AmCham EU

SPEAKING FOR AMERICAN BUSINESS IN EUROPE

Our position

The EU’s Cybersecurity Strategy: recommendations towards a revision

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.

Executive summary

The EU has made a lot of progress under the 2013 EU Cybersecurity Strategy. It has created a comprehensive regulatory and institutional environment to increase cyber resilience across the Union. Moving forward, better tackling cybercrime, further improving cyber security including in emerging domains like the Internet of Things (IoT), and cooperating more closely with international partners will remain important priorities. In all three respects, AmCham EU urges the EU to:

- Focus on the harmonious implementation of the already existing regulatory instruments to improve the coherence of cybersecurity policies across the Digital Single Market;
- Continue to build upon the positive experiences of public-private partnerships. Collaboration and information-sharing with the business community will be essential to build effective cyber resilience in pragmatic risk-based approaches;
- Engage proactively with international partners, especially the US, to advance cyber policy matters such as cyber norms, cyber defence as well as law enforcement cooperation in cyberspace at the intergovernmental level, to ensure that trust in the foundations of our connected world is not undermined.

Introduction

AmCham EU welcomes the European Commission’s ambition to evaluate and revise the European Union’s (EU) first Cybersecurity Strategy[1] published in 2013. This paper outlines a number of recommendations related to the focus areas of the upcoming review as identified by Andrus Ansip, European Commission Vice-President for Digital Single Market[2]. Moving forward, better tackling cybercrime, further improving cyber security including in emerging domains like the Internet of Things, and cooperating more closely with international partners will remain important priorities.

1. Directly tackling cybercrime

The EU has already laid down robust foundations for the fight against cybercrime by adopting the Directive on attacks against information systems[3] in order to harmonise Member States’ substantive cybercrime law along the lines of the Budapest Convention, and by creating the European Cybercrime Centre (EC3)[4] at EUROPOL to advance the cooperation between national law enforcement agencies.

AmCham EU is aware that in responding to the expectations voiced by the Council[5], the Commission is exploring[6] practical solutions to help law enforcement gain lawful access to electronic evidence. AmCham EU members, several of whom are involved in ongoing expert consultations on this topic, are of the view that:

- To the extent feasible, voluntary information sharing and cooperation mechanisms between law enforcement agencies and businesses, that are respectful of applicable laws and consistent with jurisdictional boundaries, should be preferred and encouraged. Good information sharing can detect patterns and trends to enable organisations to better guard against cyber attacks. However, this is subject to government and regulator assurances to industry concerning the subsequent use of such sensitive and confidential information, given potential risks to reputation, market confidence and liability. Several successful botnet takedown operations conducted jointly by EC3 constituents, third-country authorities and relevant market operators in recent years have provided conclusive evidence that such approaches are workable and effective, benefiting both private and public sectors.
- Where information needs to be obtained across jurisdictional boundaries, whether within the European Single Market or in relation to third countries, the compulsion of firms to grant direct extraterritorial law enforcement access to privately held information is not an acceptable proposition and should not be contemplated. For private sector firms handling personal and/or sensitive personal data, it is vital to be able to protect the privacy of their customers of which they need to guarantee the trust. This requires, in any way, business operators to palliate the lack or ineffectiveness of proper cross-border mutual legal assistance treaties, arrangements and procedures. Compelling them to share data, not only risks being an ineffective way to access data, it risks damaging customers’ trust in their service providers and also risks damaging business’ reputation and client relationships.
- Various Member States maintain different substantial and procedural rules to govern their law enforcement agencies’ access to information held by businesses. Furthermore, Member States sometimes follow diverging principles to exercise their jurisdictional competence in cyberspace. These are fragmenting factors

[1] Commission Communication JOIN(2013) 1 final

[2] Speech by Vice-President Ansip at the Munich Cybersecurity Conference on 16 February 2017

[3] Directive 2013/40/EU

[4] Commission Communication COM(2012) 140 final

[5] Council Conclusions of 9 June 2016 on improving criminal justice in cyberspace and on the European Judicial Cybercrime Network

[6] Commission Non-Paper of 7 December 2016: Progress Report following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace

in the Digital Single Market and potentially limit the effectiveness of the cross-border action taken against cybercrime. The startegy of the EU should be to seek and advance the approximation of those national rules and principles to the fullest possible extent, similarly to how the 2016 Law Enforcement Data Protection Directive[7] approximates Member States' privacy legislations imposed on their law enforcement agencies.

