The Prague Proposals

The Chairman Statement on Cyber Security of Emerging and Disruptive Technologies

Prague 5G Security Conference 2021

Prague, 1 December 2021

Emerging and Disruptive Technologies (EDTs) are new technologies or a fundamental change in deployment of current technologies that may have a transformative effect on the way society functions and whose unexpected, malicious, untrustworthy, or improper use has the potential to affect or disrupt national and individual security. This document is focused on the EDTs within the field of information and communication technologies.

PREAMBLE: THE NEED FOR STRATEGIC CONSIDERATIONS IN THE DEPLOYMENT AND MANAGEMENT OF EMERGING AND DISRUPTIVE TECHNOLOGIES

Fifth Generation (5G) wireless network infrastructure will form the backbone of the digital economy as it enables higher speed and lower latency connectivity. It also has the ability to further support the potential of Emerging and Disruptive Technologies (EDTs) such as Artificial Intelligence, Quantum Communication Infrastructure, Big Data Advanced Analytics, Massive Internet of Things and Autonomous Systems. These technologies are expected to significantly impact all sectors and in particular those critical to national security, such as healthcare, transport, and energy, including governments and their citizens. EDTs have significant potential to provide countless benefits to society as they are critical to the digital transformation of society, can save costs, and improve access to services. However, the increasing reliance of societies on these technologies could have serious national security and societal implications if EDTs and the data they rely on were to be disrupted or compromised. The ubiquitous and interconnected nature of digital systems across multiple sectors and states will also expand risks to the attack surface to possible disruption by cyber means, including the vulnerabilities of critical systems to disruption and hostile interference. This reinforces the importance of secure and resilient infrastructure, integrity of data development of technologies with regard to national and individual security.

Increased EDTs' deployment within society will largely depend on the underlying infrastructure, such as 5G networks. Evolving network and communication infrastructure continues to introduce new security and trust paradigms that will impact EDTs differently. For example, the speed and scale of 5G networks will be a critical enabler for autonomous vehicles and adaptive artificial intelligence. Securing 5G, next generation infrastructure and EDTs is therefore a question of national security and governments' strategic interests. The security of 5G and next generation infrastructure together with the associated security of EDTs should be addressed through a risk-based approach, taking into consideration both technical and non-technical risks[1]. Secure and resilient supply chains, as well as a diverse and competitive marketplace of trustworthy vendors for EDTs, are fundamental to the security and prosperity of our digital societies. Technological expansion and advancements should be considered in the context of a complex geopolitical landscape in which technology has become a means to advance divergent geopolitical goals through the imposition of new standards, regulations, and norms. The origin of technologies can affect its design, development, and diffusion. Data is one of the most valuable commodities of our time, used for civil, commercial, and military purposes by governments and the private sector across the world. Since some EDTs rely heavily on data, governments as well as other entities should implement appropriate measures and risk-based mechanisms to help to ensure confidentiality, integrity, the availability of data to reduce the risk of data corruption, to increase confidence in information and decision making, and appropriate privacy protections.

[1] As is introduced at the Prague Proposals 2019 or for EU countries also in the The EU Toolbox for 5G security.

THREAT LANDSCAPE OF EDTS

The development and deployment of EDTs has generally had a positive impact on society and has brought benefits to our citizens, businesses, and governments. The expansion of EDTs also inevitably brings inevitable and significant changes to the threat landscape by introducing new security challenges. Current threats will be continuously present and may pose more risks and cause more damage as states' and societies' dependence on information and communication systems deepens. EDTs will also possibly bring new vulnerabilities and expand the threat landscape. While certain threats presented by EDTs are already known at present, some are more difficult to predict. Security should be taken into account when developing and deploying EDTs (and their relevant standards) in order to address these threats and prevent potential vulnerabilities proactively in an adequate and timely manner.

This document focuses on EDTs whose deployment and mass distribution are closely interconnected with the rise of 5G and next generation telecommunication networks. The purpose of this document is to draw attention to the risk profiles and threat landscape of EDTs and provide guidance for governments in developing, building, deploying, managing, governing, regulating, or acquiring current and future EDTs. The threat landscape intends to be forward-looking and non-exhaustive. Other risks and threats may already exist or might appear in the future.

