The Prague Proposals

The Chairman Statement on cyber security of communication networks in a globally digitalized world

Prague 5G Security Conference

Prague, 3 May 2019

PREAMBLE: COMMUNICATION NETWORKS IN GLOBALLY DIGITALIZED WORLD

Communication is the cornerstone of our societies. It defines almost every aspect of our lives. Yet the rapid development and scale on which we use communication technologies increases our dependency and vulnerabilities.

5G networks and future communication technologies will transform the way we communicate and the way we live substantially. Transportation, energy, agriculture, manufacturing, health, defense and other sectors will be significantly enhanced and altered through these next generation networks. High-speed low-latency technology is expected to allow for a true digital evolution, stimulating growth, innovation and well-being. Automatization of everyday activities and the use of the internet of things in its full potential will be made possible.

These developments, however, invoke major risks to important public interests and have national security implications. Today, malicious actors operate in cyber space, with the intention to undermine cohesion of our societies and paralyze the proper functioning of states or businesses. This includes attempts to control or disrupt our communication channels and the information transmitted. In digitalized societies, this can have serious consequences.

Security of communication channels has therefore become vital. Disruption of the integrity, confidentiality or availability of transmitted information or even the disruption of the service itself can seriously hamper everyday life, societal functions, economy and national security. Communication infrastructures are the cornerstone of our societies, with 5G networks to become the building blocks of a new digital environment.

ON THE IMPORTANCE OF SECURITY OF 5G NETWORKS

Considering that security of 5G networks is crucial for national security, economic security and other national interests and global stability, the chair believes that the architecture and functions of 5G networks must be underpinned by an appropriate level of security.

EU Member States underline their own ongoing process aimed at defining a common EU approach on the issue of cybersecurity of 5G networks as initiated by the European Commission with the publication of its Recommendation published on 26 March 2019.

With the intention to support ongoing discussions how to decrease the security risks associated with developing, deploying, operating, and maintaining complex communication infrastructures such as 5G networks, the chair recognizes existence of the following perspectives:

Cyber security not only a technical issue

Cyber security cannot be regarded as a purely technical issue. A safe, secure and resilient infrastructure requires adequate national strategies, sound policies, a comprehensive legal

framework and dedicated personnel, who is trained and educated appropriately. Strong cyber security supports the protection of civil liberties and privacy.

Both technical and non-technical nature of cyber threats

When dealing with cyber security threats, not only their technical nature, but also specific political, economic or other behaviour of malicious actors which seek to exploit our dependency on communication technologies should be taken into account.

Possible serious effects of 5G networks disruption

Due to the wide application of 5G based networks, unauthorized access to communications systems could expose unprecedented amounts of information or even disrupt entire societal processes.

Nation-wide approach

Policies and actions taken to ensure a high level of cyber security should not be aimed and carried out only by primary stakeholders (i.e. operators and technology suppliers), but should also be reflected by all relevant stakeholders in other areas and sectors which significantly influence the general level of security, e.g. education, diplomacy, research and development, etc. Safeguarding cyber security of communication infrastructure is not solely an economic or commercial issue.

Proper risk assessment essential

Systematic and diligent risk assessment, covering both technical and non-technical aspects of cyber security, is essential to create and maintain a truly resilient infrastructure. A risk based security frameworks should be developed and deployed, taking into account state of art policies and means to mitigate the security risks.

Broad nature of security measures

Cyber security measures need to be sufficiently broad to include whole range of security risk, i.e. people, processes, physical infrastructure, and tools both on the operational and strategic level.

No universal solutions

The decision on the most optimal path forward when setting the proper measures to increase security should reflect unique social and legal frameworks, economy, privacy, technological self-sufficiency and other relevant factors important for each nation.

Ensuring security while supporting innovation

Innovation is the main driver of development and economic growth in modern societies. It also fosters new security solutions. Policies, laws, and norms, should allow security measures to be flexible to manage the interface between security and specific national conditions. Through this flexibility, creativity and innovation should be encouraged.

Security costs money

Achieving a proper level of security sometimes does require higher costs. Increased costs should be tolerated if security necessitates it. At the same time, security does not necessarily imply higher costs.

