Kaspersky's submission to the ITU open consultation of the CWG-Internet on International internet-related public policy issues on harnessing new and emerging telecommunications/ICTs for sustainable development

Kaspersky is grateful for the opportunity to provide comments and share its vision on the international internet-related public policy issues to ensure a safe, secure, trusted and resilient internet sphere for the prosperity of the global community. Below we provide our opinion to each of the four designated questions.

1. **How will new and emerging telecommunications/ICTs impact both the internet and sustainable development, including the digital economy?**
2. **What are the opportunities and challenges for the adoption and growth of the new and emerging telecommunications/ICTs and internet?**[1]

1.1. The internet and ICTs are transforming societies, businesses, national economies and governance policies. Emerging technologies such as the internet of things (IoT), cloud computing, innovative digital platforms and blockchain technologies are also becoming an indispensable part and condition for modern economies and businesses to prosper.

1.2. It is estimated[2] the global digital transformation could contribute more than US$100 trillion to society and industry by 2025, while the economic impact of the automation of our work, knowledge as well as robots and autonomous vehicles used in everyday life could reach between €6.5 trillion and €12 trillion annually by 2025, including gains in productivity and benefits in areas such as healthcare and security. Computing[3], artificial intelligence (AI) and robotics[4] are considered as an important factor enabling digital transformation with a strong impact on productivity, employment, the way business models work and how public services function.

1.3. At the same time, the internet and ICTs not only bring opportunities but create challenges as well. For instance, the development and use of AI has already raised the question of ethical norms and ethical standards, while the emergence of the IoT makes both policymakers and industry players think more about safety and liability to ensure legal clarity for consumers and producers in case of incidents and defects. Below we would like to summarize both opportunities and challenges in detail.

1.4. Integration of the internet and ICTs into national economies and societies brings clear advantages:

- Increased productivity and jobs. Both the digitalization of traditional industry sectors and growth of start-ups could bring innovation and employment benefits[5] by creating a new kind of qualified workforce, including highly skilled technical experts in AI, data analytics and cybersecurity, and creating new jobs.
- Enhanced efficiencies in public policy, society and industrial sectors. The wide use of ICTs is leading to the transformation of the public sector and its services, making it more accessible, efficient and transparent for society's needs. At the same time, digital transformation could help traditional industry sectors to explore new margins and produce new goods in a less resource-intensive and time-consuming way due to data science, data analytics and AI. Finally, the internet and emerging technologies

[1] Note: we combine two questions into one as they seem to us very similar.
[2] http://reports.weforum.org/digital-transformation/
[3] http://www.oecd.org/internet/oecd-digital-economy-outlook-2017-9789264276284-en.htm
[4] https://www.oecd-ilibrary.org/docserver/f1a650d9-en.pdf?expires=1541780412&id=id&accname=guest&checksum=7170CA99F193A6A34CDE5F9DF8DB7197
[5] https://www.oecd.org/innovation/transformative-technologies-and-jobs-of-the-future.pdf

such as blockchains could make citizens more engaged in democratic processes, e.g. through blockchain-enabled voting[6] assuring greater security, anonymity and transparency as well as through social media platforms which enable closer policy and societal multistakeholder discussions.

- Labor empowerment. ICTs and the internet could empower people in general and, in particular, women, ethnic minorities, people with disabilities, etc., by increasing opportunities for work and professional development due to the huge amounts of data and information used in the way we live, work, spend time with our families and friends, travel, communicate, etc. From this perspective, the digital transformation looks promising as it has the potential to make communities closer and more united.