ARTIFICIAL INTELLIGENCE (AI)

Artificial Intelligence refers to the ability of machines to perform tasks that normally require human intelligence[2]. AI technologies are already being used, and we expect 5G and the future generations of networks to expand the scope and applications for AI in unprecedented ways. AI technologies have brought numerous benefits, efficiencies and cost saving improvements. AI technologies will increasingly become a basic building block of many other technologies and technological solutions, including quantum computing, smart cities, and autonomous systems. AI systems with a sufficient quantity and quality of data are able to generalize or make inferences based on new data similar but not exactly the same as the training data.

A key security risk associated with AI is data sabotage where either the quantity or the quality of dataset is adjusted to negatively affect the operation of a given algorithm. AI technologies often utilize algorithms, whose processes and outcomes are at times difficult to identify, trace and understand. Therefore, there are risks that sabotage attempts or other malicious system disruptions could go undetected. It is of paramount importance that AI technologies are developed with security in mind from the outset to ensure quality, trustworthy, impartial, and unbiased solutions. It is vital that AI is technologies are developed in line with shared democratic values, an awareness of unconscious bias, and respect for human rights in order to reduce the risk of both malicious use and unintended consequences. Ongoing research investment in trustworthy AI and in the synergies of AI and 5G will be important.

[2] NATO STO report Science & Technology Trends 2020-2040, p. 50.

QUANTUM COMMUNICATION INFRASTRUCTURE (QCI)

When Quantum computers of sufficient capability are buildable and sustainable, they have the potential to break public key encryption algorithms widely used today to protect data securely exchanged over communication networks. QCI plays a key role in countering and solving these challenges. It is based on newer developments in quantum mechanics and uses quantum key distribution technology, to enable the near instantaneous detection of communication. However, secure quantum communication is still an immature technology with significant potential vulnerabilities that need to be addressed, including the need to secure authentication of users. In order to protect users, the security of QCI must consistently be anchored as a central component in the development process of this technology in the sense of a security-by-design approach.

In addition, secure deployment of quantum communication technologies requires access to either fiber optic cables or laser-based communication arrays that utilize satellites. Development of quantum communication technologies would lay down the foundations for distributed QCI systems with many nodes and links, i.e., quantum networks.

BIG DATA ADVANCED ANALYTICS (BDAA)

Big data is the cornerstone of data-driven economies. BDAA are advanced analytical methods for understanding and visualizing large volumes of information. Governments depend on data flows and collect and analyze big data in order to make well informed strategic decisions, including in both economic and national security contexts. The purpose of BDAA is to gather, aggregate, process and analyze large amounts of data that will be used to (among other things) improve AI technologies and forecast trends in various critical sectors. A key risk associated with BDAA is its vulnerability to alternate data results that can be used for malicious training of AI technologies. BDAA is also susceptible to data confidentiality breaches which could potentially result in the disclosure of sensitive information to adversaries. If compromised, BDAA could generate false or malicious results which could have a detrimental impact on national security and the protection of sensitive personal data. The risk of BDAA being misused (e. g. for mass surveillance) also raises serious human rights concerns. Finally, it is important to note that big data analysis is also based on algorithms, thus sabotage may be difficult to detect. The integrity of information is fundamental to many aspects of computation and communication and underpins security and trust in a range of systems.

AUTONOMOUS SYSTEMS

The proliferation of information and communication technologies has led to the expansion of autonomous systems. Autonomous systems have the ability to respond to various situations by independently generating and selecting different courses of action in order to accomplish goals based on knowledge and contextual understanding[3]. More robust technologies will enable the development of greater levels of autonomy. These systems based on human design and algorithms require minimal human-machine interaction, and often there is no remote control in real time. The dependence of autonomous systems on 5G and next generation infrastructure can place users, especially in the military domain, at high-risk of cyber espionage and intellectual property theft. Similarly, in the civilian

[3] NATO STO report Science & Technology Trends 2020-2040, p. 59.

domain, it also presents specific risks, for example, through the global expansion of autonomous vehicles and construction of 5G corridors. They could pose both security and safety risks for citizens across the world.

