CONSULTATION RESPONSE

AmCham EU’s response to the public consultation on public-private partnership on cybersecurity

*   *   *

AmCham EU speaks for American companies committed to Europe on trade, investment and competitiveness issues. It aims to ensure a growth-orientated business and investment climate in Europe. AmCham EU facilitates the resolution of transatlantic issues that impact business and plays a role in creating better understanding of EU and US positions on business matters. Aggregate US investment in Europe totalled more than €2 trillion in 2015, directly supports more than 4.3 million jobs in Europe, and generates billions of euros annually in income, trade and research and development.

*   *   *

American Chamber of Commerce to the European Union (AmCham EU)
Avenue des Arts/Kunstlaan 53, 1000 Brussels, Belgium
Register ID: 5265780509-97
Tel: +32 (0)2 513 68 92 | www.amchameu.eu

Secretariat Point of Contact: Roger Coelho, roger.coelho@amchameu.eu +32 (0)2 289 10 18

11 March 2016

Introduction

AmCham EU represents a broad array of private organisations who research and develop, supply as well as use cybersecurity solutions, in the IT sector as well as in all other industry sectors subject to digitisation. We therefore welcome the Commission's consultation on cybersecurity challenges in the Digital Single Market.

The importance of cybersecurity for the digital economy, current and future challenges

In AmCham EU members' experience, defending against cybersecurity threats has – or in any case ought to – become integral to business risk management in a number of areas, ranging from the protection of intellectual property against cyberespionage, to the protection of personal data and other sensitive or confidential information from theft, through the prevention of financial or identity fraud, extortion and other cybercriminal threats, all the way to defence against industrial sabotage. These threats are relevant in every sector that relies on connected technologies and they will become even more so as the Internet of Things, Smart Infrastructures, eHealth/mHealth, Smart Mobility, Industry 4.0, M2M communications, the app economy and other mobile, web-enabled and/or cloud-powered developments unfold. In the long run, by 2020 and beyond, all these challenges will converge to make cybersecurity a critical component of the resilience of Europe's digital economy, the integrity of all digital transactions in Europe, and ultimately the functioning and the competitiveness of the European Digital Single Market in the global economy.

Cybersecurity maturity in Europe

Whereas high performing, innovative and highly competitive technologies are generally available on the European market to help defend against cyberthreats, cybersecurity will always remain a combination of people, process and technology. Public and private organisations' level of preparedness can vary very greatly from total lack of awareness to advanced maturity: adequate education, training and professional qualification of people are still missing in many cases; suitable processes and organisational measures may not always be in place, well designed or properly enforced; and relevant technologies are not necessarily used by those who need it, or they may be used inadequately. This can be explained by a number of factors, most of which pertain to insufficient awareness and sub-optimal resource allocation to cybersecurity in many organisations.

Regulatory barriers hindering effective cybersecurity

However there are also regulatory and technical market barriers even within the EU Digital Single Market which make it difficult or unreasonably costly for organisations in certain local markets or business verticals to access state of the art cybersecurity products and services. In particular regulatory measures for forced localisation, local technological mandates as well as product or service certification requirements occasionally mean that operators subject to such restrictions don't have access to the best available technologies, and have to rely on lesser local alternatives if any. While bearing in mind every Member State's legitimate sensitivities in all matters of security, AmCham EU believes that the European Digital Single Market vision is a unique opportunity to address this issue, and the European Commission should focus specifically on removing as many of the unjustified market access barriers as possible, the case being through public intervention and even regulatory means.

Protectionism as a threat to effective cybersecurity

As a rule of thumb, what matters in cybersecurity is the outcome that is achieved, not the specific means of achieving it, and even less the geographical origin of the solutions used. Therefore AmCham EU firmly warns against any approach that would define cybersecurity policy, standardisation, procurement or research and development objectives in any terms other than effective protection against threats, which at any rate are and will remain global in their origins as well as in their potential impacts. In particular AmCham EU is very concerned by the regional mindset that transpires from questions 2.2 and 2.3 in section II of the consultation, which specifically ask organisations about “the reasons behind [their] decision to choose non-European ICT security products/services over European ones”. It cannot be stressed enough: an ICT security product or service being European or otherwise has no inherent bearing on its effective performance nor is it clear what a ‘European’ solution is – whether it refers to the location of the development capabilities, R&D, supply chain or merely the global HQ. Moreover, the vast majority of enterprises or other organisations operate in a multi-vendor environment, including for their network and information system security, so it is not as simple as choosing one vendor over another, regardless of their country of origin. As such, these questions are not directly relevant to the assessment of the overall level of cybersecurity in the European Digital Single Market.

Desirable objectives and outcomes of an industrial strategy for cybersecurity in Europe

Whether there are European technologies among the best available cybersecurity solutions in the market is a totally different question, the answer to which is not related to cybersecurity, but to the business environment (e.g. ease of doing business, access to financing, resources for innovation, research-to-market cycles) and to the policy frameworks (e.g. regulatory environment, compliance requirements, market access restrictions, export controls) governing the development and the marketability of such technologies in and from Europe. Encouraging the strengthening of the EU’s cybersecurity industrial base is a legitimate business and policy objective for the EU and its Member States to pursue. Many AmCham EU members are actively engaged in efforts in that direction, whether through their direct investments and local presence or through their European partnerships.

Having said that, the purpose of strengthening this industrial base should be to achieve superior cybersecurity outcomes by attracting and leveraging any resource, even non-European, that can contribute to this objective. Doing so simply for the purpose of displacing non-European technologies from the European Digital Single Market, even taking the risk of substituting them with inferior alternatives, should be an absolute no-go. It could gravely harm Europe’s overall protection level from cyberthreats, it would very likely make European bred technologies highly ineffective and uncompetitive globally, and as a result such an industry policy would not be sustainable and would be bound to fail.

Should digital sovereignty, whatever that may mean, become a proclaimed political objective, Europe will be much better served by attracting the best cybersecurity solutions available globally. By pursuing effective international partnership and cooperation strategies to defend the European cyberspace from threats and attacks instead of isolating itself from the global market and being left alone with home-grown vulnerabilities, incompatible bespoke technologies and unscalable local solutions, resulting in weaker defences, higher threat exposure and ultimately less sovereignty and relevance in cyberspace.