1.5. The wide use of ICTs and emerging technologies in the digitalization of national economies, industries, public sector and society brings challenges which we have to address as well:

- Cyber-risks. Kaspersky has been in the global cybersecurity business for more than 22 years and saw many developments over that time. Without proper and robust cybersecurity, digital network infrastructure would remain highly vulnerable to cyber-risks, including industrial attacks, data breaches and supply chain risks. Cybersecurity also enhances a country’s preparedness to respond to the challenges of cyberspace – e.g. poor cybersecurity hampers growth and trust in ICTs as it leads to a lack of confidence in online systems and services, thus discouraging investment and usage. All of these risks require not only multi-layered cybersecurity solutions[7] but also a coherent approach to regulations – installing proper governance models, defining security measures for the industry, designating competent authorities (e.g. CERTs), and setting up incident reporting processes for threat information sharing.
- People’s confidence and trust in digital transformation. New innovative products raise concerns among policymakers and consumers about their safety for both business and individual use. Industrial supply chains are also becoming increasingly complex, meaning greater attention needs to be paid to the security of third-party vendor solutions. Recent data leakage scandals (e.g. Cambridge Analytica, the Marriott data breach, etc.), together with the growing complexity of the technologies used by both business and consumers, have given more prominence to questions regarding data protection, data management and the trustworthiness of vendors. The risk of declining trust in technologies, digital transformation and authority would spread fear, doubt and, as a result, increase the vulnerability of both the economy and society.
- Market fragmentation and trade barriers. Different players on the market have different capacities for merging ICTs and emerging technologies into their existing business operations – while big enterprise have more resources, SMEs are usually lagging behind[8] the process due to budget and staff constraints. However, there could be also sector-specific conditions leading to market fragmentation – e.g. firms in the most digital-intensive sectors enjoy a 55% higher mark-up than other firms, and cross-border acquisitions of digital-intensive firms grew 20 percentage points more than those in other sectors over 2007-15[9]. Reducing barriers to trade and investment, and addressing changing dynamics, can foster more market openness. At the same time, rapidly developing technologies proceed faster than policymaking and regulation, which leads to a fragmented market because of inconsistent requirements and factors and an unfair playing field.
- Digital divide. Studies show that not all people will benefit from the growth in use of the internet and ICTs, and there are two dimensions to this issue. First, diverse cultural, economic and infrastructure backgrounds[10] could accentuate the digital divide and, therefore, lead to tensions between communities (a good example is the EU Digital

[6] https://polys.me/
[7] https://www.kaspersky.com/enterprise-security/industrial
[8] https://www.telegraph.co.uk/business/ready-and-enabled/smaller-firms-lag-behind-on-innovation/
[9] https://www.oecd.org/newsroom/oecd-urges-more-action-on-bridging-digital-divides-boosting-skills-and-enhancing-access-to-data-at-going-digital-summit.htm
[10] https://www.pewresearch.org/fact-tank/2019/05/31/digital-gap-between-rural-and-nonrural-america-persists/

Economy and Society Index, DESI, which illustrates divisions even within the bloc[11]). Second, we can observe growing gender, political and cultural divides[12], which are becoming even more acute due to digital transformation.

- Investment in Research and Development. To survive in a world of rapidly advancing technology and enhance the competitive advantages on the global market, national economics need massive investments in data analytics, robotics, AI and cybersecurity. This is a crucial point in the further digitalization of various sectors, including telecoms, financial services, the transportation and automotive industry, retail and healthcare[13].
- Lack of digitally prepared and competent workforce. Various studies show that around 30% of jobs[14] are expected to undergo substantial changes in terms of the quantity and quality of their tasks, while 133 million new roles may emerge[15] that are more adapted to the new division of labor between humans, machines and algorithms. At the same time, the European Commission estimated[16] around 44% of the EU population and 37% of the labor force have insufficient levels of the required skills for digital transformation.
- Increasing uncertainty for business and people. There are several dimensions to this problem. Emerging technologies and a lack of understanding of how safe or indeed necessary they are (e.g. in terms of facial recognition[17]) create uncertainty among people and business. At the same time, a lack of aligned ICT regulations and market fragmentation create massive uncertainty for businesses, especially for SMEs.

