whose influence he falls,
- meets the safety standards that are common in the market at the time of delivery and is willing to commit to meeting them in the future.

The above-mentioned points are not intended to be used as criteria for assessing the credibility of suppliers for operators; Part 3 of the Recommendation deals with the proposal of specific evaluating criteria for the operators.

3 The criteria for strengthening the trustworthiness of the suppliers

When selecting a supplier, operators and other representatives of the electronic communications sector may consider the following criteria, which reflect the basis set out in section 2 of the Recommendation, and whose fulfillment increases the likelihood of selecting a trustworthy supplier. In such case, it is appropriate to apply the criteria to all procured supplies of technologies that are relevant to the security of the 5G networks, considering the significance of each specific supply for the technological unit. It is therefore possible and appropriate to apply the criteria in the given circumstances to both the suppliers who enter into a direct contractual relationship with the customer and, to a reasonable extent, to their suppliers and subcontractors, if the nature and circumstances of the supply allow it.

The selected state institutions that prepared the Recommendation are fully aware that it is the state that is best equipped to assess the strategic criteria for the trustworthiness of suppliers and that some information necessary for such an assessment is available only to the selected state security institutions. However, as already mentioned in Part 1 of the Recommendation, pending the establishment of a legal framework for the trustworthiness assessment, the selected state institutions offer the following non-binding criteria to operators and all other interested parties in the electronic communications sector to be taken into account when selecting suppliers according to their considerations and possibilities.

Although the criteria in the Recommendation have been prepared with maximum regard to their applicability in practice, **the inability to assess or to take into account any of the criteria or non-fulfillment of a criterion by the supplier does not automatically mean unsuitability of the supplier or a high risk associated with a supplier.** The suitability of the application and the weight of each criterion for the trustworthiness of the supplier must always be assessed with regard to the context of the relevant supply, including the significance of the supply for the technological unit.

The Recommendation does not aspire to set a maximum or minimum number of criteria that a supplier should meet in order to be considered trustworthy; the recommendation should serve as one of the guides to be used for the selection of appropriate criteria. **The Recommendation does not change or limit any obligation of the bodies and persons obliged under the Cyber Security Act or a Cyber Security Decree.**

3.1 Strategic criteria

The business activities of each supplier are based in a certain state-law framework. This framework is usually defined by the law of the country in which the supplier resides and by its cultural environment. However, suppliers often also fall under the jurisdiction (i.e. legal and cultural environment) of other states. From the security point of view, it is therefore appropriate (according to the possibilities of the specific entity) to analyze and assess the criteria reflecting

the compliance of legal norms, principles and customs by which the supplier is bound by various legal systems, with standards, principles and customs of the Czech law.

The strategic criteria increasing the credibility of the supplier are, in particular:

- The supplier and his controlling entities[6] are based in an EU member state or in the North Atlantic Alliance (hereinafter referred to as "NATO").
- The supplier is based in a state, (i.e. it is subject only to the legal systems of such states) which is a contracting party of international agreements on cyber security, has existing agreements on cooperation in the field of security or similar arrangements with the Czech Republic, or is subject to such rules. These are in particular:
  - the EU member states and the states ensuring adequate protection of personal data in the sense of Article 45 of the General Data Protection Regulation (GDPR)[7]
  - states that are a contracting party of one of the agreements on the exchange and mutual protection of classified information with the Czech Republic[8],
  - states that are a contracting party of the Government Procurement Agreement[9],
  - states that are a contracting party of the so-called Budapest Convention on Cybercrime[10].

[6] In the sense of § 74 et seq. Act No. 90/2012 Coll., on business corporations, as appropriate.

[7] In the case of non-EU countries, these will be, in particular, those covered by the Commission's decision on adequacy under Article 45 of the General Data Protection Regulation (GDPR). For an overview of current Commission decisions, see ÚOOÚ. Transmission based on the decision on the appropriate level of protection of personal data [online]. Available at: https://www.uoou.cz/predavani-zalozene-na-rozhodnuti-o-odpovidajici-urovni-ochrany-osobnich-udaju/ds-5065

[8] National Security Agency. International agreements on the exchange and reciprocal protection of classified information [online]. Available at: https://www.nbu.cz/cs/mezinarodni-vztahy/941-mezinarodni-smlouvy-o-vymene-a-vzajemne-ochrane-utajovanych-informaci/

[9] WTO. Parties, observers and accessions: Agreement on Government Procurement [online]. Available at: https://www.wto.org/english/tratop_e/gproc_e/memobs_e.htm

[10] COUNCIL OF EUROPE. Chart of signatures and ratifications of Treaty 185 [online]. Available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=aLFDJWbF

- The supplier resides in a state (i.e. it is subject only to the legal systems of such states) which is not publicly warned against by the security institutions of the Czech Republic in connection with the conduct of intelligence or other operations that harm the interests of the Czech Republic or the EU or NATO member states[11].
- The supplier is willing to commit by means of a statement declaring that he is legally and factually able to refuse to disclose confidential information from or about his customers to third parties. In case of a legal information obligation, the supplier refers to the relevant provisions in legal regulations.

