AmCham Estonia
American Chamber of Commerce Estonia

DIGITAL RESILIENCE

AMCHAM ESTONIA DIGITAL SOCIETY COMMITTEE POSITION PAPER

Intro

Digital technologies have the potential to solve some of society's most difficult challenges, such as climate change and healthcare, and foster the birth, development and growth of new ventures that will create and finance the future of Estonia.

As a Digital Frontrunner, Estonia has a good chance to reap the benefits of digitization, however it requires that Estonia continues to drive an ambitious national agenda on digitization, innovation and entrepreneurship. But since Estonia is a small and export driven country, its success largely also depends on the EU's ability to develop a positive policy agenda that promotes open economy, free trade, digital innovation and transatlantic relations and that avoids protectionism and harmful regulation.

We urge Estonia to continue to use its role as a digital leader and soft power to push for a positive EU agenda following elections this year, including by working closely with partners and like-minded countries. This could be done via initiatives such as the declaration that Prime Minister Kallas signed and initiatives that seek to deepen the positive outlook in a more digital context for example led by Minister Riisalo.

Europe's Place as a Leader in Technology and Innovation

Europe is at a critical juncture. In the early 2000s, the GDP per capita of the US and the EU were on par. However, by 2023, the GDP per capita in the US had doubled that of the EU ($80k vs $40k). The EU has been progressively losing its global competitiveness and falling behind in innovation. Thirty years after its formal establishment, the EU's Single Market remains largely incomplete. A business in Tallinn still faces significant barriers to offering services in Amsterdam, Vilnius, or Athens. The EU is no longer a fertile ground for innovation, technology development, and the growth of world-class companies.

One of the main drivers of the EU's loss of global competitiveness is the slow adoption of technology and innovation. Europe lags behind in all major technological developments, whether it's cloud computing, Artificial Intelligence, or quantum computing.

First, a mindset shift is needed in Europe. Policymakers should view the tech sector as a key partner in achieving its goal of building an Open Strategic Autonomy, and leverage available technology assets (computing power, e-commerce platforms, open-source AI models) to build its own autonomy. This requires a change in perspective: from 'what new technologies need to be regulated in the next five years' to 'how can we stimulate/make sure that these new technologies come from Europe and European citizens benefit from it'.

The private sector, particularly tech companies, have made significant investments in data centres, leading to the development of cloud computing, cloud-based AI applications, and edge services, which are crucial for driving innovation in Europe. It's estimated that US firms alone have invested a substantial USD 597 billion towards ICT infrastructure and cloud solutions in Europe. The relationship between tech companies and the EU is

marked by mutual dependencies. Tech companies make long-term investments in the EU because it is a competitive market and offers political stability. In return, the investments of tech companies can support the EU's strategic autonomy agenda and help it regain its leadership in innovation and technology.

Secondly, a robust and complete Digital Single Market with truly harmonized regulation is crucial to addressing Europe's problems and reversing its loss of competitiveness. Companies looking to scale up in Europe often cite a lack of regulatory harmonization and regulatory inefficiency as significant barriers to growth.

In addition to reforms on regulatory enforcement across the EU and increased investments in R&D to support EU businesses to take risks and innovate, we believe it's necessary for Estonia to stress the importance of adopting a pro-innovation approach. An example could be embracing AI and adopting an open approach to AI, which would allow Europe to reap the benefits of AI applications.

Europe has all the necessary resources to reclaim its position as a global leader in technology and innovation. The EU is home to some of the world's best universities, top scientists and engineers, and the world's most innovative companies, including from Estonia. A mindset shift is necessary to leverage the EU's potential and turn it into a force to be reckoned with. It's crucial that Estonia advocates for a strong framework for innovative reforms, and that the next European Commission acts on it to ensure the EU doesn't fall behind in the race for innovation.

