AmCham Estonia
American Chamber of Commerce Estonia

DIGITAL RESILIENCE

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. They 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. On that note, we strongly support the letter that Prime Minister Kaja Kallas and nine other Prime Ministers sent to Ursula Von der Leyen, highlighting key elements such as the need to focus on long-term competitiveness, "open strategic autonomy", new innovative technologies, better regulation, data flows, an ambitious trade policy and cooperation with key partners. 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 next year, including by working closely with partners and like-minded countries. This could be accomplished 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.

1. Geopolitical Crisis Calling For Policies That Are Secure by Design

It has been more than a year since Russia's unprovoked invasion of Ukraine and the war continues to be a tragedy. We stand firmly with the people of Ukraine as they face incredible suffering and we will continue to do so. Russia's actions are threatening the fundamental values upon which our societies are based and we are cognizant of the importance of this war, both for the people of Ukraine, for broader geopolitical dynamics and cybersecurity. Given the current crisis, it is clearer than ever that policies need to be secure by design and that we should further the cohesion of the Transatlantic alliance. Also, we support the idea to create a dedicated mechanism at the EU level to ensure that all technology policy initiatives and regulations are assessed for unintended effects on security and alliance cohesion as proposed by the Munich Security Conference last year.

2. Artificial Intelligence (AI)

AI presents an immense economic opportunity, but we also recognize 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 is currently discussing 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. However, we are concerned that some proposed amendments from the European Parliament and the Council dramatically expand the scope of the original proposal for the AI Act in ways that could raise the cost and limit the availability of low-risk AI in the EU, undermining innovation, and competitiveness in Europe, and limiting interop-

erability of markets while providing few benefits to consumers. We urge Estonia to advocate for a risk-based and use case specific approach and ask for a regulation that only focuses on applications that will potentially cause significant, irreversible harm. The proposed Annex III should remain as proposed by the Council and the AI Act should leave room for innovation in AI, I general-purpose AI technologies as they are used by many developers, startups and SMEs in Europe and represent an important opportunity for the EU to play a lead role in the AI ecosystem.

It is crucial that the AI Act maintains its risk-based and use specific approach and only introduces requirements for high-risk GP-AI systems and foundation models. In the AI Act, proposed targeted requirements for general purpose AI and foundation models (FM) would not only impose significant compliance burdens for companies but also would ban the development of most Foundation Models in Europe (as training on the internet would not be possible given requirements proposed). A total of 150 executives and dozens of Europe's largest companies (e.g., Siemens, Renault, and Airbus) underlined in July in an open letter that such limitations could lead to companies leaving the bloc, investors withdrawing from AI development in Europe and the creation of a "critical productivity gap" compared with other countries. We are equally concerned by echoes or recent discussions among EU institutions supporting an asymmetric approach to regulating foundation models and GPAI in the EU AI Act, and join the CCIA and Dot Europe in expressing our concern regarding this approach that will not ensure the necessary guardrails in ways that will facilitate European innovation and competitiveness.

Companies should be empowered to manage their own compliance processes, whether through contractual agreements between AI providers and users or through internal processes for companies that develop high-risk AI systems using 'in-house' GP-AI/foundation models.

Non-commercial and open source general purpose AI/foundation models should be exempt, so as to promote research and innovation, and encourage broader access to large scale AI models.

Simply banning certain data categories, or their categorization as such will make it harder to achieve fairness, prevent bias or detect harmful content and should hence be avoided. The AI Act is proposing to ban certain uses that do not represent risk. EU institutions should be cautious against generalization and sweeping approaches that risks impacting EU competitiveness and harming local innovation ecosystems. Risks to fundamental rights should be addressed horizontally and not limited to certain specific technologies.

In addition, the terminology of the Act (e.g., "provider" and "user") does not sufficiently distinguish between roles in the AI value chain (i.e., AI developers, deployers, end users, and other actors); and the Act's obligations do not consider these parties' different roles or provide clarity on which parties are responsible. Companies want to understand clearly how and when to comply with the requirements of the Act. Clarification is needed on which parties have responsibility for the obligations under the Act, and place the direct legal obligations on deployers of AI systems, who are best suited to know whether their use of a particular AI system will be high risk and fall under the Act's scope. As is common in manufacturing and in the GDPR, such deployers can then require that developers make contractual commitments to assist them with compliance. Lastly, we seek commitment from the EU that it will align the AI Act with international standards and definitions, e.g., as developed in the OECD, to ensure interoperability of AI services and regulatory regimes and respect for existing bilateral regulatory engagements. We equally urge EU institutions to clearly define and differentiate between foundation models and general purpose AI systems.