[11] These public notices may be e.g. part of the Security Information Service's annual report [online]. Available at: https://www.bis.cz/vyrocni-zpravy/), MILITARY INTELLIGENCE annual reports [online]. Available at: https://www.vzcr.cz/vyrocni-zpravy-o-cinnosti-vojenskeho-zpravodajstvi-41) or the Reports on the state of cyber security in the Czech Republic (National Cyber and Information Security Agency) [online]. Available at: https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/zpravy-o-stavu-kb/).

3.2 Business criteria

Many suppliers have been operating in the market for a long time and thus have a certain reputation and history of behavior in business relationships. Awareness of the supplier's business practices is another important aspect that is important to consider when choosing a supplier. In order to assess the supplier's trustworthiness, it is also appropriate to have relevant information on the ownership structure, financing, management structure of the supplier and other factors that have a significant impact on the supplier's business behavior.

The business criteria that increase the trustworthiness of the supplier are in particular:

- The supplier has a transparent ownership and management structure of the company and communicates or allows the customer to monitor significant changes in these structures.
- The customer is not aware that an effective control of the economic activity[12] is exercised over the supplier by a state that does not meet some of the strategic criteria relevant to the states (see section 3.1 of the recommendation).
- The customer is not aware of the supplier being covertly or non-transparently financed or receiving non-transparent financial support or other financial resources that are not commercially justified.
- The customer is not aware of the supplier or his representatives[13] acting unethically or systematically unethically, contrary to the care of a proper manager or in violation of international trade rules and in case of their previous operation in the Czech Republic also in serious violation of the Czech law.[14]

[12] Pursuant to § 5 of Act No. 34/2021 Coll., On the assessment of foreign Investments and on the amendment o related acts (Act on the Assessment of Foreign Investments), adequately.

[13] Pursuant to § 436 section 1 and following the act no. 89/2012 Coll., of the Civil Code, adequately.

[14] E.g. that the supplier or his representatives have not been convicted of intentionally committing a criminal offense in the Czech Republic.

3.3 Technical and security-related criteria

Although non-technical criteria for assessing the supplier‘s credibility are highlighted across this recommendation, it should be acknowledged that the technical aspects of supplies to 5G networks are crucial for the security of 5G networks as well. The supplier’s approach to security-related and technical rules and processes and the willingness to be transparent in this regard is an important sign of his trustworthiness.

Technical and security-related criteria increasing the trustworthiness of the supplier are in particular:

- The supplier is able to prove that he uses the so-called security by design principle in his products and that he practices effective security rules and processes.
- The supplier and the solutions he offers comply with the standards in the field of personal data protection and intellectual property protection, including their compliance with legal regulations in these areas.
- The supplier is willing to commit to complying with the safety rules he has established with the customer.
- The supplier is able and willing to provide the customer with accurate information about his supply chain. The supplier controls and enforces compliance with the safety rules he agreed upon with his own suppliers.
- The supplier is able and willing to provide the customer with accurate information about the origin and composition of individual supplied components, both software and hardware, which have an impact on the safety of the supplied technological solution.
- The supplier is willing to commit to report the vulnerabilities that exist in the technological solution supplied by him or that will be discovered in the future.
- The supplier is able and willing to provide the customer with information on cyber or other security related incidents that concern the customer or that have a significant impact on the customer‘s activities or on the delivered technological solution.
- The supplier is willing to commit to enable the customer to perform independent security audits at the supplier and to make conclusions from the independent penetration testing of the delivered technological solution available to the customer.
- The supplier provides the customer with information regarding updates and maintenance of the supplied technological solution and is willing to provide the customer with updates correcting vulnerabilities known to the supplier during the life cycle of the delivered technological solution.
- The supplier is willing to commit not to intentionally integrate or deliberately allow the integration of vulnerabilities into the delivered technological solution.

Conclusion

The aim of this recommendation is to present the view of the state on assessing the trustworthiness of suppliers of technologies for 5G networks and a supporting guide for the selection of trustworthy suppliers.

Security is a key and an essential part of functioning of the systems that are critical for the proper operation of the state. It must be integrated from the very beginning of their construction, including the selection of the supplier of these systems. In order to meet this requirement, it is necessary (among other things) to have a good understanding of who these technology suppliers and manufacturers are, whether they are trustworthy and whether they act ethically and in accordance with the Czech law.

Although this recommendation focuses on the selection of trusted suppliers for the 5G networks of the strategically most important infrastructure in the Czech Republic with implications for national security, the recommended criteria are universal principles. It is therefore possible to apply them in a similar way in other areas when implementing technologies.