AmCham EU
SPEAKING FOR AMERICAN BUSINESS IN EUROPE

Feedback response

EU Cybersecurity Package

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 2016, directly supports more than 4.5 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
Speaking for American business in Europe

Avenue des Arts/Kunstlaan 53, 1000 Brussels, Belgium • **T** +32 2 513 68 92
info@amchameu.eu • amchameu.eu • European Transparency Register: 5265780509-97

EU Cyber Strategy

We acknowledge the EU's legitimate ambition to strengthen its cyber industrial base with a focus on emerging technologies.

Cybersecurity has no borders. The threats facing Europe are global in nature, maintaining and improving international cooperation with public and private partners is and will remain essential to keep Europe safe, secure and resilient. This is equally true for financing research, development and innovation as well as for attracting foreign direct investment and for promoting international trade in cyber technologies.

We are particularly pleased to see the EU standing up against cybersecurity being used as an excuse to raise trade barriers. We very much count on the EU and its Member States to lead by example in this respect. We look forward to being actively involved in the public-private dialogue on defining a 'duty of care' in cybersecurity. In particular, a dialogue on the conditions under which self-certification will be acceptable is needed. Cybersecurity is not static, it will develop over time as technologies evolve and new threats occur. This will be a defining element of the concept of 'duty of care'. We believe that all players in the ecosystem have a shared responsibility, including not only technology vendors and service providers, but also users themselves.

We fully agree on the importance of developing cyber awareness and skills and are prepared to do industry's fair share in that regard, provided that public actors can also second the necessary support and resources for initiatives such as awareness raising campaigns on cyber security best practices. The insurance industry for example is well placed to drive behavioural change in the market place. More consideration should be given to the important role of cyber insurance in expanding the adoption of best practices.

Implementation of the NIS Directive:

We agree with the Commission that the transposition and implementation should be as harmonised as possible. In particular for Digital Service Providers, we welcome the Commission's effort to define a common baseline across the single market by way of the implementing measure they proposed. At the same time care must be taken not to undermine the light touch approach agreed by the legislators. Too detailed one-size-fits-all rules and thresholds as proposed may not be suitable for every situation.

EU Cybersecurity Act: ENISA

Converting ENISA to the permanent EU Cybersecurity Agency is a sensible move. It will be very important for ENISA to keep and enhance its ability to cooperate with the industry as well as with international partners and international standards certification bodies such as the US NIST and ISO. In addition, AmCham EU looks forward to strengthening the good relations developed with the Agency.

EU cybersecurity Act: ICT certification

We believe that going for a voluntary approach is the right thing to do. We hope that this approach will be preserved, and certifications will not be made mandatory (directly or indirectly) in a later stage. We appreciate the Commission's effort to better integrate the Digital Single Market by

proposing the recognition of EU certificates in all member states, or assuring mutual recognition of national schemes. We urge Member States to not undercut this approach.

We would like to see more private sector involvement in the design of the certification framework and of the particular schemes to be developed under it. Indeed, keeping as close to the market is essential for the voluntary framework to be successful.

EU Coordinated Cyber Crisis Response Mechanisms

We strongly support EU efforts in this area because there is truly a real need for more effective cross-border cooperation against cyber crises.

We understand that such cooperation mechanisms are intergovernmental in nature, yet we do urge the Member States to make room for private sector involvement. On the one hand, a lot of the information to be shared in the context of crisis response will originate from the private sector, who already has valuable experience in collecting, classifying and sharing relevant cyber threat intelligence, and thus helping to enable a collaborative security ecosystem. On the other hand, many response actions will have to be carried out by private sector entities, especially where cyber crises impact commercial infrastructures and services.

Cyber Defence and Cyber Diplomacy

We support the EU's efforts to drive the international promotion of confidence building measures and the development of norms of acceptable state behaviour in cyberspace. On top of this, we urge the Commission, the EEAS and the Member States to work closely with international partners and allies on these issues, especially the U.S.

We also support the EU's commitment to value-based cyber capacity building in third countries and suggest using existing platforms like the UN-ITU and the GFCE to best combine and leverage the resources made available by the EU on the one hand, and other contributors such as private industry on the other.