1.6. We, at Kaspersky, strongly believe that digital development should work for and not against national economies to ensure the cybersecurity and safety of citizens. That's why we support the new reality that requires governments to act both as a stimulus for progress and as a guarantor of the security of this process. ***Such an approach requires thorough thinking and the development of coherent public policies through multistakeholder consultation with private companies, academia and civil society.***

3. How can governments and the other stakeholders harness the benefits of new and emerging telecommunications/ICTs?

1.1. We believe that coherent policy actions developed in close consultation with companies, industry and civil society, have a significant role to play in the beneficial use of new and emerging ICTs. In particular, this involves the following priorities:

- Promoting digital skills and entrepreneurship through the modernization of education and training systems. Human resources are the most important asset in national economies. Therefore, it is necessary to upgrade institutional learning and education to spread cognitive, technical and managerial skills that are becoming crucial for emerging sectors and services. As an example, at Kaspersky, we coordinate our education initiatives within Kaspersky.Academy[18] where we provide courses – from student cybersecurity courses around the globe to cybersecurity courses and certification for professionals and businesses. The key priority is empowering women in cybersecurity – for that, we conducted[19] a study together with Deloitte to learn more

[11] https://ec.europa.eu/digital-single-market/en/desi
[12] http://www.oecd.org/internet/oecd-digital-economy-outlook-2017-9789264276284-en.htm
[13] https://worldinvestmentreport.unctad.org/world-investment-report-2017/chapter-4-investment-and-the-digital-economy/
[14] https://www.oecd.org/about/secretary-general/launch-of-2019-skills-outlook-thriving-in-a-digital-world-paris-may-2019.htm
[15] http://www3.weforum.org/docs/WEF_Future_of_Jobs_2018.pdf
[16] https://ec.europa.eu/digital-single-market/en/digital-skills-jobs-coalition
[17] https://edps.europa.eu/press-publications/press-news/blog/facial-recognition-solution-search-problem_en
[18] https://academy.kaspersky.com/?from=RU
[19] https://www.kaspersky.com/blog/closing-gender-gap-cybersec/20053/

about the obstacles facing women in cybersecurity and launched courses for girls and women (e.g. the recent case[20] in collaboration with the Umniah Cyber Security Academy to empower Jordanian women in the 'cyber').

- Building a data-driven economy. Data is becoming the new economic high-value resource and here it is important to enable: (1) free movement of non-personal data across borders and sectors for business purposes; (2) data portability, i.e. easier switching of cloud service providers for professional users; and (3) availability of data for competent authorities to make sure the data remains accessible for regulatory and supervisory control. The free flow of non-personal data should also be based on two principles: (1) reusable and interoperable by default across sectors, industries and regions for automated processes; and (2) accessible by default – business-to-business and government-to-business datasets generated by the public sector should also be open to businesses and individuals to speed up the emergence of value-added information products as well as to serve as key data sources for the development of AI.

- Ensuring a level playing field and evidence-based competition. Access to a free, open and secure internet is a prerequisite for rules-based trade and development in the digital economy[21]. It is therefore important that countries adhere to the principles of reciprocity, fair competition, smart regulation and transparency in their digital trade. Besides, inclusive powerful digital ecosystems require: (1) market openness to technology leaders from around the world; (2) transparent and evidence-based competition rules and procurement policies; and (3) development of attractive and agile investment frameworks. It is also very important to ensure that SMEs and start-ups are engaged in digital transformation. A good example of empowering SMEs in cybersecurity is the non-commercial public-private partnership launched by the French government[22] to protect SMEs and French citizens against cyberattacks – companies, including Kaspersky, together with the French National Cybersecurity Agency (ANSSI) provide SMEs and citizens with both preventive and mitigation measures to minimize and mitigate cyber-risks accordingly.

- Overcoming fragmentation in the regulation of ICTs. A coherent policy to ensure the beneficial use of ICTs and emerging technologies requires multistakeholder consultations with industry and private companies to develop security requirements, certification requirements, standards and other regulatory measures which meet industry and consumer needs and avoid creating unnecessary burdens for technological development. Development of national policies and strategies would serve as a long-term roadmap with necessary policy actions and increase awareness among businesses and consumers of the priorities in digital development. A good example of such efforts is the European cybersecurity certification framework laid down by the EU Cybersecurity Act which Kaspersky actively supports through close consultations with both the European Commission and ENISA (the EU's cybersecurity agency). Together with a community of experts and other companies the framework aims to develop sector-specific voluntary security requirements and certification (cloud, IoT, 5G, ISC SCADA) to increase trust in cybersecurity products and services.