3. Product Liability Directive

The EU Commission's proposal for a revised Product Liability Directive (PLD) proposes extending strict product liability rules to software and related services. We support the underlying objective to ensure a high level of legal certainty for companies and trust for consumers, but we strongly caution against the inclusion of standalone software in the PLD because strict liability

deviates from the legal norm that liability should entail fault and is reserved for situations that bear a risk of severe damage to persons or property. Also, strict liability for standalone software will in most cases not be justified given software's fundamentally different nature and risk profile from physical goods. Software can be readily fixed through remote updates, and bugs are generally accepted as inherent to software development. Software developers often lack control over how their software is integrated along the supply chain, and standalone software cannot physically act upon any person or property. This greater legal exposure for software developers could have profound unintended consequences, such as: i) a chilling effect on innovation and digitization in Europe; ii) higher priced devices and software, to compensate the manufacturer/developer for higher potential costs; iii) worsened software performance and a trend toward basic functionality for users (in light of the security-performance trade-off for software development); iv) potentially holding developers liable for user harm caused by taking action to prevent exploits (for example, where taking such action results in lost user data); v) reduction in coverage of, or complete removal of, useful factual information made available by the software.

We also believe the extension of damages to material damages caused by psychological harm will lead to great legal uncertainty. As written, the provision does not propose sufficient conditions that must be met to link psychological harm with any single product. Unlike physical injury, psychological harm depends greatly on the consumer at hand and their given context. Requiring that the psychological harm be "medically attested" is an insufficient threshold. Ideally, several psychiatrists or physicians would need to be consulted and ideally, these professionals would be court-appointed for absolute objectivity. Including it as a damage in a no-fault liability regime introduces great legal uncertainty and a constant risk of litigation, as economic operators will find it impossible to predict where one consumer may experience psychological harm whereas many others will not.

Though the Commission's proposal does not reverse the burden of proof, the text presents a de facto reversal for scientifically or technically "complex" products (Article 9.4). This notion is undefined in the text (though Recital 34 provides several examples and names outright e.g. machine learning) and open to the discretion of national courts, making it unclear to economic operators whether their product will be determined complex. These Articles (as well as Recitals 3 and 34) put digital products and services, advanced software, AI systems on unequal footing vis–à-vis more traditional moveable`s.

The disclosure of evidence also presents a problem in that it is very broad and the provisions for confidentiality (Article 8.2-4) are too weak. It is imperative that confidentiality safeguards apply to all disclosures and not only information "used or referred to in the course of the legal proceedings" (Article 8.4). The PLD proposal also fails to detail the consequences in the event that there is a confidentiality breach. We also note defendants do not enjoy similar rights to request disclosure of documentation (such as proof of purchase, regular data back-ups, or heeding of company warnings about product use) to prepare their defense, as should be the case. This balance is important, especially given that a defendant's refusal to disclose evidence invokes a presumption of defectiveness (Article 9.2.a).

We are also concerned about the extension to cover 'related' services, the absence of precise definition of software, new disclosure mechanisms and that it introduces no-fault (strict) liability for online marketplaces which goes further than the Digital Services Act. We hope that Estonia can play a positive role in improving the proposal.

4. European Media Freedom Act

We support the Commission's objective to safeguard media pluralism and editorial independence but we are worried about Article 17 which suggests implementing a mechanism whereby the identification of media service providers (MSP) is based on self-declaration, without any third-party verification or safeguards. As the proposal is written, almost anyone can claim that they are an MSP without any checks and

balances. Given how the criteria are set out in the Regulation, 'Russia Today' could have qualified as a media service provider deserving of these additional protections if the law had been in place just a few years ago. It's hard to believe that 'Russia Today' wouldn't have been protected and that it would have made it difficult for platforms to take quick action when Russia started to invade Ukraine and escalated its disinformation activities.

