Input to the Dutch public consultation on 5G security measures

Appropriate cybersecurity measures are necessary to deliver trust in the digital infrastructure, the foundation of the Fourth Industrial Revolution. Nokia is committed to an open and transparent dialogue with policy makers and regulators to help shape the future and deliver on the promise of the digitized world.

In case of questions, please contact:

Ruud Klein Schiphorst, Nokia Netherlands Country Senior Officer

ruud.klein_schiphorst@nokia.com

1 About Nokia

Nokia is a provider of world class, secure and reliable telecom infrastructure, software and services. We recognize our role and our responsibility to contribute to improving cybersecurity given our outstanding position in the global market. Therefore, we are grateful for the opportunity to share our comments in this public consultation.

To date, we have concluded over 100 commercial 5G contracts worldwide, including in 5G leading markets of the US, Japan and Korea where first 5G deployments were run on Nokia gear. For instance, Nokia delivered core and Radio Access Network (RAN) for world's first nationwide 5G-SA deployment (T-Mobile, US). Nokia is currently No.1 for ownership of granted patents that the researchers found essential to the 5G standard. Nokia Bell Labs pioneered many of the fundamental technology innovations that are being adopted into 5G standards (e.g. Massive MIMO beam management, mobile edge computing). Nokia is also a market leader for telecom software, a key domain given that virtualization and cloudification are the dominating trends in the network architecture.

Nokia's business is built on a foundation of trust. We embed security and privacy into all our products; our "Design for security" process ensures that security is designed in and managed throughout a product's lifecycle, supported by a rich set of technologies, tools and procedures. Nokia also has a trusted and sustainable supply chain. Its resilience relies on implemented business continuity plans providing flexibility and reliability to minimize disruption to operations in a time of crisis; multi sourcing (i.e., availability of alternative sourcing); and implemented processes to manage critical component inventories. Additionally, we play an active role in key standardization bodies that are shaping the latest in security standards and best practices.

Nokia helps operators to improve the security of networks through a wide-ranging end-to-end security products portfolio and security services including security risk assessment, security solution integration and managed security operations. Our solutions address risks related to misconfiguration of networks; lack of access controls; and exploitation of Internet of Things (IoT), handsets and smart devices with best-in-class solutions.[1] Further, Nokia's NetGuard Adaptive Security Operations is the telco market's most comprehensive Security Orchestration, Analytics and Response (SOAR) solution. Providing end-to-end security, the suite integrates audit compliance, privileged access, threat intelligence, network-based malware detection, and certificate management.

[1] More information about Nokia's contribution to 5G Security: https://onestore.nokia.com/asset/207438

2 Importance of security in 5G era

5G will have a positive and significant impact on productivity, and it will extensively transform global economies – by 2030, we believe it will deliver $8 trillion in value around the world. 5G will connect everyone to everything and digitally transform even the most physical aspects of our lives. Every industrial segment, public service or critical infrastructure will be touched by the 5G revolution. Realizing network as a service and the diversity of 5G use cases will make securing the network more complex. Availability, confidentiality and integrity of all user, management and control functions need to evolve to cater to dynamic networks, an increased number of players involved in service delivery, and a wide variety of devices (including IoT), users, and applications. The more indispensable 5G networks become, the bigger the risk of them being tampered with, and therefore the bigger the prize for malicious actors to interfere with them (hackers and hostile domestic and foreign agents). Because of how crucial the networks will become for the national economy, and for national security, we understand the need to introduce new requirements on companies providing the 5G networks.

3 Need for an EU-level alignment and preference for EU 5G cybersecurity scheme

Already today in Europe network and security operation centers (NOC and SOC) operate across national borders. Further, intense European roaming and interdependences within the European Single Market mean that any cyber-attack and network security breach at a national level may have consequences for the whole European Union (EU). This calls for aligned implementation of concrete 5G technical security measures across the EU. Nokia respectfully suggests revisiting which of the new obligations are best introduced at the national level in Netherlands, and which should be better discussed in the context of the future 5G cybersecurity certification on the basis of the EU Cybersecurity Act.

4 Specific provisions

Specific provisions proposed are ambitious and meaningful. However, we recommend changing measure D.3. Security assurance would best be provided by globally recognized procedures of Security by Design, as well as by the newest security assurance scheme developed by the industry GSMA: Network Equipment Security Assurance Scheme (NESAS), whereby compliance is assessed by independent auditors. We discourage mandating pen-testing as it incurs disproportionate delays and costs. Pen-testing is not commonly mandated by regulators, not even in countries with the strictest cybersecurity rules (while occasionally implemented by operators at their own

discretion). In addition, as noted above, we recommend developing a 5G security assessment scheme at the EU level. Further, provision D.3.c (issues identified shall be resolved before deployment) should be amended. Operators should be required to present a plan to address identified vulnerabilities based on their gravity and urgency. An obligation to indiscriminately resolve all vulnerabilities, regardless of their criticality classification, may dramatically delay deployments. For lower priority vulnerabilities some lead time post deployment should be acceptable. Finally, to avoid negative impact on the EU Single Market, provision of managed services from other EU countries should still be possible. For this reason, Nokia stresses again the importance of avoiding deviations of rules in various European countries and we call for a unified EU-level framework.

5 Definition of critical elements

Several criteria may be applied to assess criticality of network elements that need to be governed by special provisions:

- Vulnerability of the elements for remote attack

All network elements which can be remotely controlled or managed are sensitive. A malicious actor can use remote access to switch off this part of the network. As such, the Radio Frequency and Baseband Units as well as active antennas for mMIMO have critical aspects and should be subject to appropriate safeguards.

- Virtualization increases “critical” footprint

The new 5G architecture, characterized by virtualization, blurs the distinction between mobile access and core. For instance, mobile access (RAN) can be realized in a variety of topologies, ranging from the “classical” distributed networks based on specific hardware, to virtualized architectures (vRAN/VNF) based on large numbers of Edge Clouds. The Edge Cloud will not be dedicated to the RAN but will also host part of the Core, mainly gateways, and applications to implement the low latency use cases that are supported with 5G. The definition of what constitutes “critical elements” should be broad enough to capture all those scenarios.

- Application

Criticality of networks and specific networks elements should be evaluated based on (potentially disrupted) applications underpinned by those networks. Even a short failure in connectivity in a limited geographic area could result in a deadly consequence (e.g., disruptions of connected car services). As such, undisrupted access to connectivity becomes as crucial as undisrupted access to electricity. Critical infrastructure might be defined by its uses related to the “open strategic autonomy” (term proposed by the EU):

- Government networks and data centres.

- Infrastructure used by providers of basic products and services: energy, food, raw materials, railways, airports, telecoms, banks, internet exchanges, water utilities, hospitals.
- Infrastructure critical for high value enterprises/enterprises of key strategic importance for the nation's economy.

Moreover, application of the specific network/network element may evolve in time.

6 Technical rules cannot replace strategic measures

Supplier's capability of providing and maintaining secure hardware and trustworthy software is of key importance. However, ultimately technical means do not provide sufficient guarantees, and trust between involved parties is essential. Providers of telecommunication technology and services have privileged position in terms of access to, and knowledge about a telecommunication network, its components and management. It is important to assess if there are no reasons to fear that this privileged position would be leveraged in the future to conduct or facilitate "malicious actions" such as, for example, undue access to data or manipulation of network functions. That is why technical measures must be supplemented by strategic measures as defined in the EU 5G toolbox (Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures). It lists specific measures to address risks related to non-technical vulnerabilities (e.g., risk of interference by a third country or dependency risks).