- Building a human-centric digital economy by enhancing user trust in ICTs. We believe that to build a human-centric digital economy, it is necessary to enhance trust and privacy through greater transparency of ICTs, including processes and algorithms, as well as transparency of government-led policies and priorities in this field. As an example, Kaspersky has been developing its **Global Transparency Initiative (GTI)**[23] for more than two years – a set of clear and practical measures that increase transparency and accountability in cybersecurity. We are pioneering new principles for

[20] https://academy.kaspersky.com/news/kaspersky-and-umniah-cyber-security-academy-to-empower-jordanian-women-in-cybersecurity/
[21] https://www.europarl.europa.eu/doceo/document/TA-8-2017-0488_EN.pdf
[22] https://www.cybermalveillance.gouv.fr/
[23] https://www.kaspersky.com/transparency-center

cybersecurity through: (1) openness of our data management processes; (2) two Transparency Centers already operating in Zurich and Madrid and two more planned in 2020 for source code reviews and security briefings about the company's products and operations; (3) third-party independent assessment of our engineering practices; and (4) Vulnerability Management through the Bug Bounty program with rewards of up to $100k for the most critical flaws in Kaspersky's systems.

- Increasing the cyber-resilience of digital network infrastructure. Critical infrastructure protection is the core of cybersecurity risk management – knowing threats and actively working to address them. A comprehensive regulatory and strategic approach should be the first step forward – we believe that governments need a critical infrastructure cybersecurity strategy and laws assuring: (1) clearly designated priorities among the critical services and infrastructures together with sector-specific CERTs and authorities, which together with the private sector would develop sector-specific guidelines and introduce minimum security baselines for critical infrastructure; (2) private-to-government and private-to-private threat information sharing about cybersecurity threats, vulnerabilities, and incidents; (3) transparent national coordinated vulnerability disclosure with open policies for government handling and disclosure of vulnerabilities; (4) government-industry supply chain security task force; (5) platforms for facilitating public-private partnerships in cybersecurity; and (6) multistakeholder consultations for developing a coordinated approach to AI, IoT, 5G and other emerging technologies. A good example of a balanced and structured approach to critical infrastructure protection is the EU NIS Directive which established transparent governance and reporting requirements.

- Transforming the public sector for more digital government services. We believe e-government projects would make public services not only cheaper and more accessible for society but would also ensure the availability and transparency of public services for better-informed and responsible citizens.

4. What are the best practices for promoting human skills, institutional capacity, innovation and investment for new and emerging telecommunications/ICTs?

1.1. We strongly believe that synergies between public and private sectors and talent acquisition are important factors for greater government capabilities in digital transformation. For that we would like to highlight two best practices:

- Large-scale national awareness campaigns. Governments can develop and launch nationwide campaigns to engage numerous actors of various sizes in developing a holistic understanding of how ICTs and emerging technologies should be integrated into everyday life for greater benefits. A successful example of such actions in cybersecurity is the European Cybersecurity Month[24], which in 2018 led to a total of 532 activities across 33 countries in Europe on a wide range of topics.

- Competence network for greater coordination between research centers, SMEs, companies. We recommend exploring opportunities for establishing a competence network for research and development programs that would give governments the opportunity to clearly define calls for the necessary technologies, tools and projects. Research centers, universities, SMEs, companies, industry, etc. would all have the opportunity, through a transparent selection process and eligibility criteria, to take part in collaborative projects to receive government funding. This is necessary to make market needs and national ICT programs better aligned.

[24] https://cybersecuritymonth.eu/

About Kaspersky
Kaspersky is a global cybersecurity company founded in 1997. Kaspersky's deep threat intelligence and security expertise is constantly transforming into innovative security solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. The company's comprehensive security portfolio includes leading endpoint protection and a number of specialized security solutions and services to fight sophisticated and evolving digital threats. Over 400 million users are protected by Kaspersky technologies and we help 270,000 corporate clients protect what matters most to them. Learn more at www.kaspersky.com.

Contact
For more information, or to discuss the contents of this submission in more detail, please contact Anastasiya Kazakova, Public Affairs Manager (+7 968 648 6005 | Anastasiya.Kazakova@kaspersky.com)