MASSIVE INTERNET OF THINGS (IOT)

IoT devices can be connected to a network, and they are typically envisioned as large-scale distributed systems that support gathering, analyzing, and utilizing data in dynamic and intelligent ways. The availability and nature of IoT devices is expected to drastically increase their capabilities concurrently with 5G and next generation network deployment. Some consumer IoT devices have been known for low levels of security, and therefore could serve as an entry point to connected networks. With the use of IoT devices in critical sectors such as healthcare, industry, energy, or smart cities, the security risks range from espionage, privacy violations, and data alteration, to corruption of whole systems essential for public safety and national security.

EDTs and their threat landscape can intersect and overlap in various ways. Interconnected EDTs may impact the security of existing infrastructure, as well as 5G and next generation infrastructure. EDTs could even have a direct impact on the security of networks, including the 5G and next-generation networks (e. g. AI could be used to monitor or manage various systems, including telecommunication infrastructure).

THE EDTs PROPOSALS

The opportunities, risks and threats posed by EDTs require adaptation of existing policy responses and the creation of new tools, frameworks and approaches based on shared democratic values and respect for universal human rights. The Chair therefore suggests the following set of proposals which governments should consider when developing, building, deploying, managing, governing, or acquiring current and future EDTs:

RISK-BASED APPROACH

- Governments, as well as other relevant actors (based on their roles, the context, and their ability to act) should make systematic and diligent risk assessments on a continuous basis, evaluate both technical and non-technical risks associated with EDTs and take adequate risk mitigation measures.
- Address applications identified as high-risk by developing, adopting, and implementing long-term risk-mitigation mechanisms.

PRINCIPLES-BASED APPROACH

- Adaptive overarching security outcomes under various scenarios should be set. Moreover, flexibility should be promoted in order to achieve such outcomes.
- To avoid hindering innovation and investment, regulation should not be rigid within the technology sector as fast-paced changes and developments are not only common, but often desirable.

SUPPLY CHAIN SECURITY AND TRUST

- Responsible behavior of providers, vendors and supply chains is critical. Suppliers and providers should ensure the security of EDTs' supply chains including taking action to protect the integrity of algorithms, prevent the installation of backdoors, and extraction, and alteration or poisoning of data or outcomes.
- Governments should adopt mechanisms that evaluate the risk of dependencies associated with suppliers and supply chains. Governments should consider the extent to which suppliers may be subject to unlawful foreign influence, which may cause risk to national security. Measures that may raise the risk of foreign influence include: the extent to which suppliers can be compelled by law or practice to aid or abet activities of foreign governments known to have engaged in malicious activities, or the extent of extra judicial control or undue foreign influence suppliers are subject to, including through unfounded subsidization.
- Governments are encouraged to consider the extent to which suppliers are subject to, and covered by, rights and obligations consistent with the rule of law, human rights, and democratic values, as well as the robustness of intellectual property protections.
- Governments should promote the importance of how critical infrastructure sectors source their equipment, as degradation, destruction or the malfunctioning of systems may have detrimental effects on national security.

TRANSPARENCY

- Governments should advocate for transparency through assessment of ownership, partnership, and corporate governance structures of suppliers of critical components. Such an approach should also be encouraged across the whole supply chain.
- Transparency in EDTs' supply chains should be a key industry value and suppliers should be able to clearly communicate the security measures taken in the development of their products. Transparency in supply networks promotes awareness of risks, identifies bottlenecks, and then assists organizations in determining whether alternative sources of critical inputs are needed.
- Explainability and traceability should be promoted throughout the technology lifecycle, especially within the algorithms some EDTs rely on. Users should have confidence in the underpinning methodology of these EDTs and analysis of the system's outcomes and responses should be enabled.

SECURITY THROUGHOUT THE LIFECYCLE

- Governments should adopt best practices that promote on openness, interoperability, robustness, safety and security best practices so that, in conditions of normal use, foreseeable use or misuse, or other adverse conditions, they function appropriately and do not pose an unreasonable safety risk.
- Furthermore, governments should promote standards, transparency, respect for privacy, protection of personal data and responsible use of EDTs from the outset of their product design, through to their development, deployment, governance, and use.
- Governments should foster to protection of both systems and end users from potential threats and vulnerabilities, such as unauthorized access or interference. Considering security at all stages, beginning with design, will enhance a product's resilience to future risks.