Supply chain security

Shared responsibility of all stakeholders should drive supply chain security. Operators of communication infrastructure often depend on technology from other suppliers. Major security risks emanate from the cross-border complexities of an increasingly global supply chain which provides ICT equipment. These risks should be considered as part of the risk assessment based on relevant information and should seek to prevent proliferation of compromised devices and the use of malicious code and functions.

Bearing in mind these perspectives, the chair calls upon a responsible development, deployment, and maintenance of 5G networks and future communication technologies, considering the following proposals and best practices.

PRAGUE PROPOSALS

The Chairman suggests following proposals in four distinct categories in preparation for the roll out of 5G and future networks.

A. **Policy**

- Communication networks and services should be designed with resilience and security in mind. They should be built and maintained using international, open, consensus-based standards and risk-informed cybersecurity best practices. Clear globally interoperable cyber security guidance that would support cyber security products and services in increasing resilience of all stakeholders should be promoted.
- Every country is free, in accordance with international law, to set its own national security and law enforcement requirements, which should respect privacy and adhere to laws protecting information from improper collection and misuse.
- Laws and policies governing networks and connectivity services should be guided by the principles of transparency and equitability, taking into account the global economy and interoperable rules, with sufficient oversight and respect for the rule of law.
- The overall risk of influence on a supplier by a third country should be taken into account, notably in relation to its model of governance, the absence of cooperation agreements on security, or similar arrangements, such as adequacy decisions, as regards data protection, or whether this country is a party to multilateral, international or bilateral agreements on cybersecurity, the fight against cybercrime, or data protection.

B. **Technology**

- Stakeholders should regularly conduct vulnerability assessments and risk mitigation within all components and network systems, prior to product release and during system operation, and promote a culture of find/fix/patch to mitigate identified vulnerabilities and rapidly deploy fixes or patches.
- Risk assessments of supplier's products should take into account all relevant factors, including applicable legal environment and other aspects of supplier's ecosystem, as these factors may be relevant to stakeholders' efforts to maintain the highest possible level of cyber security.
- When building up resilience and security, it should be taken into consideration that malicious cyber activities do not always require the exploitation of a technical vulnerability, e.g. in the event of insider attack.
- In order to increase the benefits of global communication, States should adopt policies to enable efficient and secure network data flows.
- Stakeholders should take into consideration technological changes accompanying 5G networks roll out, e.g. use of edge computing and software defined network/network function virtualization, and its impact on overall security of communication channels.
- Customer – whether the government, operator, or manufacturer -- must be able to be informed about the origin and pedigree of components and software that affect the security level of the product or service, according to state of art and relevant commercial and technical practices, including transparency of maintenance, updates, and remediation of the products and services.

C. **Economy**

- A diverse and vibrant communications equipment market and supply chain are essential for security and economic resilience.
- Robust investment in research and development benefits the global economy and technological advancement and is a way to potentially increase diversity of technological solutions with positive effects on security of communication networks
- Communication networks and network services should be financed openly and transparently using standard best practices in procurement, investment, and contracting.
- State-sponsored incentives, subsidies, or financing of 5G communication networks and service providers should respect principles of fairness, be commercially reasonable, conducted openly and transparently, based on open market competitive principles, while taking into account trade obligations.
- Effective oversight on key financial and investment instruments influencing telecommunication network development is critical.
- Communication networks and network service providers should have transparent ownership, partnerships, and corporate governance structures.

D. **Security, Privacy, and Resilience**

- All stakeholders including industry should work together to promote security and resilience of national critical infrastructure networks, systems, and connected devices.
- Sharing experience and best practices, including assistance, as appropriate, with mitigation, investigation, response, and recovery from network attacks, compromises, or disruptions should be promoted.
- Security and risk assessments of vendors and network technologies should take into account rule of law, security environment, vendor malfeasance, and compliance with open, interoperable, secure standards, and industry best practices to promote a vibrant and robust cyber security supply of products and services to deal with the rising challenges.
- Risk management framework in a manner that respects data protection principles to ensure privacy of citizens using network equipment and services should be implemented.