- The due process safeguards regarding law enforcement access to data are vitally important. On top of market fragmentation, Industry has two main concerns regarding legal uncertainty: (1) the lack of clarity on the due process safeguards that national legislations may or may not offer, and (2) the lack of coherence or consistency between the rules of different Member States. Moreover, without a clear and single European benchmark for both law enforcement and business communities on minimum due process safeguards under the rule of law[8], considerable compliance and reputational risks develop that may erode public trust in businesses. This may also weaken the EU's credibility and posture when negotiating similar safeguards with third countries. Therefore the EU's Strategy should aim to affirm and flesh out that common baseline, and to drive the convergence of Member States' legislations towards it.

2. Guaranteeing network security, including improving the security of the Internet of Things

Since the publication of the European Cybersecurity Strategy, several significant steps have been taken to improve network (and information) security in the Digital Single Market. Through the adoption of the eIDAS Regulation[9], the second Payment Services Directive (PSD2)[10], the NIS Directive[11] and the GDPR[12] (in particular its provisions on the security of processing and the notification of personal data breaches), a comprehensive set of requirements has been introduced for network and information system operators. These requirements offer frameworks for operators to assess and manage cyber risk, to detect, remedy and report incidents, and to check and demonstrate compliance though measures like audits, subject to supervision and dissuasive sanctions in case of non-compliance. Moreover, the network and information security rules of the Telecom Framework Directive and the confidentiality requirements of the ePrivcacy Directive are currently discussed as part of the negotiations on the new European Electronic Communications Code and in the draft ePrivacy Regulation.

With the exception of certain provisions of the eIDAS Regulation in force since 1 July 2016, all of the above have yet to be agreed, transposed, implemented or enter into force. The priority for now should be to let this already very comprehensive regulatory framework settle in and start demonstrating its value and effectiveness, as it is designed to govern the cybersecurity of digital information, infrastructure, identities and interactions. Considering any further regulatory initiatives in this area would be premature and could further constrain Digital Single Market operators' already stretched ability to absorb new compliance costs. Only once the current legislative efforts play ou, it will be possible to assess whether there are any gaps or market failures that warrant further regulatory intervention.

In the meantime, improving network and information security in the Digital Single Market on the basis of existing and upcoming instruments will be first and foremost a matter of:

[7] Directive (EU) 2016/680

[8] The European Court of Justice refers to 'the limits of what is strictly necessary and [can therefore] be considered to be justified within a democratic society'

[9] Regulation (EU) N°910/2014

[10] Directive (EU) 2015/2366

[11] Directive (EU) 2016/1148

[12] Regulation (EU) 2016/679

- Significantly improving Member States' cooperation, notably through the mechanisms created by the NIS Directive;
- Advancing market integration and maximising coherence and consistency wherever possible through the delegated acts and implementing measures of legislation already in place or in the making;
- Leveraging market dynamics to advance policy objectives such as resilience, transparency and interoperability by supporting the development of internationally recognised and globally scalable market-driven standards where necessary. In order to truly develop effective cyber resilience, industry needs global leadership from regulators and policymakers in partnership with the business community;
- Instead of legislation, promoting, encouraging and harnessing business innovation through new tools such as cyber-insurance and self-certification regimes, would be a constructive way to improve the adoption of cybersecurity best practices by stakeholders of all sizes and of all cyber maturity levels across the Digital Single Market. Approaching cybersecurity in a risk-based manner is key to ensure effective resilience throughout the supply chain;
- Renewing the mandate[13] of ENISA beyond 2020 (and perhaps permanently), strengthening its powers and increasing its resources so it can contribute even more substantially to raising cybersecurity awareness, is important[14]. As a pan-European body, ENISA has great potential to: collect cyber expertise; disseminate best practices; conduct European cyber exercises; collaborate with public and private stakeholders across the EU and beyond; inform cybersecurity related policy decisions; help cyber capacity building and training; clarify scope of the application where needed and ensure consistency across Member States support the emergence of better harmonised and coherent cybersecurity guidelines and requirements in the EU; and contribute to the integration and completion of the Digital Single Market from the cybersecurity standpoint; and
- Building trust through the pursuit and encouragement of open, inclusive and transparent public-private partnerships for information exchange, best practice sharing, collective policy shaping, collective cybersecurity, and related research, development and innovation. Important initiatives are for instance the contractual public-private partnership on cyber (Cyber cPPP), the Network and Information Security Platform (NISP), the European Multi Stakeholder Platform on ICT Standardisation (MSP), the existing Cloud Select Industry Groups (C-SIGs) and the Alliance for IoT Innovation (AIOTI). Two-way information flows are vital as relationship-building is key to developing and maintaining trust and common understanding. Even with improved *ex ante* resilience, no network is impenetrable, and these relationships are key to effective anticipation and response to cyber incidents.