Artificial Intelligence (AI)

AI presents an immense economic opportunity, but we also recognise that the use of AI raises certain concerns. AI is not itself inherently good or bad; the key is developing and deploying it responsibly and ensuring regulation is risk-based and use case specific while allowing for continued innovation and practical application of this transformative technology. The EU approved the first law on how to regulate AI. We support the Commission's objective to ensure a proportionate, risk-based approach to AI regulation, and hope this can be a helpful start for a global discussion around AI governance. As we move to intense work on the code of practice with the AI industry, we urge Estonia to advocate for solutions that will benefit European AI providers and will increase the number of national champions in the AI space.

Payment Services Regulation

Valued at €240 trillion in Europe in 2021, electronic payments are essential to Europe's economy. As the legislative framework governing electronic payments, the Payment Services Regulation (PSR) must deliver logical and common-sense rules that make EU citizens' lives simpler. As part of achieving this, we call to advocate for removing Art. 59 from the text, as it unjustifiably makes industry accountable for fraudsters' impersonation scams. It also poses privacy challenges for users of both end-to-end encrypted messaging services and SMS, as it is also not technically possible to monitor and remove them for an E2EE messaging service.

A pure shift of liability to the Payment Service Providers (PSP) for impersonation scams is akin to putting a band aid over a gaping wound: it will not fix the underlying problem long-term. The focus must instead be on raising consumer awareness and detecting criminals through public-private collaboration.

The PSR can play a key role tackling frauds and scams and mitigate the harm suffered by consumers when engaging in fraudulent transactions. To make the law effective, policymakers should focus on understanding the role each actor plays along the value chain, from PSPs to platforms and other intermediaries, and identify the actions that each entity is best suited to take to to mitigate these harms.

Any liability extension to online including platforms or hosts, would run counter to the core principles established by the eCommerce Directive and reinforced in the Digital Services Act, namely that: (1) hosts are not liable for illegal content on their services absent actual knowledge , and (2) the prohibition against requiring hosting services, including platforms and private messaging services, to generally monitor their services for illegal content.

All measures should align with the recently adopted Digital Services Act, its intermediary liability principles which provide the relevant liability framework for hosting services, including platforms and messaging services, with regard to the takedown of illegal content in the EU which the PSR should fully complement and not replace.

Instead of undermining the well-balanced framework drafted by the European Commission with broad, far-reaching and unjustified liability extensions, policymakers should focus on fostering the cooperation between PSPs and other entities that can collaborate to prevent fraud. These measures should include knowledge and information sharing that can help financial institutions build adequate preemptive measures. Similarly, shifting the liability entirely to the PSP discourages consumers from being diligent themselves. Systems and campaigns should be put in place to help them to better recognise, avoid and report scams.

EU Cloud Security Services

The EU Cloud Services Certification for Cybersecurity ("EUCS") has the potential to drive a step-change in baseline European enterprise and public sector cybersecurity for cloud deployments, particularly in light of the increased risks posed to European security in 2022. The EUCS has raised concerns among industry, EU Member States but also EU trading partners (e.g. US, Japan, Australia, Canada), as in its earlier drafts it was discriminating against CSPs based on country of HQ, risking to cut off European businesses and governments from the most secure cloud services and cyber protections at a time when these institutions continue to be negatively impacted by malware, ransomware and DDOS attacks. We therefore appreciate that the Commission has taken the concerns of industry, Member States and trading partners (like Japan, US) on EUCS seriously and is seeking to move forward with the scheme in a way that does not discriminate against non-EU cloud providers. We encourage Member States to keep engaging in this process and to vote in favor of a solution that would maintain EUCS as a technical cybersecurity scheme open to all providers.

Stimulate Digital Transformation Through Cloud Adoption

We recommend that you stimulate digital transformation and growth by increasing cloud adoption by introducing a Cloud First policy, e.g. inspired by the UK, Iceland and the NL, and a strategy based on a flexible multi-cloud strategy and solid foundations for portability and interoperability.

Cloud first means that public organizations need to provide a clear explanation if they decide against the option.

