ITI Promoting Innovation Worldwide

2 March 2020

Policy Recommendations for a European Tech Agenda

Europe's opportunity to preserve an enabling environment for innovation and ensure its global competitiveness and security

The Information Technology Industry Council (ITI) is the premier advocate and thought leader for the global technology industry. ITI's membership comprises 70 of the leading technology and innovation companies from all corners of the information and communications technology (ICT) sector, including hardware, software, digital services, semiconductor, network equipment, cybersecurity, and Internet companies.

The technological innovations of ITI's members, and the digitalisation of the economy more broadly, bring innumerable benefits to European industry and society. The tech sector empowers European companies of all sizes and across industries – from agriculture to education, financial services to manufacturing, healthcare to energy and transportation – to leverage frontier innovations towards competition and success in the global marketplace. Whether it is sensors that detect health and safety hazards for workers in real time, or artificial intelligence that allows doctors to analyse complex medical data faster than ever, technology allows us to address some of the most challenging issues of our time and improve the quality of everyday life for Europeans. The tech sector is also already taking significant steps to help prepare the workforce of the future for the shifting skills and competencies that are required in the 21st century.

Tech policy is a crucial priority in the 2019-2024 EU term, one on which Europe has an opportunity to play an international leadership role on policy issues that are increasingly global. ITI and its members believe that building trust and fostering the public interest in the era of digital transformation are essential. Our companies have made great strides in bringing the positive societal benefits of transformative technologies to fruition and remain committed to upholding the fundamental principles of privacy, inclusivity, transparency, and democracy that underpin European society. We believe in the importance of preserving an enabling environment for innovation to ensure Europe's global competitiveness and security. Europe's digital infrastructure is the foundation for that. 5G is a core element to support digital transformations in industry and society, estimated to enable more than €2.2 trillion worth of economic output in Europe by 2030.

ITI has developed recommendations outlining concrete steps that policymakers can take, in partnership with industry, academia, civil society, and other stakeholders, to effectively implement the ambitious agenda for **"Shaping Europe's Digital Future"** launched by the European Commission in February 2020. Our recommendations address the economic and social implications of technology and the role of our industry, in a manner that supports innovation, while recognising the public interests at stake.

Read ITI's full EU Policy Recommendations here.

Global Headquarters
700 K Street NW, Suite 600
Washington, D.C. 20001, USA
+1 202-737-8888

Europe Office
Rue de la Loi 227
Brussels - 1040, Belgium
+32 (0)2-321-10-90

info@itic.org
www.itic.org
@iti_techtweets

Cyber and Supply Chain Security

Policy should reflect shared responsibility and the changing nature of cyberspace

ITI's members are global companies with complex supply chains, including both producers and users of cybersecurity products and services. Cybersecurity risks have intensified as the world's digital infrastructure has become increasingly interconnected and magnified by major technological shifts like cloud, IoT, AI, and 5G. We support the EU's continuous work with its international partners to strengthen cybersecurity.

Cybersecurity is integral to the EU's economy and competitiveness. While cyberspace holds great benefits for society, it also presents opportunities for misuse and exploitation. Cybersecurity concerns hinder innovation and growth, jeopardise trust, and threaten national security, economic growth, and individual rights. Increasingly sophisticated adversaries target European governments, organisations, and citizens, and attack the **global supply chains** of essential products in the EU's digital infrastructure. While both ICT companies and governments are focusing on managing supply chain risks and the security of networks, malicious behavior is an increasing and ever-evolving threat for both the public and private sectors. Industry is in the process of building security into products, services, *and* supply chains, along with providing security solutions, while governments play a key role in advancing cybersecurity best practices. The EU has acknowledged that cybersecurity is crucial to Europe and identified cybersecurity as one of its top priorities. As cybersecurity threats diversify, malicious cyber activities not only threaten the global economy (and the Single Market), but also Europe's democracies, freedoms, and values. The tech industry's interests in and shared goal of improving cybersecurity are fundamentally aligned with those of the EU.

Cybersecurity policy must reflect a shared responsibility and the changing nature of cyberspace. Security is a continuous process of risk management, technology development, and process improvement that must evolve with today's highly complex and dynamic environment. Cybersecurity is a shared responsibility – neither governments nor companies can address it alone. A range of policy tools and approaches is available to meet our shared security objectives, including risk management, threat information sharing, technological innovation, education, and raising awareness. These tools and approaches must be manageable and interoperable – too many silos can create a risk of overlooking or failing to connect the dots between incidents and events across networks. Static or overly prescriptive rules will not provide a lasting solution to cybersecurity concerns, since they quickly become outdated as business models and technology change and cyber adversaries evolve.

Data localisation measures weaken cybersecurity by creating a single point of failure in a given jurisdiction. Still, often due to misconceptions about improving security or access to data, some governments continue to pursue data localisation measures, creating attractive hacking targets and making data vulnerable to natural disasters and technical failures. The EU should discourage such policies.

Our Recommendations

1. **Promote international best practices in cybersecurity.** We recommend that Europe's future cybersecurity policies support and align with international industry-backed approaches to risk management, such as the ISO/IEC 27000 family of information security management systems standards. Other tools providing a common language to manage cybersecurity risks (such as the U.S. NIST Cybersecurity Framework) should also be considered in the upcoming NIS Directive review.

2. **Align EU cyber certification with international standards.** The EU Cybersecurity Act's certification framework should be implemented in a way that is adaptive and risk-based. Existing international standards should be the basis for developing certification schemes – including in the ongoing SOG-IS framework, the cloud security working group and potential schemes regarding IoT or 5G security. Continuous support for countries in developing capacity will also be crucial to enhance cyber hygiene and best practices.

3. **Develop a multi-stakeholder, public-private approach to cybersecurity.** As many countries launch multi-stakeholder initiatives to address cybersecurity vulnerabilities with different sectors, such as IT, finance and telecoms, we recommend the EU continue to seek active participation of the private sector, including in the form of consultation or comment, in order to direct its resources where cyber risk is most critical and imminent, as well as active partnership to facilitate mechanisms to deal with the complex nature of global cybersecurity challenges.

4. **Address supply chain security collaboratively**. Supply chain security will be critical as the EU moves to deploy 5G networks, and the EU should promote the adoption of baseline security requirements in the supply chain aligned with international best practices, encompassing risks in both product and service-oriented suppliers. A risk-based approach to supply chain security, which extends to network security and therefore 5G security, in which evidence-based risk assessments are conducted throughout the supply chain is another important fundamental. The EU should seek to develop incentives to encourage ICT vendors, including in 5G and consumer and industrial IoT, to adopt supply chain and cyber hygiene, including for example transparency in how organisations manage supply chain risks. Lastly, public-private partnerships can be an efficient way to help companies implement cyber hygiene and mitigate supply chain risks.

5. **Advance policies to recognise the growing complexity of emerging technologies.** To realise the tremendous promise and digital transformation of new technologies, we need equivalent security transformation and policy solutions. The EU clearly understands the cybersecurity risks resulting from emerging threats and should cultivate cooperation with the private sector and global partners, and also participate in the development of global, voluntary, and consensus-based standards and best practices.