Specifically with regard to IoT, current and future users have legitimate needs for privacy, security, resilience, transparency and interoperability. At the same time, the IoT is still an emerging technological area in the earliest days of its development and growth. The EU must ensure it enables an environment that allows safe, responsible innovation, and does not unintentionally limit innovation, hinder market access or undermine the competitiveness of the EU market in comparison to the rest of the world.

Full use should be made of already existing instruments to address any concrete and proven issues or market failures that may arise in the IoT space. These nascent technologies, whose future attributes, properties, performance and possible uses cannot even be anticipated yet, should not be subjected to rigid, prescriptive and unnecessary regulation. In particular, AmCham EU members remain concerned that pushing for generic or blanket cybersecurity labelling of IoT products could result in counter-productive technology mandates, new market access barriers or roadblocks to innovation without necessarily bringing any real cybersecurity or privacy benefits which could not be otherwise achieved on the basis of already existing instruments.

[13] Regulation (EU) N°526/2013

[14] AmCham EU's reply to the public consultation on ENISA, here.

The GDPR creates a robust framework for the development of market-driven, verifiable and enforceable codes of conduct and certification schemes with respect to the protection, privacy and security of personal data collected, processed and transferred by, in, from or to IoT devices and infrastructures. Likewise the eIDAS Regulation also creates the appropriate legal basis and contains the necessary security requirements to govern the digital trust services that may be used for the secure authentication of users, devices and applications in IoT environments. Equally, the NIS Directive is technology neutral and business model agnostic enough to ensure that the cyber risk management, incident reporting and audit requirements applicable to essential service operators and digital service providers in scope extend as needed to the IoT systems that these operators and providers may use.

The EU's Strategy should address the privacy and security aspects of the IoT by fully considering the roll-out of IoT technologies and the regulatory compliance efforts that businesses will be conducting under already existing legislative instruments. This will also ensure that these compliance requirements are duly and adequately designed into the roll-out of IoT technologies in the Digital Single Market, under the supervision and enforcement powers of the relevant competent authorities.

3. Working closely with our partners around the world

Cyber threats being oblivious to geographical and jurisdictional borders, the cyber resilience of the European Digital Single Market will depend greatly on the EU's ability to work effectively and efficiently with foreign partners to adopt common approaches to detecting, mitigating and managing cyber risk at the international level. From AmCham EU's perspective, as a matter of priority, the EU should:

- Continue and deepen the already existing EU-US Cyber Dialogue. This would consolidate trust in the transatlantic relationship and facilitate the development and adoption of well aligned cyber policy approaches. Concrete measures should be adopted both to create similar environments for businesses to operate in the EU and in the US and to create a common model that can be credibly positioned as the benchmark for other regions of the world to follow, adopt or adhere to;
- Cooperate and seek transatlantic alignment in particular around the common values and principles of international law shared by the EU and the US which should govern the elaboration of international cyber norms and confidence building measures in cyberspace;
- Advance strategic cooperation (such as between ENISA and US NIST) and encourage operational collaboration (such as between ISACs in the US and CSIRTs in the EU) to improve the collective awareness and resilience in the transatlantic cyberspace and market;
- Preserve and sustain the EU-US Privacy Shield and the Umbrella Agreement as indispensable tokens of trust and practical instruments of cooperation for the undisrupted flow of digital data between the EU and the US, including in the interest of better and more effective cybersecurity cooperation and trade between the US and the EU Digital Single Market, as well as to contribute to tackling cybercrime effectively in the transatlantic dimension; and
- Promote further regulatory convergence between the EU and the US on cybersecurity relevant matters, including by aligning the export control rules and practices in the EU and in the US in relation to cyber technologies.