We welcome the progress of the cloud bill in Estonia clarifying the requirements for the public sector to adopt cloud services. However, as the wording is not encouraging the adoption of cloud services it risks that the Public Sector in Estonia falls behind others in adopting and utilizing cloud services. This in turn will have a negative impact on the security of public services and on innovation in general.

International Tax Reform

The OECD is negotiating a global tax reform with the aim to reallocate taxing rights targeted at the world's largest companies (Pillar 1) and new standards around global minimum taxation (Pillar 2). We are supportive of the OECD process and we are hopeful that Estonia will continue to support a robust, multilateral framework that doesn't discriminate against products and services, and we hope that harmful targeted taxes such as Digital Services Taxes (DSTs) will no longer be considered at national or European levels. DSTs are problematic in that they narrowly target certain activities and companies and are designed to operate outside the principled framework of business taxation. They create concerns around tax and legal certainty and the legitimacy of an international tax system that has been built around multilateral coordination. This is the system that underpins all global trade and cross-border investment and the reason why it's important that Estonia supports the OECD framework.

Estonia's Cybersecurity Landscape: Capitalizing on Digital Legacy

In an age where digital technologies play an increasingly significant role in steering the progress of nations, Estonia stands as a beacon of innovation and dexterity in the cyber arena. With a proven track record as a digital frontrunner, Estonia embodies the epitome of a nation that has seamlessly blended tradition with technology, carving a niche for itself in the global digital landscape.

Heading deeper into the digital era, Estonia already understands that the decisions made today will shape its digital future. It is imperative that Estonia continues leveraging its stature as a digital powerhouse to further amplify its influence and contribute constructively to the EU's policy framework, fostering an environment that nurtures innovation, entrepreneurship, and responsible digitization.

Recommendations:

Legislation and Regulation

Advocate for balanced and foresighted regulations at the EU level that foster innovation without compromising security and privacy. Estonia should be at the helm, guiding discussions around harmonious legislation that accommodates the rapid advancements in the digital sphere without imposing undue restrictions. Similarly, on a national level, Estonia should aim to harmonize regulators in the digital sphere.

Cybersecurity Expertise and Innovation Hub

Establish Estonia as a hub for cybersecurity research and innovation, inviting collaborations with universities, industries, and governments globally. Innovation topics should focus beyond cyber securing and defending, it should include space sector, tackling digital divide, data privacy in the age of AI and sustainable digitalisation. This could pave the way for the development of state-of-the-art cybersecurity solutions, give a further boost to the start-up industry and putting Estonia at the forefront of cyber-technology advancements.

International Collaboration and Diplomacy

Utilize Estonia's standing as a digital leader to foster collaborations and alliances with like-minded nations, focusing on sharing knowledge, and facilitating dialogues on important issues such as data privacy, cybercrimes, and digital trade policies. Estonia should further enhance its leading positions by championing forums and summits that focus on crafting cohesive international cyber policies that promote free trade and digital innovation.

Empowering the next generation of cyber professionals

Become the leader in the development of educational programs and initiatives to nurture a workforce adept in cybersecurity and technological transformation. By fostering a culture of learning and expertise in this field, Estonia can contribute significantly more to the global demand for cyber professionals, enhancing its competitive edge in the international arena.

Developing a Resilient Cyber Infrastructure

Estonia should continue its trajectory of building a robust and resilient cyber infrastructure that not only protects its digital assets but also serves as a blueprint for other nations to emulate. Innovation hubs and simulation environment enabled collaborative initiatives with private sector enterprises could be a pivotal move in this direction, driving innovation and securing digital platforms.

Developing Cyber Crisis Management Centre

Developing an Estonian Cyber Crisis Coordination Management Centre could serve as a hub for collaborative crisis management efforts encompassing various sectors within Estonia and extending to cooperative platforms in the EU and globally. This centre should be mandated to conduct regular cyber crisis simulation drills, foster public awareness, and facilitate knowledge sharing and research development in the field of cyber resilience. Furthermore, the centre should actively collaborate with international partners, promote innovation, and nurture a proactive and resilient cyber ecosystem capable of foreseeing and mitigating future challenges effectively.