We have also seen rogue actors impersonate media services in the past to post harmful content. As it stands, the proposal from the Commission does not include safeguards to prevent this type of abuse. In addition, by expecting VLOPs to decide whether to accept a self-declaration, Article 17 and Recital 33 are placing the responsibility of determining who qualifies as a media service provider on VLOPs – yet VLOPs are not equipped to apply the criteria currently outlined in Article 17 across 27 different Member States. We are worried that it will become much harder for platforms to fight against e.g. harmful disinformation if bad actors will be granted a special privilege so that platforms cannot stop their harmful content from spreading. As the war in Ukraine has shown, it is important that platforms are ready and agile to respond to new and emerging threats. The EMFA must not be a step back in the fight against misinformation/disinformation and it must be compatible with and acknowledge the frameworks already in place in existing EU laws, notably the Digital Services Act, the EU Code of Practice on Disinformation, Audiovisual Media Services Directive, the Digital Markets Act - all which have been recently adopted or implemented. It's important to remember that actions taken by platforms under their community guidelines or terms of services are not left unchecked. The Digital Services Act requires providers of online platforms to provide internal complaint-handling systems (Article 20) and out-of-court dispute settlement (Article 20) for those who disagree with them (including MSPs). So there are already sufficient safeguards for MSPs when VLOPs moderate their content. We urge Estonia to push for improvements that ensure full harmonization with the DSA. Ultimately, legislators need to improve the text by:

- Narrowing the definition of media service providers in Article 2.
- Introducing safeguards for the vetting of media service providers and simplifying the vetting process by making national regulatory authorities responsible for reviewing and approving the eligible media service providers. The information should be added to a media ownership database and shared with the European Board for Media Services, who should then be required to share this information with the VLOPs. The Board shall have the opportunity to appeal a certification. The media service provider shall have the opportunity to appeal to the Board, if certification by the competent authority was not granted.
- Rejecting temporary must-carry obligations and rigid turnaround times for complaints. It's dangerous to require that VLOPs should carry content provided by media service for a certain period of time. It would effectively restrict a platform's ability to take immediate and effective action to remove harmful content.
- If however the EU decide that VLOPs must not remove media content from their platform because of the media privilege, VLOPs must at least be able to restrict the content in some way, for example by deploying default security protections, such as a warning interstitial or an age gate. The scope of Article 17 should thus only cover the removal of media services to protect users from harmful or inappropriate content effectively and without delay, in particular children and minors.

5. 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. However, the inclusion within the scheme of provisions related to data and operational sovereignty would

fundamentally depart from established international cybersecurity standards and present a serious barrier to widespread adoption. Security operational best practice and resilience will suffer as cloud customers will lose their ability to implement global security mitigations, benefit from threat telemetry data gathered from other regions and move data from compromised regions to secure storage centers as attacks unfold.

It best serves European cybersecurity interests to progress with a narrowly focused, technical scheme (ie. removal of the sovereignty controls) rapidly. Political dialogue about digital sovereignty should be separated from the EUCS debate and ultimately resolved in a way that allows national states to determine whether specific controls are necessary - and whether the trade-offs those controls may pose for security and cloud-led innovation are acceptable to meet their national digital sovereignty needs.

6. 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.

7. 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.

8. 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:

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 digitalization. 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 center

Developing an Estonian Cyber Crisis Coordination Management Center 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 center 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 center should actively collaborate with international partners, promote innovation, and nurture a proactive and resilient cyber ecosystem capable of foreseeing and mitigating future challenges effectively.

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.

AMCHAM DIGITAL SOCIETY COMMITTEE (DSC)

Purpose of the Committee:

DSC is investigating how digitalization has an effect on individual preferences, social values, corporate goals and public policy-making. Our aim is to raise awareness among companies and Estonian public in general by introducing best practices in managing and benefitting from technological innovation. We do so by arranging thematic workshops and speaker events with local and foreign professionals.

DSC focuses on the following topics:

- R&D and Intellectual Property
- Digital Single Market
- 5G
- Data protection and international transfers
- AI
- E-Commerce
- Cyber Security and Online Safety