- Governments should endorse security-by-design principle when making purchasing decisions, so that consumers and providers alike can have a reasonable level of trust in technology products.

DEMOCRATIC VALUES, HUMAN RIGHTS AND ETHICAL STANDARDS

- Governments should ensure respect for of human rights, democratic values, and freedoms in the context of the use of technology and in standard-setting bodies.
- Governments should support an open, interoperable, reliable, and secure internet by promoting a human-centric, ethical, and responsible approach to technologies. Additionally, governments should also prevent malicious abusive practices in the telecommunication and technology sector inconsistent with recognized human rights principles, including unauthorized surveillance.
- Technology supply chains are often globalized. Thorough due diligence assessments should be made in order to ensure suppliers have transparent corporate practices and abide by ethical corporate behavior.

PROMOTE R&D AND DIVERSIFICATION

- Limited competition reduces supply chain resilience. Governments should enable environments that facilitate vendor diversification and competitiveness, particularly through lower barriers to entry and market-based innovation. Such an approach should prevent dependence on a small number of suppliers, particularly those considered to be high risk, or a single country in the technology supply chain.
- Governments should support secure, open, interoperable, transparent, and innovative systems, platforms, and devices. A focus on developing multi-stakeholder, consensus-based, global, and interoperable and human-centric technical standards for these technologies via international standard development bodies should therefore be a priority.
- Governments should consider funding R&D for new technologies and solutions and should implement policies that support transparent financing which creates a level playing field.
- Governments should promote a policy environment that supports an agile transition from the research and development stage to the deployment and operation stage for trustworthy technologies.
- Likeminded governments should collaborate to commercialize R&D more effectively and to realize economies of scale.

CAPABILITIES DEVELOPMENT AT A STRATEGIC LEVEL

- Governments should develop and maintain appropriate capabilities (policy, legal, analytical, and technical) to be able to conduct strategic EDTs assessments.
- Governments should develop the ability to identify and forecast emerging technologies, including also by exploring the relationships, linkages and overlaps between different EDTs.
- Governments should perform risk assessments to understand the impact of EDTs on national security and resilience; to identify and understand how adversaries use EDTs; and to take appropriate steps to mitigate the associated risks.

- Governments should make expert informed judgements about EDTs through a whole-of-government strategic approach. Governments should prioritize the adoption of secure EDTs, including in the public sector, as they bring numerous benefits to society.

RESPONSIBLE TECHNOLOGY TRANSFERS

- While promoting technology flows in an interconnected and global ecosystem, Governments should take measures to prevent the misuse of technology by malicious actors, that may cause concerns. Such measures could include export controls (where applicable), and other effective means. These measures should apply, to knowledge transfer and cooperation, including those that occur through with a focus on global academic and industry cooperation.
- Governments should adopt national investment screening mechanisms to verify the ownership structure of investors in critical technologies to mitigate the risk of a hostile takeover of critical assets and technology that could have a detrimental impact on strategic interests and national security.

NEED FOR A COMMON APPROACH AND INTERNATIONAL COOPERATION

In order to promote the safe, secure, and trustworthy deployment of EDTs, governments should adopt a holistic and multi-stakeholder approach. Governments should cooperate and coordinate their efforts in a whole-of-government and whole-of-society approach. It is crucial that governments understand the importance of partnerships and strategic dialogues with the private sector, civil society, academia, and other stakeholders due to their crucial roles in the field. In the absence of public trust enabled by collaboration and transparency, EDTs are unlikely to be widely adopted.

International cooperation is fundamental. All like-minded governments are welcome to join the Chair of the Prague 5G Security Conference in implementing and promoting these proposals. Governments should continue to share expertise and capabilities of national experts on EDTs. It is crucial to exchange best practices on mitigation measures and collaborate on research and development. Governments should also work together to avoid strategic dependencies, and to bolster our collective resilience against the threats of authoritarianism.

The Chair invites all governments to publicly support these Prague Proposals on Cyber Security of Emerging and Disruptive Technologies.